Автентифікація користувачів у системах Інтернету речей

Валерія Лукащик[1], Тетяна Гріненко[2]

1. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м. Харків, пр. Науки, 14, E-mail: valeriia.lukashchyk@gmail.com

2. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м. Харків, пр. Науки, 14, E-mail: tetiana.grinenko@nure.ua

Коротка анотація – Thesis is devoted to 'Internet of things' systems, relevance and prospects for their development. Also reviewed information security problems of 'Internet of things' devices and IoT systems. Comparative analysis of user authentication techniques was carried out to further development a method for its evaluation.

Ключові слова – Автентифікація, біометрична автентифікація, Інтернет речей.

I. Вступ

Сучасний етап розвитку суспільства характеризується зростаючою популярністю інформаційних технологій. В даний час відбувається новий виток технічного розвитку цивілізації, який полягає в переході до автоматизації не тільки процесів на виробничих підприємствах, але і процесів, що протікають у повсякденному житті кожної людини. Ідея полягає у використанні великої кількості невеликих малопотужних з обчислювальної та енергетичної точки зору пристроїв для виконання однотипних простих завдань. Така технологія узагальнено має назву Інтернет речей. У сучасному суспільстві Інтернет речей вже став невід'ємною частиною життя багатьох людей. Завдяки появі бездротових мереж, постійного зростання пропускного обсягу Інтернет-з'єднання та впровадження нових підключених пристроїв усе більша кількість людей оточує себе мережевою інфраструктурою, що допомагає і вирішує завдання, які до цього доводилося вирішувати самостійно.

II. Актуальність та перспективи розвитку

Інтернет речей (англ. Internet of things, IoT) - концепція обчислювальної мережі фізичних предметів («речей»), оснащених вбудованими технологіями для взаємодії один з одним або з зовнішнім середовищем, яка розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси, що виключає з частини дій і операцій необхідність участі людини [1, 2].

Класифікація Internet of Things за взаємодією між пристроями та :

–BAN (Body Area Network) – людиною, все, що так чи інакше знаходиться на користувачі: розумний годинник, футболки, кросівки, окуляри та інше [3];

–LAN (Local Area Network) – особистою територією: датчики вимірювання різних параметрів, об'єднаних в «розумний дім» [3];

–WAN (Wide Area Network) – міським простором, розумні міста: велосипеди, автомобілі, поїзди, автобуси, літаки, підключені до Інтернету; електростанції, об'єднані в одну мережу і автоматично перерозподіляють навантаження та інше [3];

–VWAN (Very Wide Area Network) – всесвітнім простором, розумна планета, де кожен пристрій може взаємодіяти з будь-яким іншим [3].

На фоні багатьох теорій та моделей розвитку, що жваво обговорюються як на міжнародних, так і на національних форумах, в останні 10-15 років особливу увагу привертає тема впровадження та використання практично у всіх сегментах соціальної активності людства технологій Інтернету речей. Якщо підсумувати численні різноманітні прогнози експертів та фахівців, то можна очікувати у 2025 – 2030 роках наступне [4]: 80-100 мільярдів підключень до мережі Інтернет (сьогодні – біля 16 млрд.); 7-19 трильйонів дол. буде складати світовий ринок IoT; один трлн. євро – ринок технологій IoT у Європі; Індустрія 4.0, як складова Інтернету речей, дозволить отримати додатковий дохід: 30 млрд. євро – Німеччина та 110 млрд. євро – Євросоюз. Прогнозується, що у 2030 році технології Інтернету речей дозволять забезпечити: 10-15 % економії бюджету на охорону здоров'я; 10-15 років збільшення тривалості життя; 40-50 % збільшення врожайності; 15-20 % збільшення пропускної здатності доріг у містах; до 85-90 % зменшення кількості автомобілів; у 10-15 разів зменшення витрат на логістику тощо.

III. Автентифікація користувачів в IoT

Завдання автентифікації – упевнитися, що користувач дійсно має право доступу до пристроїв, додатків та інформації, якою вони оперують.

Для коректної автентифікації користувача необхідно, щоб користувач пред'явив автентифікаційну інформацію – якусь унікальну інформацію, якою повинен володіти тільки він і ніхто інший.

Існує три основних типи автентифікації інформації:

–користувач, що перевіряється, знає якусь унікальну інформацію (автентифікація за допомогою пароля);

–користувач має якийсь предмет з унікальними характеристиками або вмістом (смарт-карта, USB-токен і т.д.);

–автентифікаційна інформація є невід'ємною частиною користувача (відбиток пальця і інші види біометричної автентифікації).

Головним напрямком для вирішення проблем інших методів автентифікації – є вдосконалення методів автентифікації користувачів за рахунок застосування біометричних технологій, які дозволяють забезпечити доступ до інформаційних систем виключно легітимним користувачам, а також обмежити доступ

до інформаційних систем зловмисникам. На даний момент спостерігається тенденція трансформації біометричних технологій в повноцінний компонент систем захисту, тому все більшого поширення набувають системи біометричної автентифікації користувача. Системи біометричної автентифікації – системи, які використовуються для автентифікації особи користувача на основі його біометричних даних [5].

В процесі біометричної автентифікації еталонний і пред'явлений користувачем зразки порівнюються з деякою допустимою похибкою, яка встановлюється заздалегідь. Похибка підбирається для встановлення оптимального співвідношення двох основних показників біометричної автентифікації [6]:

–FRR (False Reject Rate) – коефіцієнт помилкової відмови, також називається помилкою 1-го роду (ймовірність того, що людина може бути не розпізнана системою);

–FAR (False Accept Rate) – коефіцієнт помилкового прийняття, також називається помилкою 2-го роду (ймовірність того, що одна людина може бути прийнятий за іншу).

Обидві характеристики отримують розрахунковим шляхом на основі методів математичної статистики і вимірюються у відсотках. Чим нижче ці показники, тим точніше розпізнавання об'єкта. Для найпопулярніших на сьогоднішній день методів біометричної автентифікації середні значення FAR і FRR виглядають наступним чином (табл. 1).

ТАБЛИЦЯ 1

СЕРЕДНІ ЗНАЧЕННЯ FAR І FRR

Біометричний метод	FAR	FRR
Відбиток пальця	0.001%	0.6%
Геометрія руки	0.3%	4%
Сітчатка ока	0.0001%	0.4%
Рисунок вен	0.0008%	0.1%
Розпізнавання по 2d образу обличчя	0.4%	7%
Райдужна оболонка ока	0.00001%	0.016%

При побудові ефективної біометричної системи контролю доступу недостатньо високих показників FAR і FRR, тому для якісного аналізу також необхідно використовувати й інші показники:

–можливість підробки біометричних параметрів для автентифікації і доступу до системи;

–швидкість автентифікації, а також можливість швидкого безконтактного сканування біометричних параметрів;

–стабільність або незмінність біометричних параметрів в умовах навколишнього середовища та з плином часу;

–вартість реалізації біометричної системи контролю доступу та доступність самих систем на українському ринку.

Висновок

На сьогоднішній день Інтернет речей стрімко входить як у повсякденне життя людей, так і у важку промисловість та критичні системи. Для коректного функціонування локальних і глобальних мереж необхідно мати чіткий і непохитний зв'язок між приладами цих мереж, а також враховувати усі вимоги інформаційної безпеки цих приладів та систем. Адже від правильності функціонування усіх частин IoT інколи залежить людське життя.

Особливу увагу потрібно приділяти додаткам та пристроям, за допомогою яких виконується контроль системи та пристроїв IoT. А саме, автентифікації користувачів у системі. Усе більше пристроїв володіє великими об'ємами інформації, що стосуються користувача, отже постає проблема несанкціонованого доступу, яка може бути вирішена за допомогою впровадження надійних засобів автентифікації.

Необхідно застосовувати ті чи інші технології і засоби автентифікації залежно від рівня загроз і частоти виникнення ймовірних небезпечних подій. При цьому ризики повинні не тільки оцінюватися на етапі проектування, а й відслідковуватися в процесі експлуатації обраних засобів.

Література

[1] Internet of Things [Електронний ресурс] //Gartner IT Glossary – Режим доступу https://www.gartner.com/it-glossary/internet-of-things/ - 30.10.2019

[2] Kevin Ashton. That 'Internet of Things' Thing. In the real world, things matter more than ideas. (англ.). RFID Journal.

[3] Rob Van Kranenburg: What is IoT? [Електронний ресурс] //Counsil - Режим доступу https://www.theinternetofthings.eu/rob-van-kranenburg-what-iot - 30.10.2019

[4] Баранов О.А. Огляд правових проблем Інтернету речей : матеріали науково-практичної конференції ["Інтернет речей: проблеми правового регулювання та впровадження"], (Київ, 24 жовтня 2017 р.) ; упоряд. : В.М. Фурашев, С.Ю. Петряєв. – К. : Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського". – Вид-во "Політехніка", 2017. – 238 с.

[5] Strategy Analytics: Internet of Things [Електронний ресурс] // Strategy Analytics – Режим доступу https://news.strategyanalytics.com/press-release/iot-ecosystem/strategy-analytics-internet-things-now-numbers-22-billion-devices-where - 31.10.2019

[6] Биометрические системы идентификации и аутентификации [Електронний ресурс] – Режим доступу: http://globuss24.ru/doc/ biometriceskie–sistemy–identifikacii–i–autentifikacii – 31.10.2019