МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТУСА

В. Г. Крижановський, С. П. Сергієнко, Д. В. Чернов

Безпека інтернету речей (IoT). Захист особистого життя людини

Навчально-методичний посібник

Вінниця
ДонНУ імені Василя Стуса
2020

УДК 004.77(075.8)
К 822

Рекомендовано до друку вченою радою факультету інформаційних та прикладних технологій (протокол № 2 від 21 жовтня 2019 р.)
Автори:
В. Г. Крижановський, проф. кафедри радіофізики та кібербезпеки;
С. П. Сергієнко, доц. кафедри радіофізики та кібербезпеки
Д. В. Чернов, доц. кафедри радіофізики та кібербезпеки

Рецензент: *П. К. Ніколюк,* д-р фіз.-мат. наук, проф., проф. кафедри комп'ютерних технологій.

К 822
Безпека інтернету речей (IoT). Захист особистого життя людини: навчально-методичний посібник / В. Г. Крижановський, С. П. Сергієнко, Д. В. Чернов. Вінниця: ДонНУ імені Василя Стуса, 2019. 128 с.

Розглядаються особливості захисту інформації у системі Інтернету речей (IoT), які мають перспективи широкого впровадження, та потенційно становлять велику загрозу для кібербезпеці.

Посібник рекомендовано для студентів вищих навчальних закладів за напрямами «Прикладна фізика. Технології Інтернету речей», «Кібербезпека» та «Комп'ютерні науки та інформаційні технології. Інтелектуальні інформаційні технології».

УДК 004.77(075.8)

«…ужасные замораживающие бомбы были приобретены сепаратистами в Мюнхене на оптовом складе холодильных установок и оказались бракованными суперфризерами… В сочетании с молекулярными детонаторами (широко применяются подводными археологами на Амазонке для отпугивания пираний и кайманов) суперфризеры были способны дать мгновенное понижение температуры до ста пятидесяти градусов ниже нуля в радиусе двадцати метров».

А. и Б. Стругацкие. Хищные вещи века. 1964 г.

ВСТУП

Інтернет речей (Internet of Things, IoT) – крок до повсюдного проникнення комунікацій та обчислення, яка зараз широкому загалу найбільш відома у зв'язку з поняттями «Розумний будинок» та «Індустріальний Інтернет речей», одночасно є найбільшою загрозою в плані кібербезпеки. В даному посібнику розглядається широке коло проблем, пов'язаних як з сучасним, так і з перспективним впровадженням IoT. Автори сподіваються, що посібник буде корисним при вивченні відповідних курсів та виконанні кваліфікаційних робіт

1. ЗАГАЛЬНІ АСПЕКТИ КІБЕРБЕЗПЕКИ В IoT

1.1. Інтернет речей: наслідки для безпеки та конфіденційності

Ключові моменти

- Інтернет речей (IoT) створює нові ризики для безпеки, яких виробники пристроїв та розробники додатків не передбачали.
- Пристрої, які стали частиною IoT, дозволяють зберігати, аналізувати, контролювати та обмінюватися величезною кількістю даних з іншими мережевими пристроями та користувачами.
- Конфіденційність користувачів опиняється під загрозою через їх обмежений вибір можливостей та контроль щодо збору, збереження та розповсюдження їх даних.
- Існує ризик неадекватної правової бази, що регулює Інтернет речей, це вимагає термінових заходів з юридичного аналізу та може стимулювати нові підходи до законодавства.

1.1.1. Стан розвитку Інтернету речей

Нова технологія надала користувачам можливість перевіряти стан своєї домашньої безпеки зі своїх смартфонів, запускати машину за допомогою програми для мобільних телефонів, а також дистанційно відкривати та закривати свої гаражні ворота з будь-якої точки світу. Ці технології стають частиною так званого Інтернету речей (IoT). В основному розумінні IoT означає підключення повсякденних предметів (наприклад, телевізорів, приладів та тренажерів) до Інтернету. Це дозволяє здійснювати моніторинг у режимі реального часу та широкий збір даних про майно, людей, рослини та тварин [1,2].

По-перше, розумні будинки та офіси стали частиною IoT. Зокрема, ці розумні будинки та офіси дозволяють дистанційно контролювати вимикачі світла, двері, вікна, жалюзі та температуру. Наприклад, WeMo від Belkin дозволяє користувачам контролювати живлення (наприклад, споживання енергії), побутову електроніку та побутову техніку, воду та Wi-Fi зі смартфона. HomeKit від Apple, ще один розумний домашній продукт, полегшує управління системами сигналізації, системами спостереження, ліхтарі та двері, серед інших об'єктів, через IPhone або IPad. Інші доступні технології дозволяють користувачам керувати своїми будинками та робочими місцями через браслети. Наприклад, браслети Reemo дозволяють користувачам контролювати медіа (телефони, відеоігри, стереосистеми та телевізори), безпеку (сигналізацію та системи спостереження), клімат (термостати, каміни, розумні вентилятори та внутрішнє опалення), а також живлення (розетки, вимикачі та регулятори яскравості) у своєму будинку за допомогою жестів руками. Ці типи пристроїв

дозволяють здійснювати моніторинг у реальному часі майна, рухів та діяльності людей вдома та офісів.

По-друге, розроблені пристрої, що можна носити на тілі, які можуть контролювати діяльність та життєво важливі показники людей. Fitbit – це фітнес-пристрій, який відстежує та здійснює моніторинг в режимі реального часу пройденої відстані користувача, зроблених кроків, піднятих сходів, спалених калорій та якості сну, 24 година на добу. Hexoskin – це одяг, який контролює частоту дихання та частоту серцевих скорочень, і навіть відстежує режим сну користувача. Інші пристрої, що носять на одязі, обіцяють відстежувати звички сну новонародженого, збираючи дані, наприклад, чи немовлята лежать на спині чи животі, частота дихання, температура шкіри і навіть у деяких випадках рівень кисню в крові та частота серцевих скорочень. Ці пристрої дозволяють здійснювати спостереження в режимі реального часу за людьми, внутрішньою роботою їхніх тіл та рухами та діяльністю людей.

По-третє, рослини, сади та сільське господарство стали частиною IoT. Наприклад, Oso Technologies PlantLink забезпечує моніторинг вологості рослин в режимі реального часу, тим самим надаючи користувачам засоби для відстеження того, коли їх рослини потребують води. Що стосується сільського господарства, OnFarm дозволяє користувачам здійснювати моніторинг врожаю через дані від датчиків, погоди, карт та заходів захисту.

Нарешті, тварини стали частиною IoT. Голландська компанія Sparked використовує датчики у великої рогатої худоби для моніторингу та відстеження їх здоров'я та рухів. Домашніх тварин також контролюють та відстежують за допомогою пристроїв IoT. Наприклад, Whistle має пристрій, який контролює стан здоров'я та діяльність домашніх тварин. Крім того, Tagg, який зараз купує Whistle, має пристрій, який відстежує місцезнаходження домашніх тварин за допомогою системи глобального позиціонування (GPS) та їх діяльності. Тому пристрої IoT дозволяють здійснювати моніторинг тварин, як і власності, людей та рослин, їх діяльність та пересування в режимі реального часу.

Таким чином, IoT є взаємопов'язаною системою, де живі та неживі об'єкти у фізичному світі та датчики, що знаходяться в них або приєднані до них, підключаються до Інтернету через бездротові та дротові мережеві з'єднання. Цими елементами можна управляти та контролювати віддалено за допомогою програм, розроблених для забезпечення зондування, автоматизації та зв'язку від машини до машини (M2M). Остання, комунікація M2M, дозволяє пристроям перекладати дані відповідно до контексту та приймати відповідні, своєчасні та цінні рішення на основі показань. Таким чином, IoT покращує ефективність завдяки M2M-зв'язку та

дозволяючи користувачам відстежувати людей, предмети та місця, серед іншого, в режимі реального часу за меншими витратами з будь-якої точки світу за допомогою Інтернет-з'єднання.

1.1.2. Пристрої, не побудовані з думкою про безпеку

Пристрої IoT не тільки контролюють користувача або ціль, але й збирають та передають інформацію про користувача та ціль. Зокрема, IoT збирає дані та передає цю інформацію підключеним пристроям, де такі дані зберігаються, обробляються та можуть бути прочитані користувачем із мобільних пристроїв, таких як смартфони чи планшети. Відповідно, пристрої IoT мають можливість масово визначати, отримувати, аналізувати, контролювати та розподіляти дані. Ці пристрої також збільшують обсяг даних, які збираються, обробляються, зберігаються та передаються між пристроями IoT. Навіть такі медичні пристрої, як радіологічні машини (наприклад, рентгенівські апарати), біомедичні пристрої, інфузійні насоси для ліків, роботи аптечних диспансерів, дефібрилятори серця, кардіостимулятори та хірургічні та анестезіологічні пристрої, серед інших, стали частиною IoT. Ці підключені до IoT пристрої були створені для підвищення ефективності та якості життя та забезпечення повсякденних зручностей для користувача.

Тим не менше, зручність цих пристроїв коштує витрат, а саме безпеки. Насправді більшість пристроїв IoT були побудовані без урахування безпеки. Дійсно, у багатьох із цих пристроїв виробники зробили «задні двері» та стандартні паролі, записані в текст програмного забезпечення. Крім того, стандарти безпеки та конфіденційності цих пристроїв не були визначені належним чином. Врешті-решт, поспіх із впровадженням технології IoT випередив створення та впровадження засобів безпеки та захисту конфіденційності та стандартів для цих пристроїв.

1.1.3. Ризики, пов'язані з IoT

IoT створює більший простір атаки, формуючи більше точок доступу до Інтернету, які потрібно надійно контролювати. Чим більша поверхня атаки, тим існує більше вразливостей, які можна використати. Тому запуск нових пристроїв в Інтернеті вдома, в офісі чи в інших областях створює безліч нових проблем, що викликають загрозу. Ці нові загрози були визначені Європолом у 2014 році: «Оскільки більше об'єктів підключено до Інтернету та створюються нові типи критичної інфраструктури, ми можемо очікувати (більше) цілеспрямованих атак на існуючі та нові інфраструктури, включаючи нові форми шантажу та схеми вимагання (наприклад, програм-викупників для розумних автомобілів або

розумних будинків), викрадення даних, фізичні травми та можлива смерть, а також нові типи ботнетів» [3].

В першу чергу ці нові пристрої, що пов'язують майно, людей, рослини та тварин з Інтернетом, вразливі для хакерів. Зловмисник може отримати несанкціонований доступ до пристроїв IoT через їх налаштування, оскільки ці пристрої підключені до Інтернету і не мають необхідних захисних заходів. Через ці вразливості особиста інформація, зібрана пристроями IoT, може бути об'єктом зловживання. Зокрема, якщо пристрій збирає та зберігає особисті, медичні та/або фінансові дані, хакер може викрасти цю інформацію для сприяння крадіжці особистих даних.

Ці вразливості також дають можливість компрометувати ці пристрої. Пристрій IoT, який був скомпрометований, може бути використаний для запуску атаки відмови в обслуговуванні (DoS) або може бути використаний для розповсюдження шкідливого програмного забезпечення (тобто зловмисного програмного забезпечення). Справжні випадки – це медичні вироби. Виробники медичних виробів не враховують злом та зловмисне програмне забезпечення при розробці своїх продуктів, навіть незважаючи на те, що такі пристрої все частіше стають доступними для Інтернету. Цими пристроями можна дистанційно керувати, а налаштування цих пристроїв можна віддалено змінювати. Ці пристрої додатково містять задні двері, які роблять їх вразливими до потенційно небезпечних для життя атак у разі внесення змін до існуючих налаштувань. Зокрема, зловмисники, які знають паролі пристроїв за замовчуванням, можуть експлуатувати бекдор і змінювати критичні налаштування або взагалі замінювати авторизоване програмне забезпечення. Залежно від пристроїв, ці дії можуть спричинити серйозні захворювання, травми та навіть смерть. Це свідчить про те, що безпека цих пристроїв є першорядною. У США Закон про переносимість медичного страхування та обліковість 1996 року вимагає, щоб медичні вироби та додатки для медичних виробів мали відповідні запобіжні заходи для захисту від кібератак та несанкціонованого доступу, видалення, зміни або розкриття даних із цих пристроїв. Крім того, в Європейському Союзі стаття 10c Директиви 2007/47 / ЄС (про внесення змін до Директиви 90/385/ЄЕС та Директиви 93/42/ЄЕС) передбачає, що виробники медичних виробів не повинні розміщувати на ринку або вводити в експлуатацію будь-які медичні пристрій, які можуть порушити безпеку та здоров'я пацієнтів; такі пристрої, якщо їх знайдуть, слід вилучити з ринку або заборонити або обмежити їх розміщення на ринку чи введення в експлуатацію.

Пристрій IoT або пристрої, які не мають відповідних запобіжних заходів (наприклад, антивірусне та антишпигунське програмне забезпечення, брандмауери та системи виявлення вторгнень/системи захисту від

вторгнень), можуть поставити під загрозу всю систему IoT. Кінцеві точки, які погано захищені, таким чином стають шлюзами для кібератак, які прагнуть виграти ці пристрої, змінити їх налаштування або зробити їх непридатними протягом певного періоду. Недостатній захист пристроїв IoT та даних, зібраних, збережених та переданих ними, може в подальшому призвести до порушення даних, внаслідок чого дані осіб викрадаються або порушуються. Відповідно, точки бездротового доступу, бази даних та функції збору даних пристроїв та програм IoT повинні бути захищені від злому та порушень безпеки.

1.1.4. Захист IoT

Якщо проблеми безпеки широко розповсюджені в пристрої IoT, який було визнано вразливим, потерпілі клієнти можуть пред'явити позови щодо колективної позови та відповідальності за товари проти виробників пристроїв IoT. Інші зацікавлені сторони IoT (наприклад, розробники додатків) також можуть нести відповідальність; це буде визначатися рівнем, якщо такий є, їх відповідальності за подію, яка спричинила шкоду чи шкоду, яка була заподіяна. Більше того, у США компаніям можуть пред'являти звинувачення за несправедливі або оманливі дії, що негативно впливають на безпеку споживачів. та конфіденційність згідно із Законом про Федеральну торгову комісію від 1914 р. У грудні 2013 р. Федеральна торгова комісія США розпочала свою першу дію проти TRENDnet щодо їх пристроїв IoT (це камери спостереження, які використовувались для спостереження за домом та немовлятами). Комісія постановила, що практика TRENDnet спричинила або може спричинити значну шкоду споживачам, яка не компенсується перевагами для споживачів або конкуренції та споживач не може їй розумно запобігти. Дії та практика відповідача являють собою несправедливі або оманливі дії чи практики у сфері торгівлі або зачіпають її, порушуючи розділ 5 (а) Закону про Федеральну торгову комісію, 15 США § 45 (а). Федеральна торгова комісія США звинуватила TRENDnet у слабій практиці безпеки та введенні клієнтів в оману, стверджуючи, що їх пристрої IoT захищені. Насправді ці пристрої мали несправне програмне забезпечення, що призвело до розкриття приватного життя сотень споживачів; конкретно, хакер експлуатував підшкірне програмне забезпечення та розміщував посилання на потокові канали приблизно 700 споживчих камер.

Цей випадок та подібні до нього демонструють необхідність інфраструктури IoT бути стійкою до кібератак. Щоб запобігти цим атакам, слід впровадити системи контролю доступу, щоб забезпечити доступ до пристроїв лише авторизованим користувачам. Також необхідні суворі заходи автентифікації для запобігання доступу до пристроїв та даних IoT.

Крім того, у пристрої повинні бути вбудовані засоби безпеки. Розглянемо медичні вироби. Виробники медичних виробів можуть запобігти фальсифікації їхніх пристроїв, видаливши бекдор-акаунти та вимагаючи цифрового підпису всього програмного забезпечення. Паролі та імена користувачів за замовчуванням на цих та інших пристроях IoT також слід скинути.

Більше того, для захисту пристроїв Інтернету речей та виявлення загроз необхідні активні wal відновлювальні стіни та використання комплексної системи безпеки (наприклад, антивірусного та антишпіонського програмного забезпечення та систем виявлення вторгнень / систем запобігання вторгненню). Одним із прикладів такого програмного забезпечення є Bitdefender. В даний час Bitdefender просуває один зі своїх продуктів, бокс Bitdefender, як можливість захищати повсякденні об'єкти, підключені до домашньої мережі, від шкідливого програмного забезпечення. Крім того, для захисту пристроїв IoT необхідні загальноприйняті методи безпеки та стандарти. Однак однаковий рівень безпеки не буде потрібен для кожного пристрою IoT. Пристрої, які збирають конфіденційну інформацію, представляють фізичну безпеку або ризики для безпеки (наприклад, дверні замки, духовки або інсулінові помпи) або підключаються до інших пристроїв або мереж таким чином, щоб зловмисники мали доступ до цих пристроїв або мереж, повинні бути більш надійними захищені, ніж, наприклад, пристрої, які просто контролюють кімнатну температуру, пробіг або споживання калорій. Відповідно до цих міркувань, стаття 17 Директиви ЄС про захист даних (Директива 95/46 / ЄС) диктує, що обраний рівень безпеки повинен відповідати ризикам, пов'язаним із інформацією, що збирається, зберігається та передається.

1.1.5. IoT загрожує конфіденційності користувачів

У майбутньому все більше і більше пристроїв стануть частиною IoT. Це очевидно завдяки збільшенню кількості нових технологій, які підтримують IoT. Нібито існує мільярд пристроїв IoT; кожен з яких призначено для збору, зберігання та передачі великої кількості даних. Ці дані можуть бути легко використані для надання інформації в режимі реального часу про людину, стан її здоров'я та фінансів, місцезнаходження, контакти, звички, поведінку та діяльність. Окрім розкриття цих типів особистої інформації, ці дані можуть також використовуватися для спостереження та виявлення змін у розпорядку людей та проявах незвичної поведінки. Зрештою, пристрої IoT створюють середовище, де інформацію про кожну людину можна зберігати, аналізувати, контролювати, робити доступною та ділитися з іншими мережевими пристроями та потенційно іншими користувачами. З огляду на те, що величезна кількість

інформації про фізичних осіб збирається, обробляється, зберігається та обмінюється між пристроями IoT, людьми та компаніями, існує значна можливість створити детальний облік приватного життя мільйонів користувачів.

Конфіденційність є основним правом людини і захищається у внутрішніх (наприклад, Закон Великобританії про права людини 1998 р.), Регіональних (наприклад, Європейська конвенція з прав людини та Американська конвенція з прав людини) та міжнародних документах з прав людини (наприклад, Загальна декларація про права людини, Права та Міжнародний пакт про громадянські та політичні права). Важливим елементом конфіденційності є право та можливість зберігати певні речі в таємниці. Користувачі IoT можуть мати труднощі «тримати речі в таємниці», оскільки [повний] розвиток можливостей IoT може вплинути на поточні можливості анонімного використання послуги і загалом обмежують можливість залишатися непоміченими. Іншим важливим елементом конфіденційності є право контролювати інформацію, якою інші користуються та мають доступ до себе. Користувачам може бути важко контролювати свою інформацію, оскільки зв'язок та обмін даними між пристроями IoT «можуть запускатися автоматично, а також за замовчуванням, без того, щоб особа про це знала». Більше того, «сучасні методи, пов'язані з аналізом даних та перехресним збігом передавати ці дані для вторинного використання, незалежно від того, пов'язані вони з ціллю, призначеною для початкової обробки. Таким чином, треті сторони, які вимагають доступу до даних, зібраних іншими сторонами, можуть захотіти використовувати ці дані для абсолютно інших цілей». Наприклад, дані, зібрані з пристроїв IoT, можуть бути використані для прийняття рішень щодо кредитування, страхування або працевлаштування. Це може бути особливо проблематичним, якщо зібрані дані IoT використовуються без відома та згоди користувачів або коли точність даних не встановлена. Ці існуючі обмеження щодо контролю та вибору користувачів щодо збору, зберігання та передачі даних IoT загрожують конфіденційності користувачів.

1.1.6. Захист конфіденційності

Європейський Союз має всеохоплюючий закон про захист даних, Директиву 95/46 / ЄС.32 Директива 95/46 / ЄС та її транспонування до законодавства держав-членів ЄС регулює обробку та передачу персональних даних та надає споживачам засоби захисту від несанкціонованого розголошення, доступу та / або використання своїх персональних даних. У Канаді Закон про захист персональної інформації та електронні документи 2000 року є основним законом про захист даних та

конфіденційність, який регулює придбання, використання та розкриття особистої інформації організаціями під час комерційної діяльності.

На відміну від Європейського Союзу та Канади, США не має переважного закону про захист даних, що регулює приватний сектор. Однак він має закон про захист даних, який регулює державний сектор; а саме, Закон про конфіденційність 1974 року. Цей закон вимагає від державних органів захисту персональних даних, обмежує обмін цією інформацією, дає можливість громадянам звертатися до цивільних засобів захисту та передбачає кримінальне покарання за порушення цього закону. І навпаки, для приватного сектору на федеральному рівні дотримується галузевий підхід до захисту даних та конфіденційності із застосуванням законів, що регулюють збір, використання та розкриття певних форм особистої інформації, таких як медичні дані (наприклад, переносимість медичного страхування та Закон про підзвітність 1996 року) та фінансові дані (тобто Закон про модернізацію фінансових послуг 1999 року).

Застосування цих законів до виробників пристроїв IoT, розробників додатків та інших учасників IoT може бути обмеженим. Насправді Державна служба відповідальності уряду США визначила, що застосовність Закону про модернізацію фінансових послуг 1999 року та Закону про чесну кредитну звітність 197035 року до торгових посередників інформації була обмеженою. Відповідно, засоби захисту даних та порушення конфіденційності існують у певних цільових областях (наприклад, несанкціонований доступ до фінансових та медичних даних, їх використання або розкриття), але не поширюється на всіх, хто збирає, передає, розкриває чи іншим чином використовує дані. Однак такий підхід ефективно не вирішує проблеми захисту даних та конфіденційності, що виникають при розгортанні та використанні пристроїв IoT. Навіть Федеральна торгова комісія США визнала, що існуюче галузеве законодавство не призначене для вирішення питань захисту даних та конфіденційності, що виникають внаслідок використання певних пристроїв та програм IoT. Зокрема, у січні 2015 року Федеральна торгова комісія США заявила, що стандарти Закону про переносимість та підзвітність медичного страхування (HIPAA) мають бути оновлені, оскільки деякі медичні пристрої, що стосуються споживачів IoT, збирають подібну конфіденційну інформацію, яка для лікарів та страхових компанії охоплюється HIPAA. Цей дефіцит у чинному законодавстві демонструє необхідність змін у існуючій законодавчій базі, яка може впоратися з ризиками, спричиненими IoT.

Для захисту персональних даних пропонується саморегулювання з боку споживачів. Особи повинні мати можливість контролювати та вибирати, які дані збираються, хто їх збирає та коли це відбувається. IoT в основному є сховищем даних для кожного аспекту життя людини.

Принаймні, «[а] застосування повинні сприяти здійсненню прав суб'єкта даних на доступ, модифікацію та видалення особистої інформації, зібраної пристроями IoT», як каже законодавство ЄС. Крім того, згода користувачів надається на використання пристрою IoT та дані, зібрані пристроєм, повинні інформуватися та надаватися вільно. Користувачі не повинні отримувати економічних покарань або погіршувати доступ до можливостей своїх пристроїв, якщо вони вирішать не використовувати пристрій або певну службу. Наразі користувачі можуть бути покарані або відмовлені у доступі до важливих служб за рішення не брати участь або надати підтверджену згоду на збір їх даних. В автомобільній промисловості США «споживачам, які вирішили не погодитися на збір даних», може бути відмовлено у доступі до цінних характеристик автомобіля. Наприклад, згода на обмін інформацією про геолокацію в маркетингових цілях може бути єдиним способом для споживача увімкнути навігаційну функцію в своїх транспортних засобах.

Для захисту персональних даних їх слід зберігати лише за потреби, а дані, які більше не потрібні, слід періодично видаляти. Також слід практикувати мінімізацію даних; тобто зібрані дані повинні обмежуватися лише тим, що необхідно для ефективного функціонування пристрою та програми. Це не тільки зменшує шкоду, пов'язану з порушенням даних, але також мінімізує ризик того, що дані будуть використовуватися таким чином, щоб відхилятися від очікувань користувачів. Справді, з даними IoT існує значний ризик, що може виникнути повзучість місії (або функції), де інформація, отримана від певних пристроїв, буде потім використана для більш широкого набору програм, що не входять до вихідних цілей для збереження даних. Тип даних, що збираються, та їх подальше використання повинні бути чітко окреслені в політиці конфіденційності IoT. Користувачі повинні уважно переглянути ці правила, коли вони розкривають, яку інформацію збирають, зберігають, використовують та потенційно передають третім особам.

Загалом, існуючі практики недостатньо вирішують проблеми безпеки та конфіденційності, які порушує IoT. В ідеалі слід розробити універсальний набір стандартів конфіденційності та безпеки. Бар'єром для створення універсального набору стандартів конфіденційності та безпеки є різне бачення країн (і навіть компаній) цих питань. Крім того, загальні стандарти конфіденційності не будуть прийняті в країнах, які не надають конфіденційності таку саму важливість та/або не надають їй особливого статусу права людини (наприклад, Китай), як інші країни (наприклад, Великобританія). Зараз практикується виконання національних законів, що регулюють ці питання, і загальний поштовх до саморегулювання виробників і підприємств IoT. Однак саморегулювання не буде достатнім.

Дані користувачів є цінними; як такі, компанії більше схильні до збору та обміну цією інформацією, ніж утримання від збору або видалення після збору. Однак ця практика може змінитися, якщо відсутність такого захисту конфіденційності неминуче негативно позначиться на доходах компаній (наприклад, користувачі можуть відмовитись від використання цих технологій, коли їх конфіденційність не захищена належним чином). Зрештою, саморегулювання не спрацює, оскільки компанії зацікавлені у просуванні власних інтересів та збільшенні своїх прибутків, замість того, щоб захистити конфіденційність користувачів.

1.1.7. Висновок по підрозділу 1.1

IoT з'єднує та обмінюється інформацією про неживі та живі об'єкти. Все, що стосується медичних пристроїв та побутових приладів, підключається і стає частиною IoT. Нові та мінливі прояви вразливості спостерігаються при використанні IoT та його поширеності в суспільстві.

Захист пристроїв IoT – це багатогранний і складний процес. Існуючий ризик неадекватної правової бази вимагає термінових заходів з правового аналізу та може вимагати нових підходів у законодавстві. Для ефективної боротьби з існуючими вразливими місцями IoT рекомендується провести ретельний аналіз існуючої законодавчої бази та розробити нові елементи для усунення ризиків, пов'язаних із розгортанням IoT, де це необхідно.

1.2. Кібербезпека та Інтернет речей: вразливості, загрози, зловмисники та атаки

Пристрої Інтернету речей (IoT) швидко стають повсюдними, тоді як послуги IoT стають найпоширенішими. Їх успіх не залишився непоміченим, а також збільшується кількість загроз та атак на пристрої та служби IoT. Кібер-атаки не є новиною для IoT, але оскільки IoT буде глибоко вплетене в наше життя та суспільство, стає необхідним активізуватися і серйозно поставитися до кіберзахисту. Отже, існує реальна потреба у захисті IoT, що в результаті призвело до необхідності всебічного розуміння загроз та атак на інфраструктуру IoT [1-5].

1.2.1. Загальні запитання

Недавній бурхливий розвиток Інтернету речей (IoT) та його здатність пропонувати різні види послуг зробили його найбільш швидкозростаючою технологією з величезним впливом на соціальне життя та бізнес-середовище. IoT поступово пронизує всі аспекти сучасного людського життя, такі як освіта, охорона здоров'я та бізнес, включаючи зберігання конфіденційної інформації про приватних осіб та компанії, операції з фінансовими даними, розробку продуктів та маркетинг.

Величезна дифузія підключених пристроїв у IoT створила величезний попит на надійну безпеку у відповідь на зростаючий попит мільйонів або, можливо, мільярдів підключених пристроїв та послуг у всьому світі.

Кількість загроз зростає щодня, а атаки збільшуються як за кількістю, так і за складністю. Кількість потенційних зловмисників не лише зростає разом із розміром мереж, але й інструменти, доступні потенційним зловмисникам, стають все більш досконалими, ефективними та ефективними [6, 7]. Тому для того, щоб IoT реалізував найповніший потенціал, йому потрібен захист від загроз та вразливостей.

Безпека була визначена як процес захисту об'єкта від фізичних пошкоджень, несанкціонованого доступу, крадіжок або втрат шляхом збереження високої конфіденційності та цілісності інформації про об'єкт та надання інформації про цей об'єкт при необхідності. Для Kizza [7] ніщо не є безпечним станом будь-якого предмета, матеріальним чи ні, оскільки жоден такий об'єкт ніколи не може знаходитись у абсолютно безпечному стані і при цьому бути корисним. Об'єкт безпечний, якщо процес може підтримувати свою максимальну внутрішню цінність за різних умов. Вимоги безпеки в середовищі IoT не відрізняються від будь-яких інших систем ІКТ. Отже, забезпечення безпеки IoT вимагає збереження найвищої

внутрішньої вартості як матеріальних об'єктів (пристроїв), так і нематеріальних (послуг, інформації та даних).

Треба сприяти кращому розумінню загроз та їхніх атрибутів (мотивація та можливості), що походять від різних зловмисників, таких як організації та розвідка. Процес виявлення загроз для систем та системних вразливостей необхідний для визначення надійного повного набору вимог безпеки, а також допомагає визначити, чи захищене рішення захисту від шкідливих атак [8]. Окрім користувачів, уряди та розробники IoT повинні зрештою розуміти загрози та мати відповіді на наступні запитання:

1. Які є активи?
2. Хто є основними суб'єктами?
3. Які загрози?
4. Хто є акторами загроз?
5. Якими можливостями та рівнем ресурсів володіють актори загроз?
6. Які загрози можуть вплинути на які активи?
7. Чи захищений поточний дизайн від загроз?
8. Які механізми безпеки можна використовувати проти загроз?

1.2.2. Передумови

IoT [2 - 4] є продовженням Інтернету у фізичний світ для взаємодії з фізичними сутностями з оточення. Суб'єкти, пристрої та послуги є ключовими поняттями в домені IoT, як показано на рис. 1.1 [9]. Вони мають різне значення та визначення серед різних проектів. Тому необхідно добре розуміти, що таке сутності, пристрої та служби IoT (детально обговорено в підрозділі 1.2.3).

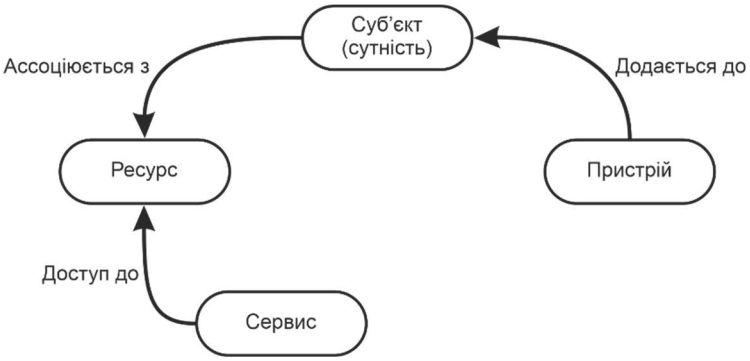


Рис. 1.1. Модель IoT: ключові концепції та взаємодії

Суб'єктом в Інтернеті речей може бути людина, тварина, автомобіль, логістичний ланцюг, електронний прилад або закрите або відкрите середовище. Взаємодія між сутностями стає можливою за допомогою апаратних компонентів, званих пристроями, таких як мобільні телефони, датчики, виконавчі механізми або RFID-мітки, які дозволяють суб'єктам підключатися до цифрового світу.

За сучасного стану технологій Machine-to-Machine (M2M) є найпопулярнішою формою застосування IoT. В даний час M2M широко застосовується в енергетиці, транспорті, роздрібній торгівлі, управлінні державними послугами, охороні здоров'я, водній, нафтовій та інших галузях промисловості для моніторингу та контролю споживачів, машин та виробничих процесів у світовій промисловості тощо [10]. За підрахунками, програми M2M досягнуть 12 мільярдів з'єднань до 2020 року та отримають приблизно 714 мільярдів євро доходів.

Окрім усіх переваг програми IoT, існує кілька загроз безпеці оглянутих у [17]. Підключені пристрої чи машини надзвичайно цінні для кібер-зловмисників з кількох причин:

1. Більшість пристроїв IoT працюють без нагляду людей, тому зловмиснику легко отримати фізичний доступ до них.

2. Більшість компонентів IoT взаємодіють через бездротові мережі, де зловмисник може отримати конфіденційну інформацію шляхом прослуховування.

3. Більшість компонентів IoT не можуть підтримувати складні схеми безпеки через низьку потужність та обчислювальні ресурси.

Крім того, кіберзагрози можуть бути спрямовані проти будь-яких активів та засобів IoT, що потенційно може спричинити пошкодження або вивести з ладу роботу системи, загрожуючи широкому загалу чи завдаючи серйозної економічної шкоди власникам та користувачам [11]. Приклади включають атаки на системи домашньої автоматизації та управління системами опалення, кондиціонування, освітлення та систем фізичної безпеки. Інформація, зібрана від датчиків, вбудованих в системи опалення або освітлення, може інформувати зловмисника, коли хтось перебуває вдома чи поза ним. Окрім іншого, кібератаки можуть бути розпочаті проти будь-якої державної інфраструктури, наприклад, комунальних систем (енергосистеми чи водоочисні споруди), щоб зупинити постачання жителів водою чи електроенергією.

Питання безпеки та конфіденційності дедалі більше турбують користувачів та постачальників у процесі переходу до IoT. Звичайно, легко уявити розмір шкоди, заподіяної в разі атаки чи пошкодження підключених пристроїв. Загальновизнано, що використання будь-якої технології IoT у наших будинках, на роботі чи в бізнес-середовищі відкриває двері

для нових проблем безпеки. Користувачі та постачальники повинні враховувати та бути обережними з такими проблемами безпеки та конфіденційності.

1.2.3 Розуміння пристроїв та послуг IoT

У цьому розділі визначено та класифіковано основні поняття домену IoT, які є важливими з точки зору бізнес-процесів, та описано взаємозв'язки між компонентами IoT (пристроями IoT та послугами IoT).

А. Пристрій IoT

Це апаратний компонент, що дозволяє об'єкту бути частиною цифрового світу. Його також називають розумною річчю, яка може бути побутовою технікою, медичним приладом, транспортним засобом, будівлею, фабрикою та майже будь-якими об'єднаними в мережу та оснащеними датчиками даними про фізичне середовище (наприклад, температуру, вологість, детектори присутності та забруднення), виконавчі механізми (наприклад, вимикачі світла, дисплеї, жалюзі з моторним керуванням або будь-яку іншу дію, яку може виконувати пристрій) та вбудовані комп'ютери.

Пристрій IoT здатний взаємодіяти з іншими пристроями IoT та системами ІКТ. Ці пристрої спілкуються за допомогою різних засобів, включаючи стільникові (3G або LTE), WLAN, бездротові та інші технології [12]. Класифікація пристроїв IoT залежить від розміру, тобто, маленького або звичайного; мобільність, тобто мобільна або фіксована; зовнішнє або внутрішнє джерело живлення; незалежно від того, підключені вони з перервами чи постійно; автоматизовані або неавтоматизовані; логічні або фізичні об'єкти; і нарешті, незалежно від того, чи є вони об'єктами з підтримкою IP або не об'єктами IP.

Характеристиками пристроїв IoT є їх здатність спрацьовувати та/або відчувати, здатність обмежувати потужність/енергію, підключення до фізичного світу, періодичний зв'язок та мобільність. Деякі мають бути швидкими та надійними та забезпечувати надійну безпеку та конфіденційність, а інші – ні. Деякі з цих пристроїв мають фізичний захист, тоді як інші – без нагляду.

Насправді, в середовищах IoT пристрої повинні бути захищені від будь-яких загроз, які можуть вплинути на їх функціональність. Однак більшість пристроїв IoT вразливі до зовнішніх та внутрішніх атак через свої характеристики. Складно реалізувати та використовувати потужний механізм безпеки через обмеження ресурсів з точки зору обчислювальних можливостей IoT, пам'яті та заряду акумулятора.

Б. Послуги IoT

Послуги IoT сприяють легкій інтеграції об'єктів IoT у світ сервісно-орієнтованої архітектури (SOA), а також в науку про послуги. За словами Томи [13], послуга IoT – це операція між двома сторонами: постачальником послуг та споживачем послуги. Це спричиняє встановлену функцію, дозволяючи взаємодію з фізичним світом шляхом вимірювання стану сутностей або шляхом ініціювання дій, які ініціюватимуть зміну сутностей.

Послуга забезпечує чітко визначений та стандартизований інтерфейс, пропонуючи всі необхідні функціональні можливості для взаємодії з сутностями та пов'язаними з ними процесами. Послуги надають функціональність пристрою, отримуючи доступ до його розміщених ресурсів.

В. Безпека в пристроях та послугах IoT

Забезпечення безпеки передбачає захист як пристроїв IoT, так і служб від несанкціонованого доступу зсередини пристроїв та зовні. Безпека повинна захищати послуги, апаратні ресурси, інформацію та дані як при переході, так і при зберіганні. У цьому розділі ми виявили три ключові проблеми з пристроями та послугами IoT: конфіденційність даних, конфіденційність та довіра.

Конфіденційність даних представляє фундаментальну проблему в пристроях та послугах IoT [27]. В контексті IoT не тільки користувач може отримати доступ до даних, але й авторизований об'єкт. Це вимагає розгляду двох важливих аспектів: спочатку, механізму контролю доступу та авторизації та другого механізму автентифікації та управління ідентифікацією (IdM). Пристрій IoT повинен мати можливість перевірити, чи сутність (особа чи інший пристрій) має дозвіл на доступ до послуги. Авторизація допомагає визначити, чи дозволено особі чи пристрою отримувати послугу після ідентифікації. Контроль доступу передбачає контроль доступу до ресурсів шляхом надання або заборони засобів за допомогою широкого набору критеріїв. Авторизація та контроль доступу важливі для встановлення безпечного зв'язку між низкою пристроїв та служб. Основним питанням, яке потрібно вирішити в цьому сценарії, є спрощення правил контролю доступу, що створюються, розуміються та маніпулюються ними. Іншим аспектом, який слід враховувати при конфіденційності, є автентифікація та управління ідентифікацією. Насправді ця проблема є критично важливою в Інтернеті речей, оскільки декільком користувачам, об'єктам / речам і пристроям потрібно аутентифікувати один одного за допомогою надійних служб. Проблема полягає у пошуку рішення для безпечної обробки ідентифікації користувача, речей / предметів та пристроїв.

Конфіденційність є важливою проблемою пристроїв та послуг IoT через повсюдний характер середовища IoT. Суб'єкти пов'язані, а дані

передаються та обмінюються через Інтернет, роблячи питання конфіденційності користувачів чутливою темою у багатьох наукових роботах. Конфіденційність при зборі даних, а також обмін даними та управління ними, а також питання безпеки даних залишаються відкритими питаннями досліджень, які слід вирішити.

Довіра відіграє важливу роль у встановленні безпечного спілкування, коли низка речей спілкується в непевному середовищі IoT. У IoT слід враховувати два виміри довіри: довіра до взаємодії між сутностями та довіра до системи з точки зору користувачів. На думку Коєна [14], надійність пристрою IoT залежить від компонентів пристрою, включаючи апаратне забезпечення, такі як процесор, пам'ять, датчики та виконавчі механізми, програмні ресурси, такі як програмне забезпечення на базі апаратного забезпечення, операційна система, драйвери та програми, а також джерело живлення. Для того, щоб завоювати довіру користувачів / послуг, повинен існувати ефективний механізм визначення довіри до динамічного та спільного середовища IoT.

1.2.4 Погрози безпеці, атаки та вразливості

Перш ніж розглядати загрози безпеці, спочатку слід ідентифікувати системні активи (компоненти системи), що складають IoT. Важливо розуміти опис активів, включаючи всі компоненти, пристрої та послуги IoT.

Актив – це економічний ресурс, щось цінне та чутливе, що належить суб'єкту господарювання. Основними активами будь-якої системи IoT є апаратне забезпечення системи (включаючи будівлі, машини тощо), програмне забезпечення, послуги та дані, пропоновані службами.

А. Вразливість

Уразливості – це слабкі місця в системі або її конструкції, які дозволяють зловмиснику виконувати команди, отримувати доступ до несанкціонованих даних та/або проводити атаки відмови в обслуговуванні. Вразливості можна знайти в різних сферах систем IoT. Зокрема, це можуть бути слабкі місця в апаратному чи програмному забезпеченні системи, слабкі сторони в політиці та процедурах, що використовуються в системах, та слабкі сторони самих користувачів системи.

Системи IoT базуються на двох основних компонентах; системне обладнання та системне програмне забезпечення, і обидва вони мають дизайнерські помилки досить часто. Апаратні вразливості дуже важко виявити, а також ускладнити їх виправлення, навіть якщо вразливість була виявлена завдяки апаратній сумісності та сумісності, а також зусиллям, необхідним для її виправлення. Вразливості програмного забезпечення можна знайти в операційних системах, прикладних програмах та

програмному забезпеченні для управління, таких як протоколи зв'язку та драйвери пристроїв. Існує низка факторів, що призводять до дизайну програмного забезпечення, включаючи людські фактори та складність програмного забезпечення. Технічні уразливості зазвичай трапляються через людські слабкості. Результати нерозуміння вимог включають запуск проекту без плану, поганий зв'язок між розробниками та користувачами, брак ресурсів, навичок та знань, а також невдале управління та контроль системи.

Б. Незахищеність

Незахищеність (exposure) – це проблема або помилка в конфігурації системи, яка дозволяє зловмиснику проводити діяльність зі збору інформації. Однією з найскладніших проблем IoT є стійкість до впливу фізичних атак. У більшості додатків IoT пристрої можуть залишатися без нагляду і, ймовірно, розміщуватися в місці, доступному для зловмисників. Така незахищеність підвищує ймовірність того, що зловмисник може захопити пристрій, витягти криптографічні секрети, змінити їх програмування або замінити їх на шкідливий пристрій під контролем зловмисника.

В. Загрози

Загроза – це дія, яка використовує слабкі місця в системі та має негативний вплив на неї. Загрози можуть походити з двох першоджерел: людини та природи. Природні загрози, такі як землетруси, урагани, пожежі та пожежі, можуть завдати серйозної шкоди комп'ютерним системам. Від природних катаклізмів можна застосувати небагато захисних заходів, і ніхто не може запобігти їх виникненню. Плани відновлення після стихійних лих, такі як резервні та резервні плани, є найкращим підходом до захисту систем від природних загроз. Людські загрози – це ті, які спричинені людьми, наприклад, зловмисні загрози, що складаються з внутрішніх (хтось має санкціонований доступ) або зовнішніх загроз (осіб чи організацій, що працюють поза мережею), які прагнуть завдати шкоди та порушити роботу системи. Людські загрози класифікуються за наступним:

- Неструктуровані загрози, що складаються з переважно недосвідчених людей, які використовують легко доступні інструменти злому.
- Структуровані загрози, оскільки люди знають вразливості системи та можуть розуміти, розробляти та використовувати коди та сценарії. Прикладом структурованої загрози є Advanced Persistent Threats (APT) [15]. APT – це складна мережева атака, спрямована на отримання цінної інформації в бізнесі та урядових організаціях, таких як обробна промисловість, фінансова промисловість та національна оборона, з метою крадіжки даних.

Коли IoT стає реальністю, все більша кількість повсюдних пристроїв збільшує кількість загроз безпеці, що має наслідки для широкої громадськості. На жаль, IoT постачається з новим набором загроз безпеці. Зростає усвідомлення того, що нове покоління смартфонів, комп'ютерів та інших пристроїв може бути націлене на шкідливе програмне забезпечення та вразливе до атак.

Г. Атаки

Атаки – це дії, спрямовані на заподіяння шкоди системі або порушення нормальної роботи шляхом використання вразливостей за допомогою різних методів та інструментів. Зловмисники запускають атаки для досягнення цілей як для особистого задоволення, так і для компенсації. Вимірювання зусиль, які повинен витратити зловмисник, виражене через їхній досвід, ресурси та мотивацію, називається вартістю атаки. Актори атаки – це люди, які становлять загрозу для цифрового світу. Вони можуть бути хакерами, злочинцями або навіть урядами [1]. Додаткові деталі обговорюються в підрозділі 1.2.6.

Сама атака може мати різні форми, включаючи активні мережеві атаки для моніторингу незашифрованого руху в пошуках конфіденційної інформації; пасивні атаки, такі як моніторинг незахищених мережевих комунікацій для дешифрування слабо зашифрованого трафіку та отримання інформації про автентифікацію; близькі атаки; експлуатація інсайдерами тощо. Поширені типи кібератак:

(а) Фізичні атаки: такий тип атаки підробляє апаратні компоненти. Завдяки необмеженому та розподіленому характеру Інтернету речей, більшість пристроїв, як правило, працюють у зовнішньому середовищі, яке дуже сприйнятливе до фізичних атак.

(б) Розвідувальні атаки - несанкціоноване виявлення та відображення систем, служб або вразливостей. Прикладами розвідувальних атак є сканування мережевих портів, sniffers пакетів, аналіз трафіку та надсилання запитів по інформацію про IP-адресу.

(с) Відмова в обслуговуванні (DoS): Цей вид атаки є спробою зробити машину або мережевий ресурс недоступними для запланованих користувачів. Через низькі можливості пам'яті та обмежені обчислювальні ресурси, більшість пристроїв в Інтернеті речей вразливі до атак енергоресурсів.

(г) Атаки доступу – сторонні особи отримують доступ до мереж або пристроїв, до яких вони не мають права доступу. Існує два різні типи атак доступу: перший – це фізичний доступ, завдяки якому зловмисник може отримати доступ до фізичного пристрою. Другий – це віддалений доступ, який здійснюється до підключених до IP пристроїв.

(e) Напади на конфіденційність: захист конфіденційності в Інтернеті речей стає все більш складним завданням через великі обсяги інформації, яка легко доступна за допомогою механізмів віддаленого доступу. Найпоширенішими атаками на конфіденційність користувачів є:

• Видобуток даних: дозволяє зловмисникам виявити інформацію, яка не передбачається в певних базах даних.

• Кібершпигунство: використання методів злому та шкідливого програмного забезпечення для шпигунства або отримання секретної інформації осіб, організацій чи уряду.

• Підслуховування: прослуховування розмови двох сторін.

• Відстеження: переміщення користувачів можна відстежувати за унікальним ідентифікаційним номером пристроїв (UID). Відстеження місцезнаходження користувачів полегшує їх ідентифікацію в ситуаціях, коли вони хочуть залишатися анонімними.

• Атаки на основі пароля: зловмисники намагаються дублювати дійсний пароль користувача. Цю спробу можна зробити двома різними способами: 1) атака за словником - випробування можливих комбінацій літер і цифр для вгадування паролів користувачів; 2) атаки грубої сили - використовуючи інструменти злому, щоб спробувати всі можливі комбінації паролів для розкриття дійсних паролів.

(f) Кіберзлочини: Інтернет та інтелектуальні об'єкти використовуються для використання користувачів та даних для отримання матеріальної вигоди, таких як крадіжка інтелектуальної власності, крадіжка особистої інформації, крадіжка бренду та шахрайство [1].

(g) Деструктивні атаки: Кіберпростір використовується для створення масштабних руйнувань та руйнування життя та майна. Прикладами руйнівних атак є атаки тероризму та помсти.

(h) Атаки системи наглядового контролю та збору даних (SCADA): Як і будь-які інші системи TCP / IP, система SCADA вразлива до багатьох кібератак. На систему можна атакувати будь-яким із наступних способів:

1) Використання відмови в обслуговуванні для вимкнення системи.

2) Використання троянських програм або вірусів для управління системою. Наприклад, у 2008 році розпочалась атака на іранський ядерний об'єкт в Натанці з використанням вірусу на ім'я Stuxnet.

1.2.5. Основні цілі безпеки та конфіденційності

Щоб досягти успіху в реалізації ефективної безпеки IoT, ми повинні знати про основні цілі безпеки наступним чином:

А. Конфіденційність

Конфіденційність є важливою функцією безпеки в Інтернеті речей, але може не бути обов'язковий у деяких сценаріях, коли дані подаються публічно. Однак у більшості ситуацій та сценаріїв конфіденційні дані не повинні розголошуватися або зчитуватися несанкціонованими організаціями. Наприклад, дані пацієнтів, приватні бізнес-дані та / або військові дані, а також облікові дані та секретні ключі повинні бути приховані від несанкціонованих осіб.

Б. Цілісність

Для забезпечення надійних послуг користувачам IoT цілісність є обов'язковою властивістю захисту в більшості випадків. Різні системи в Інтернеті речей мають різні вимоги щодо цілісності. Наприклад, система віддаленого моніторингу пацієнтів матиме високу перевірку цілісності щодо випадкових помилок через чутливість інформації. Втрата або маніпуляція з даними може статися внаслідок спілкування, що потенційно може спричинити втрату людських життів.

В. Аутентифікація та авторизація

Всюдисущий зв'язок IoT посилює проблему автентифікації через природу середовищ IoT, де можливий зв'язок між пристроєм до пристрою (M2M), людиною до пристрою та / або людиною до людини. Різні вимоги до автентифікації вимагають різних рішень у різних системах. Деякі рішення повинні бути надійними, наприклад, автентифікація банківських карток або банківських систем. З іншого боку, більшість з них повинні бути міжнародними, наприклад, ePassport, тоді як інші повинні бути локальними. Властивість авторизації дозволяє виконувати певні операції в мережі лише уповноваженим особам (будь-який аутентифікований об'єкт).

Г. Доступність

Користувач пристрою (або сам пристрій) повинен мати можливість отримати доступ до послуг у будь-який час, коли це потрібно. Різні апаратні та програмні компоненти пристроїв IoT повинні бути надійними, щоб надавати послуги навіть у разі наявності зловмисних об'єктів або несприятливих ситуацій. Різні системи мають різні вимоги щодо доступності. Наприклад, системи моніторингу пожеж або моніторингу охорони здоров'я, ймовірно, матимуть вищі вимоги щодо доступності, ніж датчики забруднення доріг.

Д. Підзвітність

При розробці методів безпеки, що використовуються в безпечній мережі, підзвітність додає надмірності та відповідальності за певні дії, обов'язки та планування реалізації політик мережевої безпеки. Підзвітність сама не може зупинити атаки, але корисна для забезпечення належної роботи інших методів безпеки. Основні проблеми безпеки, такі як

цілісність та конфіденційність, можуть бути марними, якщо не піддаються підзвітності. Крім того, у випадку інциденту з відмовою, суб'єкт господарювання буде відстежуватись за своїми діями через процес підзвітності, який може бути корисним для перевірки внутрішньої історії того, що сталося, і хто насправді відповідальний за інцидент.

Е. Аудит

Аудит безпеки – це систематична оцінка безпеки пристрою чи послуги шляхом вимірювання того, наскільки він відповідає набору встановлених критеріїв. Через багато помилок та вразливостей у більшості систем, аудит безпеки відіграє важливу роль у визначенні будь-яких слабких місць, що можуть використати дані, які піддають ризику дані. В IoT система, необхідна для аудиту, залежить від програми та її вартості.

Ж. Безвідмовність

Властивість не відмови дає певні докази у випадках, коли користувач або пристрій не може відмовити в дії. Безвідмовність не вважається важливою властивістю безпеки для більшості IoT. Це може бути застосовним у певному контексті, наприклад, платіжних системах, де користувачі або провайдери не можуть відмовити в здійсненні платіжної дії.

З. Цілі щодо конфіденційності

Конфіденційність – це право суб'єктів господарювання визначати ступінь взаємодії з навколишнім середовищем та наскільки організація готова ділитися інформацією про себе з іншими. Основними цілями конфіденційності в Інтернеті речей є:

• Конфіденційність на пристроях – залежить від фізичної та комутаційної конфіденційності. Конфіденційна інформація може витікати з пристрою у випадку крадіжки або втрати пристрою та стійкості до атак бічних каналів.

• Конфіденційність під час спілкування – залежить від наявності пристрою, цілісності та надійності пристрою. Пристрої IoT повинні спілкуватися лише тоді, коли є необхідність, щоб зменшити розкриття конфіденційності даних під час спілкування.

• Конфіденційність при зберіганні – для захисту конфіденційності даних, що зберігаються на пристроях, слід враховувати наступні дві речі:

- Можливі обсяги необхідних даних слід зберігати на пристроях.
- Регламент повинен бути розширений, щоб забезпечити захист даних користувача після закінчення терміну служби пристрою (видалення даних пристрою (Wipe), якщо пристрій викрадено, загублено або не використовується).

• Конфіденційність при обробці – залежить від пристрою та цілісності зв'язку. Дані повинні розголошуватися або зберігатися у третіх сторін без знання власника даних.

• Конфіденційність особистих даних – ідентичність будь-якого пристрою повинна виявляти лише уповноважена особа (людина / пристрій).

• Конфіденційність місцезнаходження – географічне положення відповідного пристрою має виявляти лише уповноважена організація (людина / пристрій).

1.2.6. Зловмисники, мотивація та можливості

Зловмисники мають різні мотиви та цілі, наприклад, фінансову вигоду, впливаючи на громадську думку та шпигунство, серед багатьох інших. Мотиви та цілі зловмисників варіюються від окремих зловмисників до складних організованих злочинних організацій.

Зловмисники також мають різний рівень ресурсів, вміння, доступ та толерантність до ризику, що веде до рівня переносимості атаки, що відбувається. Інсайдер має більше доступу до системи, ніж сторонні. Деякі зловмисники добре фінансуються, а інші працюють з невеликим бюджетом або взагалі відсутні. Кожен зловмисник вибирає атаку, яка є доступною, атаку з хорошою віддачою інвестицій на основі бюджету, ресурсів та досвіду. У цьому розділі зловмисників класифікують за характеристиками, мотивами та цілями, можливостями та ресурсами.

А. Мета та мотивація атаки

Урядові веб-сайти, фінансові системи, веб-сайти новин та засобів масової інформації, військові мережі, а також системи державної інфраструктури є головними об'єктами кібератак. Значення цих цілей важко оцінити, і оцінка часто варіюється між нападником і захисником. Мотиви нападів варіюються від крадіжки особистих даних, крадіжки інтелектуальної власності та фінансового шахрайства до критичних атак на інфраструктуру. Перелічити, що спонукає хакерів атакувати системи, досить важко. Наприклад, крадіжка інформації про кредитні картки в наш час стала хобі хакерів, а організації електронного тероризму атакують державні системи, щоб зацікавити політику та релігію.

1.2.7. Класифікація можливих зловмисників

Як правило, слід вважати зловмисника типу Долев-Яо (DY) [16]. Тобто зловмисник, який фактично є мережею і який може перехоплювати все або будь-яке повідомлення, коли-небудь передане між пристроями IoT та концентраторами. DY-зловмисник надзвичайно здатний, але його можливості трохи нереальні. Таким чином, безпека буде набагато сильнішою, якщо наша інфраструктура Інтернету речей буде спроектована на

стійкість до несанкціонованих зловмисників. Однак DY-зловмисникові бракує однієї здатності, якою можуть володіти звичайні зловмисники, а саме фізичного компромісу. Таким чином, захищені від втручання пристрої також дуже бажані. Ця мета, звичайно, недосяжна, але фізичний опір втручанню все ж є дуже важливою метою, яка разом із можливостями виявлення втручання (очевидне втручання) може бути достатнім захистом першої лінії.

У літературі зловмисники класифікуються на два основні типи: внутрішні та зовнішні. Внутрішні зловмисники – це користувачі з привілеями або дозволеним доступом до системи, яка має або обліковий запис на сервері, або фізичний доступ до мережі. Зовнішні зловмисники – це люди, які не належать до мережевого домену. Усі зловмисники, як внутрішні, так і зовнішні, можуть бути організовані різними способами та залучати окремих зловмисників до шпигунських агентств, що працюють на те чи іншу країну. Вплив вторгнення залежить від цілей, яких потрібно досягти. Окремий зловмисник може мати маленькі цілі, тоді як шпигунські агентства можуть мати більші мотиви. Цим буде обговорено різні типи зловмисників на основі їх кількості, мотивів та цілей.

А. Фізичні особи

Індивідуальні хакери – це професіонали, які працюють поодинці та мають на меті лише цільові системи з низьким рівнем безпеки. Їм бракує ресурсів або досвіду професійних хакерських команд, організацій чи шпигунських агентств. Окремі цілі хакерів порівняно невеликі за розміром або різноманітністю, а атаки, що проводяться, мають порівняно менший вплив, ніж ті, що здійснюються організованими групами. Методи соціальної інженерії найчастіше використовуються окремими зловмисниками, оскільки вони повинні отримувати базову інформацію про цільову систему, як-от адресу, пароль, інформацію про порти тощо. Загальнодоступні веб-сайти та веб-сайти в соціальних мережах є найпоширенішими місцями, де загальних користувачів можна обдурити. хакери. Більше того, операційні системи, що використовуються на ноутбуках, ПК та мобільних телефонах, мають загальні та відомі вразливості, якими користуються окремі зловмисники.

Фінансові установи, такі як банки, також є основною мішенню для окремих зловмисників, оскільки вони знають, що такі типи мереж здійснюють фінансові операції, які можна зламати, і, таким чином, зловмисники можуть маніпулювати інформацією в своїх інтересах. Викрадення інформації про кредитні картки має давню історію з окремими хакерами. З ростом електронної комерції легше використовувати викрадені дані кредитної картки для придбання товарів та послуг.

Окремі хакери використовують такі інструменти, як віруси, хробаки та нюхачі, щоб використовувати систему. Вони планують атаки на основі доступності обладнання, доступу до Інтернету, мережевого середовища та безпеки системи.

Однією з окремих категорій хакерів є інсайдер. Інсайдери – це уповноважені особи, які працюють проти системи, використовуючи інсайдерські знання або привілеї. Інсайдери можуть надати критичну інформацію для сторонніх зловмисників (сторонніх виробників) для використання вразливостей, які можуть увімкнути атаку. Вони знають слабкі місця в системі та те, як працює система. Особиста вигода, помста та фінансова вигода можуть спонукати інсайдера. Вони можуть нанести ризик від низького до високого залежно від їх мотивації.

Б. Організовані групи

Злочинні групи стають все більш знайомими з постійними комунікаціями та технологіями IoT. Крім того, коли вони стають більш комфортними для технологічних застосувань, ці групи можуть більше усвідомлювати можливості, що надаються інформацією про маршрутизацію інфраструктури різних мереж. Мотивація цих груп досить різноманітна; їх цілі, як правило, включають певні організації для помсти, крадіжки комерційної таємниці, економічного шпигунства та націлювання на національну інформаційну інфраструктуру. Вони також передбачають продаж особистої інформації, такої як фінансові дані, іншим злочинним організаціям, терористам і навіть урядам.

Вони дуже здатні з точки зору фінансового фінансування, досвіду та ресурсів. Можливості злочинних груп з точки зору методів та прийомів від помірного до високого залежно від того, які цілі. Вони дуже вміло створюють бот-мережі та шкідливе програмне забезпечення (наприклад, комп'ютерні віруси та програмне забезпечення) та методи атак за відмовою в обслуговуванні. Організовані злочинці, швидше за все, матимуть доступ до коштів, тобто вони можуть найняти кваліфікованих хакерів, якщо це необхідно, або придбати інструменти для атак "наводь і натискай" у підпільній економіці, за допомогою яких можна атакувати будь-які системи. Такі злочинці можуть зчинити більший ризик, ніж окремі хакери, і готові інвестувати в профілактичні атаки.

Кібертероризм [11] – це форма кібератаки, яка націлена на військові системи, банки та конкретні об'єкти, такі як супутники, та телекомунікаційні системи, пов'язані з національною інформаційною інфраструктурою на основі релігійних та політичних інтересів. Терористичні організації залежать від Інтернету для розповсюдження пропаганди, збору коштів, збору інформації та спілкування зі співавторами у всіх частинах світу. Інша поширена група злочинних організацій тягне за собою

хактивістів. Хактивісти – це групи хакерів, які беруть участь у таких діях, як відмова в обслуговуванні, шахрайство та / або викрадення особистих даних. Крім того, деякі з цих груп мають політичну мотивацію, такі як Сирійська електронна армія (CEO), Іранські кібервійська та китайські підрозділи з кібер-арфа.

В. Розвідувальне управління

Спецслужби різних країн наполегливо намагаються досліджувати військові системи інших країн для конкретних цілей, наприклад, промислового шпигунства та політичного та військового шпигунства. Для досягнення своїх цілей установам потрібна велика кількість експертів, інфраструктура, починаючи від дослідницьких та дослідницьких організацій, забезпечуючи технології та методології (апаратне забезпечення, програмне забезпечення та засоби), крім фінансових та людських ресурсів.

Такі установи мають організовані структури та складні ресурси для досягнення своїх цілей вторгнення. Такі агенції є найбільшою загрозою для мереж і вимагають жорсткого підходу та моніторингу для захисту від загроз інформаційних систем першочергового значення для будь-якої країни та військового закладу.

1.2.8. Обговорення та висновки

Експоненціальне зростання IoT призвело до більших ризиків безпеки та конфіденційності. Багато таких ризиків пов'язано з уразливістю пристроїв, яка виникає в результаті кіберзлочинності хакерами та неналежним використанням системних ресурсів. IoT потрібно будувати таким чином, щоб забезпечити простий і безпечний контроль використання. Споживачі потребують довіри до того, щоб повністю прийняти IoT, щоб насолоджуватися його перевагами та уникати ризиків безпеки та конфіденційності.

Більшість пристроїв та служб IoT піддаються ряду загальних загроз, про які вже говорилося раніше, таких як віруси та атаки «відмова в обслуговуванні». Вживати простих кроків, щоб уникнути таких загроз та боротися з вразливими місцями системи, недостатньо; таким чином, необхідно забезпечити безперебійний процес реалізації політики, що підтримується суворими процедурами. Процес розробки безпеки вимагає глибокого розуміння системних активів з подальшим виявленням різних уразливостей та загроз, які можуть існувати. Необхідно визначити, що таке активи системи та від чого активи повинні бути захищені. У цій роботі активи були визначені як усі цінні речі в системі, матеріальні та нематеріальні, які потребують захисту. Деякі загальні активи IoT включають системне обладнання, програмне забезпечення, дані та інформацію, а також активи, пов'язані із послугами, наприклад репутація служби.

Було показано, що надзвичайно важливо зрозуміти загрози та слабкі місця системи, щоб виділити краще пом'якшення системи. Крім того, розуміння потенційних атак дозволяє розробникам систем краще визначити, куди слід витрачати кошти. Найбільш відомі загрози описуються як DoS, фізичні атаки та атаки на приватне життя.

Було обговорено три різні типи зловмисників, а саме окремі напади, організовані групи та спецслужби. Кожен тип зловмисників має різні рівні кваліфікації, ресурси фінансування, мотивацію та толерантність до ризику. Дуже важливо вивчити різні типи акторів нападу та визначити, хто з найбільшої ймовірності атакує систему. Описуючи та документуючи всі загрози та відповідні суб'єкти, легше зрозуміти, яка загроза може використати яку слабкість у системі. Як правило, передбачається, що зловмисник IoT має всі можливості DY-вторгнення на додаток до деякої обмеженої фізичної компромісної сили. Ми припустимо, що фізичні компромісні атаки не масштабуються, і тому вони лише в гіршому випадку вплинуть на обмежену популяцію загальної кількості пристроїв IoT. Отже, архітектура IoT повинна бути спроектована для того, щоб справлятися зі зруйнованими пристроями та бути компетентною у виявленні таких випадків. Зроблено висновок, що зловмисники використовують різні методи, інструменти та техніки для використання вразливостей системи для досягнення своїх цілей або завдань. Розуміння мотивів та можливостей зловмисників важливо для організації, щоб запобігти потенційній шкоді. Щоб зменшити як потенційні загрози, так і їх наслідки, необхідні додаткові дослідження, щоб заповнити прогалини в знаннях щодо загроз та кіберзлочинності та надати необхідні кроки для пом'якшення ймовірних атак.

1.2.9. Висновки

IoT стикається з низкою загроз, які необхідно визнати, щоб вжити захисних заходів. У цьому документі були представлені виклики безпеці та загрози безпеці Інтернету речей. Загальною метою було виявити активи та задокументувати потенційні загрози, атаки та уразливості, з якими стикається IoT.

Був наданий огляд найважливіших проблем безпеки IoT, з особливим акцентом на проблеми безпеки, пов'язані з пристроями та послугами IoT. Визначено проблеми безпеки, такі як конфіденційність, конфіденційність та довіра суб'єктів господарювання. Ми показали, що для того, щоб створити більш безпечні та доступні пристрої та послуги IoT, потрібно вирішити проблеми безпеки та конфіденційності. Дискусія також була зосереджена на кіберзагрозах, що включають акторів, мотивацію та можливості, що підсилюються унікальними характеристиками кіберпростору. Було продемонстровано, що погрози з боку спецслужб та

злочинних груп, швидше за все, важче перемогти, ніж загрози окремих хакерів. Причина полягає в тому, що їх цілі можуть бути набагато менш передбачуваними, тоді як очікується, що вплив окремої атаки буде менш серйозним.

Було зроблено висновок, що багато роботи ще потрібно зробити у сфері безпеки IoT як з боку постачальників, так і з боку кінцевих користувачів. Для майбутніх стандартів важливо усунути недоліки існуючих механізмів безпеки IoT. Як майбутня робота, мета полягає в тому, щоб глибше зрозуміти загрози, що стоять перед інфраструктурою IoT, а також визначити ймовірність та наслідки загроз проти IoT. Визначення відповідних механізмів безпеки для контролю доступу, автентифікації, управління ідентифікацією та гнучкої системи управління довірою слід враховувати на початку розробки продукту.

1.3. Загрози кібербезпеки додатків IoT та сервісних доменів

Ми зараз живемо в епоху пост ПК, де смартфони та інші бездротові портативні пристрої змінюють наше середовище, роблячи його більш інтерактивним, адаптивним та інформативним. Названа Інтернетом речей (IoT), що переростає в Internet of Everything, нова екосистема поєднує бездротові сенсорні мережі, хмарні обчислення, аналітичні дані, інтерактивні технології, а також інтелектуальні пристрої для надання рішень, в які об'єкти вбудовані з мережевим зв'язком та ідентифікатор для посилення взаємодії між об'єктами. Інновації IoT прогресують і надають різноманітні розумні рішення або програми. Від електронного транспорту до електронного охорони здоров'я; розумний спосіб життя для електронного виробництва та багатьох інших електронних рішень. У цьому середовищі зростаюча тенденція кібератак на системну інфраструктуру в поєднанні з властивими системі вразливими місцями викликає занепокоєння не лише у постачальників, але й у споживачів. Ці проблеми безпеки повинні бути вирішені, щоб забезпечити довіру користувачів, щоб сприяти широкому визнанню і використовувати потенціал IoT. З точки зору налаштувань програмного, апаратного та програмного забезпечення інфраструктури, цей документ розглядає деякі з основних областей додатків та послуг IoT та аналізує виклики кібербезпеки, які, швидше за все, будуть стимулювати дослідження IoT у найближчому майбутньому.

1.3.1. Вступ

За даними IBM, очікується, що пристрої, підключені до Інтернету, перевищуватимуть кількість людей, а розвиток зв'язку триватиме так, що до 2020 року кількість підключених пристроїв складе близько 50 мільярдів [17]. Це розповсюдження підключених пристроїв у активній мережі створило те, що стало відомим як Інтернет речей (IoT). Платформа, на якій датчики та виконавчі механізми легко поєднуються з навколишнім середовищем, обмінюючись інформацією, щоб скласти загальну операційну картину. Система IoT починається з рівня, де ідентифікується один об'єкт, використовуючи унікальний глобальний ідентифікатор, який може бути глобально адресований. Рівень інформації, отриманої при доступі до об'єкта, у цьому випадку може бути таким низьким, як статичні дані, які зберігаються на тегах ідентифікації радіочастот (RFID). Тому IoT описується як об'єкти з унікальним ідентифікатором, що мають зв'язок з Інтернетом; є (в інтерактивному режимі) доступним для інших об'єктів, що називаються "речами". IoT вийшов із зародку і є наступною революційною технологією перетворення Інтернету на повністю інтегрований майбутній Інтернет (речей). Цей розвиток стимулюється недавнім

збільшенням впровадження та інтеграції бездротових мережевих технологій, бездротових сенсорних мереж (WSN), тегів RFID, а також виконавчих вузлів. Що стосується цієї концепції, стверджується, що розширення комунікаційних мереж за допомогою фізичних об'єктів ще більше прискорить кількість підключених пристроїв, а також обсяг інформації, якою можна обмінюватися через Інтернет.

IoT пропонує повсюдне підключення для широкого кола пристроїв, послуг та програм. Сюди входять інтелектуальні комп'ютери, смартфони, офісне обладнання, автомобілі з бездротовим підключенням, системи освітлення, опалення та вентиляції та кондиціонування (HVAC), побутова техніка та багато інших. Щоб увімкнути IoT, пристрій („річ") повинен знаходитись у мережі та під'єднуватися до комунікаційного вузла. Різні технології комунікаційних мереж (інфраструктури), такі як 3G, LTE, Wi-Fi, Bluetooth, ZigBee, Z-wave, Sigfox тощо, забезпечують послуги зв'язку для розгортання IoT на багатьох платформах послуг.

З розвитком IoT, як очікується, хмарні обчислення стануть основою для всесвітнього розповсюдження інформації, аналізу даних (або обчислень) та зберігання. Очікується, що хмарні рішення, такі як Microsoft Azure, Amazon Web Services (AWS), Google Docs тощо, забезпечують стандартні шлюзи для взаємозв'язку фізичних об'єктів з обчислювальними та комунікаційними можливостями у широкому діапазоні програм, служб і технологій. Обговорюються прогрес, можливості та виклики середовища всюдисущих обчислень «ubicomp» та визначаються дві найважливіші технології для розвитку майбутньої інфраструктури ubicomp, як хмарні обчислення та Інтернет речей. Таким чином, загальноприйнятим вважається, що у міру дозрівання IoT хмарні обчислення будуть виконувати функції приймача даних від різних всюдисущих датчиків, а також будуть платформою для аналізу великих даних, аналізу та інтерпретації даних, що генеруються IoT. Крім того, різні хмарні рішення все частіше пропонуються для надання користувачам сумісних веб-програмних інтерфейсних програм для взаємодії та взаємодії користувачів.

Наприклад, стверджували, що для того, щоб IoT з'явився з успіхом, традиційні обчислювальні платформи та підключення до Інтернету повинні бути розширені за межі традиційного мобільного зв'язку, що пов'язує людей, і перерости у об'єднання об'єктів та впровадження інтелекту в наше середовище. Завдяки цій фундаментальній основі можна досягти розумного підключення та контекстно-обчислювальних обчислень. Безумовно, з урахуванням того, що мільярди пристроїв, як очікується, будуть підключені до екосистеми IoT, передбачається генерувати величезні обсяги даних, які доведеться зберігати, обробляти та представляти у бездоганній, ефективній та легко інтерпретованій формі. У цьому випадку

хмарно-орієнтовані обчислення будуть потрібні як платформа для забезпечення підтримки віртуальної інфраструктури служб IoT. Послуги включатимуть моніторинг, зберігання, обчислення (та / або аналітику), візуалізацію та надання послуг клієнтам. Бачення IoT можна побачити з орієнтації на "Інтернет" та "Thing". Інтернет-орієнтована архітектура залучає Інтернет як послугу, що є основним напрямком IoT, тоді як дані надаються об'єктами. У архітектурі, орієнтованій на речі, розумні об'єкти займають центральне місце в послугах і додатках IoT.

Основними занепокоєннями, викликаними інтеграцією IoT-Cloud, є той факт, що від інфраструктурного до сервісного доменів хмарні моделі перебувають під різними проблемами безпеки, такими як атака служб додатків, атака цілісності даних, конфіденційність, довіра, ідентичність, стандартизація тощо. ймовірно, відкриється, коли дві платформи злиються, порушуючи деякі фундаментальні питання досліджень, які потрібно дослідити. Відповідно, дослідження, проведене Міжнародною корпорацією даних (IDC), стверджує, що, хоча керівники підприємств визнають діловий потенціал IoT, вони глибоко скептично ставляться до властивих системі викликів безпеці. Крім того, зазначається в дослідженні, більшість керівників підприємств визнали, що мало розуміють або недооцінюють загрози безпеці, які створює IoT. У відповідному дослідженні KPMG заявила, що порушення безпеки споживчих даних, а також нещодавні напади на системи кіберінфраструктури у всьому світі змушують користувачів IoT втрачати довіру та уникати постачальників рішень, які не вживають відповідних заходів для захисту своїх систем [18]. Питання викликів кібербезпеки на платформах IoT є головним глобальним питанням, яке вимагає цілісної оцінки як дослідницьких, так і промислових спільнот. У цій роботі проводиться оцінка загроз, пов'язаних із безпекою, які, ймовірно, можуть перешкодити успіху впровадження IoT та довірі споживачів.

1.3.2 Концепція IoT

За останнє десятиліття Інтернет-технології зробили революцію у взаємозв'язку між людьми безпрецедентними масштабами та швидкістю. Очікується, що наступна революція створить взаємозв'язок між різними об'єктами, що призведе до того, що експерти назвали розумним середовищем. Оскільки ми переходимо від www (веб-сторінки статичних сторінок) до web2 (веб-мережі соціальних мереж) до web3 (всюдисущі обчислення – або павутина речей), потреба у даних на вимогу з використанням складних інтуїтивних запитів продовжує значно зростати. Цю епоху можна було б назвати епохою після ПК, коли смартфони та пов'язані з ними пристрої змінюють наше середовище та спосіб взаємодії «речей»

(включаючи людей). Речі в новому середовищі стають більш інтерактивними, а також інформативними. Марк Вайзер (батько повсюдної обчислювальної техніки), визначив нову екосистему як «розумне середовище у фізичному світі, яке насичено і непомітно переплітається з датчиками, виконавчими механізмами, дисплеями та обчислювальними елементами, які безперешкодно вбудовуються в повсякденні об'єкти і з'єднуються через безперервна мережа». Стверджується, що зростання повсюдних обчислень формується за рахунок хмарних обчислень та IoT.

Вважається, що IoT як концепція була винайдена Кевіном Ештоном у поданні, де він стверджував, що «додавання RFID та інших датчиків до повсякденних об'єктів створить Інтернет речей та закладе основи нового століття машинного сприйняття» [19]. З тих пір ідея просунулась у своєму прийнятті як у науково-дослідній, так і в промисловій екосферах. Роман та ін. [20] стверджують, що в основному пристрій IoT як неоднорідний об'єкт матиме доступний, адресований і читабельний аналог в Інтернеті, завдяки чому IoT відкриває канал зв'язку з будь-яким іншим об'єктом, надаючи та отримуючи послуги в будь-який час і в будь-якому місці, і будь-яким чином. З цієї точки зору, більшість «речей» (наприклад, люди, домашні тварини, сільськогосподарські тварини та комп'ютери, книги, машини, побутова техніка та їжа) будуть в Інтернеті в тій чи іншій формі, що призведе до еволюції Інтернету всього (IoE) (рис. 1.2), що демонструє безліч ознак (рис. 1.3).

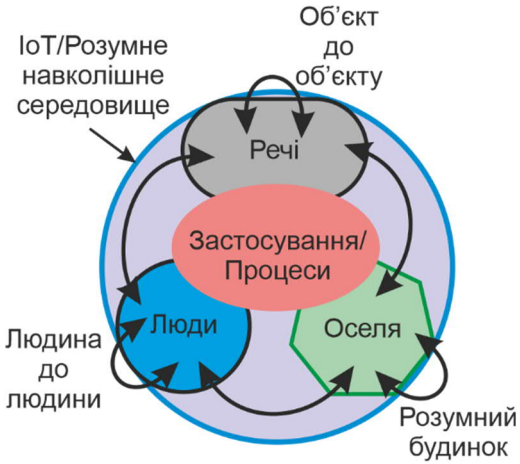


Рис. 1.2. Футуристична екосистема Інтернету Всього (Internet of Everything – IoE)

Рис. 1.3. Характеристики футуристичного IoE

У 2005 році Міжнародний союз електрозв'язку (МСЕ) запропонував концепцію Інтернету речей у Мережевих звітах МСЕ за 2005 рік. У звіті описано еру IoT як епоху, коли машина автоматично подаватиме сигнал, коли водій допустить помилку; коли портфель міг нагадати перевізнику, що він забув взяти; одяг повідомляє пральній машині їх кольори та вимоги до температури тощо.

Європейський дослідницький кластер з питань Інтернету речей (IERC) визначає IoT як інтегровану частину майбутнього Інтернету з наступними характеристиками (рис. 1.4).

З тих пір у ряді досліджень було розглянуто різні аспекти IoT. Наприклад, Роман та ін. [20] надав явний аналіз особливостей та проблем безпеки Інтернету речей у перспективі розподілених систем. Серед обговорюваних питань були ідентифікація та автентифікація, контроль доступу, протокол, відмовостійкість, довіра та управління.

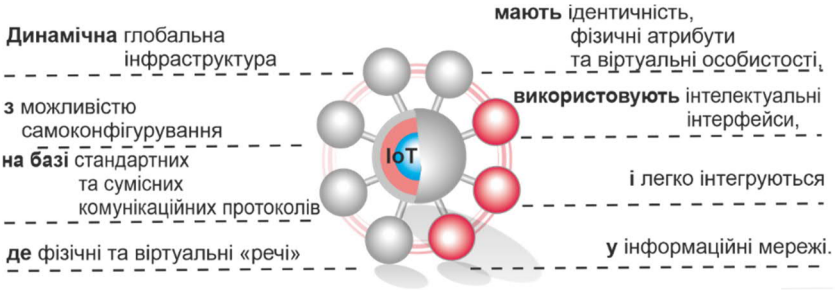


Рис. 1.4. Визначення IoT за IERC

1.3.2.1 Інфраструктура IoT

Встановлено, що в цілому інфраструктура IoT (рис. 1.5) складається з різноманітних апаратних ресурсів, таких як WSN, RFID-мітки, виконавчі пристрої, зчитувачі, камери, контролери, GPS, датчики (магнітометри, сенсори ультразвуку та інфрачервоного світла), процесори пристроїв, термінали та інші шлюзи датчиків. Більше того, на рівні програмного забезпечення більшість об'єктів IoT вбудовані в кремнієві інтегральні схеми (IC) та наноелектроніку, орієнтовані на мініатюризацію, низьку вартість та підвищену функціональність у проектуванні бездротових ідентифікованих систем або вузлів із підтримкою зв'язку. Теги RFID та обладнання WSN залишаються двома найбільш відомими ресурсами апаратної інфраструктури IoT. Технологія RFID дозволяє передавати дані на невелику відстань. Він складається з активної або пасивної радіочастотної (RF) мітки, прикріпленої до відстежуваного елемента, та радіочастотного зчитувача / випромінювача. Пасивний тег забирає енергію від свого зчитувача, тоді як активний тег RFID отримує живлення від свого вбудованого пристрою.

Обладнання WSN містить інтерфейси датчиків, блоки обробки, блоки трансиверів та джерело живлення.

З іншого боку, програмне забезпечення, що підтримує IoT, варіюється від програмних операційних систем до прикладного програмного забезпечення з хмарними програмними рішеннями (SaaS) та мобільною ОС (iOS, android, Blackberry) як основою. Інші програмні рішення включають мережеві та пристрої ОС, які в основному базуються на мікроядрах (наприклад, TinyOS, TinyDB, Nano-RK, LiteOS, VM). Інші включають програмне забезпечення для розробки додатків, таке як HTML, JavaScript, Ajax, PHP та Ruby. Інтеграція програмного забезпечення IoT на додаток до загальних програмних послуг також підтримує візуалізацію даних, системну інтеграцію, віддалений контроль доступу та інтерфейс прикладних програм (API).

1.3.3. Виклики IoT в галузі кібербезпеки

На думку Романа та співавт. [20], однією з ключових проблем, яку потрібно подолати, щоб проштовхнути IoT у реальний світ, є безпека. Проблеми безпеки, пов'язані з IoT, узгоджуються з традиційними цілями безпеки (SO) інформаційних систем (IC), які стосуються конфіденційності, цілісності та доступності даних. Більше того, існують інші проблеми безпеки, які, схоже, визначаються IoT. Наприклад, злиття хмарних обчислень та IoT піддає платформи IoT індукованим хмарою уразливостям, таким як ті, що містяться у OWASP top 10.

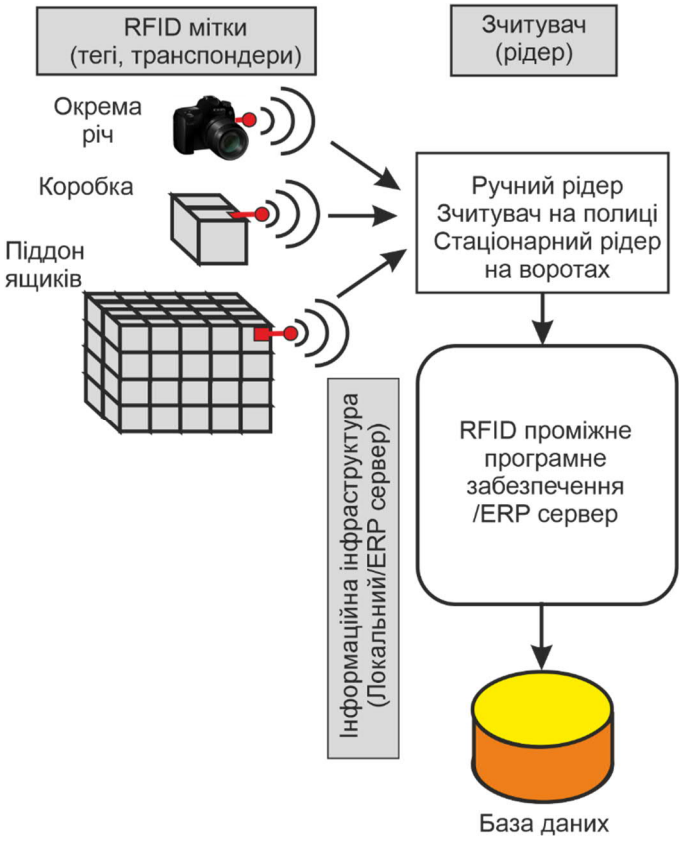


Рис. 1.5. Операційна структура RFID

На малюнку 1.6 нижче представлені вразливості, спричинені хмарою, виявлені у 2015 році із загальної бази даних вразливостей. Ці вразливості, властиві хмарним додаткам, можуть вплинути на рішення та послуги IoT у міру їх появи.

Інший суттєвий вектор ризику можна знайти в неякісних продуктах та послугах IoT. Вони можуть загрожувати життєздатності послуг IoT. Наприклад, погано розроблені, виготовлені та застарілі, або підроблені товари представляють дуже значні ризики для програм, що підтримують IoT. Щодо цього питання, підприємства у всьому світі страждають від незліченних годин грошових витрат та втрат місій через несподівані несправності обладнання та системи, спричинені неякісним або

неналежним технічним обслуговуванням, поганими та неточними порадами некваліфікованого обслуговуючого персоналу. Крім того, автори заявляють про низьку ефективність роботи персоналу, за яким працює контракт, і навіть неточні дані ділового партнера і, можливо, пристрої IoT можуть прийматися для інформаційних процесів та важливих бізнес-рішень.

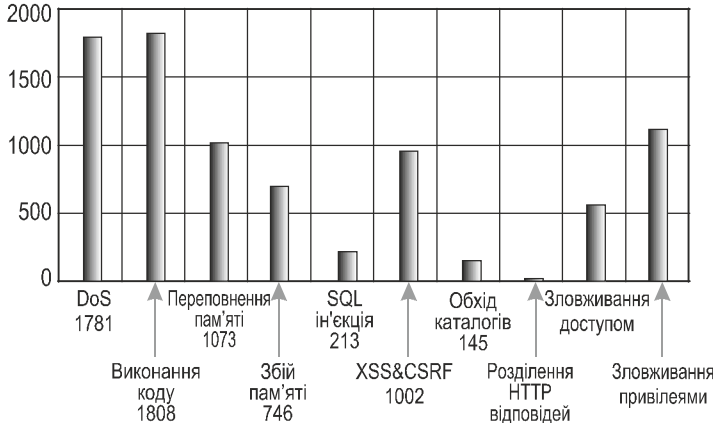


Рис. 1.6. Вразливості, виявлені у 2015 році

Більше того, більшість проблем кібербезпеки IoT лежать у властивих системі вразливих місцях, які піддають налаштування інфраструктури різним атакам. Джерела можуть включати програмне забезпечення, обладнання (пристрій), системні програми, дані, а також мережеві інтерфейси чи порти. Крім того, двосторонні зв'язки зв'язку між об'єктами до об'єктів залишають систему відкритою для мережевих атак та збою протоколу. Інші пов'язані атаки включають бездротове скремблювання, прослуховування, атаки "людина посередині" та атаки на модифікацію та введення повідомлень. Наприклад, пристрої на основі IP сприйнятливі до помилкової конфігурації IP, яка іноді виявляє недетерміновану поведінку з точки зору атаки. Ідентифікація помилок IP неминуче знижує продуктивність та надійність системи. Більше того, хоча інтеграція IoT та хмарних обчислень розширює програми та послуги IoT, інтеграція також відкриває інфраструктуру IoT та взаємозалежні системи загальнодоступним мережам та глобальному шлюзу. На додаток до IP-спуфінгу, шлюзи обслуговування (як локальні, так і глобальні) можуть стати ідеальними пунктами для вторгнень, DoS, атак введення та інших атак на основі Інтернету та мережі.

До них додається, що більшість інтерактивних додатків IoT користуються Інтернетом та / або мобільними пристроями, розроблені переважно з інтерфейсом програмування програм (API) як архітектурою коду інтерфейсу з використанням PHP, Java, XML та HTML. Нерозпакований API може бути сприйнятливий до різних атак, що піддають всю систему шкідливим атакам. Наприклад, у CVE-2016-7413 вразливість без використання у функції wddx_stack_destroy у ext / wddx / wddx.c у PHP до 5.6.26 та 7.x до 7.0.11 дозволяє віддаленим зловмисникам викликати відмову в обслуговуванні через документ XML wddxPacket, в якому відсутній кінцевий тег для елемента поля набору записів, що призводить до неправильної обробки виклику wddx_deserialize. Подібним чином, у CVE-2016-4539, функція xml_parse_into_struct у ext / XML / xml.c у PHP до 5.5.35, 5.6.x, 5.6.21, 7.x та до 7.0.6 дозволяє віддаленим зловмисникам викликати відмову в обслуговуванні (помилка недочитаного буфера та сегментації) або, можливо, мати інший вплив через створені дані XML у другому аргументі, що призвело до нульового рівня синтаксичного аналізатора.

Загалом, системи IoT розробляються з урахуванням безпеки, однак помилкова конфігурація безпеки може відбуватися на будь-якому рівні архітектури зв'язку IoT або будь-якій частині системного додатку. Наприклад, на рівні програмного забезпечення пристрої IoT, такі як теги RFID (мікросхеми), як правило, мають внутрішню пам'ять або батареї, що живляться самостійно; Коливання напруги в електромережі або альтернативні струми (змінного струму) можуть призвести до збоїв пристроїв пам'яті, що призведе до втрати даних. Крім того, переривчасті коливання потужності в напівпровідникових приладах призводять до втрати сигналу, що призводить до потенційної несправності системи. Інші проблеми безпеки в пристроях IoT включають несумісність компонентів, а також атаки на основі пристроїв (фізичні), такі як стихійні лиха, незаконне використання пристрою (наприклад, викрадення) та маскування. Щоб подолати ці виклики, знадобляться інноваційні дослідження та комплексні системні рішення, орієнтовані на архітектурний дизайн системи, програмно-апаратне забезпечення, реконфігурацію, зміцнення мережі та динамічне проектування системних додатків.

1.3.3.1 Кібер-атака на IoT

З вищевказаних викликів ми представляємо таксономію атак кібербезпеки на комунікації від об'єкта до об'єкта, аналізуючи вразливості системи перед потенційними акторами загроз. У цій систематиці обговорюється шість типів вразливостей. Це помилкова конфігурація IP, SQL ін'єкція, DoS, виконання коду, пошкодження пам'яті, а також XSS і CSRF. Відповідні вектори загроз включають фізичну (пристрій) атаку,

прикладну (програмне забезпечення) атаку, мережеву атаку, атаку вебінтерфейсу та атаку даних. У таблиці 1 представлена запропонована матриця вразливості та загрози [17]. У стовпцях 3 та 4 вектори загроз відповідають відповідним вразливостям.

Таблиця 1

Матриця вразливості–загрози

Вразливості (V)	Вектори кібератаки (AV)	Матриця вразливості–загрози	
		Вектор атаки	Вразливості
Помилкова конфігурація IP (IM)	Атака на прилад (DA)	DA	IP, MC, CE, D
SQL ін'єкція (SI)	Атака на додаток (AA)	AA	SI, D, CE
DoS (D)	Мережева атака (NA)	NA	SI, D, CE
Виконання коду (DE)	Атака на Web інтерфейс (WiA)	WiA	SI, D, XC, IP
XSS і CSRF (XC)	Атака на цілісність даних (DA)	DA	SI, CE
Пошкодження пам'яті (MC)			

1.3.3.2 Вектори атаки

1.3.3.2.1 Атака на пристрій

Цей тип атаки здатний зламати пристрої IoT. Його головна мета полягає в компрометації важливих архітектурних функцій системи (залежно від задіяних пристроїв). У системі управління запасами, що працює на основі RFID, успішний зловмисник може зруйнувати всю мережу (особливо коли базовий пристрій (наприклад, сервер є цільовим пристроєм). У мережі близького радіусу (NAN) в електромережі атака пристрою може вплинути на стійкість мережі, що в крайньому випадку може призвести до розподілених атак відмови в обслуговуванні по всій сітці. Атаки на пристрої можуть бути спричинені помилковою конфігурацією IP, пошкодженням пам'яті та неправильно виконаним кодом в операційній системі пристрою на рівні проміжного програмного забезпечення.

1.3.3.2.2 Атака служби додатків

Це тип атаки, який компрометує системні програми (Інтернет, Мобільні, Системні тощо), які запускаються на різних компонентах системи.

Типовий додаток IoT запускає кілька сеансів як на локальному, так і на серверному рівнях. У більшості випадків ці програми можуть належати постачальникам послуг програм (ASP) або стороннім постачальникам. Як зазначалося раніше, кібератаки на ці програми можуть напевно скомпрометувати інші взаємозалежні системи.

Загальні уразливості цього типу атак включають введення SQL, виконання коду та DoS. Більшість програм із підтримкою IoT розроблені з використанням Raspberry Pi, що базується на ядрі Linux. Уразливості в ядрі піддають залежні програми різним формам атак програм. Наприклад, у CVE-2016-8658 перенесення потоку буфера на основі стека у функції brcmf_cfg80211_start_ap у драйверах / net / wireless / broadcom / brcm80211 / brcmfmac / cfg80211.c в ядрі Linux до 4.7.5 дозволяє локальним користувачам спричинити відмову в обслуговуванні (збій системи) через довгий інформаційний елемент SSID в команді до сокета Netlink. Подібним чином, у CVE-2016-5344, кілька цілочисельних надлишків у драйвері MDSS для ядра Linux 3.x, як використовується в внесках Qualcomm Innovation Center (QuIC) Android для пристроїв MSM та інших продуктів, дозволяють зловмисникам спричинити відмову послуги через велике значення розміру, пов'язане з mdss_compat_utils.c, mdss_fb.c та mdss_rotator.c.

1.3.3.2.3 Мережева атака

Це атака, метою якої є компрометація взаємозв'язку між пристроями шляхом затримки пересилання повідомлень або втрати повідомлення. Мережеві атаки можуть зруйнувати обчислювальні процеси в системах конфігурації IoT. У домашніх мережах (HAN) цей тип атаки спрямований на руйнування функціональних можливостей моніторингових або взаємопов'язаних пристроїв. Подібним чином, у сусідській мережі (NAN) цей тип атаки може ізолювати або заборонити підключеним пристроям доступ до життєво важливої інформації із сусідніх пристроїв або звернення до запиту обміну повідомленнями із сусіднього пристрою. Причини таких атак включають введення SQL, DoS та виконання коду.

1.3.3.2.4 Атака веб-інтерфейсу

Цей тип атаки представляється в результаті перерахування облікового запису, відсутності блокування облікового запису або слабких облікових даних. У цьому випадку зловмисник використовує для доступу до веб-інтерфейсу слабкі протоколи автентифікації (або захоплення облікових даних у простому тексті, або перерахування облікових записів). Атаки на веб-інтерфейс можуть бути викликані міжсайтовими сценаріями (XSS), міжсайтовою підробкою посилань (CSRF), помилковою

фігурацією IP та ін'єкцією SQL. Інші джерела включають небезпечний дизайн веб-інтерфейсу та слабкі дані облікового запису. Атака порушує цілісність пристрою та може призвести до відмови в обслуговуванні. Наприклад, у CVE-2016-7571 вразливість міжсайтових сценаріїв (XSS) у Drupal 8.x до 8.1.10 дозволяє віддаленим зловмисникам вводити довільний веб-сценарій або HTML за допомогою векторів, що включають виняток HTTP. Подібним чином у CVE-2016-8581 у заголовку User-Agent процесу входу в систему AlienVault OSSIM та USM до 5.3.2 існує постійна вразливість XSS, яка дозволяє зловмиснику викрадати ідентифікатори сеансів зареєстрованих користувачів під час перегляду поточних сеансів. адміністратором.

1.3.3.2.5 Атака цілісності даних

Це атака, в результаті якої агент загроз намагається скомпрометувати системні дані, вставляючи, змінюючи або повністю видаляючи дані (що зберігаються або передаються), щоб обдурити розумний пристрій, щоб прийняти неправильні рішення або порушити його цілісність. Атаки даних можуть бути спричинені ін'єкцією SQL та виконанням коду, який може виконуватися віддаленим зловмисником.

1.3.4 Домени додатків і послуг IoT

Беручи до уваги нещодавні досягнення платформ IoT, майже неможливо передбачити численні програми IoT, маючи на увазі постійні інновації в технологіях, послугах та постійні потреби в галузі. Поточні домени додатків включають (але не обмежуються) незалежний спосіб життя (розумні будинки), розумні міста, розумну енергію (розумна мережа та вимірювання), розумну мобільність та транспорт, охорону здоров'я, роздрібну торгівлю та логістику, моніторинг навколишнього середовища, розумне виробництво (рис. 1.7).

З усіма цими сферами пов'язані проблеми безпеки, де специфікації домену викликають різні проблеми. Деякі з них є дуже очевидними і, як правило, обговорюються як порушення безпеки, пов'язане з відкриттям медичного обслуговування для зловживання дуже особистою інформацією; торгівля / роздрібна торгівля може відкритись для зловживання грошима / фінансами, але також швидко розвивається домен розумного життя / розумного міста викликає занепокоєння щодо безпеки, пов'язані із загрозами, про які йдеться в Розділі 1.3.3.

Рис. 1.7. Галузі застосування IoT

1.3.4.1 Розумна сітка

Є величезні можливості зробити місто «розумним» з точки зору IoT. Домен охоплює зондування активності та відстеження подій, включаючи інтерактивні об'єкти в розумному середовищі. Додаток IoT у розумному місті передбачає величезну різноманітність вимог як до інфраструктури, так і до технологій. Однією з областей, що виникають із величезними потенціалами IoT, є енергетична сфера / розумна енергія.

Розумна енергія (мережа) – це своєрідний «Інтернет», в якому енергетичний пакет управляється подібно до пакета даних – через маршрутизатори та шлюзи, які можуть самостійно визначити найкращий шлях для досягнення пакетом пункту призначення з найкращими рівнями цілісності. Концепція «Інтернет енергії (IoEn)» визначена як мережева інфраструктура, що базується на стандартних та сумісних трансиверах зв'язку, шлюзах і протоколах, що дозволяють в реальному часі балансувати між локальним та глобальним виробленням, зберіганням, розподілом та оптимізацією попиту. Стандарт IEEE 2030 щодо інтелектуальної енергетики визначає широкомасштабну мережу (WAN), польову мережу / зону сусідства (FAN / NAN) та домашню мережу (HAN) як основні компоненти інтелектуальної мережі.

1.3.4.1.1 Розумне вимірювання

За словами Вермесана та Фрісса, IoEn повинен запропонувати інноваційну концепцію розподілу електроенергії, зберігання енергії, моніторингу мережі та зв'язку, як представлено в [21]. IoT як підтримуюча платформа підтримує розподіл енергії як коли, так і де потрібна енергія. Таким чином, моніторинг споживання енергії здійснюється на всіх рівнях; від місцевих (домашніх) пристроїв до національного та міжнародного пункту розповсюдження [20]. Розширений процес моніторингу в електромережі відомий як інтелектуальне вимірювання [22], також відоме як інфраструктура попереднього вимірювання (AMI) (рис. 1.8).

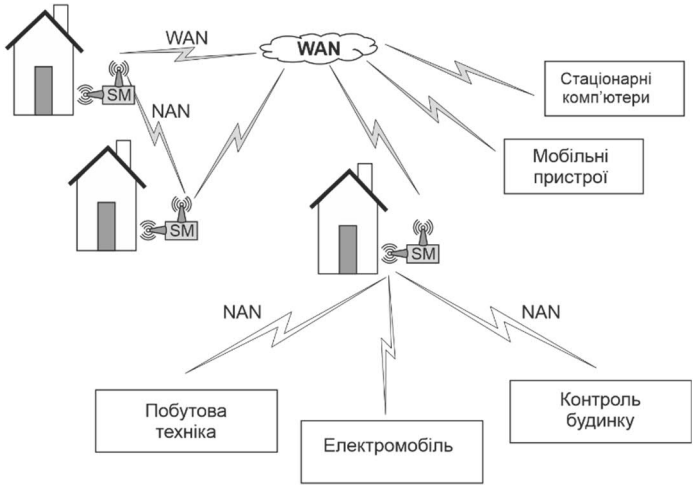


Рис. 1.8. Комунікаційна архітектура розумного вимірювання

За даними Azasoo та Tweneboah-Koduah, інтелектуальне вимірювання стало інноваційною системою для моніторингу розподілу енергії, споживання та виставлення рахунків за рахунок зближення енергетики, інформаційних та комунікаційних технологій [22]. AMI забезпечує двосторонню передачу інформації для відстеження споживання енергії (як джерела даних для виставлення рахунків споживачам), а також для відстеження відключень. Дані, зібрані AMI, використовуються для інформування споживачів про їх споживання енергії. У цьому випадку AMI надає платформу для взаємозв'язку розумних лічильників, інтелектуальних приладів, пристроїв управління, точок доступу та центрів обробки комунальних послуг. За сценарієм розумної енергії розумні лічильники надають користувачеві інформацію про миттєве споживання енергії, таким

чином дозволяючи ідентифікувати та усунути витратні пристрої, а також забезпечуючи платформу для оптимізації індивідуального споживання енергії, а також виставлення рахунків споживачам.

1.3.5 Експериментальна оцінка кібератак на підключений IoT-пристрій (SQLi та DoS Attack): кейс розумного вимірювання

Тут демонструємо, як виконуються SQL-ін'єкції та DoS-атаки проти пристроїв, підключених до Інтернету речей, з розумним вимірюванням. Демонстрація була проведена на самозапущеному віртуальному сервері. В обох випадках результати показують успішну кібератаку на підключені пристрої IoT, що мають віддалений сервер (див. Рис. 1.9 нижче).

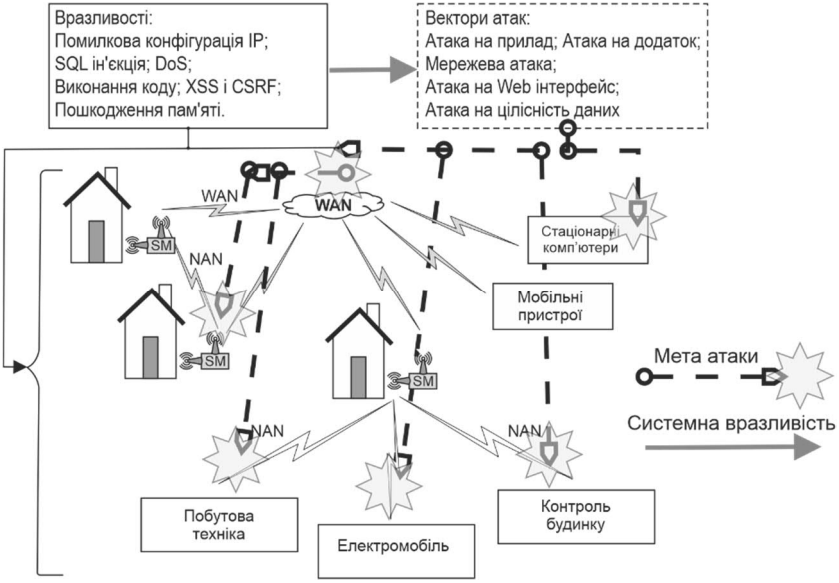


Рис. 1.9. Розумні вимірювання та відповідні вектори атак

Атака ін'єкції SQL – алгоритм (рис. 1.10)

```
Print header information
 for URL in target URLs
  for payload in get request payloads
   response = send get request probe to server
```

```
  if response.status code == 500
    print payload and exist for manual attack
for paylaod in post request payloads
  response = send post request probe to server
```

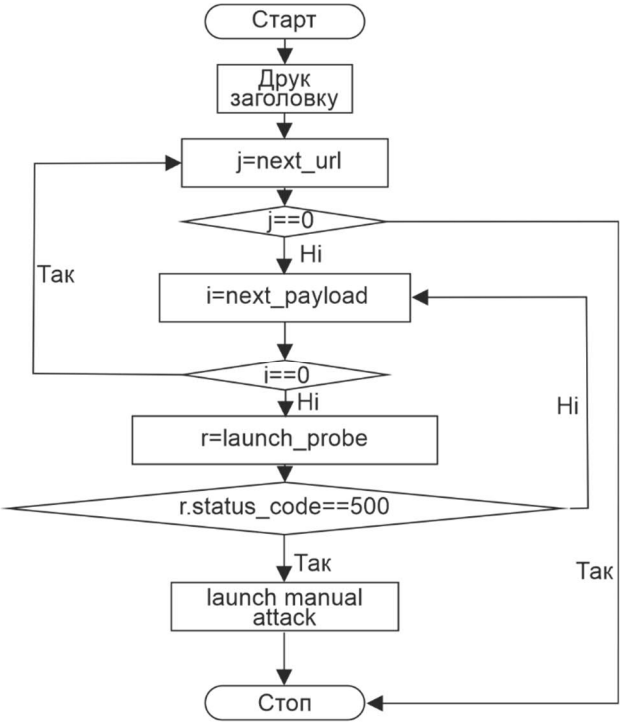


Рис. 1.10. Блок-схема атаки ін'єкцій SQL

Атака введення SQL (за допомогою Python)

```
This function delivers a payload to the smart
metering gateway using an http ‘get’ method.
To do this, the payload is added to the url. The url
sends a request to @params payload {string}. The
request parameters for example
requests.get('http://www.test.com/', params=payload)
will map to http://www.test.com/?key=value
###
def http_get(url, payload):
```

r = requests.get(url, params=payload)
return process_responds(r)
###
The function processes a request to a smart metering
gateway to determine if a probe is positive or
negative. A positive probe indicates an
open/unprotected port (vulnerability).
Probing Get (assuming query is contracted: where id
= <defined_param>
('Params ', {'make': '""'})
('Url: ',
'http://metering.grid.com/metering/meter/topup_histo
ry')
data been sanitised
data been sanitised
data been sanitised
data been sanitised
Probbing Post
data been sanitised
data been sanitised
data been sanitised
data been sanitised
Vulnerability: Weakness found (SQL injection)
Threat: data sanitised
Effect: sensitive information could be disclosed by injection attack
Impact: Data confidentiality and integrity could be compromised

Атака відмови в обслуговуванні (рис. 1.11)

DoS attack on the Application layer

Attack url: http://metering.smartmeter.com/metering/server/dashboard

Tool: loadtest (https://www.npmjs.com/package/loadtest) requires nodejs to be installed

Test parameter: $ loadtest http://metering.aborsour.com/metering/server/dashboard -t 50 -c 10 --rps 1000.

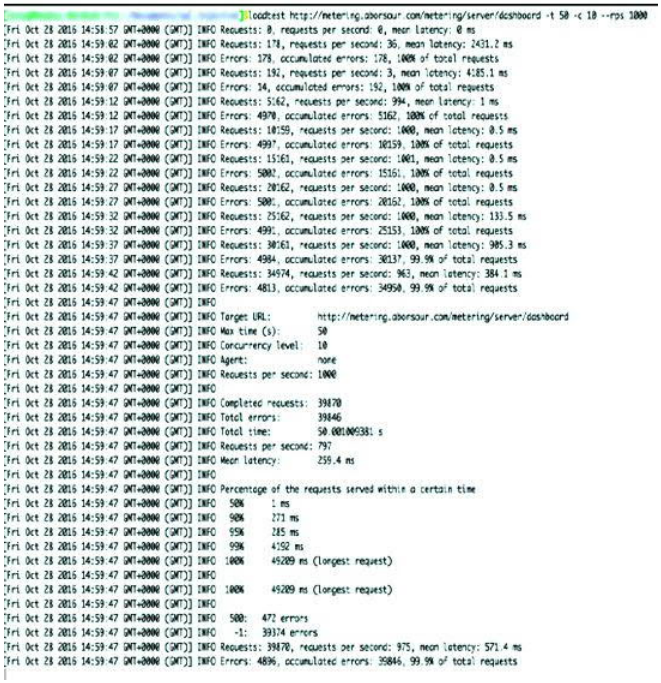


Рис. 1.11. Скріншот реакції на атаку DoS

1.3.6 Обговорення

Наведений вище експеримент базується на інтелектуальному вимірюванні зв'язку, як показано в [22]. Ідея запуску атак SQLi та DoS на розумну систему вимірювання підкреслює їх суттєвий вплив на розподілену мережеву систему (Рис. 1.10, 1.11). У випадку атаки введення SQL (експеримент 1), запит на корисне навантаження було надіслано на розумний шлюз вимірювання для перевірки на наявність уразливостей. Шлюз, який виступає в ролі основного сервера в налаштуваннях сусідньої мережі (NAN), відповів заголовком повідомлення ACK, щоб прокласти шлях для успішної атаки (скомпрометованих даних) на систему. Це означає, що вразливість SQL-ін'єкцій в архітектурі інтелектуального вимірювання може дозволити віддаленим аутентифікованим користувачам виконувати довільні команди SQL через створені серіалізовані дані як на сервері інформаційної системи вимірювання (MISS) як в інтелектуальних установках вимірювання HAN, так і в NAN (рис. 1.10). Наприклад, вразливість введення SQL на сторінці входу в пристрої інтерфейсу

користувача може дозволити віддаленим зловмисникам виконувати довільні команди SQL через створену URL-адресу.

У других експериментах (DoS-атака) (див. Рис. 1.11) було виконано кілька (ненормальних) віддалених запитів (1000) на Сервер вимірювальної інформаційної системи (MISS) для одночасних з'єднань за 50 с. MISS міститься в HAN та NAN для інтелектуального вимірювання. Наш результат показує, що подрібнення сервера призвело до виконання деяких довільних кодів (рис. 1.11). У цій атаці передача буфера в протоколі Point-to-Point по Ethernet (PPPoE) в шлюзі клієнта, коли на сервері налаштована автентифікація CHAP, дозволяє віддаленим зловмисникам спричинити відмову в обслуговуванні або виконати довільний код через створені пакети надіслані під час автентифікації. Наприклад, у CVE-2016-8666 стек IP в ядрі Linux дозволяє віддаленим зловмисникам викликати відмову в обслуговуванні (споживання стека та паніку) або, можливо, мати невстановлений вплив, запускаючи використання функцій GRO (gro-receive та gro-complete) для пакетів із тунельним укладанням.

1.3.7. Висновок

Оглянуто спробу оцінити таксономію різних вразливих системних вразливих місць, які піддають інфраструктуру Інтернету речей та додатки різним векторам кіберзагроз та обґрунтовують зусилля щодо цієї нової технології. Обговорення включає виявлення різних вразливих місць, притаманних домену додатків та сервісам. Було виконано два різні сценарії (тести) атак щодо налаштування інтелектуальної комунікаційної інфраструктури вимірювання. Результати тестів показують, що вразливі системи IoT (будь то додатки, апаратні засоби, програмне забезпечення чи програмне забезпечення) можуть бути зловживанні різними суб'єктами загроз через створені вектори.

Нарешті, надзвичайно важливо продовжувати дискусію, одночасно вимагаючи від виробників пристроїв та постачальників компонентів розробити та впровадити рішення, щоб протидіяти загрозам від кібер-супротивників, щоб гарантувати споживачам максимальну довіру до інновацій та трансформації IoT.

1.4. Безпека та конфіденційність в Інтернеті речей

Інтернет речей (IoT) – це технологія, яка здатна змінити спосіб життя в багатьох секторах, починаючи від транспорту і закінчуючи охороною здоров'я, від розваг до взаємодії з урядом. Ця фантастична можливість також представляє низку значних викликів. Зростання кількості пристроїв та швидкість цього зростання створює виклик нашій безпеці та свободам, коли ми боремося за розробку політики, стандартів та управління, що формують цей розвиток, не заважаючи інноваціям. У цій роботі обговорюється розвиток IoT, різні його визначення та деякі ключові сфери застосування. Міркування щодо безпеки та конфіденційності, які стоять попереду, обговорюються як загалом, так і в контексті цих програм [4].

Вступ

Інтернет речей (IoT) проголошується як розвиток, який може внести кардинальні зміни в наш спосіб життя. Він визнаний стимулюючим фактором, який підвищить ефективність у ряді областей, включаючи транспорт та логістику, охорону здоров'я та виробництво. IoT допоможе в оптимізації процесів за допомогою вдосконаленої аналітики даних та стане каталізатором для нових сегментів ринку, використовуючи свої кіберфізичні характеристики, породжуючи наскрізні програми та послуги.

Еволюція IoT. Ідея підключення "речей" до Інтернету поширюється значно далі, ніж використання терміну "Інтернет речей". На початку 1980-х років студенти Університету Карнегі-Мелона встановили підключені до Інтернету фотодатчики до торгового автомата для безалкогольних напоїв, що дозволило їм підрахувати кількість розлитих банок. Це дозволило кожному, хто має доступ до Інтернету, визначити, скільки напоїв було видано і, отже, скільки залишилось.

Ще до створення першої веб-сторінки Джон Ромкі та Саймон Хаккет представили тостер, який був підключений до Інтернету в 1990 році. Презентація Ромкі на конференції Interop 1990 представляла підключений до Інтернету тостер Sunbeam Deluxe Automatic Radiant Control, і він виник в результаті виклик на минулорічній конференції від Дена Лінча, президента Interop, до Ромкі. Лінч пообіцяв Ромкі центральну сцену на заході, якщо він досягне успіху. Тостер був підключений за допомогою протоколу TCP/IP і мав контролер простої інформаційної бази управління мережевим протоколом управління (SNMP MIB); однією з його функцій було ввімкнення та вимкнення живлення. Перше використання терміну «Інтернет речей» з'явилося набагато пізніше і широко

приписується Ештону (Ashton 2009), коли він використовував його як заголовок презентації в Procter and Gamble в 1999 році.

Зростання IoT. Швидко зростає кількість пристроїв, підключених до Інтернету. Ряд аналітиків, зокрема Cisco та Ericcson (Дейв Еванс та Ганс Вестбург, відповідно), передбачали, що до 2020 року до Інтернету буде підключено 50 мільярдів пристроїв. Звичайно, ці оцінки важко стверджувати з упевненістю, і обидва тепер переглянули свої оцінки вниз. Еванс, який зараз працює в Stringify, прогнозує 30 мільйонів, за якими Еріксон оцінює 28 мільярдів до 2021 року. Однією з причин, через яку важко передбачити зростання, є те, що сьогодні немає навіть невідповідних цифр щодо кількості пристроїв, підключених до Інтернету. Мало того, що є суттєва різниця в цифрах із використанням тих самих визначень, але питання, що стосується різних інтерпретацій IoT, також має вплив. Деякі цифри чітко вказують на різницю між пристроями «машина-машина» (M2M) та пристроями IoT, такими як GSMA, аналіз яких M2M фокусується на стільниковому підключенні M2M і виключає обчислювальні пристрої в побутовій електроніці, такі як смартфони, електронні читачі, планшети, а також інші типи технологій з'єднання M2M, які підтримують ширший всесвіт Інтернету речей (IoT). У звіті Machine Research за 2015 рік передбачається, що загальна кількість M2M-з'єднань зросте з 5 мільярдів у 2014 році до 27 мільярдів у 2024 році. Nordrum (2016) зауважив, що в 2016 році Гартнер підрахував, що було 6,4 млрд. пристроїв (без смартфонів, планшетів і комп'ютерів), міжнародна корпорація даних оцінила 9 млрд. (з тими ж винятками), а IHS оцінила 17,6 млрд. (Включаючи смартфони, планшети та комп'ютери). Подібне дослідження Juniper Research підрахувало, що налічується 16 мільярдів пристроїв.

Незважаючи на відсутність узгоджених показників кількості підключених пристроїв IoT, видно, що кількість пристроїв величезна, і зростання було, і, як прогнозується, швидким.

Визначення IoT. Пишучи про своє перше використання терміна IoT, Ештон зауважив, що термін «все ще часто неправильно розуміють». Дійсно, сьогодні існує багато визначень та інтерпретацій IoT (Atzori, Iera та Morabito 2010; Bandyopadhyay and Sen 2011; Malina et al. 2016). Цього можна було очікувати, якщо брати до уваги широку громадськість або дослідників, які нечітко цікавляться цією галуззю, але більш дивно, коли більша кількість дослідників-спеціалістів різняться у визначенні. Наприклад, IEEE у своєму Спеціальному звіті: IoT (IEEE 2014) описує IoT як «мережу елементів – кожен вбудований датчиками – які підключені до Інтернету». З іншого боку, інша серпнева експертна організація,

Інженерна робоча група (IETF), заявляє, що «у баченні IoT» речі «дуже різноманітні, такі як комп'ютери, датчики, люди, пускачі, холодильники, телевізори, транспортні засоби , мобільні телефони, одяг, їжа, ліки, книги тощо». Після семінару-практикуму в 2008 році Генеральний директор Інформаційного суспільства та ЗМІ Європейської Комісії (DG INFSO) та Європейська технологічна платформа з інтеграції розумних систем заявили, що «річ» – це «об'єкт, який неможливо точно визначити» (INFSO 2008). Розглянувши низку проектів, що стосуються IoT, Стратегічна програма досліджень Кластеру європейських дослідницьких проектів (CERP) щодо IoT (Vermesan et al. 2011) дала власне визначення IoT. Це також сприймається як наявність недоліків (Uckelmann, Harrison, and Michahelles 2011), оскільки у визначенні використовувались компоненти, згадані раніше стосовно інших бачень, таких як загальнодоступні або всюдисущі обчислення, і це ускладнило відрізнити від них концепції. IoT можна розглядати як пов'язаний із низкою різних технологій, бачень та напрямків досліджень та походить від них. Станкович (2014) визнав, що дедалі частіше збігаються принципи та питання досліджень та злиття принципів та дослідницьких питань у п'яти різних дослідницьких спільнотах: IoT, мобільні обчислення, всепроникні обчислення, бездротові сенсорні мережі та кіберфізичні системи. Atzori, Iera та Morabito (2010) вважає, що IoT є зближенням трьох ключових бачень: орієнтованих на речі (наприклад, RFID, NFC, бездротові датчики), орієнтованих на Інтернет (наприклад, IP для розумних об'єктів) та орієнтована на «семантику» (наприклад, міркування над даними).

Хоча, враховуючи його еволюцію, очевидно, що IoT об'єднує різноманітні ключові сфери, що ускладнює проблему визначення та розрізнення IoT. Беручи до уваги тісний взаємозв'язок з іншими баченнями та досягненнями, а також відсутність загального розуміння визначення та розміру IoT, а також того, що таке «речі», не дивно, що в межах безпеки існують проблеми у сфері безпеки, конфіденційності та політики IoT. Для цілей цієї статті ми використовуватимемо інтерпретацію «речей», запропоновану IETF.

Зв'язок з M2M та Інтернетом усього. Хоча комунікація M2M в даний час є загальновживаним терміном, особливо з огляду на дискусію, що стосується Четвертої промислової революції та промислового IoT, вона має довшу історію, ніж ця. Основні рішення з управління парком та рішення наглядового контролю та збору даних (SCADA) протягом декількох десятиліть спиралися на комунікації M2M (Morrish 2014), і навіть до цього використання засобів зв'язку M2M дозволяло використовувати банкомати та системи продажів.

M2M передбачає прямий зв'язок між пристроями без участі людини. Цей зв'язок може здійснюватися через будь-який канал, провідний чи бездротовий, і кількість технологій, стандартів та протоколів зв'язку велика і зростає. Зв'язок може відбуватися через мережу, включаючи стільникові мережі (GSM, 3G, 4G), або безпосередньо між пристроями (не проходячи через базову станцію, посередника або точку доступу) способом «точка-точка», кожен з яких має різну поверхню атаки. Деякі з ключових комунікаційних технологій включають Wi-Fi, RFID, виділену комунікацію короткого радіусу дії (DSRC), Bluetooth, Bluetooth Low Energy (нещодавно іменований Bluetooth Smart), NFC та Zigbee. Ці технології різняться за частотою, діапазоном та охопленням і визначаються різними стандартами, як представлено в таблиці 1.2.

На додаток до цих різноманітних комунікаційних технологій існують спеціальні стандарти, такі як стандарт Meter-Bus, розроблений для дистанційного зчитування лічильників газу та електроенергії (EN 13757-x). В рамках розумного домашнього середовища ISO / IEC розробили ISO/IEC 14543-3 (Домашні електронні системи), а CENELEC (Європейський комітет з електротехнічної стандартизації) розробив EN 50090-x (Електронні системи для дому та будівель).

Слід зазначити, що існує різноманітна мережа описів невідомого X: дослідження ABI (ABI 2017) розглядає IoT як паралельний розвиток, наприклад, до Інтернету людей та Інтернету цифрових пристроїв. Буксманн та інші обговорити розвиток Інтернету послуг (Buxmann, Hess та Ruggaber 2011), в той час як АББ розробляє продукти та послуги для Інтернету речей, послуг та людей. Четверта промислова революція розробляється в рамках Індустріального IoT (Sadeghi, Wachsmann та Waidner 2015), порядок денний пов'язаних автомобілів перетворюється на Інтернет транспортних засобів (Gerla et al. 2014), і є ще більш незрозумілі події, такі як Інтернет речей, пов'язаних зі здоров'ям тварин (Smith et al. 2015).

Нещодавно Cisco та Qualcomm виступили за використання терміну «Інтернет усього» (IoE). Хоча деякі стверджують, що цей термін, можливо, був розроблений компанією Cisco як маркетинговий трюк, безумовно, є певна користь у визначенні системи, яка виходить за рамки багатьох типових застосувань IoT, особливо з огляду на її розвиток поза середовищем M2M. Оскільки M2M можна вважати підмножиною IoT, IoE можна вважати надмножиною IoT.

Концепція IoE об'єднує чотири ключові елементи: людей, процес, речі та дані. Тут речами є фізичні датчики, пристрої, виконавчі механізми та інші предмети, що генерують дані або отримують інформацію з інших джерел.

Таблиця 1.2

Комунікаційні технології, що використовуються в M2M та IoT системах

Технологія	Стандарт	Частота	Відстань	Швидкість	Коментарі
WiFi	IEEE 802.11	2,4/5 ГГц	50 м	500 Мбіт/с	Високе енергоспоживання
ZigBee	IEEE 802.15.4	2,4 ГГц	100 м	250 кбіт/с	Висока безпека
Z-Wave	ZAD 12837	900 MHz ISM	50 м	40 кбіт/с	Домашні системи
Sigfox	Sigfox	900 MHz ISM	10 км	1 кбіт/с	Низьке енергоспоживання
Neul	Neul	458 MHz	15 км	100 кбіт/с	Дешевий IoT
LoRaWAN	LoRaWAN	Промисловий діапазон		50 кбіт/с	Батарейне живлення
RFID	ISO/IEC 18000	НЧ та промисловий діапазони	<2 м	40 кбіт/с	
NFC	ISO/IEC 18092	13,56 МГц	<20 см	424 кбіт/с	
GSM/3G/4G	GSM, UMTS/HSPA, LTE	900/1800/1900/2100 МГц	50 км	10 Мбіт/с	Високе енергоспоживання
Bluetooth LE	IEEE 802.1	2,4 ГГц	50 м	1 Мбіт/с	Низьке енергоспоживання
6LoWPAN	RFC6282	Промисловий діапазон	невідомо	невідомо	
HomePlug	IEEE 1901	<100 МГц	<100 м	10-500 Мбіт/с	Розумна мережа
Thread	Based on IEEE 802.15.4	2,4 ГГц	<100 м	250 кбіт/с	До 250 пристроїв
DSRC	IEEE 802.11p	5 ГГц промислова частота	300 м	27 Мбіт/с	Зв'язок автомобілів
WiMax	IEEE 802.16	2,3, 2,5, 3,5 ГГц	10 км	10 Мбіт/с	

Замість того, щоб бути обмеженими для людини, ми можемо розглянути створені людиною та пов'язані з ними системи, такі як соціальні мережі, а також програми охорони здоров'я, добробуту та фітнесу. Дані аналізуються та обробляються для створення корисної інформації для розумних рішень та для управління механізмами. Ця концепція IoE дозволить не тільки дослідити IoT як систему, що включає машини та людей, але також об'єднає послуги, контекст, середовища та інтелект – дані та процес (Bojanova, Hurlburt, and Voas 2014). У контексті визначення IETF IoT це бачення IoE може бути значно меншим, ніж фундаментальним зрушенням.

Підводячи підсумок, IoT розвинувся, використовуючи широкий спектр основних технологій з ряду ключових бачень. Він еволюціонував завдяки розвитку окремих, часто різнорідних громад, кожна з яких має дещо інші загальні цілі. Крім того, ці розробки були зроблені в різних областях застосування, часто з використанням специфічних та власних стандартів. Цей дифузний характер розвитку призвів до неминучої відсутності гармонізації та спільного бачення, перешкоджаючи стандартизації та ефективному регулюванню. Саме ця відсутність стандартизації та регулювання спричинила багато існуючих проблем безпеки та конфіденційності в Інтернеті речей, і залишила техніків та користувачів без необхідної інформації та контролю щодо обслуговування, оновлення та вирішення проблем, що виникають із пристроями та послугами. Відсутність узгодженості, нагляду, розуміння та протоколів означає, що аналіз ризиків для безпеки, оцінка ризиків та реалізація контрзаходів є набагато складнішими завданнями, ніж при більш спрямованому та скоординованому шляху розвитку. Характер зростання, як швидкий, так і значний, означав, що вплив цих проблем є значним і вимагає негайного відшкодування.

У [4] представлено обговорення проблем безпеки та конфіденційності в Інтернеті речей, проілюстрованих у ряді ключових програм. Спочатку в статті представлений огляд широко розповсюджених програм IoT та різних класифікацій програм, що зустрічаються в літературі. У ній викладено ряд конкретних областей застосування, перш ніж представити дискусію щодо загальних питань безпеки та конфіденційності в Інтернеті речей. Потім обговорюється вплив IoT на проблеми безпеки та конфіденційності, перш ніж будуть зроблені остаточні висновки та рекомендації у ключових сферах.

Застосування IoT. IoT робить значний вплив у низці доменів, і ряд дослідників надали розуміння та аналіз його програм. Представляючи програми IoT, дослідники мають власну класифікацію доменів та

програм. Кожна таксономія має свої достоїнства і залежить не тільки від мети, яку потрібно досягти, але також від визначення та контексту IoT, що розглядається. Деякі дані представлені в Таблиці 1.3 (додаткова інформація про програми IoT).

Таблиця 1.3

Деякі галузі (домени) IoT та ключові програми, згадані в літературі

Домен	Ключові програми
Транспортування та логістика	Логістика; допоміжне керування автомобілем; мобільні квитки; моніторинг навколишнього середовища; доповнені карти
Піклування про здоров'я	Відстеження охорони здоров'я; ідентифікація та автентифікація; збирання даних; зондування
Розумне середовище (будинок, офіс, завод)	Комфортні будинки та офіси; Промислові заводи; Розумний музей та тренажерний зал
Особисті та соціальні	Соціальні мережі; історичні запити; втрати; крадіжки.
Футуристичне	Таксі-робот; міська інформаційна модель; покращена ігрова кімната.
Промисловість	Управління поставками; транспортування та логістика; аерокосмічна; авіація; автомобільна Телекомунікації; медичні технології;
Суспільство	охорона здоров'я; розумна будівля; будинок та офіс; ЗМІ; розваги; придбання квитків
Навколишнє середовище	Сільське господарство та селекція; переробка; сповіщення про лихо; екологічний моніторинг.
Розумна інфраструктура	Розумні мережі; розумні будинки та будівництво; розумна якість повітря; Інтелектуальна система руху; розумне паркування; поводження з відходами.
Ланцюг поставок та логістика	Відстеження продукції (датчики RFID); зменшення підробок; простежуваність продукту.
Побутова автоматизація	Споживання енергії та води; прилади дистанційного управління; системи виявлення вторгнень; збереження мистецтва та товарів.
Розумне сільське господарство	Підвищення якості вина; зелені будиночки; поля для гольфу; мережа метеостанцій; компост; гідропоніка.
Розумна вода	Портативний моніторинг води; виявлення витоків хімічних речовин у річках; дистанційне вимірювання басейну.

Домени додатків були представлені як промисловістю, так і науковими колами. Наприклад, у галузевій брошурі Libelium (2015) перераховано 61 програму для IoT у ряді доменів з використанням різних сенсорних плат. Наукові зусилля включають Atzori, Iera та Morabito (2010), які класифікують заявки на чотири короткострокові категорії (транспорт та логістика; охорона здоров'я; розумне середовище – будинок, офіс, завод; особисті та соціальні) та довгострокову футуристичну категорію. У Miorandi et al. (2012) автори використовують шість категорій, зберігаючи сферу охорони здоров'я, одночасно змінюючи інші. Однак найголовніше, що вони не враховують особисту та соціальну сферу, а замість цього вводять категорію безпеки та спостереження. Whitmore, Agarwal та Xu 2015 використовують модифіковану класифікацію, засновану на розгляді оновленого огляду літератури, що найбільш суттєво спирається на роботу Atzori, Iera та Morabito (2010) та Miorandi et al. (2012). Ця класифікація відмовляється від часового футуристичного погляду та реорганізує сфери транспорту та логістики та інтелектуального середовища, визнаючи значну роль IoT у ланцюгах поставок та його зв'язку з галуззю логістики, таким чином розробляючи категорію спеціально для ланцюгів поставок та логістики. Далі представлена нова категорія, інтелектуальна інфраструктура, яка розширює область розумних середовищ Atzori та вводить аспекти інфраструктури транспорту. Занелла та ін. (2014) зосереджують увагу на розумному місті, тоді як Da Xu, He та Li (2014) концентруються на галузевих додатках IoT, і включають розгляд нішевого випадку IoT, що застосовується до пожежогасіння. Автори цієї останньої статті поширюють свою роботу на більш широкі програми (Li, Da Xu та Zhao 2015), поєднуючи її з концепціями Atzori та Miorandi. Перера та ін. (2014) та Bandyopadhyay and Sen (2011) в значній мірі спираються на звіт CERP про IoT (Vermesan et al. 2011). Цей звіт визначає три основні сфери застосування для IoT: промисловість, навколишнє середовище та суспільство. Однак у звіті виявляється, що важко виділити будь-який із цих доменів, і, скоріше, програми та послуги застосовуються на внутрішньому та міждоменному рівні. Натомість ми повинні розглянути додатки (які підтримують один або декілька з вищезазначених доменів) та послуги, які забезпечують певну функціональність або потребують на внутрішньому або міждоменному рівні. Отже, якщо організації бажають врахувати ризик кібербезпеки, робити це на рівні домену буде оманливим, хоча, мабуть, інтуїтивно зрозумілим. Той факт, що існує низка способів розгляду доменів та додатків, повинен говорити нам про те, що такий спосіб думати про ризик є безрезультатним. Хоча моделювання загрози та оцінка ризиків у різних доменах можуть мати подібні теми, вони, ймовірно, матимуть кардинально різні ризики. Таким чином, замість того, щоб

розглядати ризик кібербезпеки на рівні домену, нам слід вивчити низку програм IoT, які перебувають на міждоменному рівні. Зараз ми обговорюємо невеликий вибір програм, які несуть значний ризик кібербезпеки, що представляє великий вплив та/або ймовірність нападу.

Підключені та автономні транспортні засоби. Застосування датчиків в автомобільному секторі було однією з найбільших областей зростання (Meola 2016). У транспортних засобах є значна кількість датчиків, що використовуються для всього, від роботи двигуна до контролю системи, контролю викидів та гальм. Приклади включають системи контролю тиску в шинах з підтримкою Bluetooth, положення кривошипа, положення кулачка, абсолютний тиск у колекторі та положення дросельної заслінки. Сенсори також вбудовуються, щоб утворити невід'ємну частину транспортної інфраструктури, і у Великобританію було вкладено значні інвестиції, наприклад, у впровадженні Програми розумних автомагістралей Англії на шосе (Phull 2012). Інші ініціативи включають розвиток інфраструктури та комунікацій у міському середовищі. UKCITE (www.ukcite.co.uk) – це проект у Великобританії, що фінансується як Центром підключених та автономних транспортних засобів, так і Innovate UK (частина інвестиційної програми у 100 мільйонів фунтів стерлінгів на дослідження та розробки), що передбачає оснащення понад 40 миль міської дороги, подвійні проїзні та автостради з технологією зв'язку. Використання зв'язку «Автомобіль до інфраструктури» (V2I) дозволяє покращити транспортний потік, особливо в міському та приміському середовищі (Faezipour et al. 2012). Зв'язок між транспортними засобами, так званий зв'язок V2V, за допомогою таких технологій, як DSRC, довгострокова еволюція для транспортних засобів та Visible Light Communications, дозволяють розміщувати автомобілі взводом з метою зменшення споживання енергії та попередження про інциденти. Розгортання таких інтелектуальних транспортних систем, що використовують технологію Edge і Cloud, може допомогти в управлінні аваріями, трафіку на основі місцезнаходження та сповіщеннях про погоду, тим самим підтримуючи допоміжне керування (Atzori, Iera та Morabito 2010).

Здоров'я, добробут та відпочинок. Використання датчиків є невід'ємною частиною нових медичних та медичних технологій. IoT може бути інтегрований у численні медичні послуги та додатки (Dohr et al. 2010; Bui and Zorzi 2011; Islam et al. 2015). Послуги охорони здоров'я, які будуть найбільш корисними, включають проживання за допомогою навколишнього середовища (значна сфера застосування, яка передбачає використання розумних будинків, щоб дозволити спостереження за

пацієнтами та догляд у незалежних умовах); Інтернет мобільного здоров'я (інтеграція медичних датчиків у мобільні технології); семантичний медичний доступ (використовуючи семантику, додатки охорони здоров'я IoT можуть використовувати механізми медичних правил для аналізу великої кількості даних датчиків); та побічна реакція на ліки (шляхом маркування лікарських засобів та вивчення медичної бази даних можна уникнути будь-якої потенційної побічної реакції, такої як алергія або реакція з іншими препаратами). Програми охорони здоров'я, які вже були розроблені або мають бути розроблені, включають моніторинг артеріального тиску та діабету, моніторинг температури тіла та реабілітації, моніторинг насичення киснем та управління інвалідними візками (Stachel et al. 2013).

Індустрія 4.0. Очікується, що один із найбільших наслідків IoT у всьому світі відбудеться завдяки появі Четвертої промислової революції, в якій технології IoT повинні бути включені в кожну фазу виробничого процесу. Це передбачатиме перехід від автоматизованих до інтелектуальних виробничих процесів (Thoben, Wiesner та Wuest 2017), включаючи кіберфізичні системи, автоматизовану робототехніку, аналіз великих даних та хмарні обчислення (Федоров та ін., 2015). IoT можна використовувати протягом усього життєвого циклу розробки завдяки впровадженню інтелектуально підключених машин із попереджуючим обслуговуванням, що забезпечує розумніший процес виробництва, забезпечуваний за допомогою інтелектуальної логістики, що дозволяє швидко, гнучко та економно виготовляти. Оптимізовані методи прийняття рішень та інноваційні методи планування у поєднанні з технологією інтелектуальних мереж означатимуть максимізацію енергоефективності рослин.

Логістика. Завдяки великій кількості відправлень та збільшенню запасів технології IoT можуть динамічно підтримувати логістику, дозволяючи постачальнику послуг підвищувати операційну ефективність, одночасно збільшуючи автоматизацію та зменшуючи ручні процеси (Macaulay, Buckalew та Chung 2015) Використання IoT в логістиці може мати помітний вплив на розумне управління запасами, виявлення пошкоджень, видимість у реальному часі, точний контроль запасів, оптимальне використання активів, прогнозне обслуговування та управління вантажем (Uckelmann, Harrison, and Michahelles 2011). Застосування технології RFID до логістики (Sun 2012) дозволяє промисловості прогнозувати інформацію, визначати майбутні тенденції, оцінювати ймовірність аварії та дозволяти достроково прийняти заходи виправлення. Це може покращити здатність підприємств реагувати на ринок та підтримувати пропозицію з урахуванням ризиків.

Розумна сітка. В останні роки відбулося різке збільшення інвестицій у дослідження та розробку інтелектуальних мереж, що підштовхнуло Великобританію до лідируючих позицій у європейському впровадженні широкого спектру життєздатних рішень інтелектуальної мережі (DECC 2014). Smart Grid – це інтелектуальна енергосистема, яка включає інформацію та зв'язок із існуючими системами передачі та розподілу (Li et al. 2011). Це стало можливим завдяки використанню датчиків, цифрових лічильників та контролерів з інструментами аналізу для моніторингу та оптимізації роботи мережі, запобігання відключенню електроенергії та відновлення живлення (Li et al. 2011). Розвиток Smart Grid допоможе задовольнити вимоги розумних міст з численними інтелектуальними системами, що створюють системи управління енергією в будівлях та громадах (CEMS) (Karnouskos 2010). Сенсори IoT можуть допомогти ідентифікувати пристрої, підключені до мережі, і надсилати споживачеві інформацію про енергію в режимі реального часу.

Будинки, будівлі та офіси. Попит на розумні домашні пристрої суттєво зріс, за період з 2010 по 2016 рік, за даними IHS Markit (IHS 2016), було відвантажено понад 161 мільйон одиниць; більше половини цих пристроїв було поставлено в 2016 році, що на 64 відсотки більше порівняно з попереднім роком. Це збільшення включало придбання інтелектуальних систем управління енергією, таких як термостати Nest, рішень безпеки, таких як розумні замки в серпні, та персональних домашніх помічників, таких як Google Home, Bosch's Mykie та Amazon Alexa.

Окрім зростання кількості споживачів інтелектуальних технологій, також спостерігається різкий попит в офісному середовищі. У новому звіті Британської академії земельних та робочих технологій (British Land 2017), в якому представлено понад 1000 робітників, майже третина з яких були особами, що приймають рішення, виявлено, що 88 відсотків респондентів виявили бажання краще контролювати своє робоче середовище. Дослідження показало, що розумний офіс матиме значний вплив на ефективність діяльності компанії та навколишнє середовище, прогнозуючи зростання продуктивності праці на 37 відсотків, підвищення лояльності на 38 відсотків, а добробут та щастя покращиться більш ніж на 40 відсотків. Це зростання попиту на IoT у будинках, будинках та офісах сприятиме розвитку розумних міст (Zanella et al. 2014).

Роздрібна торгівля. Завдяки збільшеним перевагам сенсорних технологій IoT може покращити споживчий досвід у роздрібних магазинах та на підприємствах. Наприклад, моніторинг та контроль

експлуатаційних даних та продуктивності обладнання дозволять підприємствам покращувати ефективність, відстежуючи прогрес у реальному часі (Lee and Lee 2015). Датчики з часом генерують великі обсяги даних, які можна використовувати для визначення потенційних недоліків та допомагати бізнесу адаптуватися за допомогою аналізу великих даних та бізнесу. Розуміння ринкових тенденцій та запитів споживачів за допомогою розширеного аналізу ринку призведе до реактивної та ініціативної пропозиції, що може обмежити втрату ресурсів та розвиток подій, які в підсумку не зможуть знайти попит. Завдяки посиленому впровадженню IoT роздрібні торговці можуть не тільки забезпечити відповідні закупівлі та постачання, але й запропонувати споживачам різні товари, які можуть більше відповідати їхнім потребам. Наприклад, користувач може придбати якусь побутову електроніку, але можуть бути товари, які можуть запропонувати відповідну кількість сумісності, терміну служби батареї тощо як альтернативу. Це рішення може бути отримано на основі інформації, зібраної з датчиків, і може працювати приблизно так само, як коли ми вирішимо оновити наші пакети мобільних телефонів або Інтернету, отримуючи поради від постачальників щодо найбільш підходящої послуги для наших потреб. Задоволення споживачів також можна досягти за допомогою підключеної роздрібної торгівлі, а також за допомогою розпізнавання споживачів та контекстних пропозицій (Macaulay, Buckalew, and Chung 2015).

Сільське господарство. Розумні технології також розробляються в аграрному секторі. Польова інформація традиційно отримується за допомогою ручних механізмів звітування, що може призвести до неточностей у даних. Щоб максимізувати та впорядкувати виробництво сільськогосподарських товарів шляхом систематичного підвищення ефективності та зменшення ручної праці, датчики та технології IoT можуть сприяти науковому вирощуванню з підвищеною якістю (Chen and Jin 2012). Це стає можливим завдяки моніторингу параметрів навколишнього середовища, таких як тиск повітря, вологість та напрямок вітру за допомогою бездротових датчиків, які можуть допомогти вирощуванню через адаптацію сільськогосподарських потреб. Крім того, від виробничих процесів до споживання на ринку, ланцюг постачання продуктів харчування потребує підтримання відповідних методів консервації, які можна вдосконалити за допомогою сенсорних технологій та всеосяжних обчислень (Atzori, Iera та Morabito 2010). Важливість простежуваності харчових продуктів була підкреслена в огляді Еліот (Elliott 2014). IoT може відігравати значну роль у покращенні забезпечення, логістики та управління ланцюгами поставок за допомогою систем відстеження та відстеження.

Розваги та ЗМІ. Розваги та медіа також розглядаються як сектор, який може отримати вигоду від досягнень Інтернету речей (Мартін 2016), а також розробляються дослідження послуг обміну медіаконтентом через домашні мережі Інтернету речей (Hu et al. 2013). Це надає можливість як персоналізувати вміст безперешкодно, так і спростити обмін мультимедіа. Реклама може бути персоналізована для окремих громад та сімей. Також очікується, що фільтрація потенційного вмісту за віком вплине на індустрію розваг (eMarketer 2016). Інші додатки, такі як спеціальний збір новин на основі місцезнаходження користувача, також планується збільшити (Bandyopadhyay and Sen 2011). Ігрова індустрія є значним напрямком сектору розваг, і в ньому IoT може мати значний вплив. Ми вже бачили величезну популярність Pokémon Go, і поєднання IoT та систем доповненої реальності може зіграти важливу роль у розробці нових ігрових вражень.

Проблеми безпеки в IoT. По мірі того, як IoT розширюється і стає все більш вплетеним в тканину нашого повсякденного життя, а також стає все більш важливим компонентом нашої критичної національної інфраструктури, забезпечення її систем стає життєво важливим. Захист систем може базуватися на ряді принципів, від ЦРУ щодо інформаційної безпеки (конфіденційність, цілісність та доступність), до п'яти стовпів забезпечення інформації (конфіденційність, цілісність, доступність, автентичність та невідмова) і Parkerian Hexad (конфіденційність, цілісність, доступність, автентичність, володіння та корисність) (Parker 1998). Дослідницькі статті, що обговорюють міркування щодо безпеки, що стосуються кіберфізики (на відміну від інформації) та систем IoT, різняться залежно від принципів, які вони приймають. Більшість дослідників обмежують увагу правилами ЦРУ. Parkerian Hexad, хоча його спочатку пропонували як покращення для подолання обмежень ЦРУ, часто відкидають; справді, корисність Hexad залишається предметом дискусій серед фахівців з безпеки (Feruza and Kim 2007). Інші виходять за рамки цих попередніх принципів і включають надійність, безпеку, стійкість, ефективність та живучість (див., Наприклад, Sterbenz et al. 2010). Безумовно, варто розглянути всі ці компоненти безпеки, особливо в складних кіберфізичних системах, таких як IoT. Однак тут використовується три найширші категорії ЦРУ, розуміючи, що компроміси можуть бути як фізичними, так і інформаційними активами. Ми обговорюємо деякі найважливіші проблеми, висвітлюючи, які принципи знаходяться під загрозою компромісу. Однак слід визнати, що це не вичерпний перелік викликів безпеці.

Фізичні обмеження пристроїв та комунікацій. У будь-якій області застосування пристрої IoT, як правило, вбудовані в процесори з низькою потужністю та низькою площею, і визнано, що «Інтернет-протокол може і повинен застосовуватися навіть до найменших пристроїв» (Mulligan 2007). Обмеження для пристроїв IoT обмежують можливість швидкої обробки інформації – обмежений процесор, пам'ять та енергетичний бюджет. Це означає, що потрібні складні форми безпеки, які відповідають конкуруючим цілям – висока продуктивність та мінімальне споживання ресурсів. Обмеження в розмірі та потужності найбільше впливають на зусилля щодо збереження конфіденційності та цілісності в системах IoT. Наприклад, найбільший пакет фізичного рівня в IEEE 802.15.4 (нагадаємо, що Zigbee та 6LoWPAN, наприклад, обидва базуються на цьому стандарті) становить 127 байт (Montenegro et al. 2007). Враховуючи, що накладні витрати на кадр можуть становити 25 байт, максимальний розмір кадру на рівні управління доступом до медіа становить 102 байти. Для захисту конфіденційності може застосовуватися шифрування, але слід зазначити, що захист рівня зв'язку додатково зменшує цей максимальний розмір кадру. Якби використовувався AES-CCM-128 (Advanced Encryption Standard, що використовує 128 біт, працює в так званому режимі CCM, режимі роботи, призначеному для забезпечення автентифікації та конфіденційності), це зайняло б 21 байт, залишивши лише 81 байт . З іншого боку, використання AES-CCM-32 споживатиме лише 9 байт, залишаючи 93 доступними. Розробити належним чином безпечні та надійні системи є складним завданням, оскільки зв'язок між вузлами часто відбувається через «канали з втратою та низькою пропускною здатністю» (Heer et al. 2011).

Для безпеки за допомогою цифрових підписів потрібна інфраструктура відкритого ключа, і це є серйозним викликом для систем IoT. Інфраструктура відкритих ключів може захистити як від втрати конфіденційності, так і від втрати цілісності. Однак навіть процес шифрування за допомогою відкритого ключа вимагає обчислювальних ресурсів та ресурсів пам'яті, які виходять за рамки багатьох бездротових сенсорних систем, особливо коли потрібна часта передача даних (Doukas et al. 2012).

Неоднорідність, масштабність та спеціальний характер. Визнано, що високий рівень неоднорідності (Sicari et al. 2015; Misra, Maheswaran, and Hashmi 2016), що ускладнюється великим масштабом систем IoT, посилить загрози безпеці для поточний Інтернет. Роман, Наджера та Лопес (2011) зазначають, що неоднорідність має «великий вплив на протокол та послуги мережевої безпеки, які повинні бути впроваджені в IoT». Рішення безпеки повинні впоратися з об'єктами з різними

апаратними специфікаціями, а також повинні забезпечити автентифікацію та авторизацію вузлів IoT (Malina et al. 2016), а також ключову угоду (Suo et al. 2012). Неоднорідність IoT означає, що не можна вважати, що всі пристрої можуть мати повний стек протоколів.

Крім того, потенційна кількість послуг та варіантів виконання послуг, поряд з необхідністю обробки різнорідних ресурсів, вимагає управління послугами; ці виклики матимуть несприятливий вплив на безпеку систем IoT (Miorandi et al. 2012). Відсутність відкритих стандартів та використання патентованих рішень представляє значну проблему, оскільки рішення щодо безпеки повинні інтегруватися з «чорними ящиками». Дозвіл розробникам впроваджувати безпеку, засновану на їх власних стандартах, може призвести до «безпеки через невідомість» (Phillips, Karygiannis та Huhn 2005), визнаної як недосконала техніка в межах безпеки. Проблеми безпеки ще більше загострюються через те, що «перехідні та постійні випадкові відмови є звичним явищем, а відмови – це вразливості, якими можуть скористатися зловмисники» (Stankovic 2014), і що спеціальна природа IoT вимагає адаптації існуючих методів (Sicari та ін. 2015). Очевидно, що зі збільшенням кількості пристроїв, підключених до Інтернету, зростають і проблеми безпеки та конфіденційності (Cha et al. 2009).

Багато компонентів IoT, особливо у сферах охорони здоров'я, транспорту та логістики, також є мобільними. Це представляє виклик у забезпеченні адаптації рішень безпеки до мобільного середовища, взаємодії з багатьма різними компонентами та системами, кожна з яких потенційно пропонує різні налаштування, протоколи та стандарти.

Автентифікація та управління ідентифікацією. Управління особистими даними стосується унікальної ідентифікації об'єктів, а автентифікація перевіряє відносини ідентичності між двома сторонами (Mahalle et al. 2010). У звіті CERP (Vermesan et al. 2011) визнається, що необхідні подальші дослідження щодо «розробки, зближення та взаємодії технологій ідентифікації та автентифікації, які можуть діяти у глобальному масштабі».

Аутентифікація в IoT є критично важливою, оскільки без відповідної автентифікації конфіденційність, цілісність та доступність систем можуть бути порушені. Це пов'язано з тим, що якщо суперник може автентифікуватися як законний користувач, він матиме доступ до будь-яких даних, які має користувач, і може бачити (порушує конфіденційність), змінювати (порушуючи цілісність), а також видаляти або обмежувати доступність (порушуючи доступність) у так само, як і користувач може.

Автентифікація та ідентифікація користувачів в Інтернеті речей залишається важливою проблемою. В даний час пари імені користувача / пароля є найпоширенішою формою автентифікації та ідентифікації користувачів в електронних системах, хоча можуть використовуватися інші форми, такі як спільні ключі, цифрові сертифікати або біометричні дані (Gessner et al. 2012). Однак бачення IoT як повсюдного знищить багато інтерфейсів фізичної взаємодії, через які передаються імена користувачів та паролі.

У традиційних електронних середовищах можливість скористатися перевагами механізмів єдиного входу (SSO) може бути корисною, дозволяючи користувачам лише раз пройти автентифікацію для взаємодії з різними службами. Такі системи, як Shibboleth OpenID та OAuth2, не були розроблені для виконання систем IoT, і хоча проводиться робота з адаптації OAuth2, вона поки що не може забезпечити широко розповсюджену систему єдиного входу в середовищах IoT. Громадяни, що перебувають у середовищі IoT, можуть побажати вибрати свого постачальника ідентифікаційних даних, і це складно використовувати сучасні протоколи.

Крім того, мобільність, конфіденційність та анонімність вимагають подальшого аналізу та досліджень (Riahi et al. 2013). Ці системи IoT, що мають мобільні послуги, матимуть користувачів, які проходять через різні архітектури та інфраструктури, що належать різним провайдерам. Управління особистістю користувачів у таких мобільних, неоднорідних середовищах, що мають багато власності, може бути складним завданням. Поки конфіденційність у IoT обговорюється в наступному розділі, проблема анонімності в IoT представляє особливу проблему, особливо в мобільних середовищах. Хоча може існувати прагнення до анонімності, користувачі також хочуть хорошого рівня обслуговування, і це часто вимагає розуміння

«Кому» надається послуга. Крім того, якщо існує потреба у стійких послугах, то підзвітність бажана. Очевидно, що в справді анонімній системі підзвітності важко досягти. Псевдонімність може забезпечити баланс між анонімністю та підзвітністю. У системах псевдонімів дії людини пов'язані з випадковим ідентифікатором, а не з ідентичністю. Псевдонім може містити постійний ідентифікатор, щоб гарантувати, що послуга може бути запропонована від початку до завершення. Для того, щоб бути ефективними в системах IoT, залишається проблемою для псевдонімів працювати стандартизовано в кількох доменах.

Не лише ідентифікація та автентифікація користувачів потребує розгляду. Також необхідно виявити та перевірити службу та пристрої в системах IoT. Виконати надійну автентифікацію пристроїв у IoT може

бути складно, «через природу пристрою або контекст, в якому він використовується» (Sarma and Girão 2009). Без належних процесів автентифікації неможливо забезпечити дані, що надходять із передбачуваного пристрою, або були отримані передбачуваним пристроєм. Якщо пристрої належним чином автентифіковані, все ще існує необхідність аутентифікації служби, оскільки певні служби матимуть доступ до певних даних.

Авторизація та контроль доступу. Було визнано, що існує необхідність «здійснювати контроль доступу до [Інтернету речей] на краю мережі на пристрої або, принаймні, локальному контролеру доступу для пристрою» (Cerf 2015). Важлива роль у встановленні того, чи має користувач, після ідентифікації та перевірки, дозвіл на доступ до запитуваних ресурсів (Abomhara and Køien 2014). Контроль доступу вимагає спілкування між сутностями (часто обмеженими для сутностей програмного забезпечення, а не людей, оскільки користувачі впливають на систему через сутності програмного забезпечення, які вони контролюють), щоб вимагати та надавати доступ. Існують різні моделі контролю доступу, такі як дискреційний контроль доступу (ЦАП – де адміністратор визначає, хто може отримати доступ до ресурсів); контроль доступу на основі ролей (RBAC – надання доступу на основі ролі, яку виконує запитувач); та контроль доступу на основі атрибутів (ABAC – де права надаються через політики, що оцінюють атрибути користувача, запитуваного ресурсу та середовища, з якого зроблено запит).

Ефективний контроль доступу в контексті IoT є складним завданням. Хоча бажано використовувати модель контролю доступу, яка усуває розсуд, використання RBAC та ABAC, як відомо, є складним завданням для малопотужних пристроїв IoT. Крім того, RBAC вимагає визначення ролей. У багатьох системах IoT існує ймовірність того, що кількість ролей буде швидко зростати, і, отже, обробка всіх цих ролей, особливо під час оновлення системи, стає важкою, якщо передбачається точний контроль доступу. ABAC стикається з подібними проблемами, особливо в децентралізованих архітектурах. Ні ABAC, ні RBAC «не забезпечують масштабованих, керованих, ефективних та дієвих механізмів ... і [тому] не здатні ефективно підтримувати динамічність та масштабні потреби контекстів IoT» (Gusmeroli, Piccione та Rotondi 2013). RBAC, ABAC і DAC – це всі моделі списку контролю доступу (ACL), і альтернативним підходом є використання підходів, заснованих на можливостях. Ці методи включають запитувача, який має посилання або можливість, що дозволяє отримати доступ до послуги. Для цього потрібне довідкове повідомлення, яке можна повідомити, відкликати, просити, і яке можна вважати аналогічним ключу від сейфу. Ці методи намагаються подолати деякі

обмеження моделей ACL, але вони не можуть «адаптувати доступ на основі різних атрибутів або обмежень» (Ferraiolo, Cugini та Kuhn 1995). Методи, що базуються на можливостях, включають автентифікацію особи та контроль доступу на основі можливостей (IACAC) (Mahalle et al. 2013) та контроль доступу на основі можливостей (CapBAC) (див. Gusmeroli, Piccione та Rotondi 2013).

Впровадження, оновлення, відповідальність та підзвітність. Життєво важливо, хоча це часто ігнорується під час обговорення, що впровадження та оновлення засобів захисту повинні бути керованими та дешевими. Системи IoT можуть бути географічно віддаленими і включати датчики та виконавчі механізми в екстремальних та складних умовах. Для захисту кібербезпеки системи життєво важливо усунути будь-які вразливі місця одразу після їх виявлення. Таким чином, існує необхідність віддаленого доступу, щоб дозволити ці оновлення системи. Найновіші програмні виправлення можна встановлювати динамічно, а процесом керувати за допомогою хмарних платформ; однак розробка безпечного механізму для динамічної установки є складним завданням (Maglaras et al. 2016). Слід також визнати, що оновлення можуть змінювати функціональність пристроїв, і ці зміни не завжди можуть узгоджуватися з очікуваннями користувачів (Rose, Eldridge та Chapin 2015). З цієї причини, у випадках, коли користувач несе відповідальність або контроль за застосуванням виправлення, він може прийняти рішення проти оновлення, якщо вважає, що ризик компромісу перевищує негативний вплив на функціональність (Cavusoglu, Cavusoglu та Zhang 2008). Атака Dyn у 2016 році була ілюстрацією значного впливу, який може мати ботнет, подібний неоновленим принтерам, IP-камерам, житловим шлюзам та кібер няням, при проведенні розподіленої атаки відмови в обслуговуванні. Це призводить до ще однієї значної проблеми щодо відповідальності, обов'язковості та підзвітності в Інтернеті речей. Оскільки IoT включає різні пристрої, комунікації, інфраструктуру та послуги під різним контролем та правом власності, визначення відповідальності та підзвітності залишається проблемою. Хоча юридична відповідальність може бути покладена на одну організацію, вплив, здавалося б, нешкідливого нападу на один компонент може спричинити катастрофічну, безповоротну шкоду іншій. Наприклад, якщо послуга скомпрометована через проблему в пристрої або сторонній архітектурі, наслідки з точки зору реакції клієнта можуть не вплинути на виробника пристрою або власника архітектури, а швидше на оператора послуги. Можливість таких випадків може призвести до того, що деякі сторони будуть менш стурбовані кіберфізичною безпекою, ніж мали б бути. Ситуація ще складніша, враховуючи дуже

складну поверхню атаки. Одна незначна вразливість в одному пристрої чи службі може бути використана разом з іншими, здавалося б, нешкідливими вразливими місцями в інших місцях системи, що контролюються, належать або постачаються різними сторонами. Якщо це призводить до серйозного компромісу, рівень або відповідальність кожної із сторін може бути не відразу чітким. Це ускладнює обґрунтування інвестицій у безпеку.

Проблеми безпеки в підключених та автономних транспортних засобах. Зона підключених та автономних транспортних засобів (CAV) є складною і включає безліч різних датчиків, виконавчих механізмів, інфраструктури, протоколів зв'язку та послуг. Ці послуги варіюються від невеликих простих служб, що працюють лише на декількох компонентах, до глобальних послуг, що включають значні частини критичної національної інфраструктури. Ця робота не може охопити всі типи системи та потенційні та реалізовані атаки. Однак можна виділити деякі найбільш значущі атаки.

Сучасні транспортні засоби мають від 70 до 100 вбудованих електронних блоків управління (ЕБУ) для таких програм, як гальмування, рульове управління, трансмісія, підвіска та управління двигуном. Датчики, що подають інформацію до цих ЕБУ, включають Інформаційно-розважальну систему, Системи контролю тиску в шинах, Камеру, LIDAR, РАДАР, датчики гальма та двигуна. Зв'язок з ЕБУ здійснюється через цілий ряд мереж, включаючи CAN (Controller Area Networks), FlexRay, MOST (Media Oriented System Transport) та LIN (Local Interconnect Network). Різні виробники використовують різні мережі, але сучасні транспортні засоби матимуть ряд таких типів мереж. Однак ці протоколи були розроблені з пріоритетом ефективності та безпеки, а не безпеки. Checkoway та ін. (2011) та Кошер та ін. (2010) використовували різні бортові та віддалені транспортні вразливості фізичні пристрої кінцевих точок, такі як бортові діагностичні блоки (OBD), та зовнішні засоби зв'язку, такі як DSRC та Bluetooth. Більш розголошеною була робота Міллера та Валлесека у 2015 році, в якій вони використовували дистанційне виконання для використання вразливості (в поєднанні зі слабкістю в віддаленому доступі Sprint UConnect®) у Jeep Cherokee (Mansfield-Devine 2016). Вони змогли керувати транспортним засобом, коли він рухався.

Незважаючи на те, що в даний час ймовірність кібератаки на підключений транспортний засіб вважається низькою, зростаюча важливість цих транспортних засобів та розвиток таких технологій, як вимога-програмне забезпечення, роблять це значним ризиком для цілісності та доступності підключених та автономних транспортні системи. Окрім

фінансової мотивації, ми, швидше за все, бачимо спроби компрометувати ці системи терористами, національними державами та хактивістами.

Багато додатків у CAV включають поєднання особистих та транспортних даних (які можуть бути пов'язані з окремими особами), які надсилаються зовні. Конфіденційність та приватність цього типу даних може бути порушена різними способами, в тому числі завдяки використанню «нюхових станцій». Також можна здійснити атаку людини посеред бездротового зв'язку, що заходить у транспортний засіб, тим самим порушуючи цілісність цих даних. Така атака людина в середині була основою віддаленої експлуатації джипу Міллером і Валасеком.

Оскільки підключені транспортні засоби взаємодіють та стають залежними від таких інфраструктур, як Cloud і Edge-cloud, ризик та вплив атак на доступність систем зростатимуть.

Проблеми безпеки в галузі охорони здоров'я, добробуту та відпочинку. Останнім часом відбувається все більше нападів, коли жертвами стали лікарні. Існує незліченна кількість потенційних та фактичних атак на окремі підключені пристрої, включаючи системи доставки ліків, електронні імплантанти, інсулінові помпи та кардіостимулятори. Однак останніми роками було виявлено напади безпрецедентні за своїми масштабами та поверхнею. Зокрема, атака MEDJACK (Storm 2015), вперше виявлена Trend Micro, вплинула на аналізатори газів крові, апарат комп'ютеризованої томографії, системи магнітно-резонансної томографії та рентгенівські апарати. Були здійснені атаки на цільові протоколи зв'язку, а також пристрої. Вади безпеки були виявлені в протоколах власного зв'язку десяти імплантованих серцевих дефібриляторів (МКБ) (Марін та ін., 2016). Ці медичні системи, очевидно, становлять ризик для кожної частини тріади ЦРУ. Окрім очевидних проблем порушення доступності та порушення цілісності, існують також питання конфіденційності. Медичні дані можна використовувати для крадіжки особистих даних або шахрайства, а також для виявлення рецептів ліків, що дозволяє хакерам замовляти ліки через Інтернет. Хакери можуть також розглянути питання вимагання та шантажу людей з певними захворюваннями, які вони не хотіли б розголошувати. Подібні атаки на конфіденційність, цілісність та доступність благополуччя з підтримкою IoT, такі як фітнес-трекери, також існують, хоча вплив порушень на доступність та потенційно цілісність є менш серйозним. Це не стосується конфіденційності інформації.

Проблеми безпеки в Індустрії 4.0. Індустрія 4.0 була оголошена як трансформаційний крок, який об'єднує дані, зв'язок та автономію для

створення Четвертої промислової революції. Однак існує низка суттєвих загроз для цих кіберфізичних систем.

Про значні кіберофізичні атаки повідомлялося протягом ряду років, і, ймовірно, існує значна кількість атак, про які не повідомляється або навіть не виявляються. Прикладами можна назвати атаку Maroochy Water Services в Австралії в 2000 році, коли каналізаційна система зіткнулася з низкою несправностей, коли насоси не працювали в той час, коли вони мали бути, а сигналізація була відключена. Це ще більше погіршилося втратою зв'язку з центрального комп'ютера з різними насосними станціями. Подібним чином Stuxnet мав швидкий і значний вплив на іранську ядерну промисловість. Більш нещодавні напади включають атаку 2014 року на німецький металургійний комбінат та збої в роботі української енергетичної мережі.

Інші атаки на конфіденційність інформації включають витік інтелектуальних даних, що може призвести до втрати конкурентних переваг на ринку. Крім того, це також забезпечить конкурентів спроможністю підірвати інновації, які ще мають бути виготовлені.

Проблеми безпеки в логістиці. IoT, здається, пропонує значну ефективність та ділові можливості в логістиці. Існують різні сценарії застосування, що неминуче створює велику поверхню атаки. Однією з визнаних атак є маніпулювання вбудованими даними, або шляхом зловмисної заміни тегів, або шляхом модифікації інформації про теги (Misra, Maheswaran та Hashmi 2016). Хоча логістика часто розглядається як частина дорожньої мережі, слід визнати, що логістика також включає залізничний, повітряний та морський транспорт. Особлива вразливість стосується модифікації деталей судна, включаючи положення, курс, вантаж, країну, під якою позначається, швидкість, ім'я та статус MMSI (Mobile Maritime Service Identity) (Balduzzi, Pasta та Wilhoit 2014). Для подальшого посилення атаки може бути використано створення підроблених суден з однаковими деталями існуючого судна, наприклад, якщо біля берегів США з'явиться іранське судно з ядерним вантажем. Це загрожує конфіденційності та цілісності системи.

Проблеми безпеки в інтелектуальній мережі. Напади на критичну національну енергетичну інфраструктуру, такі як повідомлення про напад Китаю та Росії на Сполучені Штати (див. Місра, Махешваран та Хашмі, 2016), та напади на Україну широко обговорювались у довідках, наукових роботах (див. et al. 2017), наприклад, і ширша преса. Ці атаки переважно (хоча це можна стверджувати не виключно) намагаються

порушити доступність цих кіберфізичних систем. Однак існує ряд інших атак, відомих в рамках технологій Smart Grid.

Атаки не завжди відбуваються на рівні національної інфраструктури, але можуть відбуватися далі в архітектурі. CEMS є більш локалізованими і використовуються для визначення та збалансування потреб громади в електроенергії, включаючи визначення розміру генераторів та потужності ліній електропередачі, які будуть використовуватися протягом коротких періодів часу для задоволення попиту. Вже було показано, що CEMS є вразливим до атак відмови в обслуговуванні, а також до підроблених повідомлень, що порушує доступність та цілісність.

Далі в архітектурі спостерігається значне зростання розміщення розумних лічильників. Дані британського уряду заявляють, що до вересня 2016 року у Великобританії було встановлено понад 500 000 розумних лічильників. Однак дані, передані через Інтернет за допомогою розумних лічильників, виявились неподписаними та незашифрованими (Greveler et al. 2012), що порушує конфіденційність системи.

Проблеми безпеки в будинках, будинках та офісах. Існує широкий спектр пристроїв для розумного будинку, що обіцяють інтелектуальну ефективність використання ресурсів за допомогою віддаленого та миттєвого доступу та управління. Хоча такі пристрої та послуги пропонують економічні та функціональні переваги, вони збільшують ризики безпеки. Основними ризиками, які представляють такі пристрої, є конфіденційність та конфіденційність. Деякі питання, наприклад, як споживання енергії може зробити висновки щодо профілювання, були обговорені раніше. Так само, були використані підключені домашні пристрої для атаки Dyn. Типи пристроїв, які були скомпрометовані, вже включають камери, принтери, дверні дзвінки, домашні ваги, а нещодавно, зокрема у Великобританії, домашні маршрутизатори та багато інших. Хоча можливості цих пристроїв є малими, коли потужність усіх пристроїв поєднується в бот-мережу, глобальний вплив може бути значним.

Окрім атаки на пристрої в розумних будинках та офісах, хакери націляться на системи автоматизації та управління будівлями. Ймовірно, найзначнішою атакою, що використовує доступ до підключених до Інтернету систем управління будівлею, була атака на Target. Атака виникла внаслідок компрометації компанії, що постачає Target, систему опалення, вентиляції та кондиціонування (HVAC). Компанія отримає доступ до мережі Target для віддаленого моніторингу та обслуговування, і це забезпечить точку входу в систему, з якої зловмисник може ескалювати, тим самим порушуючи конфіденційність 40 мільйонів записів клієнтів. Звичайно, доступ до будівельних систем для будинків чи офісів несе в собі

ширшу загрозу не лише конфіденційності, але й цілісності та доступності.

Проблеми конфіденційності в Інтернеті речей. Конфіденційність розглядається як основна проблема в IoT (Misra, Maheswaran, and Hashmi 2016; Sicari et al. 2015; Ziegeldorf, Morchon, and Wehrle 2014; Roman, Najera, and Lopez 2011; Gessner et al. 2012). IoT надав величезну кількість даних, що належать не лише споживачам, як це відбувається у Всесвітній павутині, але й громадянам загалом, групам та організаціям. Це може бути використано для встановлення того, що нас цікавить, куди ми йдемо та наші наміри. Незважаючи на те, що це може забезпечити великі можливості для вдосконалення послуг, це повинно бути зважено з нашим прагненням до конфіденційності. Життєво важливо, щоб споживачі довіряли послугам, якими вони займаються, з повагою до їхньої приватності. Довіра є основним елементом формування будь-яких відносин і є життєво важливим фактором у впровадженні нових технологій (Ян, Чжан та Василакос, 2014). Люди не будуть використовувати нові технології, якщо вони не мають достатньої довіри до захисту конфіденційності, безпеки та безпеки (Taddeo та Floridi 2011; IBM Watson Foundation 2015), і це особливо актуально в складних системах, таких як IoT.

Датчики, в тому числі вбудовані в мобільні пристрої, збирають різноманітні дані про життя громадян. Ці дані будуть узагальнені, проаналізовані, оброблені, об'єднані та видобуті з метою отримання корисної інформації для забезпечення інтелектуальних і повсюдних послуг. Довіра стосується визначення, коли і кому інформація повинна передаватися або розголошуватися (Yan and Holtmanns 2008).

У 2010 році засновник Facebook Марк Цукерберг з гордістю вийшов на сцену і оголосив, що «конфіденційність більше не є соціальною нормою». Про це довгий час дискутували ряд науковців. У 2006 р. Було запропоновано парадокс конфіденційності (Barnes 2006), в якому стверджувалося, що «дорослі стурбовані вторгненням у приватне життя, тоді як підлітки вільно відмовляються від особистої інформації». Ця центральна теза була предметом великої академічної роботи (вона перевищує 900 цитат), причому багато вчених демонстрували, що цей парадокс існує в різних контекстах. Однак зміни спостерігаються, і нещодавно Оксфордський Інститут Інтернету опублікував звіт, в якому детально викладено новий парадокс конфіденційності. У звіті Бланк, Болсовер і Дюбуа (2014) стверджують, що молоді люди «набагато частіше, ніж люди старшого віку, вживали заходів для захисту своєї приватності», і що новий парадокс базується на уявленні, що «соціальне життя в даний час проводиться в Інтернеті, і що СНС не надають користувачам інструментів, які б

адекватно дозволили їм управляти своєю приватністю у відповідний для них спосіб». Недавнє дослідження дослідницького центру Pew (Rainie et al. 2013) показало, що 86 відсотків користувачів Інтернету вжили заходів в Інтернеті, щоб видалити або приховати свої цифрові сліди. Застосовувані методи включали очищення файлів cookie, уникання використання їх справжнього імені, шифрування електронної пошти та використання віртуальних мереж для приховування своєї адреси IP-протоколу.

Надання користувачам більшого контролю над збором та використанням їх особистої інформації розглядається як важливий аспект забезпечення довіри до розподілених систем. Попередні проекти, такі як проект платформи для налаштування конфіденційності (P3P), були розроблені, щоб надати користувачам контроль під час використання веб-браузерів. Протокол P3P, ініціатива Консорціуму Всесвітньої павутини (W3C), ініційована в 2002 році, дозволяє веб-сайтам заявляти про використання даних, зібраних через веб-браузери. Він побудований на ідеї перекласти політику конфіденційності веб-сайтів у стандартизовану машиночитану інформацію, щоб допомогти прозорості та дати можливість вибору користувачам. На жаль, проект закінчився достроково, і реалізацій було дуже мало. Існує низка причин, на які посилається недостатність P3P, зосереджена на відсутності прийняття з боку промисловості та користувачів (Jøsang, Fritsch та Mahler 2010). Конкретні причини включають відсутність прийняття веб-сайтів (Reay et al. 2007) через те, що спонукання підприємств застосовувати технології ПЕТ (відповідність, ефективність та ризик пошкодження торгової марки) недостатньо значущі для достатньої кількості підприємств (Beatty et 2007); відсутність прийняття браузерами (Cranor et al. 2008); та відсутність прийняття з боку користувачів, включаючи культурні міркування, що впливають на міжнародне прийняття P3P (Reay et al. 2007; Reay, Dick, and Miller 2009).

Для забезпечення конфіденційності розроблено різноманітні технології підвищення приватності, включаючи віртуальні приватні мережі, безпеку транспортного рівня, розширення безпеки DNS, багатошарова маршрутизація (Onion Routing), та отримання приватної інформації (Weber 2010). Політика конфіденційності Мови – це ще один тип ПЕТ, і обговорений раніше проект P3P можна вважати належним до класу ПЕТ ППЛ (Wang and Kobsa 2009). ЗОЗ можна класифікувати як зовнішні (декларативні без примусового виконання) або внутрішні (нормативні з підтримкою примусового виконання); P3P потрапляє в колишній клас. Інші PPL включають SAML (мова розмітки тверджень безпеки), XACML (стандарт OASIS для контролю доступу), включаючи PPL, A-PPL та GeoXACML, розширення XACML; XACL; SecPAL та його розширення для визначення обробки персональної інформації, SecPAL4P; AIR

(підзвітність у RDF); XPref; P2U; EPAL; P-RBAC; FlexDDPL; Дживс; PSLang; ConSpec; та SLAng (див. Kasem-Madani and Meier 2015 та Henze et al. 2016 для отримання додаткової інформації). Незважаючи на те, що існує цілий ряд PPL, жоден з них не став фактичним стандартом, і широкомасштабне усиновлення залишається проблемою.

Згода. Як уже згадувалося раніше, важливо збалансувати оптимізоване та персоналізоване обслуговування з прагненням до конфіденційності. Одним із методів узгодження цих конкуруючих цілей є забезпечення згоди споживача на те, що їх дані збираються, зберігаються та передаються. Однак це спричиняє низку проблем. Згода традиційно базується на системі прозорості: постачальник послуги повинен чітко пояснити, які дані збираються та для чого вони повинні використовуватися. Звичайно, виникали запитання щодо того, чи ясне представлення споживачеві 70 сторінок деталей, і це зараз починають вирішуватися нормативно-правовими актами. У проекті Загального керівного документу щодо згоди Загальних положень про захист даних (GDPR) від ICO у Великобританії (ICO 2017) зазначено, що, хоча Директива про захист даних зазначає, що «будь-яке вільно надане конкретне та інформоване вказівка на його бажання, якою суб'єкт даних означає свою згоду до персональних даних, що стосуються його, що обробляється», у статті 4 (11) GDPR зазначено «будь-яке вільно надана, конкретна, поінформована та однозначна вказівка на побажання суб'єкта даних, якими він заявляє, чи чіткою позитивною дією , означає згоду на обробку персональних даних, що стосуються його або неї». Якщо IoT реалізує бачення стати повсюдним, ми будемо взаємодіяти з системами без фізичного інтерфейсу. У цьому випадку (як зазначає Peppet 2014), «надання споживачам даних та інформації про конфіденційність та можливість дати згоду є особливо складним завданням». GDPR (2016) також вимагає згоди на деталізацію та простий вилучення. Це серйозні проблеми з відсутністю відповідних інтерфейсів для надання або відкликання згоди. Ці виклики будуть не тільки в громадських місцях, але і в будинках, коли технологія IoT стає вбудованою. Наприклад, даних датчиків тиску, ІЧ-датчиків та систем RFID достатньо для того, щоб супротивник контролював і розумів людську діяльність в будинку. Як приклад, дані, пов'язані з розумним холодильником, можуть бути використані для визначення харчових звичок та здоров'я, що може вплинути на страхування життя особи у страховій компанії. Використання датчиків та інтелекту також зростає у виробництві іграшок. Розумні іграшки мають здатність розпізнавати голос дитини, аналізувати та взаємодіяти з дитиною. Ці іграшки, як правило, мають можливості зовнішнього з'єднання Bluetooth та Wi-Fi, що робить кінцеві точки

вразливими до змагальних атак (Dobbins 2015). Ці іграшки можуть розкрити особисту інформацію дітей, а також призводять до страху відстеження місця перебування дітей та роблять їх уразливими. Крім того, ці іграшки можна використовувати як прилади спостереження або викрасти, щоб поводити себе неадекватно (Chaudron et al. 2017). Це призводить до виклику виробникам іграшок включати безпеку від зародження пов'язаних іграшок (Nelson 2016). Батьки, які дарують дітям розумні іграшки, явно або явно дають згоду на збір, обробку, зберігання та передачу даних, що стосуються їхньої дитини. Однак, як правило, вони не уповноважені давати згоду на обробку даних інших дітей, за словами друга, які взаємодіють з іграшкою. Без цієї явної згоди особисті дані друга не повинні оброблятися. Однак розділити два набори даних буде складним завданням, імовірно, що іграшки будуть обробляти дані без явної згоди.

Проблеми конфіденційності в Інтернеті речей не обмежуються лише споживачами, це також може вплинути на промисловість. Промисловий IoT є більш складним, ніж традиційні системи ІКТ, через велику поверхню атаки з численними векторами атак (Sadeghi, Wachsmann та Waidner 2015). Потрібно сформулювати належне визначення вимог щодо конфіденційності (Da Xu, He та Li 2014). Окрім ризику порушення конфіденційних даних про співробітників або клієнтів, потенційна втрата інтелектуальних даних відкриває можливість конкурентам повторити знання та можливості організації-жертви, що може підірвати конкурентні переваги (Sadeghi, Wachsmann та Waidner 2015). Незважаючи на те, що розуміється, що промисловий шпигунство через внутрішню або іншу атаку може призвести до крадіжки інтелектуальної власності, існують випадки, коли непрямі компроміси з приватністю можуть призвести до витоку інтелектуального капіталу. Наприклад, якщо дані, що стосуються промислових замовлень, скомпрометовані, це не лише дає конкуренту можливість прогнозувати промислове постачання поточних товарів і матеріалів, а й майбутні товари та інноваційні технології, що зараз розробляються. Подібним чином компроміси щодо захисту даних можуть виявити фінансові показники разом із бізнес-процесами та бізнес-аналітикою галузі, що може обмежити можливість галузі позичати гроші або впливати на її страхові внески. Цьому напрямку поки що приділяється мало уваги.

Висновки та подальша робота. В цьому матеріалу ми обговорили походження IoT та те, як це створило головну проблему стандартизації та єдине загальне бачення. Це, в свою чергу, породило виклики щодо безпеки та впевненості в Інтернеті речей.

Без сумніву, найважливішим випробуванням, але також і найголовнішим, є заохочення стандартизації та координації в Інтернеті речей. Це не лише складно з точки зору процесу та технологій, але й політики. Потрібно враховувати всі зацікавлені сторони та їх суперечливі погляди на IoT. Проект P3P демонструє труднощі, пов'язані з досягненням консенсусу та довіри між сторонами, які мають різні бачення та інтереси.

Проект P3P був похвальним, але зіткнувся зі значними труднощами. Аналогічна система для IoT, безумовно, була б корисною, але складно забезпечити відповідність результатів і прийнятність для всіх. Якщо повинен бути протокол, аналогічний P3P, який повідомляє про те, як дані збираються, обробляються, зберігаються та передаються, а також пропонує користувачам можливість вибору та контролю щодо своїх даних, важливо, щоб уроки були засвоєні з P3P проекту. Важливо, щоб будь-який стандарт був успішним, проект повинен пам'ятати про політику. Прихильники конфіденційності можуть розглядати цей розвиток як промислові підробки, критику, висловлену проектом P3P; протокол не повинен дозволяти службам створювати ілюзію конфіденційності під час збору персональних даних. Слід визнати, що будь-який стандарт, ймовірно, буде лише частиною рішення, і як такий, реалізація стандарту сама по собі може не забезпечити належного захисту. Тому рекомендується використовувати стандарт разом з іншими інструментами підвищення приватності. Будь-який стандарт повинен розроблятися відповідно до законодавчих та нормативних вимог. Якщо немає вимог про відповідність або фінансових наслідків для нереалізації протоколу, ділова аргументація щодо протоколу не вдасться. Щоб максимізувати ймовірність прийняття галузі та прийняття користувачами, будь-який протокол управління згодою в IoT повинен бути таким:

- розроблені навколо чітко узгоджених принципів, щоб гарантувати відсутність повзучості місії та чіткість цілей;
- простий, економічно ефективний та реалізований;
- пам'ятаючи про будь-який вплив на поточні та майбутні бізнес-моделі;
- спільно розробляється з галузевими органами (постачальниками послуг та інфраструктури) та представницькими групами користувачів;
- розроблений відповідно до законодавчих та нормативних вимог. Якщо немає вимог про відповідність або фінансових наслідків для нереалізації протоколу, ділова аргументація щодо протоколу не вдасться.

Інша ключова сфера, яка вимагає негайної уваги, – це аспекти Інтернету речей із низьким енергоспоживанням та низьким рівнем (малий

форм-фактор). Проблеми існують у розробці рішень, стійких до атак, на таких обмежених пристроях, а також можливості виявлення, діагностики та відновлення після атак.

Ключові розробки протоколів для вирішення проблеми сильної, низькобюджетної безпеки включають роботу групи IETF 6LoWPAN, яка розробила механізми інкапсуляції та стиснення заголовків, що дозволяють надсилати та приймати пакети IPv6 через бездротові бездротові персональні мережі. Вузли в цих мережах на базі IEEE 802.15.4 можуть працювати в двох захищених режимах: режимі ACL (забезпечуючи доступ лише до надійних вузлів) та захищеному режимі (забезпечуючи конфіденційність, цілісність повідомлень, контроль доступу та послідовну свіжість). Інші протоколи, призначені для вирішення таких проблем, включають протокол Internet Host (HIP) та Datagram Transport Layer Security (DTSL). Перший є більш ефективним, але «обмежене використання HIP створює серйозні обмеження» (Garcia-Morchon et al. 2013), тоді як другий є більш сумісним, але забезпечує низьку продуктивність. Управління ключами, включаючи зберігання та обмін, залишається значним викликом для обмежених ресурсами систем IoT, оскільки багато сучасних рішень щодо безпеки покладаються на прошивку із значними накладними витратами енергії (Healy, Newe та Lewis 2009).

Аутентифікація та ідентифікація в системах IoT є фундаментальною для безпеки та конфіденційності. Очевидно, що системи, засновані на біометричній ідентифікації, можливо в поєднанні з маркером, можуть виявитися вигідними порівняно з існуючими системами, але слід подбати про те, щоб система була безпечною, але без роздратування.

У битві було досягнуто значного прогресу за забезпечення автентичності пристроїв, потоків та служб в Інтернеті речей. Зокрема, розвиток фізичних неконструйованих функцій (PUF) (Suh and Devadas 2007; Tuyls and Škorić 2007; Guajardo, Kumar, and Schrijen 2007) може зіграти свою роль у аутентифікації пристрою. PUF має складну і непередбачувану, але повторювану систему відображення входів на виходи. Для ефективної автентифікації функція повинна бути простою для оцінки та повторюваною, а для цілей безпеки її важко передбачити. Були помічені деякі слабкі місця, такі як старіння, яке може зробити реакції PUF ненадійними (Maiti and Schaumont 2011), і розробляються вдосконалені схеми із застосуванням посиленої реакції на виклик (Maiti, Kim, and Schaumont 2012). PUF комбінуються із вбудованими модулями ідентифікації абонента (eSIM) для забезпечення автентифікації та контролю доступу. ESIM використовується для вирішення питань масштабованості, сумісності та дотримання протоколів безпеки (Cherkaoui, Bossuet та Seitz 2014).

Інші сфери, що вимагають термінової уваги, включають необхідність адаптації існуючих механізмів єдиного входу або створення нових, які краще відповідають IoT. Хоча деякі підходи вирішують цю потребу, пропонуючи гібридну архітектуру, яка поєднує всі механізми за допомогою спеціально розробленого проміжного програмного забезпечення [6], ця тема все ще потребує досліджень.

Існує також необхідність у стандартизованій комунікаційній платформі та архітектурі з єдиними міркуваннями безпеки в інтелектуальних транспортних системах, що надає пріоритет включенню безпеки в кожен шар архітектури. Показано, що атаки можливі від фізичного рівня (через комунікації, такі як Bluetooth або DSRC), до мережевого рівня (наприклад, CAN, LIN тощо), до рівня засобів шляхом зміни ЕБУ, перш ніж остаточно вплинути на такі програми, як як склоочисники та замки дверей.

Різні промислові атаки IoT також показали вразливості SCADA, такі як повільні оновлення та дірки для автентифікації, що відкриває шлях для подальших векторів атак у мережі. Це викликає потребу в безпечній та надійній архітектурі, яка може захистити промисловий IoT від мережі до пристроїв кінцевих точок, що регулює функціонування галузі.

IoT дає можливість здійснити революцію в нашому житті та роботі. Однак залишається низка значних викликів, щоб забезпечити реалізацію його потенціалу без катастрофічних наслідків. Для приватних осіб та організацій доступні численні рекомендації та найкращі практики щодо безпеки в Інтернеті речей. Міністерство національної безпеки США (DHS 2016) пояснює ризики та стратегічні принципи IoT та пропонує найкращі практики для пристроїв та систем від проектування до експлуатації широкосмугового Інтернету.

Технічна консультативна група (BITAG 2016), надає звіт, який висвітлює проблеми, пов'язані зі споживачами, які встановлюють продукти IoT, аналізуючи та наголошуючи на таких проблемах, як витоки даних та порушення конфіденційності. Конкретні вимоги до безпеки підключених транспортних засобів та медичних виробів рекомендує група I Am The Cavalry (Cavalry, 2014, 2016). У стільниковому домені GSMA підготував вичерпний оглядний звіт, який досліджує доступність, ідентичність, конфіденційність та проблеми безпеки IoT, представляє вказівки щодо мобільного рішення та надає приклади в різних додатках (GSMA Association 2016a). Оглядний звіт виступає в якості підручника до Екосистеми послуг (GSMA Association 2016b) та Звітів про екосистеми кінцевих точок (GSMA Association 2016c). Остаточний звіт у наборі викладає принципи безпеки мережевої безпеки, міркувань конфіденційності та послуг, що надаються мережевими операторами (GSMA Association 2016d). Навіть з наявними вказівками, залишаються проблеми навколо проектування,

впровадження та управління IoT. У цій роботі ми обговорили деякі з цих викликів, починаючи від визначення та стандартизації IoT, закінчуючи такими специфічними проблемами, як отримання та згода на управління. Зрозуміло, що досягнуто значного прогресу, але в битві за забезпечення IoT ще потрібно пройти довгий шлях.

1.5. Безпека NFC (зв'язку в близькому полі)

1.5.1 Екосистема NFC

На рис. 1.12 показана екосистема NFC.

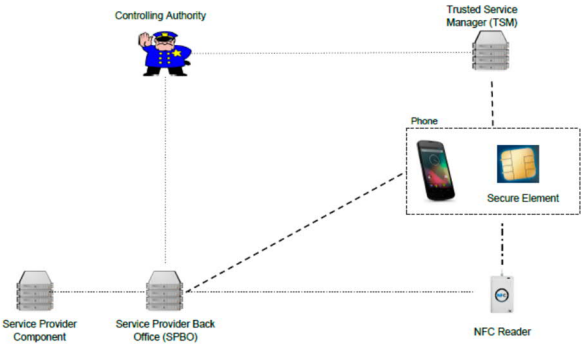


Рис. 1.12. Приблизна екосистема NFC та схема комунікацій, -·-·-· – зв'язок NFC, ------- – зв'язок через інші мережі, ····· – інший зв'язок

Розглянемо її компоненти:

1. Компонент постачальника послуг (SP). Це компонент (застарілий), який реалізує актуальні сервіси, тобто бізнес-логіку, без будь-якої служби NFC. Наприклад, для банківської програми постачальник послуг здійснює грошові операції між рахунками.

2. Бек-офіс постачальника послуг (SPBO) розширює функціональність постачальника послуг із функціями, пов'язаними з NFC. Реалізація SPBO належить розробнику служби NFC. Він може спілкуватися як з пристроєм зчитування NFC, так і з мобільним телефоном. Вибір одного з двох шляхів комунікації та інформація, що надсилається, є дизайнерським рішенням, яке розробник повинен буде зробити. Таким чином, SPBO забезпечує інтерфейс між обладнанням NFC та (застарілою) реалізацією бізнес-логіки, що дозволяє інтегрувати ці дві організації.

3. Телефон, який містить захищений елемент і підтримує NFC, архітектуру якої описано вище.

4. Зчитувач NFC – це NFC-пристрій, який підтримує зв'язок з телефоном. Він розташований на POS, тобто місце, де користувач отримує цю послугу. Зчитувач NFC спілкується з SPBO, щоб забезпечити обслуговування клієнта.

5. Довірений менеджер служби (TSM) – це надійний сторонній суб'єкт, який надає службі, яка дозволяють постачальникам послуг

дистанційний доступ, тобто віддалено встановлювати, управляти та видаляти аплети на захищеному елементі. Послуги TSM, як правило, надаються та здійснюються спеціалізованими компаніями, які стягуватимуть плату за цю послугу.

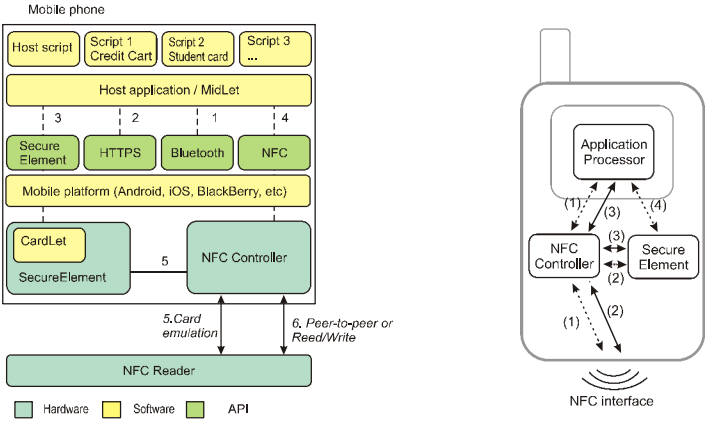
6. Контролюючий орган (CA) перевіряє, що аплети, встановлені через TSM, є нешкідливими, перш ніж їх буде встановлено на захищений елемент. Немає докладної інформації про те, як це робиться, і хто несе відповідальність за впровадження цієї функції.

Важливими сторонами в екосистемі є оператори мобільних мереж (MNOs) та постачальники послуг, які зацікавлені в використанні NFC. MNO постачає модуль ідентифікації абонента (SIM) у телефоні, який використовується для аутентифікації телефону в мобільній мережі. SIM-карта фактично є смарт-картою з організацією ISO 7816-4. Вона містить аплет для SIM-карти, але на неї також можна встановити інші аплети. Тому SIM-карту також можна використовувати як захищений елемент.

Проте використання SIM-карти обмежене MNOs. Оскільки існує безліч МНО та виробників телефонів, ПС потенційно має укладати ділові угоди з багатьма сторонами, а це є непрактично та дорого. Рішення передбачає впровадження центрального підрозділу, який називається надійним диспетчером послуг (TSM). TSM опосередковує власників захищених елементів та постачальників послуг (SP).

StolPaN / DIAD NFC framework. StolPaN (Магазин логістики та оплати за допомогою NFC) – це загальноєвропейський консорціум, що складається з університетів та компаній. Їхня основна мета полягає в тому, щоб «розробити комерційні та технічні основи для віддаленого управління службами, що підтримують NFC на мобільних пристроях». Ці системи дозволять реалізацію служби NFC для декількох телефонних платформ. DIAD NFC є угорським консорціумом, який розробляє комерційні послуги NFC, розширюючи результати StolPaN. Всі члени DIAD NFC також є членами StolPaN.

Архітектура мобільного приладу на базі NFC. Беньо та співавтори описують віртуальний машинний підхід [23, 24]. Ідея показана на рис. 1.13. Номери на цьому малюнку вказують на зв'язок NFC або API. Ці цифри використовуються для позначення цих зв'язків в тексті. На мобільний пристрій встановлено два програмні компоненти. MidLet – це програмний додаток, який встановлюється та виконується на основному ЦП телефону. Універсальний CardLet – це додатковий аплет, який встановлений на захищеному елементі.



а) б)

Рис. 1.13. Архітектура мобільного приладу

MidLet. MidLet функціонує як інтерпретатор скриптів, який може містити декілька індивідуальних сценаріїв обслуговування, кожен з яких відповідає службі NFC. З цієї причини MidLet також називається хост-додатком. Сервісний скрипт реалізує логіку для певної служби NFC, яка повинна мати місце на телефоні.

Рамки сценаріїв підтримують всі основні функціональні можливості програмування таких математичних операцій, функцій та команд керування потоками (if / else, switch / case тощо). Крім того, він підтримує команди для побудови базового графічного інтерфейсу користувача (друкувати текст, створювати кнопки, поля введення тексту тощо). API для обох NFC (з'єднання 4 на рис. 1.13а) та інших типів з'єднань (з'єднання 1, 2 на рис. 1.13а) також забезпечується за допомогою базових API-інтерфейсів операційної системи для цього.

Хост-додаток працює на кількох платформах, тобто сценарії є незалежними від платформи. Хост-додаток повинен бути встановлений один раз на мобільному телефоні. Згодом можна встановити кілька «скриптів» на телефон, тримаючи телефон до тегу NFC або перейшовши на веб-сайт. В обох випадках фактичний скрипт завантажується з сервера відділу обслуговування операцій (бек-офіс). Якщо використовується тег NFC, хост-програма несе відповідальність за читання тегу, що містить посилання на сам скрипт та завантаження сценарію. Як альтернатива, користувач може вибрати скрипт на веб-сайті, за допомогою якого постачальник послуг надсилає SMS на мобільний пристрій. Це повідомлення

містить посилання, і, у свою чергу, він запропонує початковій програмі запускати та завантажувати скрипт.

Хост-додаток забезпечує додаток із графічним інтерфейсом (скрипт-хост, на рис. 1.13а), що дозволяє користувачеві вибрати скрипт. Наприклад, коли користувач хоче платити, він може вибрати сценарій кредитної картки. Крім того, він дозволяє користувачеві встановлювати та видаляти скрипти.

CardLet. Окрім MidLet, додатки CardLet можна встановити на захищений елемент. Доступні два варіанти, які можуть співіснувати в одному і тому ж захищеному елементі: універсальний та / або спеціальний картлет.

Універсальний картлед, розроблений спеціально для використання в інтегрованій системі додатків. Функціональність картледа в цьому випадку обмежується шифруванням та розшифровуванням даних. Універсальний картлет може обробляти шифрування для декількох встановлених сценаріїв / служб, але гарантує точний поділ даних.

Універсальний CardLet можна використовувати тільки з режимом однорангової мережі NFC. У цьому випадку зв'язок NFC обробляється компонентом скрипту, який працює на хостовій програмі (з'єднання 6 на рис. 1.13а та шлях 1 на рис. 1.13б). За необхідності сценарій може отримати облікові дані з універсального аплету на захищеному елементі за допомогою API-з'єднання 3.

1.5.2. Аналіз безпеки

Питання безпеки обговорюються Benyo et al. Виявлено такі загрози:

• Загроза 1. Усі дані, що зберігаються на основному пристрої зберігання в телефоні, є потенційно небезпечними.

• Загроза 2. Відокремлене середовище виконання, надане операційною системою на головному процесорі телефону є потенційно небезпечним.

• Загроза 3. API, яке використовується для доступу до захищеного елемента з телефону, потенційно небезпечно.

Програмне забезпечення розрізняє три рівні безпеки в хост-додатках залежно від того, як і який захищений елемент використовується. Різниця полягає в тому, якою мірою вони займаються попередніми загрозами безпеки. Підсумок рівнів безпеки та загроз наведено в табл. 1.4. На підставі вимог безпеки постачальник послуг може вибрати відповідний рівень.

1. Низький рівень безпеки: захищений елемент не використовується взагалі.

2. Середній рівень безпеки: використовується універсальний картлет на захищеному елементі.

3. Високий рівень безпеки: спеціальний картлет використовується на захищеному елементі.

Низький рівень безпеки

Хоча хост-додаток забезпечує строго відокремлене середовище виконання та зберігання для кожного окремого сценарію, це не може вважатися безпечним. Однією з причин цього є те, що механізми, які реалізують це розділення, покладаються на платформу мобільних телефонів, яка може містити помилки та вразливі місця безпеки, як це показано для платформи Android [23]. Отже, противник міг би обійти ці механізми та отримати доступ до конфіденційної інформації (загроза 2).

Інша причина полягає в тому, що фізичне апаратне забезпечення для зберігання даних (флеш-диск або жорсткий диск) може бути доступним для доступу до всіх даних, включаючи ключі, які використовуються для шифрування даних (загроза 1). Отже, використання внутрішньої пам'яті телефону для зберігання даних на відміну від захищеного елемента вважається низьким рівнем безпеки.

Таблиця 1.4

Рівень захищеності та стійкість до загроз

	Загроза 1	Загроза 2	Загроза 3
Низький			✓
Середній	✓	✓	
Високий	✓	✓	✓

Середній рівень безпеки

Якщо використовується середній рівень безпеки, на захищеному елементі встановлюється універсальний картлайт, який може використовуватися для зберігання даних кількох служб. Це гарантує, що дані для кожного з послуг суворо відокремлені один від одного. Дані про цю карткову картку керуються за допомогою хостової програми, яка надає API (ініціалізація API 3, рис. 1.13а). Оскільки хост-додаток працює на самому телефоні, цей API між захищеним елементом та додатком-хостом є потенційним слабким місцем (загроза 3).

Високий рівень безпеки

Використання виділеної картки вважається високо надійним. Захищені дані не передаються між захищеним елементом і телефоном, а це означає, що API в загрозі 3 не використовується. Крім того, інформація не знаходиться на основному ЦП телефону, що підвищує його імунітет до загроз 1 і 2. Однак цей варіант вимагає значно більших зусиль у тому сенсі, що постачальник послуг несе відповідальність за встановлення CardLet на захищений елемент сам по собі, який може вимагати TSM.

Проблеми з NFC. Перший мобільний телефон з можливостями NFC був введений більше 10 років тому. Сьогодні багато телефонів обладнані можливостями NFC. Тим не менш, було сформовано кілька служб, які використовують цю технологію. Це пов'язано не лише з технічними обмеженнями. Основною проблемою є екосистема NFC, у якій різні зацікавлені сторони мають різні суперечливі інтереси.

Безпечне зберігання облікових даних у мобільному телефоні – це вимога для багатьох типів служб на базі NFC, включаючи фізичний контроль доступу. Для цього призначений захищений елемент, але його використання обмежується його власниками. Були запропоновані, розроблені та випробувані платформи, які регулюють використання захищених елементів у мобільних телефонах. Це передбачає впровадження центрального підрозділу, який називається надійним диспетчером послуг (TSM). Однак на практиці ці платформи не були широко розгорнуті. Причиною цього є те, що основні зацікавлені сторони не змогли розробити загальноприйняту бізнес-модель.

Це обмеження не тільки обмежує здатність телефону безпечно зберігати облікові дані, а й здатність телефону спілкуватися з існуючою інфраструктурою смарт-карт. Захищений елемент дозволяє телефону використовувати режим емуляції карти. Це дозволяє телефону спілкуватися з пристроями зчитування смарт-карт ISO 14443 та JIS 6319-4, які використовуються у багатьох існуючих платіжних системах, PACS та інших службах. Якщо безпечний елемент телефону не може бути використаний, це означає, що існуючу інфраструктуру смарт-карт буде потрібно замінити, що призведе до додаткових витрат.

Дві останні розробки можуть дати відповідь на вищезгадані обмеження захищених елементів.

1. Починаючи з версії 4.3, Android представив сховище облікових даних із підтримкою апаратного забезпечення для пристроїв, які підтримують це. Це потенційна альтернатива для використання захищеного елемента.

2. Починаючи з версії 4.4, Android підтримує емуляцію приймаючої карти (HCE), що дозволяє телефону спілкуватися з існуючою інфраструктурою смарт-карт без використання захищеного елемента.

Наразі (станом на 2014 рік) ці дві функції доступні виключно на останньому телефоні Android (серія Nexus) Google. Причиною цього є те, що для зберігання облікових даних із підтримкою апаратного забезпечення та HCE потрібне встановлення певного апаратного забезпечення на телефон. Проте той факт, що така велика компанія, як Google, підтримує підхід HCE (на відміну від підходу до захищених елементів) може спонукати інших виробників телефонів дотримуватися цього підходу. Деякі інші компанії в галузі оплати та NFC вже підтримують цей підхід (наприклад, Visa та NXP). З часу впровадження HCE було оголошено про деякі послуги платежів NFC. З цих причин варто дослідити потенціал цього підходу в управлінні фізичним доступом.

1.5.3. Проблеми, пов'язані з безпекою, та їх рішення

Фізичний контроль доступу – це питання, пов'язані з безпекою. Тому корисно отримати розуміння потенційних проблем безпеки. У термінології безпеки розрізняють вразливості та загрози. Вразливість потенційно впливає на безпеку, тоді як загроза безпосередньо діє на неї.

Визначення безпеки. Безпечна система повинна задовольняти набір властивостей, які широко відомі як «тріада ЦРУ» (конфіденційність, цілісність, доступність) (*CIA triad* (Confidentiality, Integrity, Availability) [24].

1. Конфіденційність

(a) Конфіденційність даних – гарантує, що конфіденційні дані недоступні неавторизованим сторонам.

(b) Конфіденційність – гарантує, що людина може контролювати, яка інформація, пов'язана з нею, зберігається в системі та кому вона доступна.

2. Цілісність

(a) Цілісність даних – гарантує, що дані в системі не змінюються неавторизованими особами чи організаціями.

(b) Цілісність системи – гарантує, що система функціонує як передбачено.

3. Доступність – забезпечує наявність системи, коли це потрібно.

Системний домен. Системний домен вказує, в яких частинах системи ми розглядаємо безпеку. Це показано на рис. 1.14. Мобільний телефон (1) є частиною системи, оскільки він зберігає облікові дані та

обробляє зв'язок NFC з пристроєм зчитування NFC. Крім того, канал зв'язку NFC розглядається в аналізі безпеки, оскільки він використовується для передачі інформації про автентифікацію.

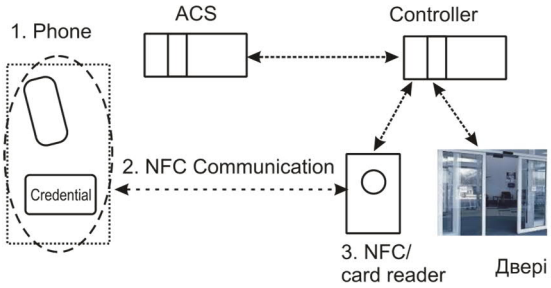


Рис. 1.14. Системний домен

Що стосується безпеки PACS, ми обмежуємо доступ до зчитувачів (3). Зчитувач, як правило, знаходиться в загальнодоступному місці, тобто його можна змінити. Безпека інших компонентів в PACS важлива для системи безпеки в цілому, але тут не розглядається. Причиною цього є те, що увага зосереджується на використанні мобільного телефону як токену в PACS з використанням NFC. Таким чином, ми розширюємо існуючий PACS, додаючи до нього мобільний телефон та технологію NFC. Крім того, існує широкий спектр PACS, що робить аналіз безпеки у всіх цих системах недосяжним.

Вразливості

Підслуховування та повторне пересилання даних

NFC використовує ефір як середовище для передачі даних через вільне місце. Потенційно ці хвилі можуть бути отримані або змінені зловмисником. Рис. 1.15 ілюструє атаку підслуховування та відтворення. Фактично кожен, хто знаходиться близько до передавача, може отримати дані. Це називається підслуховуванням.

Важливе питання щодо підслуховування трафіку NFC – це максимальна відстань, на якій супротивник все ще може отримувати дані. Переважно ця відстань повинна бути максимально мала. NFC призначений для зв'язку до 10 см.

Дистанція переданого сигналу залежить від багатьох факторів. Найважливішим є те, чи є пристрій активним або пасивним. Активні пристрої можуть мати відстань до 10 м, тоді як пасивні пристрої мають лише 1 м максимального діапазону [23, 24]. Причиною цього є те, що пасивні пристрої отримують енергію для отримання сигналу від активного

пристрою. Кількість енергії, яку можна перенести на пасивний пристрій, обмежена технікою, яка використовується для цього. Активні пристрої використовують власні джерела живлення, і, отже, їхній сигнал сильніший. Інші фактори, які можуть вплинути на дальність, – перешкоди в навколишньому середовищі, які можуть заблокувати сигнали (наприклад, стіни, будівлі). Якість апарата приймача-атакуючого (наприклад, типу антени, якості приймача) також визначає відстань, на якій сигнал може бути отриманий.

Наслідком підслуховування є те, що ненавмисний приймач може перехопити конфіденційну інформацію між відправником і одержувачем. Отже, конфіденційність інформації порушується. Розширення цієї атаки – атака повторення.

Припустимо, що мобільний телефон автентифікує до зчитувача NFC, відправивши незахищений ідентифікатор "секретності". Зловмисник може підслухувати зв'язок між телефоном і читачем, отримувати ідентифікатор та повторно надіслати або відтворити ідентифікатор з його власного телефону, коли він знаходиться біля дверей, що дозволяє йому незаконно отримати доступ до будівлі.

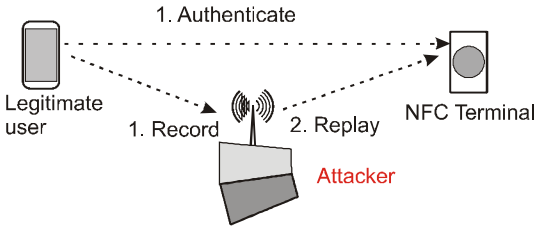


Рис. 1.15. Атаки підслуховування та повтору. Номери показують послідовність дій

Пошкодження даних та модифікація і вставка

Зловмисник не обмежується отриманням даних між телефоном і терміналом NFC. Він також може передавати дані з різними цілями. Найпростішою можливістю є пошкодження даних, показане на рис. 1.16(а), де атакуючий розбиває сигнал таким чином, що призначений приймач не може це зрозуміти. Це може бути кваліфіковане як атака «Відмова в обслуговуванні» (DoS): служба, в цьому випадку контролю доступу, стає недоступною для своїх призначених користувачів. Захищені користувачі, які прибувають до дверей, не можуть отримати доступ до будівлі. Це впливає на доступність системи.

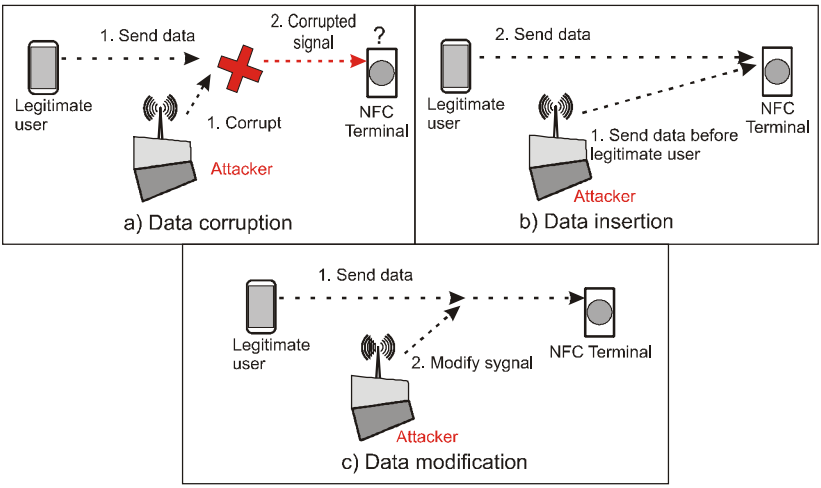


Рис. 1.16. Пошкодження, вставлення та модифікація даних

Вставка даних наведена на рис. 1.16(b). Зловмисник відповідає на отримане повідомлення, перш ніж законний одержувач може це зробити. Це може бути зроблено лише тоді, коли законний одержувач довго не відповідає, тобто він має високий час відгуку. Якщо відповідь зловмисника не надсилається, перш ніж законний одержувач починає надсилати повідомлення, ці сигнали збігаються і втручаються, і, отже, помилка не дає результату. Вставка даних впливає на властивість цілісності.

Модифікація даних наведена на рис. 1.16(c). Зловмисник змінює сигнали таким чином, що законний одержувач отримує дійсний, але змінений сигнал. У випадку з NFC цю атаку важко виконати через невелику відстань між телефоном і терміналом NFC, однак це можливо в залежності від модуляції та кодування, що використовуються на фізичному рівні.

Як показано в табл. 1.5, модуляція, що використовується в NFC, – 10 % або 100 % амплітудно-змінна маніпуляція (ASK) або з кодом Манчестера, або з модифікованою версією кодування Міллера в залежності від швидкості передачі даних, а також від того, чи є пристрій активним чи пасивним. Детальна інформація про схему модуляції тут не розглянута. Використовуючи 100 % ASK з модифікованою версією кодування Miller, можливо змінити обмежену кількість бітів у сигналі, але якщо використовувати 10 % ASK з кодуванням Манчестера модифікація даних досяжна на всіх бітах сигналу.

Наслідком цього є порушення цілісності інформації. Кожна інформація, що отримана, не може бути достовірною, оскільки вона можливо була змінена зловмисником.

Таблиця 1.5

Модуляція, яка використовується у NFC

Швидкість (КБ/с)	Активний прилад	Пасивний прилад
106	Модифікована Міллера, 100 % ASK	Манчестер, 10 % ASK
212	Манчестер, 10 % ASK	Манчестер, 10 % ASK
424	Манчестер, 10 % ASK	Манчестер, 10 % ASK

Атака «Людина-в-середині»

На рис. 1.17 ілюструється ідея атаки «Людина-в-середині» (MiTM). Дві сторони, Аліса і Боб, вважають, що вони спілкуються один з одним, але насправді вони спілкуються через Єву, нападника. Єва може здійснити це шляхом перехоплення повідомлень між Алісою та Бобом, тобто підслухати зв'язок і зашкодити передачі таком, що призначений приймач не отримує її. Згодом Єва може змінити перехоплене повідомлення та переслати його до приймача.

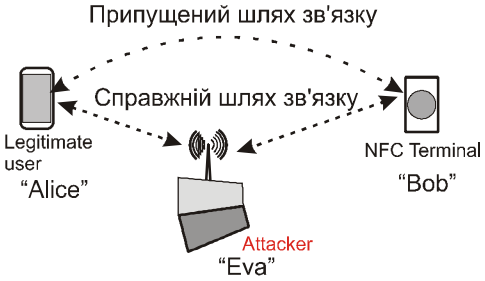


Рис. 1.17. Атака «Людина-в-середині»

Доцільність такого типу атаки можна дослідити, розглядаючи зв'язок між одним активним і пасивним пристроєм, а також між двома активними пристроями. Припустимо, що Аліса є активним пристроєм, а Боб є пасивним. У цьому режимі Аліса буде постійно генерувати РЧ-сигнал, щоб забезпечити енергію Боба. Якщо Єва досить близька до Аліси, вона може підслухати повідомлення, надіслані Алісою. Далі вона повинна переконатися, що Боб не отримує сигнал, пошкоджуючи його. Однак це порушення може виявити Боб. Отже, Боб може припинити спілкування з Алісою через виявлення перешкод.

Припускаючи, що Боб не виявить порушення, наступним кроком для Єви було б переслати модифіковане повідомлення Бобу. Це, однак, неможливо, оскільки Аліса постійно генерує ВЧ-сигнал. ВЧ сигнали Аліси та Єви зіткнуться і, таким чином, Боб не зуміє це зрозуміти.

Якщо і Аліса і Боб є активними пристроями, ВЧ-сигнал буде згенерований лише тоді, коли один із двох буде його передавати. Знову ж таки, припустимо, що Єва успішно заважає сигналу Аліси, і що це не виявлено Бобом. Тепер Єва здатна надіслати модифіковане повідомлення Бобу, тому що Аліса залишається спокійною після завершення передачі. Проте в цьому випадку Аліса також отримає модифіковане повідомлення Єви, яке означатиме, що вона може виявити напад. Висновок полягає в тому, що атака MiTM можлива в NFC, але навряд чи вона буде успішною, оскільки її легко виявити. Проте невідомо, якою мірою такі механізми виявлення втілюються в поточні системи NFC. Наслідком цього є потенційне порушення конфіденційності та цілісності.

Атака з ретрансляцією (Relay attack)

У цьому типі атаки вторинний канал зв'язку, тобто інший канал зв'язку, ніж NFC, використовується для тунелювання зв'язку між читачем та картою (або телефоном). Ця атака стала основною проблемою з введенням безконтактних смарт-карт. На рис. 1.18а показано нормальне спілкування між безконтактною смарт-карткою та пристроєм для зчитування смарт-карт. У разі атаки ретрансляції необхідні два додаткові компоненти, як показано на рис. 1.18б.

1. «Кріт» – це пристрій, що діє як зчитувач і спілкується із законною старт-картою

2. Проксі імітує законну карту, спілкуючись з кротом.

Цю установку можна використовувати в системі контролю доступу таким чином. Зловмисник розташовує проксі-сервер на пристрої для читання смарт-карт біля дверей. Співучасник атакуючого знаходиться поблизу невідомої жертви, що має законну картку. Співучасник використовує крота для ініціювання контакту з карткою. Зв'язок передається злочинцеві біля дверей, який одночасно представлятиме посередника зчитувачу. Проксі-сервер може поводитися як законна картка, спілкуючись з реальною карткою через крота, і так злочинець може отримати доступ до кімнати.

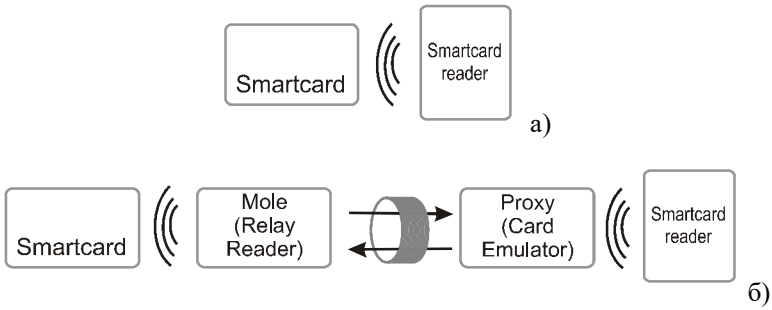


Рис. 1.18. Атака з транслюванням (релейна)

Хоча описаний сценарій ілюструє атаку ретрансляції підчас використання смарт-карт, вона також працює для NFC у мобільних телефонах. Коли телефон працює в режимі емуляції картки, налаштування є однаковими, за винятком того, що картка зараз є мобільним телефоном. Це називається зовнішньою атакою ретрансляції.

Включення обладнання NFC всередині мобільного телефону вводить новий тип ретрансляційної атаки, що називається внутрішньою атакою з транслюванням. Роланд та співавт. демонструють, як здійснити ретрансляцію на Google Wallet; мобільний платіжний сервіс на основі NFC. На рис. 1.19 показано, як можна виконати цю атаку. Зловмисне програмне ретрансляційне забезпечення встановлено на телефон жертви (ліворуч). Це програмне забезпечення пересилає повідомлення між проксі-сервером та захищеним елементом у телефоні жертви, який містить аплет Google Wallet. Таким чином, замість зовнішнього апаратного компонента, кріт тепер є шкідливим програмним забезпеченням, встановленим на телефоні жертви.

Проксі-сервер – це ще один мобільний телефон, який використовує емуляцію приймаючої карти, щоб спілкуватися з пристроєм зчитування NFC (торговий термінал на рис. 1.19), та його інтернет-з'єднання для взаємодії з телефоном жертви. На рис. 1.19 показано, як APDUs можна простежити між телефоном жертви та проксі-сервером.

Наслідком цього є те, що зловмисник може скористатися послугою від імені жертви без відома та дозволу потерпілого.

Вразливості в мобільних телефонах

За останні 20 років мобільний телефон перетворився з пристрою, який використовується виключно для розмов, в повністю функціональний комп'ютер, який може запускати власні програми для різних інших цілей. Це створює різні вразливі місця для мобільних телефонів:

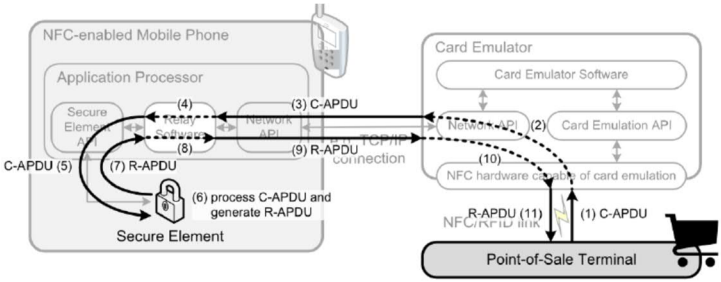


Рис. 1.19. Атака з транслюванням на Google Wallet

• Помилка виконання – законне програмне забезпечення, встановлене на телефоні (включаючи операційну систему), може містити помилки. Вони можуть експлуатуватися зловмисником, який потенційно дозволяє йому виконувати довільний код на телефоні.

• Несумісність – несумісність між окремими додатками або між додатками та операційною системою може відключити ці програми.

• Недосвідченість користувачів. Користувачі мобільних телефонів можуть не знати про певні ризики, оскільки їх технологічні знання обмежені. Наприклад, користувач може встановлювати шкідливе програмне забезпечення або підключатися до ненадійної мережі Wi-Fi. Також може бути неправильно налаштований телефон, наприклад, увімкнення bluetooth без встановлення пароля.

• Вразливості бездротової мережі – інформація, що надсилається через з'єднання Wi-Fi, може підслуховуватися та модифікуватися.

• Вразливості зовнішніх об'єктів. Зовнішні об'єкти, такі як точки доступу до Інтернету, не налаштовані належним чином, ПК з шкідливим програмним забезпеченням, можуть нанести на телефон ризик.

Операційна система Android надає ряд механізмів захисту, які стосуються деяких вразливостей. Тим не менше, Android також уразливий до помилок виконання. Відомі атаки, що обходять ці механізми безпеки, використовуючи помилки виконання. Наприклад, Davit et al. [5] описують атаку ескалації привілеїв, коли програма отримує доступ до ресурсів, які їй не передбачено.

Вкорінення – це спосіб отримати повний доступ до операційної системи телефону. Іноді це навмисно робиться власником телефону, щоб подолати обмеження, встановлені виробником телефону. Тим не менш, це також може бути викликане зловмисним програмним забезпеченням. Небезпечним наслідком цього є те, що всі механізми безпеки, надані операційною системою, можна обійти.

Висновок полягає в тому, що мобільна операційна система не забезпечує безпеку та не може бути довіреною. Це впливає не тільки на програми та дані на мобільному телефоні. Це також впливає на безпеку захищеного елемента. Сам захищений елемент є безпечним, оскільки він заснований на технології смарт-карт, але вбудований у телефон вводить ризик атаки відмови в обслуговуванні.

Коли кількість спроб аутентифікації захищеного елемента перевищує певний поріг, він буде вводити в незворотній стан BLOCKED, що означає, що апплети більше не можуть бути встановлені або видалені. Аплети, які вже встановлені, продовжують працювати нормально. Програми на телефоні можуть взаємодіяти із захищеним елементом (шлях 3 або 4 на рис. 1.1б) через API, і, отже, ці програми можуть викликати SE, щоб цільові станції було введено в режим BLOCKED. Цей API захищений, але цей захист вимагає, що основній операційній системі можна довіряти, а це не так.

Зчитувач без довіри

Зчитувач знаходиться в загальнодоступному місці. Потенційно він може бути підроблений. Наприклад, зчитувач можна замінити або змінити, якщо користувач не помітить. Це може бути використано для активації нападів, згаданих раніше в цій главі (прослуховування, введення / зміна / кодування даних та MiTM). Різниця полягає в тому, що в цьому випадку атака виконується не на каналі зв'язку NFC, а всередині зчитувача.

Наприклад, раніше було показано, що MiTM на каналі NFC є можливим, але складним для виконання. Проте, коли зчитувач модифікується, цілком можливо, що зчитувач, котрий легітимний, насправді є «людиною в середині». Це підвищує успішність цих типів нападу.

Загрози безпеці

Виявлені уразливості можуть стати загрозами. Повторимо визначення небезпеки.

• Загроза 1: незахищене зберігання – зберігання інформації в телефоні є небезпечним, адже є ризик викрадення даних з облікового запису телефону.

• Загроза 2: атака ретрансляції – внутрішня або зовнішня релейна атака.

• Загроза 3: незахищений канал зв'язку та ненадійний зчитувач. Через небезпеку природи каналу зв'язку NFC та того факту, що зчитувачам не можна довіряти, зловмисник може застосувати певні атаки, такі як

підслуховування і MiTM, що в кінцевому підсумку дозволяє йому успішно автентифікуватися у системі від імені потерпілого.

• Загроза 4: відмова в обслуговуванні – може бути виконана атака на відмову в обслуговуванні, що робить телефон непридатним для аутентифікації.

• Загроза 5: конфіденційність – зловмисник може перехоплювати інформацію, пов'язану з ідентифікацією, на інтерфейсі NFC без знання та схвалення користувача.

Загрозі 1 можна запобігти, використовуючи компонент на телефоні, який забезпечує безпечне зберігання (наприклад, захищений елемент). Загрози 3 і 5 можна вирішити, використовуючи протокол автентифікації. Загрозі 2 в даний час важко запобігти, однак можливість атаки ретрансляції може бути мінімізована шляхом прийняття ряду запобіжних заходів.

Наскільки відомо, в області DoS-атак на смарт-карти та / або NFC (загроза 4) не було проведено жодної масштабної роботи. Можливі причини цього полягають в тому, що зловмиснику нема чого отримати. У контексті Інтернету атаки DoS є важливою темою, оскільки їх легко виконувати, вимагають низької вартості, але потенційно можуть відключити послуги багатьом клієнтам.

У випадку з NFC існує дві форми DoS-атак. Сервіс можна відключити, виключивши зчитувач або канал зв'язку NFC. Ще однією можливістю є те, що шкідливе програмне забезпечення в телефоні вимикає облікові дані у телефоні. Перша вимагає, щоб атакуючий фізично знаходився в місці контролю доступу, що значно ускладнює її. Друга форма включає встановлення шкідливого програмного забезпечення на телефон користувача.

Обидва типи атак є можливими і можуть бути бажаними для зловмисника, якщо вони спрямовані на конкретного користувача або невелику групу користувачів. Але порівняно з атаками DoS в інтернеті, не так легко зашкодити «багатьом» користувачам. Крім того, наслідки цієї загрози обмежені, оскільки це лише впливає на доступність.

2. ЗАХИСТ ВІД НАВМИСНИХ ТА НЕНАВМИСНИХ ЗАГРОЗ В IOT[1]

2.1 Вступ

Інтернет речей (IoT), включаючи Індустріальний Інтернет (IIoT), стосується не лише зв'язку систем та пристроїв, а й відповідних додатків та послуг, що забезпечують моніторинг та контроль складних систем та послуг. Область застосування охоплює широкий спектр галузей, від охорони здоров'я до промислового контролю та транспортування до систем спостереження. Його розширення та зростання включає кілька технологій та дисциплін, таких як електроніка, вбудовані мережі, гібридні системи та управління. Включення інформаційних технологій (IT), а також операційних технологій (OT) створює виклик для розвитку систем та послуг, які є технологічно міждисциплінарними. Виниклі проблеми інтеграції цих технологій у нові методології проектування надійних та ефективних систем та послуг IoT є значними. В даний час навіть термінологія, що використовується різними зацікавленими сторонами, представляє проблеми та невідповідність загальному розумінню властивостей та цілей інфраструктури та програм IoT [26].

Розглядаючи цільові програми та послуги Інтернету речей, у цій главі ми розглядаємо питання безпеки та безпеки систем та сервісів Інтернету речей із підходом, який охоплює від систем до додатків (сервісів чи процесів) уніфіковано, використовуючи термінологію, що походить від обчислень, мереж та контроль, оскільки ці дисципліни становлять основні стовпи технологій IoT у всіх сферах застосування IoT. Цей підхід узгоджується з еталонними архітектурними моделями як MCE, так і Індустріального Інтернет-консорціуму. Для зручності ми розглядаємо питання безпеки в цьому розділі, дотримуючись моделі MCE, яка розділяє механізми безпеки на дві частини: одну для загальної безпеки та одну, яка залежить від програми; ми використовуємо терміни залежні від програми та залежні від процесу взаємозамінні.

Програми IoT, як правило, збирають дані за допомогою зондуючих пристроїв, обробляють ці дані та виконують дії, які варіюються від надсилання сповіщень та подання тривоги до виконання дій через виконавчі механізми у фізичних системах. Проста загальна модель для цієї операції – це модель циклу управління, яка використовується у багатьох додатках

1 Англійською застосовуються терміни Safety та Security. Safety – це умова захисту від шкоди чи інших небажаних наслідків, спричинених ненавмисною невдачею. Security – це умова захисту від шкоди чи інших небажаних наслідків, спричинених навмисними діями людини чи поведінкою людини.

доменів і зображено на рис. 2.1. У цій моделі пристрій D управляється центром управління C. Вимірювання параметрів, що цікавлять, збираються з D через датчики і передаються в C, який робить необхідні розрахунки та приймає необхідні рішення та дії для програми; якщо додаток вимагає автоматичних дій, C надсилає необхідні команди виконавчим механізмам, які керують D. Модель є загальною і охоплює застосування в різних сферах – від охорони здоров'я до транспортування та від аерокосмічної галузі до виробництва. Наприклад, у програмі охорони здоров'я датчики вимірюють параметри пацієнта, такі як температура та рівень глюкози, і направляють їх у програму моніторингу – аналогічну до центру управління, – і рішення приймаються залежно від програми; може бути надіслано повідомлення, щоб привернути увагу пацієнта або лікаря, або може бути відкрита інсулінова помпа для введення більшої кількості інсуліну. На виробничому поверсі датчики можуть виявляти надходження компонента та надсилати дані до центру управління, який, у свою чергу, надсилає відповідні команди машині, яка відповідно обробляє компонент.

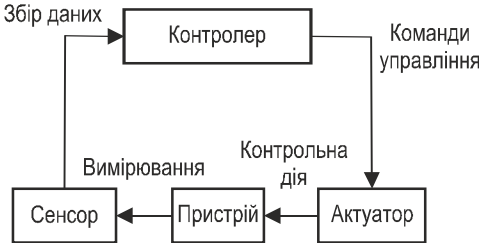


Рис. 2.1. Контур управління

Модель контуру управління, показана на рис. 2.1, реалізована на обчислювальній платформі, яка має структуру, відмінну від тієї, що вказана в моделі управління. Рисунок 2.2 показує типову ієрархічну обчислювальну структуру для промислових систем, важливий клас систем IoT, показуючи, як обчислювальні системи, мережі, датчики та виконавчі механізми зазвичай використовуються для реалізації операційних обчислювальна інфраструктура циклу управління. Датчики та виконавчі механізми приєднані до керованого пристрою («Пристрій» на рис. 2.1), програмовані логічні контролери (ПЛК) реалізують прості елементи керування – зазвичай по одному на ПЛК – а система контролю та збору даних (SCADA) реалізує контур управління для повної процес, також позначається як рослина. ПЛК у структурі – це прості промислові комп'ютери, і їх кількість різниться залежно від застосування. Наприклад, у розумній

мережі різні ПЛК можуть виконувати дії локально для кожного трансформатора, тоді як SCADA контролює всю розумну мережу; у системі управління водними ресурсами інший PLC може керувати кожним насосом, тоді як SCADA контролює систему водопостачання на промисловій ділянці.

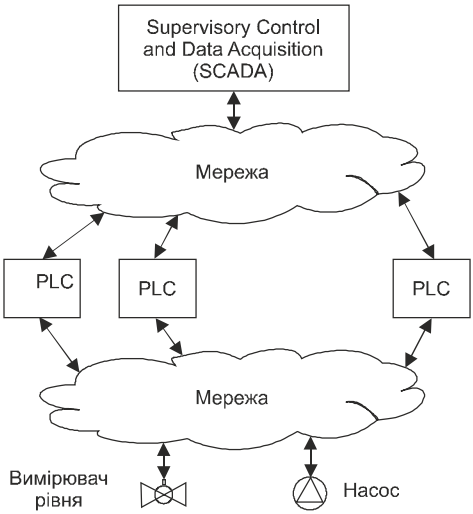


Рис. 2.2. Ієрархічна інформаційна система для контуру управління

У цьому середовищі є кілька властивостей, яких ми хочемо досягти. З контрольної точки зору ці властивості, як правило, є властивостями безпеки. Наприклад, ми хочемо уникнути перевантаження інтелектуальної мережі, уникнути переповнення бака для рідини або уникнути передозування фармацевтичної речовини, яка автоматично вводиться пацієнту. Ці властивості можуть бути порушені з кількох причин. Можливо, програміст зробив у програмі помилку, вимоги системи можуть пропустити умову, яку слід було врахувати, проміжне програмне забезпечення системи може дати неправильні пріоритети для управління процесами або, просто, зловмисна сторона може атакувати систему та змусити її вчинити неправильні дії.

Вимоги безпеки (safety) до додатків зазвичай виражаються як вимоги до контуру управління, який реалізує додатки. Ці вирази базуються на припущеннях про властивості інфраструктури, на якій реалізовано додаток. Наприклад, система управління HVAC передбачає, що вимірювання температури, які вводяться в систему, є правильними в межах

певного наближення. Це означає, що властивості безпеки базуються на припущеннях про цілісність даних, які повинні бути задоволені інфраструктурою. Загалом, вимоги безпеки (safety) включають вимоги щодо безпеки (security) інфраструктури, такі як цілісність, неявно або явно. Типовим явним властивістю безпеки є захист особистої інформації в системі управління охороною здоров'я. Таким чином, стає зрозумілим, що security також є вимогою safety, оскільки принаймні необхідна цілісність даних.

Технології IoT залучають декілька зацікавлених сторін, включаючи постачальників, постачальників послуг, регуляторні органи та клієнтів. Незважаючи на те, що інтереси незалежних зацікавлених сторін різні, і, отже, вимоги до безпеки, які вони пред'являють до технологій IoT, можуть відрізнятися, існує набір основних вимог до безпеки, які загалом відповідають вимогам усіх різних категорій зацікавлених сторін. Цей набір вимог включає (1) конфіденційність, (2) цілісність, (3) автентифікацію, (4) контроль доступу, (5) невідмова, (6) надійність, (7) безпеку та (8) конфіденційність.

Конфіденційність – це властивість, яка забезпечує захист даних, що зберігаються або передаються, від розголошення, тоді як цілісність дозволяє підтвердити (перевірити) правильність відповідних даних. Аутентифікація дозволяє ідентифікувати будь-яку сторону, яка бере участь у транзакції, будь то виробництво, обробка, передача чи отримання даних. Контроль доступу забезпечує надання послуг уповноваженим користувачам, тоді як відмова відключає учасників транзакцій, щоб відмовити в діях або їх участі. Надійність вимагає надання функціональних можливостей системи та сервісу зі специфічними властивостями, такими як безперервне обслуговування, навіть за наявності помилок і збоїв, відповідність конкретним вимогам у реальному часі тощо. для користувачів. Нарешті, конфіденційність захищає особисту інформацію від доступу несанкціонованих суб'єктів.

Наукові та інженерні методи та прийоми, що відповідають цим вимогам, загалом відомі, оскільки такі вимоги вже давно розглядаються в декількох IT-системах у широкому діапазоні прикладних областей. Однак задоволення вимог в контексті IoT та IIoT з характеристиками OT (операційних (виробничих) технологій) вимагає нових підходів через кілька додаткових факторів. Ці фактори включають моделі відмов компонентів, доступні ресурси для забезпечення безпеки, а також профіль зловмисників, включаючи їх потенційні ресурси. Ці фактори є сильними диференціаторами в процесі забезпечення безпеки в контексті IoT та IIoT з кількох причин. По-перше, вбудовані системи та системи CPS вже були розгорнуті у значно більшій кількості, ніж невбудовані (типові IT)

системи, такі як сервери, ноутбуки тощо. По-друге, більшість із цих систем мають обмежені ресурси з точки зору обчислень, зв'язку та потужності. ресурсів, а їх виробники висувають суворі вимоги до низьких витрат, щоб проникнути на великі споживчі ринки. Як результат, ці системи розгортаються в різних середовищах, включаючи ворожі, де зловмисні користувачі отримують доступ до цих систем протягом невизначеного періоду часу і з невизначеними можливостями втручатися в них. Кінцевою причиною є суворі вимоги щодо безпеки в декількох сферах, таких як автомобільна, промислова, повітроплавання тощо.

Ці фактори, що відрізняють вбудовані системи ставлять значні вимоги до їхньої безпеки, оскільки їх велике число розгортання та різноманітне робоче середовище з багатьма невідомими або непередбачуваними характеристиками призводять до великої кількості потенційних зловмисників з різними можливостями. Крім того, у багатьох доменах додатків висуваються вимоги до безпеки, які мають відношення до безпеки, надійності та конфіденційності, як у випадку транспортних систем, медичних систем, спостереження тощо. Необхідність задоволення всіх цих вимог щодо систем з обмеженими ресурсами та низькою цільовою ознакою вартості призводить до надзвичайно складних проблем та необхідності використання дешевих технологій, що дозволяють досягти необхідних цілей.

Для того, щоб визначити вимоги та механізми, необхідні для забезпечення необхідних властивостей security в контексті IoT та IIoT, ми дотримуємося шарів, показаних на рис. 2.3 він визначає наш погляд на взаємозв'язок між програми та властивостями процесу, такими як safety та конфіденційність, та механізми security та надійності, які надаються на рівні системи та використовуються як примітиви для надання властивостей програми та процесу.

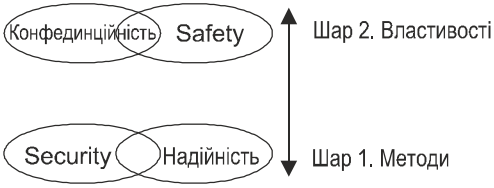


Рис. 2.3. Шари властивостей безпеки

Зображене нашарування базується на нашому підході для диференціації властивостей системного рівня, таких як безпечне зберігання, захищений зв'язок, захист від несанкціонованого доступу тощо, від властивостей, які потрібні та надаються на рівні програми. У цьому підході

ми вважаємо, що (вбудовані) системи та їх взаємозв'язки побудовані для стійкої роботи з подоланням відмов, випадкових чи зловмисних, що призводять до втрати інформації, витоку та доступності. Механізми надійності більше зосереджуються на аспектах надійності та доступності, враховуючи випадкові збої, використовуючи імовірнісні моделі для несправностей, тоді як механізми безпеки фокусуються на наданні альтернативних властивостей, наприклад, конфіденційності, автентифікації, доступності тощо на основі визначених моделей шкідливих атак. Хоча деякі властивості надійності та безпеки, такі як доступність інформації, є спільними між цими двома дисциплінами, інші, такі як конфіденційність або безперервна робота, доповнюють один одного. Як правило, надійність доповнює безпеку, оскільки зловмисник може вставляти несправності та збої – аналогічно запуску атак на механізми безпеки, без яких механізми надійності не можуть відновитись. Очевидно, що поєднання механізмів надійності та безпеки на системному рівні забезпечує надійні платформи, які є одночасно безпечними та доступними під час аварій та атак.

Безпека та конфіденційність часто описуються як вимоги безпеки у багатьох доменах програм, хоча вони багато в чому відрізняються від типових міркувань безпеки. Зазвичай захист конфіденційності та безпека є вимогами до процесів, програм та послуг, а не до загальних систем. У нашому підході конфіденційність та гарантії залежать від безпеки, оскільки вони використовують механізми безпеки для їх реалізації, такі як цілісність даних та конфіденційність. Цікаво, що безпека та конфіденційність перекриваються, оскільки конфіденційність є проблемою безпеки в деяких контекстах, таких як фінансові операції. Важливо зазначити, що, як вказує рис. 2.3, security та надійність є вимогами до конфіденційності та safety. Якщо відсутні механізми безпеки, зловмисник може порушити конфіденційність, легко збираючи дані, або може змінювати процеси та програми, що призводить до небезпечних умов.

Модель загроз, яку ми розглядаємо для систем IoT, включає як обчислювальні атаки, так і атаки даних. Обчислювальні атаки включають усі шкідливі дії в обчислювальній системі, які впливають на правильне виконання програми та / або призводять до витоку інформації. Атаки даних складають усі атаки на введені або передані дані. Ми розширюємо концепцію атак даних, включаючи помилкові атаки введення даних, які є зловмисним втручанням, які вводять в систему невідповідні (незаконні) дані. Атаки введення неправдивих даних (ПІІ) – це новий клас атак на системи Інтернету речей, які не атакують самі системи Інтернету речей, а вводять неправильні дані в систему управління, щоб призвести до неправильного рішення. У цьому відношенні це переважно атаки безпеки. Наприклад, в системі HVAC атакою введення неправдивих даних буде

введення в систему більш високої температури, а не правильного вимірювання, щоб змусити її знижувати температуру далі. Очевидно, що цей тип атак може призвести до небезпечних умов, які можуть загрожувати процесам і системам, навіть життю людини.

2.2 Безпека систем

Системи IoT – це вбудовані обчислювальні системи, що використовують архітектури, аналогічні загальним. Типова структура системи IoT показана на рис. 6.4, де система містить чотири основні підсистеми: (1) обробка, (2) пам'ять, (3) вхід / вихід та (4) потужність. Взагалі, захищена система вимагає захисту в цілому на додаток до захисту всіх її компонентів окремо. Конкретні вимоги ставляться залежно від операційного середовища та очікуваних можливостей зловмисників. Наприклад, в системі спостереження оптичні датчики (камери) повинні бути захищені індивідуально, але вся мережа повинна працювати динамічно на випадок, якщо окремі камери будуть порушені або зруйновані.

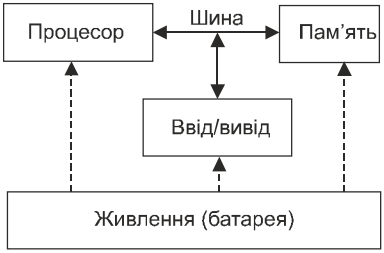


Рис. 2.4. Типова архітектура IoT вузлу

Безпека автономних систем досягається за допомогою декількох рівнів захисту, які включають фізичну та апаратну безпеку, а також надійні обчислювальні платформи. Методи протидії фальсифікації забезпечують різні рівні фізичного захисту, починаючи від доказів фальсифікації і закінчуючи реакцією на фальсифікацію та стійкістю до фальсифікації та застосовуються відповідно до вимог безпеки системи та її робочого середовища. Методи доказів фальсифікацій просто вказують, чи було підроблено пристрій. Методи реагування на фальсифікацію поєднують виявлення фальсифікації та реакцію фальсифікації, де після втручання вживаються відповідні дії; наприклад, вони знищують збережені конфіденційні дані. Методи протидії втручанню запобігають втручанню в пристрої та захищають будь-які конфіденційні дані на пристрої від атак.

Для захисту систем після їх розгортання були розроблені технології проти злому, тому їм потрібно вирішувати фізичні та апаратні атаки зловмисників із змінними можливостями у широкому діапазоні ворожих середовищ, особливо для таких критичних програм, як спостереження. Вони повинні поєднувати як фізичні, так і алгоритмічні механізми. Традиційне шифрування даних, наприклад, сьогодні не є достатнім рішенням для захисту даних, особливо в системах з обмеженими ресурсами, де шифрування можна подолати простими атаками. Атаки бічних каналів змінили атаки на криптосистеми, що використовують фізичні параметри реалізації криптографічних алгоритмів, такі як синхронізація та енергоспоживання, а не атакують самі алгоритми або вводять несправності під час криптографічних обчислень.

Складні апаратні системи, такі як процесори та мікроконтролери, сприйнятливі до фізичних та апаратних атак, подібно до виділених схем, таких як криптографічні схеми. Для захисту від таких атак потрібне спеціальне обладнання, спеціалізовані техніки проектування або навіть нові архітектурні концепції. Наприклад, чутливу програму можна захистити від атак, зберігаючи її в спеціальному дизайні пам'яті лише для виконання, що дозволяє виконувати лише інструкції, що зберігаються в пам'яті, і не допускає будь-яких інших маніпуляцій. Зашифровані шини захищають дані від витоку під час передачі даних між процесором та його пам'яттю. Контроль звернення до кешу може захищати від атак бічних каналів, уникаючи витоку інформації кешу.

Прийоми проти фальсифікації захищають від атак після розгортання системи. Нове бізнес-середовище може ввести вбудовані системи в небезпеку, встановлюючи апаратні трояни на етапі проектування та виготовлення . Вбудовані та кіберфізичні системи, як правило, широко поширені і привернули великий спектр атак. Для захисту від них потрібна комбінація програмного та апаратного забезпечення, щоб охопити всі потенційні атаки. Це особливо важливо в кіберфізичних системах та системах IoT, що включають операційні системи або спеціалізоване проміжне програмне забезпечення. Більш складні програмовані системи вимагають прийняття таких методів, як безпечне завантаження для встановлення цілісності системи, ізоляції процесів та методів атестації рівня процесів для захисту запущених процесів, а також методів перемикання контексту, обробки винятків, міжпроцесорного зв'язку, та управління пам'яттю. Загалом, зростаюча програмованість цих систем вимагає відповідних методів програмного забезпечення. Програмні методи також пропонують вигідну вартість у порівнянні з апаратними. Крім того, поєднання програмних методів з надійними обчислювальними модулями дозволяє розробляти надійні обчислювальні платформи для додатків та послуг.

2.3 Безпека мережі

Для безпечного зв'язку потрібні механізми шифрування та авторизації, а також безпечний метод маршрутизації в мережі. Традиційні схеми шифрування, такі як AES, RSA тощо, забезпечують високий рівень безпеки, що було доведено в обчислювальних системах загального призначення, але вони досить вимогливі до обчислювальних ресурсів та ресурсів пам'яті. Очевидно, що вони стають більш життєздатними кандидатами на прийняття в середовищах, де вбудовані системи отримують збільшені обчислювальні ресурси. Однак сьогодні вони все ще занадто вимогливі до обчислень для більшості вбудованих програм та послуг. Криптографія еліптичної кривої забезпечує перспективне рішення для середовищ IoT, оскільки вимагає менших обчислювальних ресурсів, ніж алгебраїчна криптографія з відкритим ключем, забезпечуючи при цьому високий рівень безпеки. Важливо, що значні зусилля витрачаються на розробку та стандартизацію відповідних алгоритмів для криптографічних примітивів для середовищ IoT з урахуванням їх характеристик. Розробка алгоритму Secure Hash-3 (SHA-3) за допомогою NIST є важливим кроком у цьому напрямку, забезпечуючи сімейство хеш-функцій та розширюваних вихідних функцій, корисних для псевдовипадкового генерування бітів, виведення ключів та цифрових підписів в IoT середовища.

Сенсорні мережі є важливим класом підмереж IoT, що потребують особливої уваги, оскільки вони зазвичай утворюють спеціальні підмережі з великою кількістю вузлів, що мають дуже обмежені обчислювальні ресурси. Таким чином, сенсорні мережеві протоколи часто повинні задовольняти більш суворі вимоги до продуктивності, ніж більш складні вбудовані системи. Ці обмеження, як правило, призводять до сенсорних мереж для реалізації криптографічних механізмів на рівні зв'язку. В таких обмежених середовищах гарною стратегією шифрування є використання механізмів різної складності, залежно від цінності переданої інформації.

Управління ключами є важливою складовою безпечного зв'язку IoT, оскільки ключі є основою криптографічних механізмів. Якщо управління ключами має слабкі сторони, ключі будуть скомпрометовані (розкриті або просочені), що призведе до неефективності будь-якої криптосистеми незалежно від її сили. Використання глобальних ключів зв'язку забезпечує рішення, але такі ключі не можуть бути попередньо визначені в мережевих системах, оскільки безпека мережі може бути легко порушена. Це призводить до необхідності розробляти та застосовувати ефективні методи генерації та розподілу ключів. Існують такі ефективні методи, в основному за допомогою тимчасових глобальних ключів та випадкового розподілу ключів. Один з таких методів використовує тимчасові

глобальні ключі та глобальний постійний ключ для встановлення головного ключа; потім він знищує глобальний ключ, щоб уникнути витоку ключа, тобто основного ризику, який має глобальні ключі. В якості альтернативного підходу можна використовувати випадковий розподіл ключів. У цьому випадку система використовує велику кількість ключів і здійснює зв'язок, вибираючи випадкові підмножини ключів. Коли розміри наборів ключів обрані належним чином, усі кінцеві точки мережі можуть успішно обмінюватися даними.

Мережеві системи, особливо через Інтернет, повинні забезпечувати передачу даних лише між уповноваженими користувачами та процесами, і щоб дані, якими обмінюються, були «законними». Зазвичай це досягається використанням брандмауерів, які зазвичай реалізуються на мережевому та прикладному рівнях, в системах кінцевих точок або в мережевій інфраструктурі. Системи IoT, як правило, мають дуже чітко визначені потреби у спілкуванні, і, отже, брандмауери можна легко налаштувати, щоб дозволити строго обмежений тип законного спілкування. Рішення про те, де слід застосовувати брандмауер, тобто на мережевому або прикладному рівні, на кінцевій системі або в мережі, залежить від системи кінцевих точок, мережі та їх доступних ресурсів, а також від топології мережі . Наприклад, спеціальні мережі потребують захисту на рівні вузлів, тоді як більш централізовані системи можуть більше покладатися на захист мережевого рівня.

Атаки відмови в обслуговуванні (DoS) та розподілені відмови в обслуговуванні (DDoS) є суттєвою загрозою для систем IoT або використання систем IoT. DoS-атаки перевантажують ресурси, такі як процесор, пам'ять та мережа, цільової системи, щоб не дати їй виконати передбачувану функціональність або обслуговувати користувачів.

Загалом існує два основних типи атак DoS. Перший тип атаки використовує вразливості, апаратне чи програмне забезпечення, надсилаючи ретельно побудовані пакети цільовій системі; типовою метою є збій цільової системи. Часто такі вразливості використовуються, оскільки системи не виправлені. Це робить системи IoT особливо вразливими до цих атак, оскільки багато систем IoT не налаштовані на автоматичне оновлення свого програмного забезпечення, а широкий спектр користувачів недостатньо обізнаний про ризики та дії, необхідні для захисту своїх систем відповідно.

У другому типі атак, розподілених відмов у обслуговуванні (DDoS), велика кількість скомпрометованих систем створює величезний обсяг мережевого трафіку до системи жертв; цей трафік також поєднується із законним. Перевантаження сукупного вхідного трафіку в цільовій системі перевантажує її ресурси і робить її нездатною обслуговувати

своїх законних користувачів. Нещодавній інцидент ботнет-атаки Mirai наочно продемонстрував, що пристрої IoT вразливі до введення зловмисного програмного забезпечення, і їх можна ефективно використовувати для запуску DDoS-атак; у справі Mirai вони напали на службу довідників Інтернету, спричинивши значні та дорогі перешкоди підключенню до Інтернету у всьому світі.

DDoS-атаки важко зупинити, оскільки вони використовують спільні мережеві служби, до яких мають доступ усі системи, підключені до мережі. Поточна версія Інтернет-протоколу (IPv4) дозволяє системам надсилати IP-пакети з довільними значеннями у полі вихідної IP-адреси, ускладнюючи виявлення джерел порушуючих IP-пакетів у багатьох атаках. Поточні зусилля щодо захисту від DDoS-атак зазвичай базуються на схемах виявлення вторгнень та зворотного відстеження для виявлення, фільтрації та трасування атаки. У виявленні вторгнень використовуються методи виявлення на основі сигнатур та аномалій, тоді як маркування пакетів та реєстрація пакетів використовуються для зворотного трасування.

2.4 Загальна безпека додатків

Взаємозв'язані системи IoT забезпечують інфраструктуру для розподілених додатків та послуг. В даний час переважна більшість розгорнутих і нових додатків дотримується моделі клієнт-сервер, де віддалені пристрої (клієнти) підключаються до серверів або хмари, загалом, для доставки інформації, таких як зібрані дані та сигнали тривоги. Зазвичай сервери збирають дані, відстежують роботу та процеси підключених до IoT пристроїв та надсилають на пристрої програми керування або дані, щоб відповідно адаптувати їх роботу. Наприклад, медичний пристрій може збирати інформацію про контрольованого пацієнта, доставляти її на централізований сервер і отримувати від сервера інформацію про налаштування, щоб належним чином адаптувати свою роботу, наприклад, змінити частоту зібраних даних або змінити алгоритм, що використовується в локальна обробка даних. Підключений автомобіль може надсилати звіти та сигнали тривоги, пов'язані з роботою двигуна, та отримувати підказку про проведення більш детального тесту на випадок тривоги або підозрілого погіршення даних.

Беручи до уваги нові моделі прикладних програм та послуг, стає зрозумілим, що системи IoT – це розподілені системи, які виконують скоординовані процеси, де кожен процес, як правило, є циклом управління, тобто процесом, який, як правило, отримує дані датчика і передає команди виконавчого механізму. Коли прийнята модель клієнт-сервер, пристрої IoT виконують простіші цикли управління, тоді як сервери виконують ієрархічно операції вищого рівня, коли вони не просто збирають дані.

В Industrial IoT ця ієрархія виражається через програмовані логічні контролери (ПЛК) як локальні, простіші та нижчі рівні пристрої (клієнти) та систему контролю та збору даних (SCADA) як централізовану серверну систему вищого рівня, яка контролює та координує повний контрольований процес.

Виходячи з цієї ієрархічної моделі додатків, ми розглядаємо два рівні розподіленого додатка з метою безпеки. Перший рівень, загальна підтримка безпеки додатків, – це той, який забезпечує загальні послуги для середовища IoT, такі як оновлення та оновлення системи, тоді як другий, процес, – це той, який реалізує конкретний процес для конкретної системи IoT, наприклад , охорона здоров'я, автомобільна, промислова тощо.

Загальна підтримка безпеки додатків включає механізми захисту від атак на розподілену відмову в обслуговуванні, безпечне оновлення тощо. Розподілені рішення про відмову в обслуговуванні використовують механізми на мережевому рівні, як описано в попередньому розділі, розширюючи їх, де це необхідно, включаючи особливості з конфігурації додатка, наприклад, розташування серверів.

Оновлення та виправлення систем IoT є ще однією проблемою, яка вимагає включення механізмів безпеки, оскільки модернізація та виправлення відкритих систем до ризиків безпеки. Функціонал для оновлення та виправлення необхідний з багатьох причин; Потрібно виправити помилки програмного забезпечення, що розгортається, і до функціональних можливостей системи IoT, можливо, доведеться додати нові функції. Однак можливість передачі коду в систему IoT підвищує ризик того, що хтось може атакувати систему, вставляючи шкідливий код замість законного, призначеного коду. Таким чином, до послуг з модернізації повинні бути включені механізми безпеки, щоб гарантувати безпечне та безпечне оновлення систем IoT. Існує кілька підходів до цього виклику. Один може обмежити або запобігти можливості оновлення програмних компонентів, які управляють критично важливими системними ресурсами, у дуже ворожих середовищах програм. Як альтернатива, в безпечніших середовищах можуть застосовуватися суворі механізми контролю доступу, щоб дозволити оновлення різних програмних компонентів різними операторами. Передача мобільного коду може бути заборонена, тоді як дротова передача коду може бути дозволена, коли зв'язок знаходиться в контрольованому середовищі. Загалом, віддалене управління системами, особливо системами IoT з обмеженими ресурсами, вимагає захищеної архітектури, яка враховує операційне середовище, а також профілі потенційних нападників.

2.5 Security та Safety прикладних процесів

Прикладні процеси, такі як процеси управління в промисловому середовищі, – це програми, які виконують необхідний код для обчислення необхідних результатів та реалізації дій процесу. Наприклад, у системі HVAC прикладний процес (програма) може приймати як вхідний запит на підвищення температури контрольованого середовища, і, як результат, він розрахує необхідне збільшення температури витягнутого гарячого повітря та його обсягу та контролюватиме і відповідно відрегулюйте відповідні виконавчі механізми для досягнення результату. У більш складних умовах, таких як інтелектуальна мережа, виявлена потреба або запит на додавання живлення до мережі призведе до розрахунків необхідної потужності, ідентифікації відповідних генераторів для активації та, нарешті, контролю відповідних виконавчі механізми, які додадуть генератори до мережі. Такі процеси застосування в середовищі (I) IoT мають вимоги безпеки, які зазвичай виражаються як властивості, яким потрібно відповідати; наприклад, в системі HVAC температура гарячого повітря повинна бути в межах заданого діапазону температур. Очевидно, що безпека задіяних обчислювальних та мережевих систем є необхідною умовою для виконання вимог безпеки; компрометація цих підсистем може призвести до неправильних розрахунків і, отже, до неправильних дій, що порушують властивості безпеки, яким потрібно дотримуватися.

Забезпечення Security та Safety в середовищах (I)IoT є однією із сфер, де виражається міждисциплінарний характер IoT: вимоги безпеки залежать від застосувань і встановлюються, в більшості випадків, розробкою керованих систем, тоді як Security – передумова Safety – вимагає методів комп'ютерної та мережевої безпеки, оскільки самі системи IoT ефективно розподіляють обчислювальні системи. Поєднання всіх вимог Security та Safety – це виклик, який останнім часом спонукав до багатьох дослідницьких та дослідно-конструкторських робіт і потребуватиме значних зусиль у майбутньому, щоб досягти ефективних рішень, які легко застосовуватись у цій галузі.

Найбільш перспективним інтегрованим підходом до Security та Safety, з точки зору обчислень, є розгляд проблеми як перевірки та моніторингу. Оскільки процеси додатків реалізуються за допомогою програм, а властивості безпеки встановлюються розробниками програм, наприклад, інженерами з управління, можна розглядати процес розробки прикладних програм як такий, де розробники програм надають специфікації програми, включаючи властивості безпеки, а потім відповідно розробляється програмне забезпечення, яке відповідає цим специфікаціям та захищає від загальних уразливостей. Таким чином, проблема безпеки та

безпеки стає проблемою перевірки та моніторингу: по-перше, це перевірка виробленого прикладного програмного забезпечення, тобто, що воно відповідає встановленим вимогам, а по-друге, моніторинг виконання перевіреної програми з метою забезпечення що він не змінений і виконується, як очікувалося, на основі специфікації.

Цей підхід є поведінковим підходом до Security та Safety, оскільки він базується на специфікації процесу подання заявки. У цьому контексті поведінка програми визначається виконуваною специфікацією, яка є початковою точкою підходу, і саме таким чином цей термін використовується в решті цього тексту.

2.6 Надійні та безпечні за дизайном програми IoT

Концепція додатків, захищених дизайном, є розширенням принципу програм правильного побудови, запроваджених півстоліття тому. Проблема, яку ставлять програми IoT, полягає в тому, що системи IoT, як правило, включають кіберфізичну підсистему, яка взаємодіє з навколишнім середовищем. Таким чином, на відміну від оригінальних концепцій, розроблених для поведінкових моделей програм з дискретними та лінійними характеристиками, моделі для кіберфізичних та IoT-систем повинні враховувати безперервні та нелінійні характеристики. Модель навколишнього середовища також необхідна, але складна, оскільки існують невизначені варіації середовища, які впливають на поведінку фізичних підсистем; крім того, необхідно моделювати середовище на різних рівнях абстракції.

Розробка надійних та захищених за проектом додатків привернула увагу кількох зусиль, які зосереджені на розробці ефективних мовних середовищ програмування. Ur / Web – це мова, яка дозволяє розробляти надійні та безпечні веб-програми за дизайном. З міркувань безпеки Ur / Web гарантує, що створений додаток не має вразливостей, таких як атаки введення коду та SQL-ін'єкцій, тоді як для надійності він гарантує, що програма не вийде з ладу під час генерації веб-сторінок, і не буде створювати мертвих посилань внутрішнього застосування тощо. Мова гарантує ці властивості надійності та безпеки завдяки збагаченій системі типу, що базується на залежних. Таким чином, Ur / Web досягає важливого результату: він забезпечує уніфіковану веб-модель, де програміст розробляє веб-додатки на одній мові програмування, які можна скомпілювати до інших веб-стандартів. Ще одним зусиллям мова Дживса зосереджується на виконанні, забезпечуючи примусове забезпечення політики безпеки та гарантуючи, що програми не порушують властивості захисту за задумом. Аналогічні зусилля були докладені для застосування цих підходів у галузі застосування кіберфізичних систем. В рамках ROSCoq працює

асистент перевірки Coq для моделювання кібер- та фізичних ресурсів роботів за допомогою розширеної логіки подій, а потім для доведення різних властивостей моделі. VeriDrone, механізм міркувань, також розроблений у Coq, забезпечує безпеку моделей кібер-фізичної системи на різних, але незалежних рівнях, тобто від моделей високого рівня до реалізацій C.

2.7 Моніторинг стану роботи

Системи моніторингу під час виконання системи безпеки можна класифікувати на основі двох параметрів: (1) метод, що описує поведінку, тобто на основі профілю або моделі, та (2) метод, який порівнює поведінку, тобто відповідність поганій поведінці або відхилення від гарної поведінки. Це призводить до класифікації за чотирма класами, як показано на рис. 2.5.

Рис. 2.5. Класифікація безпеки роботи системи моніторингу

Підходи на основі профілю контролюють параметри спостережуваної системи та будують профіль роботи системи. Системи моніторингу класу 1, які виявляють атаки шляхом зіставлення з поганою поведінкою (Клас 1 на рис.), як правило, використовують статистичні методи та методи машинного навчання для побудови профілів поганої поведінки та статистичних профілів атак. Вони є більш надійними, ніж системи на основі моделей (системи класу 2), оскільки машинне навчання, як правило, узагальнює зібрані дані, але вони страждають від високої частоти помилкових тривог, і вони не надають багато інформації для діагностики, коли спрацьовує тривога. Системи класу 3, які виявляють відхилення від гарної поведінки, зазвичай будують статистичний профіль хорошої поведінки та виявляють відхилення від цього. Ці системи насправді є більш надійними, ніж ті, що є в класі 1, оскільки вони не залежать від будь-яку минулу інформацію про атаки і, отже, вони викликають тривогу при запуску нових атак, оскільки виявляються всі відхилення від гарної

поведінки. Однак вони не тільки надають обмежену інформацію про діагностику, тобто лише те, що сталося щось надзвичайне, але вони страждають від високої частоти помилкових тривог, оскільки відхилення може бути не зловмисним чи випадковим, але це може бути і нормальним явищем, статистично прийнята поведінка профілю.

Модельні системи моніторингу, системи класу 2 та класу 4, використовують модель поведінки контрольованої системи. Такі системи популярні у високозахищеному середовищі, де успішні атаки мають високу вартість. Оскільки вони використовують поведінкову модель спостережуваної системи, ці монітори надають багату діагностичну інформацію, коли спрацьовують тривоги, на відміну від моніторів на основі профілю. Незважаючи на цю багату інформацію, монітори класу 2 обмежені, оскільки вони можуть виявляти лише відомі атаки; це походить від їх моделей поганої поведінки, які вже відомі за визначенням, тобто атаки існують. Типовими прикладами для цього класу є системи на основі підписів. Монітори класу 4 виявляють відхилення від моделі хорошої поведінки і, таким чином, надають ще вищу діагностичну інформацію, оскільки є достатні знання про точну проблему, наприклад, точну інструкцію, яка призвела до виявленого відхилення. Однак накладні витрати на виконання моделей хорошої поведінки створюють обмеження для продуктивності системи.

2.8 ARMET-підхід

Перспективним підходом, який уніфіковано вирішує питання Security та Safety в системах IoT та кіберфізичних системах, є підхід ARMET. ARMET базується на трьох основних концепціях: (1) ми можемо створювати захищені за проектом системи, (2) ми можемо відстежувати функціонування цих систем для виявлення атак або збоїв, і (3) коли є невдача або атака, ми можемо мати плани відновлення, залежно від проблеми та кількості інформації про неї. ARMET був розроблений з акцентом на промислових системах управління, але він застосовний і до інших систем IoT, оскільки їх складність програмного забезпечення порівнянна зі складністю промислових систем управління.

За допомогою підходу ARMET додаток IoT розробляється, починаючи з виконуваної специфікації, яка доказово відповідає властивостям безпеки, встановленим для програми. З цієї виконуваної специфікації отримано код програми. Враховуючи специфікацію виконуваного додатка та код програми для цільової системи, ARMET контролює поведінку програми під час її виконання, порівнюючи спостережувану поведінку із очікуваною поведінкою на основі специфікації програми; для цього проміжне програмне забезпечення виконує виконувану специфікацію

паралельно із виконанням програми в системі IoT та обчислює прогнози поведінки програми. На рисунку 2.6 показана структура проміжного програмного забезпечення ARMET, яка складається з декількох компонентів: (1) монітор безпеки під час виконання, (2) модуль діагностики, (3) модуль відновлення, (4) модель довіри, (5) модуль вибору адаптивного методу та (6) модуль резервного копіювання. Монітор безпеки під час виконання є критично важливим компонентом проміжного програмного забезпечення, який бере як вхідні дані виконувану специфікацію програми та стан системи, яка виконує код програми. Монітор спостерігає за поведінкою виконання програми, і паралельно передбачає стан виконання програми, виконуючи її специфікацію; виконання специфікації визначає очікувану «хорошу поведінку» програми та, за бажанням, відому «погану поведінку» програми, що включає відомі атаки. Порівнюючи прогнози з спостереженнями, монітор може виявити відхилення, які вказують на збій програми або атаку. Коли таке виявлення здійснюється, ARMET переходить до стадії діагностики, щоб ідентифікувати помилку або атаку на основі моделі довіри, яку вона включає. Після завершення фази діагностики вся наявна інформація використовується модулем відновлення. На основі діагностичної інформації модуль відновлення вибирає відповідний адаптивний метод відновлення та дозволяє системі відновлюватися, беручи до уваги попередні стани, що зберігаються модулем резервного копіювання. Важливо зазначити, що система буде працювати за всіх сценаріїв відмов та атак, навіть невідомих, тобто відмов і атак, які не передбачались і не включені в модель довіри. У гіршому випадку, коли модуль діагностики не надає корисної інформації, система відновиться, повернувшись до попереднього чистого стану. Крім того, підхід базується на одному припущенні: специфікація виконуваного додатка виконується в безпечному середовищі і його не можливо атакувати, тобто його прогнози завжди правильні; хоча це може здатися вагомим припущенням, звичайні довірені платформи дозволяють розробляти недорогу платформу IoT, яка відповідає цій вимогі і робить це припущення реалістичним, наприклад, Intel SGX та ARM TrustZone.

Процес розробки виконуваних специфікацій та доведення його властивостей є типовим процесом перевірки програми, який може бути реалізований за допомогою різних існуючих інструментів, що дозволяють автоматизовані або напівавтоматизовані перевірки. У випадку з ARMET, процес заснований на Fiat і використовує дедуктивний синтез для розробки надійних та надійних за проектом програм промислового управління за допомогою інтерактивного поетапного вдосконалення декларативних специфікацій; кібер- та фізичні ресурси включаються як першокласні моделі, а нефункціональні властивості, такі як безпека та

продуктивність, моделюються інтегрованими з функціональними властивостями. Очевидно, що виконувана специфікація може створити автоматично виконуваний код для цільової системи, IoT або промислової.

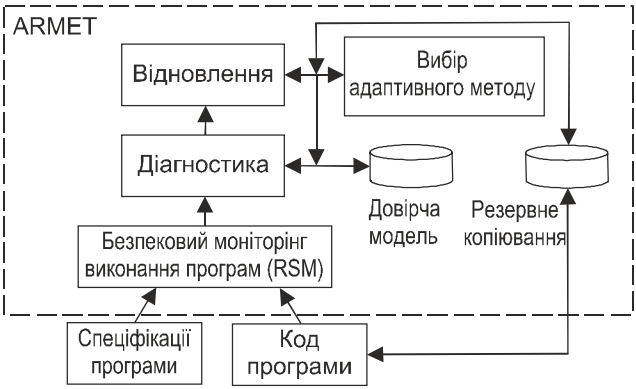


Рис. 2.6. Система ARMET

Монітор безпеки виконання ARMET (RSM) успішно виявляє невідповідність між прогнозами, що виникають при виконанні специфікації, та спостереженнями за виконанням коду програми, завдяки його виконуваній мові специфікації; що важливо, прогнози формуються автоматично. Монітор безпеки під час роботи (RSM) є першим, який офіційно підтверджено як надійний та повноцінний; доказ означає, що на моніторі також відсутні помилкові тривоги (виявлення), що є важливою, бажаною властивістю в практичних системах, де помилкові тривоги призводять до втрати ресурсів, які використовуються для дослідження помилкових тривог. Що важливо, мова специфікації ARMET дозволяє вказувати дефектну поведінку, а також плани атак, які можуть використовуватися системою моніторингу для виявлення загроз.

Підхід ARMET базується на концепції, згідно з якою систему можна вказати за допомогою виконуваної специфікації. На основі відповідної функціональної специфікації для системи можна виразити властивості безпеки та безпеки, яким повинна відповідати система, як умови специфікації, а також включити їх до специфікації. Як приклад, розглянемо випадок з резервуаром для води, який має висоту *h*, як показано на рис. 2.7, і двома насосами, які регулюються, одним для наповнення резервуара водою, позначеним «Насос, що подає», та іншим, «Насос, що викачує», для зливання води назовні; кожен з двох насосів має лише два

можливі стани, тобто відкритий або закритий. Крім того, ми припускаємо, що є датчик, який вимірює висоту води, позначену *wh*, в резервуарі.

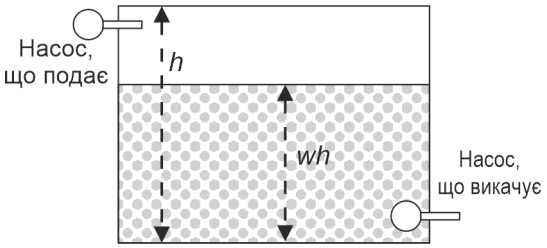


Рис. 2.7. Резервуар з водою

Ми хочемо мати систему управління водою, де користувач видає команди заливати воду або зливати воду з резервуара. Для простоти ми вважаємо, що користувач може виконати три дії: ЗАПОВНЕННЯ, ЗЛИВ або НІЧОГО, і що система працює циклово, синхронно з годинником. Отже, під час кожного циклу (годинниковий тик) може бути виконана одна дія. Дія FILL означає, що «Насос, що подає» відкривається, «Насос, що викачує» закривається, і на цей раз одиниця води заливається в бак. Дія DRAIN означає, що насосі змінюють стан, і на цей раз одиниця води стікає з бака. Коли дія НІЧОГО, тоді обидва насоси закриті, а стан резервуара залишається незмінним. В такому середовищі очевидною властивістю безпеки є те, що ми не хочемо, щоб бак переливався за будь-яких умов.

На рисунку 2.8 показана одна виконувана специфікація, написана на UML, яка реалізує три визначені дії, припускаючи, що кожна дія FILL або DRAIN має в якості параметра ціле значення для змінної water_level, яка визначає цільову висоту води, яку користувач хоче отримати; крім того, специфікація гарантує, що резервуар для води ніколи не переповнюється. У специфікації три дії визначені в переліку: SENSOR_ACCURACY визначає точність вимірювання датчика зчитування рівня води в баку, FILL_RATE – швидкість вхідної води через «Насос, що подає» (in_pump), а DRAIN_RATE – швидкість вихідної води при відкритті «Насосу, що викачує» (out_pump). TANK_MAX – висота *h* резервуара.

Коли користувач видає дію, система спочатку проводить зчитування рівня води за допомогою датчика, як зазначено в readValue, і визначає, чи відрізняється цільова висота води від виміряної висоти в межах точності датчика. Якщо цільова висота інша, то виконується відповідна дія, заливаючи воду або зливаючи воду до досягнення цільової висоти.

Властивість безпеки застосовується через передумову, яка виражається в doAction (), що гарантує, що дія FILL виконується, коли її результат призводить до висоти води, яка менша або дорівнює TANK_MAX.

Оскільки RSM є надійним і повним, доведено, що він виявляє всі обчислювальні атаки на додаток. Це означає, що буде виявлено будь-яку атаку, яка впливає на виконання програми та веде до неправильних розрахунків. Це було підтверджено кількома обчислювальними атаками [27]. Що важливо, RSM також фіксує широкий спектр атак введення неправдивих даних. Наприклад, якщо зловмисник хоче переповнити резервуар для води з прикладу і змінити показання датчика на нижче значення – з метою викликати введення більших обсягів води – RSM визначить атаку, оскільки виконання в специфікації буде розраховано інше значення рівня води, ніж значення, виміряне датчиком. Різниця між очікуваним рівнем води та показником води призведе до виявлення відхилення; це підніме сигнал тривоги і врешті-решт спричинить зупинку дії. Хоча існують складні атаки введення неправдивих даних, які не виявляються RSM, виявлення загальних атак у поєднанні з доказом того, що він виявляє всі обчислювальні атаки, робить поведінковий підхід ARMET потужним інструментом для захисту процесів та програм у просторі IoT.

2.9 Конфіденційність та надійність

Захист конфіденційності є однією з найважливіших проблем у системах IoT через законодавчі вимоги в багатьох областях програм, таких як домашнє середовище, інтелектуальні мережі та системи охорони здоров'я. Зростають обмеження та обмеження щодо збору, зберігання та обробки особистої інформації, залученої до всіх програм, включаючи IoT. Рішення щодо захисту конфіденційності можуть потребувати інтеграції цілого ряду методів і прийомів, таких як обмежене в часі зберігання конфіденційної інформації, системи контролю доступу для забезпечення доступу лише для уповноваженого персоналу, системи бухгалтерського обліку для аудиту тощо. політики та закони додатково збільшується за рахунок збільшення кількості інформації, яка розглядається як особиста чи приватна, що призводить до необхідності адаптивних та масштабованих рішень, що враховують нові політики, коли виникають відповідні законодавчі вимоги. Підхід ARMET забезпечує потужне рішення проблеми захисту конфіденційності, коли захист конфіденційності розглядається як властивість безпеки. Захист конфіденційності походить від законодавчих вимог, які можуть бути виражені як умови в інформаційній системі, тобто вони можуть бути виражені як передумови, післяумови або інваріанти в програмі; наприклад, функція, яка використовується некласифікованими користувачами, може мати обмеження доступу до певних

змінних, які доступні лише для висококласифікованих. З цієї точки зору, вимоги до конфіденційності можуть бути виражені як вимоги безпеки, уточнені в умови та застосовані за допомогою монітора виконання, наприклад RSM, який виявить усі спроби порушити визначені умови. Важливим є те, що програмованість умов дозволяє динамічно регулювати монітори часу роботи, оскільки нові умови встановлюються новою правовою базою.

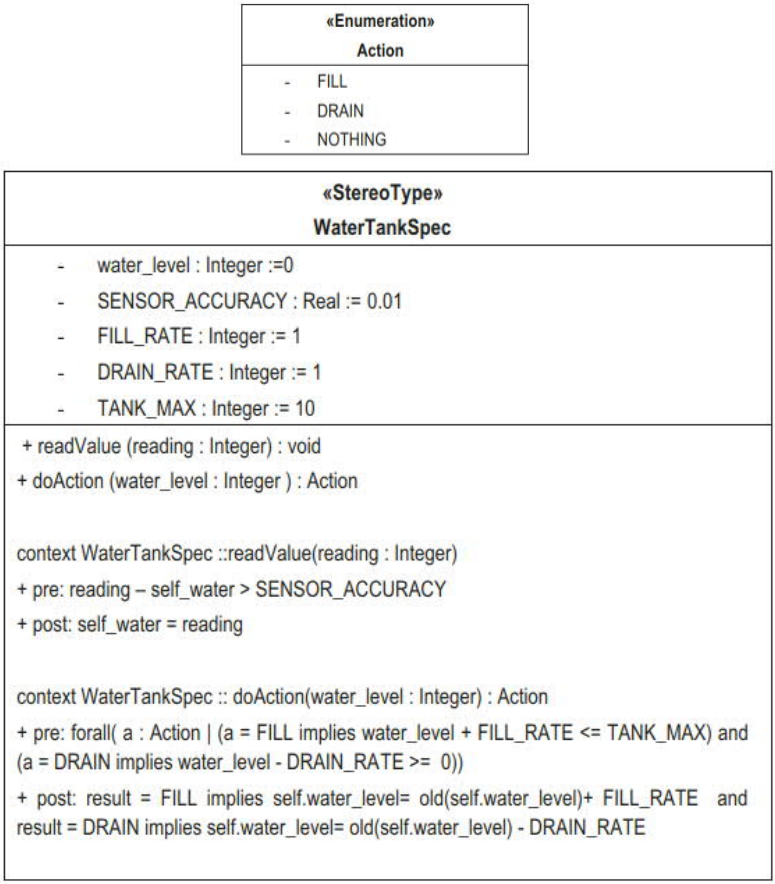


Рис. 2.8. Специфікація для роботи системи контролю ємності для води

Цікаво, що поведінковий підхід до Security та Safety забезпечує перспективне рішення проблеми поєднання надійності та безпеки в одних і

тих же рамках. Надійні системи були розроблені протягом тривалого часу з добре зрозумілими методологіями, але вони базуються на моделях несправностей, які вважають помилки та помилки випадковими. У разі атак безпеки зловмисники спеціально вставляють несправності, і моделі цих несправностей принципово відрізняються від випадкових. Поведінковий підхід до безпеки розглядає лише модель атаки, наприклад, обчислювальну чи помилкову ін'єкцію даних, і на це не впливає її походження – випадковість чи навмисне. Таким чином, він виявляє випадкові несправності та зловмисні атаки тим же методом і однаковим способом. Призначення несправності здійснюється в ARMET, наприклад, лише після виявлення та на основі наявної інформації та використаної моделі довіри. Незалежно від атрибуції, поведінковий підхід виявить проблему, забезпечуючи уніфікований підхід до безпеки та надійності.

3.ДЕЯКІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В IoT

3.1. В чому ще особливості безпеки IoT

IoT – це щось схоже з двосічним мечем. Хоча життя стає набагато простішим, коли у вас є розумний будинок з розумним замком та чайником Wi-Fi, який автоматично кип'ятить воду для вашого ранкового чаю, все це може коштувати вам значно дорожче, ніж зазначено на ціннику. У кібербезпеці IoT є компроміси з безпекою, і, на жаль, вони можуть принести більше шкоди, ніж користі, і майже змусять вас сумувати за часами, коли у вашому телевізорі не було нічого «розумного»!

Подивимось на кілька прикладів, щоб довести важливість безпеки, перш ніж ми запросимо цю технологію в наші будинки, нашу виробничу сферу та повсякденне життя [28].

Як підключені пристрої роблять вас вразливими

Хакери можуть закріпитися у вашій мережі за допомогою найбезпечніших пристроїв у вашій мережі. Ніколь Іган, генеральний директор Darktrace, фірми з кібербезпеки, розповідає про інцидент у неназваному казино в Північній Америці, де зловмисники змогли отримати доступ до бази даних гравців з високими ставками. Вони зробили це, використовуючи вразливість з низьким ризиком у розумному термометрі, який використовувався для контролю температури акваріума.

Але це лише один приклад. Давайте розглянемо ще кілька прикладів порушень безпеки IoT, перш ніж переходити до покажчиків щодо захисту пристрою IoT.

Домашні розумні побутові пристрої

Якщо ви читали звіти про те, як помилки безпеки в розумних помічниках Alexa та Google Home використовувались для фішингу та підслуховування користувачів, скажімо лише, що ви вправі турбуватися. Незважаючи на контрзаходи як Amazon, так і Google, ці пристрої продовжують компрометувати щоразу використовуючи новіші методи.

Окрім цього, є розумний холодильник Samsung, дисплей якого розроблений для інтеграції з календарем Gmail користувачів, щоб вони могли побачити, як виглядає їхній день, перш ніж вирушати з дому. За винятком того, що як би чудово це не звучало, це не зовсім так акуратно. Незважаючи на те, що SSL було розгорнуто для забезпечення інтеграції Gmail, сам холодильник не зміг перевірити сертифікат SSL / TLS, залишивши хакерам відкриті двері для потрапляння в ту ж мережу та крадіжки облікових даних для входу.

На їх честь, Samsung виправила помилку в оновленні програмного забезпечення, але це викликає занепокоєння, коли продукція надійних брендів піддається зламу. Це проливає світло на майже неминучий факт, що найчастіше функціональність має пріоритет над безпекою, навіть у компаніях, які повинні знати краще про проблеми безпеки. Більше того, у 2015 році Samsung також попередила нас про те, як вони збираються збирати та використовувати наші дані у своїй політиці щодо смарт-ТБ: "Будь ласка, майте на увазі, що якщо ваші промовлені слова містять особисту або іншу конфіденційну інформацію, ця інформація буде серед даних, захоплених та переданих третім особам за допомогою розпізнавання вашого голосу".

Слава Богу за Apple, правда? Давайте трохи затримаємося на цій думці. У лютому 2019 року в програмі Apple FaceTime було виявлено серйозну помилку, яка дозволяла зловмисникам отримати доступ до чиєїсь камери iPhone та мікрофона, *перш ніж* вони прийняли або відхилили вхідний дзвінок.

Якщо зловмисники знаходять винахідливі способи ухилитися від контролю безпеки, щоб викрасти дані, завдати шкоди або просто заважати, розумно прикласти більше зусиль на стороні безпеки. Тим не менше, якщо ви все ще любите розумний будинок, ммм ... удачі?

Пристрої IoT використовуються у великих ботнетах, як Mirai

Mirai – це зловмисне програмне забезпечення, орієнтоване на IoT, яке заражає пристрої зі слабкими даними, перетворюючи їх у мережу зомбі або ботів з дистанційним управлінням. Хоча оригінальні творці Mirai були схоплені, вони раніше випустили вихідний код шкідливого програмного забезпечення (можливо, щоб заплутати та відволікти владу), і зараз він має кілька мутацій.

Ботнети були використані для запуску декількох DDoS-атак з атакою на Університет Рутгерса та на Dyn (компанія, яка надає послуги доменних імен таким, як Netflix, Twitter тощо).

Імплантовані медичні вироби

У техніці ніщо не є священним чи пощадженим від лап кіберзлочинців. Сюди входять і медичні вироби.

На конференції Black Hat у 2018 році Біллі Pioc з WhiteScope та Джонатан Баттз з QED Secure Solutions продемонстрували, як медичні імплантати, призначені для порятунку життя пацієнтів, можуть віддалено контролюватися хакерами та маніпулювати ними, щоб завдати необґрунтованої шкоди. Двоє дослідників безпеки продемонстрували, як вони можуть вимкнути інсуліновий насос і взяти під контроль систему кардіостимуляторів, вироблену Medtronic. У відповідь Medtronic спочатку усунув повідомлення про вразливі місця як помилки "низького ризику", не

визнавши серйозності ситуації. Вони відмовились вирішити питання навіть через 570 днів після того, як дослідники вперше подали свої висновки!

Ми можемо годинами міркувати над тим, як мережу дистанційно керованих пристроїв IoT можна використовувати для виведення з ладу електромереж (або систем SCADA, що використовуються на водорозподільних станціях, для управління газопроводами тощо) або незручно звиватися при ідеї, що дитячі монітори будуть зламаний. Але що залишається впевненим, це те, що IoT тут залишається. Таким чином, виробники повинні більш уважно ставитись до ризиків безпеки (передові стійкі загрози [APT] є найбільш небезпечними), якщо ми хочемо уникнути нестримної кризи.

Які найбільші ризики безпеки IoT?

Хоча ми можемо мало говорити з цього питання, ми можемо певною мірою обмежити контроль над своїм життям, вживаючи певних заходів безпеки для захисту наших пристроїв. Фонд відкритих проектів безпеки веб-додатків (OWASP) – це глобальна некомерційна група, яка підвищує обізнаність щодо ризиків безпеки в таких доменах, як безпека вебдодатків, мобільна безпека тощо, щоб приватні особи та організації могли приймати зважені рішення.

У наведеній нижче таблиці перераховані 10 найбільш уразливих місць OWASP IoT, виявлені у смарт-пристроях у 2014 та 2018 роках:

Таблиця 3.1:

OWASP IoT Top 10 – рік 2014 проти року 2018

	Проблеми безпеки IoT 2014	Проблеми безпеки IoT 2018
1	Небезпечний веб-інтерфейс	Слабкі, вгадувані або закодовані паролі
2	Недостатня аутентифікація / авторизація	Небезпечні мережеві послуги
3	Небезпечні мережеві послуги	Небезпечні екосистемні інтерфейси
4	Відсутність транспортного шифрування / перевірки цілісності	Відсутність механізму безпечного оновлення
5	Проблеми конфіденційності	Використання небезпечних або застарілих компонентів (НОВЕ)
6	Небезпечний хмарний інтерфейс	Недостатній захист конфіденційності
7	Небезпечний мобільний інтерфейс	Небезпечна передача та зберігання даних

8	Недостатня конфігурація безпеки	Відсутність управління пристроями
9	Небезпечне програмне забезпечення / прошивка	Небезпечні налаштування за замовчуванням (НОВЕ)
10	Погана фізична безпека	Відсутність фізичного захисту

3.2. 10 найкращих порад щодо безпеки IoT для вашої організації

Якщо ваш смарт-пристрій оснащений незмінними даними або будь-яким типом механізму автентифікації / авторизації, зробіть собі величезну послугу і не купуйте його! Як ви можете бачити зі списку вразливостей OWASP Top 10 Internet of Things 2018, кілька проблем, таких як незахищені екосистеми (веб-інтерфейс, хмарний інтерфейс тощо), безпека даних та фізична безпека зберегли свої 10 найкращих позицій за попередній 2014 рік список. Це дає нам уявлення про напрямок і швидкість, з якою рухається безпека пристрою IoT. Це також порушує відповідні питання щодо ефективності та рівня прийняття рішень безпеки IoT.

Однак оскільки IoT стає такою невід'ємною частиною нашого повсякденного життя, і ми повинні зробити все можливе, щоб захистити наші підключені пристрої, наші дані та наші мережі. Ось кілька способів, як це зробити:

3.2.1. Знайте свою мережу та підключені пристрої у ній

Коли ваші пристрої підключаються до Інтернету, ці з'єднання роблять всю мережу вразливою та відкритою для зловмисників, якщо пристрої не забезпечені належним чином. Оскільки все більше пристроїв оснащується веб-інтерфейсами, легко втратити відстеження того, які з ваших пристроїв доступні по дроту. Для забезпечення безпеки важливо знати свою мережу – пристрої в ній та тип інформації, яку вони можуть розкривати (особливо якщо відповідні додатки мають функції соціального обміну).

Кіберзлочинці використовують таку інформацію, як ваше місцезнаходження, ваші особисті дані тощо, щоб стежити за зами – що може призвести до реальної небезпеки.

3.2.2. Оцініть пристрої IoT у вашій мережі

Дізнавшись, які пристрої підключені до вашої мережі, перевіряйте свої пристрої, щоб зрозуміти їхню безпеку. Безпека Інтернету речей може бути реалізована шляхом своєчасного встановлення виправлень безпеки та оновлень із веб-сайту виробника, перевірки на наявність нових моделей із посиленими функціями безпеки тощо. Крім того, перед здійсненням покупки прочитайте, щоб зрозуміти, наскільки пріоритетним є безпека для цього бренду. Запитайте себе:

Чи повідомляє будь-який з його продуктів помилки безпеки, які спричинили порушення?

Чи задовольняє компанія потреби у кібербезпеці, розкладаючи продукти потенційним клієнтам?

Як впроваджуються засоби контролю безпеки в їх розумні рішення?

3.2.3. Застосовуйте надійні паролі для захисту всіх своїх пристроїв та облікових записів

Використовуйте надійні, унікальні паролі, про які не важко здогадатися, щоб захистити всі ваші облікові записи та пристрої. Позбудьтесь паролів за замовчуванням або загальних паролів, таких як «адміністратор» або «пароль123». За потреби скористайтеся менеджером паролів, щоб відстежувати всі ваші паролі. Переконайтеся, що ви та ваші співробітники не використовуєте однакові паролі для кількох облікових записів, і обов'язково періодично їх змінюйте.

Ці кроки допомагають запобігти злому всіх ваших облікових записів, навіть коли один із них надає будь-яку конфіденційну інформацію про обліковий запис. Окрім дати закінчення терміну дії пароля, не забувайте також встановити обмеження на кількість помилкових спроб введення пароля та впровадити політику блокування облікового запису.

3.2.4. Використовуйте окрему мережу для своїх розумних пристроїв

Використання окремої мережі, ніж ваша домашня чи ділова мережа, для ваших інтелектуальних пристроїв є, мабуть, одним із найбільш стратегічних підходів до безпеки IoT. Завдяки сегментації мережі, навіть якщо зловмисники знаходять шлях до ваших смарт-пристроїв, вони не можуть отримати доступ до ваших ділових даних або пронюхати той банківський переказ, який ви зробили з вашого персонального ноутбука.

3.2.5. Змініть параметри пристрою які були встановлені за замовчуванням

Найчастіше багато наших розумних пристроїв постачаються з незахищеними налаштуваннями за замовчуванням. Що ще гірше, іноді ви не можете змінювати ці конфігурації пристрою! Слабкі облікові дані за замовчуванням, нав'язливі функції та дозволи, відкриті порти тощо повинні бути оцінені та переналаштовані відповідно до ваших вимог.

3.2.6. Встановіть брандмауери та інші авторитетні рішення безпеки IoT для виявлення вразливостей

Встановіть брандмауери, щоб блокувати несанкціонований трафік по дроту та запускати системи виявлення вторгнень / системи запобігання вторгненню (IDS / IPS) для моніторингу та аналізу мережевого трафіку. Ви також можете використовувати автоматичні сканери

вразливостей, щоб виявити слабкі місця у вашій мережевій інфраструктурі. Використовуйте сканер портів, щоб визначити відкриті порти та переглянути мережеві служби, які працюють. Встановіть, чи ці порти абсолютно потрібні, та вивчіть служби, що працюють на них, на наявність відомих вразливостей.

3.2.7. Використовуйте надійне шифрування та уникайте підключення через небезпечні мережі

Якщо ви вирішили перевірити свої смарт-пристрої віддалено, ніколи не робіть цього за допомогою загальнодоступних мереж Wi-Fi або мереж, які не використовують надійних протоколів шифрування. Переконайтеся, що власні налаштування мережі не працюють за застарілими стандартами, такими як WEP або WPA – замість цього використовуйте WPA2. Небезпечні з'єднання з Інтернетом можуть залишати ваші дані та пристрої підданими зловмисникам. Хоча сам WPA2 виявляється уразливими для ключових атак переустановлення або Krack і WPA3 схильне Dragonblood атак, установка оновлень і виправлення є єдиним способом, щоб рухатися вперед, приймаючи мінімальний рівень ризику.

3.2.8. Відключіть пристрої та функції, коли вони не використовуються

Перегляньте дозволи додатків і прочитайте політику конфіденційності цих програм, щоб зрозуміти, як вони збираються використовувати інформацію, якою ви ділитесь. Вимкніть такі функції, як віддалений доступ, голосове управління тощо, якщо ви не використовуєте їх для здійснення більш чітких перевірок безпеки Інтернету речей. Ви завжди можете їх увімкнути, якщо і коли виникає необхідність. Коли ви не використовуєте свої пристрої, подумайте про те, щоб взагалі відключити їх від мережі.

3.2.9. Вимкніть Universal Plug and Play (UPnP)

Незважаючи на те, що універсальний plug and play розроблений для безперебійної роботи з мережею без клопоту з конфігурацією, він також полегшує виявлення цих самих пристроїв для хакерів за межами вашої локальної мережі через вразливості протоколу UPnP. UPnP увімкнено за замовчуванням на декількох маршрутизаторах, тому перевірте свої налаштування та переконайтеся, що його вимкнено, якщо ви не бажаєте порушити свою безпеку заради зручності.

3.2.10. Бережіть свої пристрої в безпеці, застосовуючи фізичну недоторканість

Постарайтеся не втратити свої телефони, особливо якщо на ньому завантажені програми, які контролюють ваші пристрої IoT! Якщо у вас є, крім того, що на вашому пристрої є PIN-код / пароль / біометричний захист, переконайтесь, що у вас є можливість віддалено стерти телефон.

Налаштуйте автоматичні резервні копії або вибірково створюйте резервні копії даних пристрою, які можуть вам знадобитися

Крім того, обмежте доступ своїх смарт-пристроїв. Наприклад, чи потрібен для вашого холодильника порт USB? Надайте доступ до мінімальної кількості портів і подумайте про відсутність доступу до Інтернету (лише локальний доступ) там, де це можливо.

Інструменти аналізу безпеки IoT

Окрім розглянутих раніше рішень безпеки IoT, є ще кілька інструментів, які можна використовувати для кращої видимості та контролю над вашою мережею. Wireshark та tcpdump (утиліта командного рядка) - це два інструменти з відкритим кодом, які можна використовувати для моніторингу та аналізу мережевого трафіку. Wireshark є більш зручним для користувача, оскільки він постачається з графічним інтерфейсом і має різні варіанти сортування та фільтрації.

Shodan, Censys, Thingful та ZoomEye – це інструменти, які ви можете використовувати (наприклад, пошукові системи) для пристроїв IoT. ZoomEye – це, мабуть, найпростіший спосіб з'ясувати для нових користувачів, оскільки пошуковий запит створюється автоматично при натисканні на фільтри.

ByteSweep, безкоштовна платформа аналізу безпеки для виробників пристроїв, – ще один інструмент, який тестери можуть використовувати для запуску перевірок перед відправкою будь-якого продукту.

Резюме – безпека IoT. Незалежно від ризиків, зрозуміло, що технології IoT мають величезний потенціал. Впровадження IoT продемонструвало корисність для вирішення проблем усіх типів налаштувань та завдань, таких як допомога в житті, моніторинг навколишнього середовища, моніторинг стану здоров'я тощо. Проблема виникає, коли компанії поспішають стати найбільш «модними» і, дряпаючись на вершини, вони або взагалі не розглядають потенційних ризиків для безпеки, або не сприймають це досить серйозно.

Більш послідовні та щирі зусилля щодо розробки безпечних та надійних продуктів, підвищення обізнаності серед споживачів та проведення ретельного тестування перед випуском пристроїв можуть значною мірою вирішити багато проблем, які в даний час є скоріше результатом нехтування, ніж відсутністю навичок.

ВИСНОВКИ

Готові ви чи ні, IoT вже є частиною порядку денного підприємств та вашої оселі. Завдяки досягненням мережевих технологій контроль над підключеними пристроями став активною загрозою для людей та підприємств. Тепер команди з кібербезпеки повинні тримати руку на пульсі ботнетів, фішинг-шахрайства, недоліків IAM та безлічі інших засобів, які кіберзлочинці можуть легко використовувати для підключення пристроїв IoT.

Поширення всього, що є «розумним», викликає величезні загрози безпеці. У процесі збільшення кількості пристроїв IoT поверхня атаки різко розширюється. Тим часом, чи можуть команди безпеки встигати за зміною? Чи можуть вони гарантувати, що пристрої шифрують дані або що адміністратори регулярно проводять виправлення / оновлення апаратного та програмного забезпечення? Чи знають громадяни, які користуються пристроями IoT про правила безпечного користування?

На тлі цього величезного зростання та простоти доступу є очевидні проблеми безпеки: пристрої обмежені у витратах та обмежені ресурсами. Особи, що контролюють IoT, насправді можуть бути погано підготовлені для управління колекцією пристроїв. Це може бути навіть набір навичок – це означає, що членам команди не вистачає навичок, інструментів або знань, щоб керувати цим зв'язком.

Є впевненість у тому, що все більше і більше цих продуктів буде потрапляти до нашого середовища життя та діяльності – впорядковуючи зусилля людей та підвищуючи зручність і ефективність. Але складно визначити, скільки людей та підприємств буде надійно застосовувати IoT.

Тому видно важливість та перспективність підготовки відповідних фахівців у галузі безпеки IoT.

Список використаної літератури

1. Інформаційна безпека: навч. посібник /Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарев та ін; за заг. ред. Ю.Я. Бобало та І.В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019.–580 с.
2. M.-H. Maras, Internet of Things: security and privacy implications International. / Data Privacy Law, 2015, Vol. 5, No. 2. P/99-104
3. S. Tweneboah-Koduah, K. E. Skouby, R. Tadayoni, Cyber Security Threats to IoT Applications and Service Domains. Wireless Pers Commun. Springer Science+Business Media New York 2017. DOI 10.1007/s11277-017-4434-6
4. Carsten Maple (2017) Security and privacy in the internet of things, Journal of Cyber Policy, 2:2, 155-184, DOI: 10.1080/23738871.2017.1366536
5. Abomhara, Mohamed and Geir M. Køien. "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks." J. Cyber Secur. Mobil. 4 (2015): 65-88. DOI:10.13052/JCSM2245-1439.414
6. B. Schneier, Secrets and lies: digital security in a networked world. John Wiley & Sons, 2011.
7. J. M. Kizza, Guide to Computer Network Security. Springer, 2013.
8. N. R. Prasad, "Threat model framework and methodology for personal networks (pns)," in Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conf. on. IEEE, 2007, pp. 1–6.
9. G. Xiao, J. Guo, L. Xu, and Z. Gong, "User interoperability with heterogeneous iot devices through transformation," 2014.
10. I. Cha, Y. Shah, A. U. Schmidt, A. Leicher, and M. V. Meyerstein, "Trust in m2m communication," Vehicular Technology Magazine, IEEE, vol. 4, no. 3, pp. 69–75, 2009.
11. M. Rudner, "Cyber-threats to critical national infrastructure: An intelligence challenge," International Journal of Intelligence and Counter Intelligence, vol. 26, no. 3, pp. 453–481, 2013.
12. В.Г. Крижановський, С.П. Сергієнко Енергоефективні пристрої інтернету речей (IoT): навчально-методичний посібник./ Вінниця: ДонНУ імені Василя Стуса, 2020. 63 с.
13. M. Thoma, S. Meyer, K. Sperner, S. Meissner, and T. Braun, "On iot-services: Survey, classification and enterprise integration," in Green Computing and Communications (GreenCom), 2012 IEEE International Conference on. IEEE, 2012, pp. 257–260.
14. G. M. Koien and V. A. Oleshchuk, Aspects of Personal Privacy in Communications-Problems, Technology and Solutions. River Publishers, 2013.
15. C. Tankard, "Advanced persistent threats and how to monitor and deter them," Network security, vol. 2011, no. 8, pp. 16–19, 2011.

16. I. Cervesato, “The dolev-yao intruder is the most powerful attacker,” in 16th Annual Symposium on Logic in Computer ScienceLICS, vol. 1. Citeseer, 2001.
17. Tweneboah-Koduah, S., Skouby, K.E. & Tadayoni, R. Cyber Security Threats to IoT Applications and Service Domains. *Wireless Pers Commun* **95,** 169–185 (2017).
18. Matuszak, G., Bell, G., & Le, D. (2015). Security and the IoT ecosystem. KPMG, December 2015, 132631–G.
19. Ashton, K. (2009). That ‘Internet of Things’ thing. RFID Journal, 22, 97–114.
20. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279.
21. Vermesan, O., Friess, P. (2013). Internet of Things: Converging technologies for smart environments and integrated ecosystems. Alborg: River Publishers.
22. Quashie Azasoo, J., & Tweneboah-Koduah, S. (2016). Cybersecurity architecture in smart metering systems. In Smart living and privacy. Unpublished paper. CMI Annual Conference, Copenhagen, Denmark.
23. Bolhuis M. Using an NFC-equipped mobile phone as a token in physical access control. Thesis… University of Twente, 2014. 129 p. http://essay.utwente.nl/65419/1/thesis_nfc_martijn_bolhuis_final.pdf
24. Крижановський В.Г. Зв’язок у близькому полі (Near field communication): Методичний посібник. Вінниця: ДонНУ ім. Василя Стуса, 2018.– 32 с.
25. Чернов Д.В., Кацан М.Р., Сергієнко С.П., Крижановський В.Г. Випромінювання вищих гармонік NFC-пристроєм та його влив на безпеку транзакцій // Матеріали X Міжн. науково-практичної конф. “ІНФОКОМУНІКАЦІЇ – СУЧАСНІСТЬ ТА МАЙБУТНЄ”, присвяченої сторіччю Одеської національної академії зв'язку ім. О.С. Попова, 16-19 листопада 2020 року, ОНАЗ ім. О.С. Попова, м. Одеса 2020, с. 434-437
26. D. Serpanos, M. WolfInternet-of-Things (IoT) Systems. Architectures, Algorithms, Methodologies. Springer Int. Publishing AG 2018. 94 p.
27. Khan, M. T., Serpanos, D., & Shrobe, H. ARMET: Behavior-Based Secure and Resilient Industrial Control Systems. In Proceedings of the IEEE, Preprint. URL: http://ieeexplore.ieee. org/stamp/stamp.jsp?tp=&arnumber=8011473&isnumber=4357935
28. Lumena Mukherjee. 10 IoT Security Tips You Can Use to Secure Your IoT Devices. https://sectigostore.com/blog/10-iot-security-tips-you-can-use-to-secure-your-iot-devices/ 6.01.2021.

Зміст