Бойко Віктор Дмитрович
Національний університет «Одеська юридична академія»,
кандидат технічних наук, доцент кафедри кібербезпеки

Василенко Микола Дмитрович,
Національний університет «Одеська юридична академія»,
в.о. завідувача кафедри кібербезпеки,
доктор фізико-математичних наук, професор

ВІДКРИТІ СИСТЕМИ І ПРОТОКОЛИ ВЗАЄМОДІЇ В КОНТЕКСТІ КІБЕРБЕЗПЕКИ «РОЗУМНОГО МІСТА»

Останнім часом отримали популярність концепції розвитку «розумного міста». Існує кілька різних визначень цього терміну (див. [1]). Така ситуація пояснюється тим, що сфера питань впровадження ІТ-технологій у практику урбаністики є порівняно молодою. Сам по собі термін «розумне місто» має кілька різних визначень і перетинається з близькими за значенням термінами («цифрове місто», «інтелектуальне місто» і так далі) – детально еволюцію терміну можна простежити по роботі [2].

В якості точки відліку виникнення ідеї «розумних міст» зазвичай вказують книгу [3], в якій був використаний термін «розумне зростання» («smart growth»). Пізніше, термін «розумне місто» («smart city») був запропонований в роботі [4], який по сути є подальшим розвитком [5].

Теперішня концепція «розумного міста» бачиться як точка сходження декількох паралельних процесів, при якій інтеграція міських інформаційно-комунікаційних систем виходить на новий рівень. З таких тенденцій можна виділити наступні:

- насичення населення індивідуальними засобами комунікації (персональні комп'ютери, смартфони, планшети),
- розвиток загальноміських комунікаційних мереж (високошвидкісний мобільний інтернет),
- розвиток інтелектуальних систем управління виробництвом (АСУ ТП / ISC),

- розвиток «Інтернету речей» (IoT),
- поява інтегральних загальноміських мереж управління і спостереження за трафіком,
- поява «розумних квартир» і «розумних будинків».

В цілому, щбільшення насиченості ІТ міською інфраструктурою має в майбутньому привести до якісної переходу від розрізнених «цифрових островів» до «цифровим кластерів», а від них до «розумних міст». Накопичення цифрових технологій призведе до переходу кількості в якість і в майбутньому можна буде говорити про «розумне місто», як про цілісну, єдину інформаційну екосистему (див. [6]), в якій Інформаційні технології відіграють ключову роль.

При цьому такий перехід здійснюється самопливом, без централізованої стратегії, з некваліфікованим персоналом. Нові технології часто впроваджуються і розгортаються без жодного тестування на безпечність. Розробники віддають перевагу простоті і легкості розгортання безпеки системи. Це призводить до збільшення потенційних ризиків і загроз як інформаційній інфраструктурі розумного міста, так і функціюванню (а іноді і існуванню) розумного міста в цілому.

Відсутність єдиної міської служби кібербезпеки призводить до того, що інциденти в різних ділянках міської та суміжних інфраструктур, обробляються запізно і без загальної координації.

Технічна підтримка систем «розумного міста» утруднена і часто запізнюється. Як було зазначено вище розробники промислових та інфраструктурних інформаційних систем часто запізнюються з реакцією на нові загрози. Причини такої ситуації можна розділити на суб'єктивні і об'єктивні. До суб'єктивних, наприклад, може бути віднесений погляд розробників на міські та промислові системи, як на менш пріоритетні і другорядні в порівнянні з очевидними мішенями для атак, наприклад з фінансово-банківським сектором. Відповідно, на стадії розробки менше уваги і ресурсів приділяється забезпеченню безпеки і захисту від вторгнень.

Можна виділити кілька джерел потенційних загроз і ризиків для міської інформаційно-комунікаційної інфраструктури, які існують вже зараз і будуть наростати в майбутньому.

Глибока інтеграція міських інформаційно-комунікаційних систем – від смартфона рядового користувача до системи управління міським електротранспортом і АСУ ТП системи енергопостачання – потенційно збільшує «поверхню атаки» для зловмисників. Кожен доданий в систему елемент має свої власні уразливості, при цьому його інтеграція в загальний простір «розумного міста» означає, що зловмисник, використовуючи ці уразливості, може отримати доступ до загальноміської інфраструктури ([7]). Загальна складність системи призводить до того, що атака може породжувати різні види «ланцюгових реакцій», коли вихід з ладу одного сегмента (наприклад, управління міською енергосистемою) може вивести з ладу суміжні сегменти (наприклад, систему управління дорожнім рухом).

У більшості впроваджуваного апаратно-програмного забезпечення постійно знаходять уразливості. При цьому процес усунення сильно уповільнений і розтягнутий у часі в порівнянні з призначеним для користувача програмним забезпеченням – це особливо стосується пропрієтарного програмного забезпечення, підтримка якого здійснюється розробником без участі спільноти («community»), а значить свідомо відстає від виявлення нових загроз.

Непропорційно великий сегмент технологій покладається на бездротові рішення. При цьому існує досить багато різних протоколів взаємодії, далеко не всі з яких відповідають стандартам безпеки. Така ситуація полегшує зловмиснику доступ до об'єкта атаки, відкриває додаткові уразливості в інформаційних системах, ще сильніше розширюючи поверхню атаки.

Великою проблемою є широке використання неефективних технологій, зокрема побудованих за принципом «secure by obscure», а також таких, що використовують «повітряний зазор» як виключний засіб захисту. Дослідження атаки Stuxnet

показує, що сучасне шкідливе програмне забезпечення досить легко долає «повітряний зазор» («air gap»).

Поширеною практикою є USB Drop attack – коли зараження відбувається через флеш-накопичувачі, вільно або мимоволі підключаються до системи. Один з варіантів такого зараження навіть передбачає використання спеціального пристрою для атаки. Такий пристрій замасковано під звичайний флеш-накопичувач, проте всередині містить іншу апаратну начинку, яка спрацьовує при підключенні «помилкової флешки» в usb-порт. Таким чином, в сучасних реаліях навіть повне відключення від зовнішніх мереж зв'язку не гарантує безпеку. При цьому прагнення до створення air gap часто призводить до зниження загальної ефективності системи і підвищення витрат на її експлуатацію. Це особливо актуально для «розумного міста», де більшість систем розраховані на збір і обробку інформації в оперативному режимі і втрачають цінність для «офлайнових» контекстів. У цьому випадку організація «air gap» створює більше проблем, ніж вирішує.

Також до об'єктивних загроз належать, наприклад, складнощі з експлуатацією вже впроваджених інформаційних систем, які забезпечують експлуатацію критичних ділянок інфраструктури. Зупинка або перебої в таких системах через невдале оновлення можуть спричинити значні збитки, якщо не матеріальні втрати. Тому, оновлення систем виконується рідко і з оглядкою на можливі наслідки.

Додатковим джерелом загроз є наявність в загальній системі ділянок, що обслуговуються застарілими системами з незакритими вразливостями. Заміна таких систем зазвичай відкладається до тих пір, поки не окупляться вкладення або поки в бюджеті не з'являться кошти. При цьому їх розробники можуть вже давно зняти системи з обслуговування – а це означає, що для виявлених в процесі експлуатації вразливостей і помилок не буде випущено оновлень. При цьому, завдяки загальній інтеграції систем «розумного міста», наявність в структурі

«острівців архаїки» піддає ризику не тільки ці ділянки самі по собі, але і відкриває зловмиснику шлях до інших систем.

Чисто технічні джерела ризиків і загроз, доповнюються проблемами на організаційному рівні – відсутністю в міській структурі Єдиного центру реагування на кіберзагрози інфраструктурі, загальною бюрократизацією процесу, низькою кваліфікацією обслуговуючого персоналу, закритістю міських систем для спільноти розробників.

Вихід з ладу об'єктів інфраструктури може бути як результатом цілеспрямованої (таргетованої) атаки зловмисника (Stuxnet), так і побічним ефектом від загальної глобальної атаки на інформаційну систему. Прикладом останнього є епідемія WannaCry і Petya, які, поширившись по комп'ютерних мережах «зачепили» банківський сектор і енергетику.

Перераховані вище джерела загроз означають, що подолання захисту таких систем – питання часу. При цьому додаткову небезпеку становить те, що з деякого моменту часу намітився тренд, при якому все більше атак інтелектуальних систем проводиться не з метою самоствердження зловмисника, а з метою заробітку грошей на наслідках подолання захисту.

Об'єктом атак дедалі частіше стають об'єкти промислової та міської інфраструктури. На такі атаки з'явився попит, а це свідчить в найближчому майбутньому, що можна очікувати значне збільшення пропозиції (див. [8] і оцінку у [9]).

При цьому метою таргетованої атаки не обов'язково повинно бути виведення з ладу будь-якого об'єкта або керівної системи. Все більше атак робиться для отримання приватної і не підлягаючої розголошенню інформації (наприклад після атаки на Korea Hydro & Nuclear Power Co., Ltd. (KHNP), зловмисники отримали доступ до креслень та інструкцій для атомних реакторів [10]).

Пропрієтарні, закриті вихідні коди, протоколи взаємодії і формати даних виглядають досить логічним рішенням особливо у випадках, коли розробник бере на себе поставку і розгортання системи «під ключ», а також забезпечує подальшу

технічну підтримку, проте на практиці породжують цілий спектр проблем.

Перша з них – «vendor lock-in» – прагнення постачальників послуг замкнути клієнта на себе, монополізувавши надання послуги. Це відкриває розробнику можливість надалі вносити небажані і невигідні зміни в умови поставки послуги. Як правило, на цьому етапі в організацію і розгортання системи вже вкладені досить великі кошти, тому відхід від розробника стає невигідним, що змушує миритися з новими умовами.

Друга – можлива наявність «чорних ходів» («backdoors»). Широко поширена практика, коли розробник залишає в системі «чорний хід» – свідомо ослаблене місце в системі, про який відомо тільки розробнику і яке розробник може використовувати для технічної підтримки за запитом клієнта – наприклад для відновлення втрачених клієнтом ключів для входу в систему або випадково видалених даних. Зазвичай офіційно декларується саме ця причина.

Однак, на практиці, в системах із закритим вихідним кодом наявність «бекдорів» залишається прихованим і їх експлуатація розробниками ніяк не може бути проконтрольована, що відкриває перед розробником широкі можливості для збору конфіденційної інформації та експлуатації системи в своїх інтересах.

Третя проблема полягає в тому, що «бекдор» відносно легко може бути виявлений при аналізі системи зловмисником – і використаний ним у своїх цілях. Багато зломів засновані саме на використанні свідомо закладених в систему розробником (самостійно або на вимогу клієнтів) вразливостей.

Таким чином сучасні тренди вказують на висхідний інтерес зловмисників до «розумних міст», при цьому самі системи «розумного міста» ще недостатньо відповідають вимогам безпеки та захисту від зовнішніх загроз. При розробці, плануванні впровадженні та розгортанні «розумного міста» треба передбачати комплексну систему захисту, яка відповідала б вимогам відкритості, розширюваності та децентралізації й не

покладалася б на застарілі та неефективні методи захисту («air gap», пропрієтарні протоколи, «secure by obscure» і так далі). На наш погляд цим вимогам відповідає широке використання програмного забезпечення з відкритими вихідними кодами, що використовує відкриті стандарти зберігання, передачі й перетворення інформації та широко залучає сучасні криптографічні засоби (асиметричну криптографію з відкритими ключами) і засоби забезпечення цілісності та децентралізації зберігання даних (блокчейн).

Використання відкритих стандартів для «розумного міста» і для його систем безпеки не тільки полегшує загальну внутрішню організацію міських підсистем – «розумних будинків», підприємств, транспорту, міської інфраструктури та окремих пристроїв, але і потенційно робить можливим створення «розумних регіонів», «розумних країн» і так далі – за аналогією з наявними зараз телефонними та інформаційними мережами. На прикладі телефонних та інформаційних мереж можна показати, що збільшення розмірів і охоплення мережі підвищує як загальну цінність, так і цінність окремих її сегментів.

Перераховані вимоги можуть здатися досить жорсткими, але в принципі досяжні на поточному рівні розвитку інформаційних технологій. Існують і досить поширені відкриті системи і протоколи взаємодії. При цьому основний шлях захисту даних у відкритих системах в даний час бачиться у використанні засобів асиметричної криптографії з відкритими ключами – можна послатися на класичний приклад PGP/GnuPG, однак зразковою реалізацією такої системи на наш погляд є специфікація шифрування носіїв LUKS, яка дає приклади хорошої організації захисту даних і зручного для користувача управління ключами.

Список використаної літератури:

1. Perätalo S., Ahokangas P. (2018). Toward smart city business models. Journal of Business Models. Vol. 6, no. 2, 65–70.

2. Cocchia A. (2014). Smart and digital city: A systematic literature review. Smart city, 13–43.

3. Bollier D. (1998). How smart growth can stop sprawl: A fledgling citizen movement expands. Essential Books, 90.

4. Komninos N. (2006). The architecture of intelligent cities. Intelligent Environments. – IET, Vol. 6. 53–61.

5. Schuler D. (2001). Digital cities and digital citizens. Kyoto workshop on digital cities, 71–85.

6. Deren L., Zhenfeng S., Xiaomin Y. (2011). Theory and practice from digital city to smart city [j]. Geospatial Information, Vol. 6, 002.

7. Cerrudo C. (2015). Hacking smart cities. RSA conference, 2–18.

8. Zygiaris S. (2013). Smart city reference model: Assisting planners to conceptualize the building of smart city innovation ecosystems. Journal of the knowledge economy, Vol. 4, no. 2, 217–231.

9. Friis K., Muller L. P., Gjesvik L. (2018). Cyber-weapons in international politics: Possible sabotage against the norwegian petroleum sector. NUPI Report. Retrieved from https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2486814/NUPI_Report_2018–3.pdf

10. Lee K.-b., Lim J.-i. The reality and response of cyber threats to critical infrastructure: A case study of the cyber-terror attack on the korea hydro & nuclear power co., ltd. // KSII Transactions on Internet & Information Systems. – 2016. – Vol. 10, no. 2. – P. 857–880.

11. Bossi, S., & Visconti, A. (2015, December). What users should know about full disk encryption based on LUKS. In *International Conference on Cryptology and Network Security* (pp. 225–237). Springer, Cham.

12. Visconti, Andrea, et al. (2019). «Examining PBKDF2 security margin – Case study of LUKS.» *Journal of Information Security and Applications* 46: 296–306.

Ключові слова: розумне місто, відкрите програмне забезпечення, відкриті формати даних, відкриті протоколи взаємодії, загрози і ризики, повітряний зазор, безпеку, пропрієтарні протоколи.

Keywords: smart city, open software, open data formats, open communication protocols, threats and risks, air gap, security, proprietary protocols.

Ключевые слова: умный город, открытое программное обеспечение, открытые форматы данных, открытые протоколы взаимодействия, угрозы и риски, воздушный зазор, безопасность, проприетарные протоколы.