Міністерство освіти і науки України

Харківський національний університет радіоелектроніки
Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

рівень вищої освіти другий (магістерський)

Побудова псевдовипадкових ключів авторизації доступу в ІТС
(тема)

Виконав:

студент 2 курсу, групи БІКСзм-20-1

Прокопович-Ткаченко Д.І.
(прізвище, ініціали)

Спеціальності 125 Кібербезпека
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Безпека інформаційних і комунікаційних систем
(повна назва освітньої програми)

Керівник доктор технічних наук професор Халімов Г.З.
(посада. прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2021

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 125 Кібербезпека
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна, або освітньо-наукова)

Освітня програма «Безпека інформаційних і комунікаційних систем»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри: _____ Халімов Г.З.
(підпис)
«____»_____ 2020 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Прокоповичу -Теаченко Дмитру Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Побудова псевдовипадкових ключів авторизації доступу в ІТС

затверджена наказом по університету від 25.10 . 202 р. № Стз

2. Термін подання студентом роботи до екзаменаційної комісії _____ 2021 р.

3. Вихідні дані до роботи функція захисту – автентифікація а авторизація , криптоалгоритми на еліптичних кривих , тип системи хмаринці сервіс.

4. Перелік питань, що потрібно опрацювати в роботі
Аналіз систем цифрової ідентифікації та автентифікації хмарних сервісів
Системи цифрової ідентифікації
Аналіз сучасних алгоритмів автентифікації та авторизації.
Побудова псевдовипадкових ключів авторизації доступу.
Реалізація протоколу автентифікації та авторизації на еліптичних кривих .

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5. включається до завдання за рішенням випускової кафедри)
презентаційний матеріал у вигляді слайдів

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	08.09.21	Виконано
2	Робота з джерелами за тематикою роботи	01.10.21-21.10.21	Виконано
3	Вивчення основних понять в сфері децентралізованих систем	21.10.21-03.11.21	Виконано
4	Аналіз систем цифрової ідентифікації та автентифікації	04.11.21-22.10.21	Виконано
5	Аналіз можливого вдосконалення механізму ідентифікації в хмарних сервісах	28.10.21-04.12.21	Виконано
6	Побудова псевдовипадкових ключів авторизації доступу в ІТС	05.11.21-10.12.21	Виконано
7	Публікація тез конференцій за результатами досліджень	23.10.21-15.12.21	Виконано
8	Оформлення пояснювальної записки	11.12.21-15.12.21	Виконано
9	Захист кваліфікаційної роботи	16.12.2021	Захист

Дата видачі завдання ___08__ ____09_____2021__ р.

Студент _____
(підпис)

Керівник роботи _____ __д.т.н. проф. Халімов Г.З.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка включає в себе 114 сторінок, 34 рисунка, 2 таблиці, 30 джерел, 1 додаток.

ІДЕНТИФІКАЦІЯ, АВТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ ДОСТУПУ, ПСЕВДОВИПАДКОВІ КЛЮЧІ, ЕЛІПТИЧНІ КРИВІ, ІТС

Об’єктом дослідження є системи ідентифікації та автентифікації з використанням криптоалгоритмів на еліптичних кривих.

Предмет дослідження це процес побудови псевдовипадкових ключів авторизації доступу.

Метою роботи є забезпечення гарантованої безпеки авторизації та автентифікації користувача в інформаційній мережі на основі використання криптоалгоритмів на еліптичних кривих.

В роботі проведений аналіз проблем безпеки сучасних хмарних сервісів, цифрової ідентифікації та автентифікації, розглянуті механізми та пропонована вдосконалена система криптографічного захисту, основана на використанні криптоалгоритмів на еліптичних кривих , та внесені пропозиції , щодо вдосконалення стандартів ISO до захисту інформації в хмарних сервісах.

ABSTRACT

The explanatory note includes a 114 page, 34figures, 30 sources,
1 addition.

IDENTIFICATION, AUTHENTICATION, ACCESS AUTHORIZATION, PSEUDIC RANDOM KEYS, ELLIPTIC CURVES, ITS

The object of research is the systems of identification and authentication using cryptoalgorithms on elliptic curves.

The subject of research is the process of constructing pseudo-random keys of access authorization.

The aim of the work is to ensure guaranteed security of user authorization and authentication in the information network based on the use of cryptographic algorithms on elliptic curves.

The paper analyzes the security problems of modern cloud services, digital identification and authentication, considers the mechanisms and offers an improved cryptographic protection system based on the use of cryptographic algorithms on elliptic curves, and makes suggestions for improving ISO standards to protect information in cloud services.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IT – інформаційна технологія

API – Application Programming Interface, інтерфейс створення додатків

CA – Certification Authority, засвідчувальний центр

DID – Decentralized ID, система децентралізованої ідентифікації

DNS – Domain Name System, система доменних імен

GDPR – General Data Protection Regulation, захист персональних даних на території Європейського Союзу

ION – Identity Overlay Network

KYC – Know Your Customer, знай свого клієнта

PII – Personal Identifiable Information, особиста ідентифікаційна інформація

URL – Uniform Resource Locator, система уніфікованих адрес

CS – cloud service хмарний сервіс

SHA-2 (збірна назва односторонніх геш-функцій SHA-224, SHA-256,SHA-384 і SHA-512.

EEPROM (англ. Electrically Erasable Programmable Read-Only Memory) один з видів енергонезалежної пам'яті.

I^2C — послідовна шина даних для зв'язку

ВСТУП

Головними завданнями захисту інформації є збереження її цілісності , конфіденційності, доступності .

В сучасному світі у побудові інформаційно технічних систем (ІТС) відбувається гіперпощирення використання хмарних цифрових сервісів за допомогою яких призводиться збереження, обробка та обмін даними у різноманітних сферах держави та бізнесу. Особливо важливим стає питання безпечного використання хмарних сервісів у державних цифрових послугах. Місця фізичного зберігання таких даних вже відносять до об‘єктів критичної інфраструктури, що ставить значні завдання до їх кібернетичного захисту.

І якщо проблема фізичного захисту хмарних сервісів в ІТС та їх резервування питання більш меньш вирішено, то у зв’язку з виникненням та розповсюдженням технологій квантового кріптоаналізу та використання їх зацікавленими сторонами перед дослідниками та спеціалістами кібернетичної безпеки стає дуже складне завдання – знижчення вірогідності негативного впливу на механізми авторизації та автентифікації доступу в хмарних сервісах у вигляді відбудови новітніх криптографічних алгоритмів , що унеможливлять зловмисникам втручатись у роботу таких сервісів, або нададуть час у разі проникнення у такі системи виявити та локалізувати джерело небезпеки.

Розвиток хмарних технологій вимагає застосування захищених механізмів авторизації та автентифікації. При цьому виникає завдання побудови псевдовипадкових ключів авторизації доступу в ІТС.

Об’єктом дослідження є системи ідентифікації та автентифікації з використанням криптоалгоритмів на еліптичних кривих.

Предмет дослідження це процес побудови псевдовипадкових ключів авторизації доступу.

Метою роботи є забезпечення гарантованої безпеки авторизації та автентифікації користувача в інформаційній мережі на основі використання криптоалгоритмів на еліптичних кривих.

Для досягнення мети в роботі вирішуються наступні задачі:

1) Аналіз проблем використання та розповсюдження хмарних сервісів.

2) Аналіз кіберінциденів пов‘язаних з авторизацією та автентифікацією

3) Розробка додаткових елементів алгоритмів автентифікації та авторизації хмарних сервісів на основі алгебраїчних кривих.

4) Побудова псевдовипадкових ключів авторизації доступу

5) Реалізація протоколу авторизації та автентифікації шляхом макетуання на локальному сервері ARM архітектури.

1 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ ДОСТУПУ В ІТС.

1.1 Аналіз структури сучасних хмарних сервісів і мереж та основних вимог до хмарних сервісів та тенденції їх розвитку.

З початку першого досвіду використання хмарних технологій , технології хмарних обчислень сформувались та стали популярними у світовому бізнесі та процесах цифровізації державних послуг. Довгострокова стійкість хмарної екосистеми не визиває сумнівів, але залишається невідомим, наскільки спільні технології, такі як безсерверні, IoT, AI та «Великі дані», можуть разом задовольнити потреби держави та стати інноваційним додатком у всіх сферах життя людини. Протягом наступних 10 років оператори бізнесу можуть відчути унікальний рівень ефективності бізнесу через хмарні технології «Данні досвіду штучного інтелекту» поєднуватися з "операційними даними", щоб сприяти цій унікальній продуктивності бізнесу.

Відповідно до «Звіту про дослідження хмарних технологій» [1] "Ринок загальнодоступних хмар, до складу якого входять хмарні програми (SaaS), платформи хмарної розробки (PaaS) та платформи хмарної інфраструктури (IaaS), до 2022 року досягне 411 млрд доларів".Цей звіт також вказує на те, що незабаром IBM та Oracle припинять переважати суперників на глобальному “полі хмарних битв у публічних хмарах”, яке нещодавно перебрали Google, Microsoft, Amazon та інші. Наразі AWS, Microsoft та Google спільно володіють 55 відсотками загального ринку хмар. В *[2]* стверджує, що результати нещодавнього опитування венчурних фірм «Північний міст» показують, що 50 відсотків опитаних організацій використовують філософію «на першому місці у хмарі»; а в деяких випадках використання виключно, особливо для маркетингових потреб.

1.2 Консолідація хмарних сервісів з новітніми технологіями

Останнім часом хмарні постачальники продемонстрували рух до консолідації технологій навколо інфраструктурних платформ, баз даних і навіть додатків. Поряд з цією тенденцією, іншою помітним напрямом , який демонструють постачальники хмарних послуг, є інтеграція «кількох нових технологій», таких як робочі навантаження та галузеві стандарти.Завдяки останнім досягненням у технології тунелювання, постачальники хмарних послуг, з метою вдосконалення сервісів з локальними центрами обробки даних, швидше за все, позиціонують «гібридну хмару» з найвищою технологією управління пакетами , для чого використосуються нейромережі та квантові технології. Ця пропозиція, ініційована у 2021 році, може продовжувати змінювати маркетинг та менеджмент для постачальників хмарних послуг та постачальників послуг коммунікацій.

Іншим прикладом консолідації платформи є “мультихмара”, де наскрізне хмарне середовище може містити принаймні дві загальнодоступні та одну приватну хмару. Згідно різноманитних типів хмарних обчислень [3]

До 2021 року архітектура загальнодоступних хмар буде відрегульована відповідно до зростаючих потреб клієнтів, і багато приватних хмар будуть перетворені в гібридні хмари, що дозволить їм зв'язуватися та взаємодіяти з загальнодоступними хмарами". Управління мультіхмарного середовища можуть бути наділені або оператором бізнесу, або зовнішнім постачальником послуг. Найбільша перевага багатохмарного середовища це відсутність залежності від одного (дорогого та технологічно обмежувального) постачальника хмар.[4]

1.3 Новітні технології хмарних інформаційно-технічних систем у 2021 році

«Стандартизація та підвищена сумісність» є дві ознаки технології дозрівання, яка зараз оточує світ хмарних обчислень. [5]

Як і будь -яка технологія дозрівання, вона поставляється з безліччю суміжних технологій, призначених для роботи з основною технологічною платформою. Кілька таких нових технологій, призначених для роботи з хмарою:

- Робочі навантаження хмарного сервісу дозволяють зробити навантаження більш портативними, а потоки даних - більш мобільними. Ця еластичність публічної хмари є вимогою конкурентноздатності хмарного сервісу.
- Хмарне середовище з широкомасштабними технологічними функціями буде існувати зберігаючи при цьому безпеку та конфіденційність приватної хмари на місці згідно загальних стандартів.
- Виклики хмарних обчислень - multi-cloud поєднує в собі додаткові технологічні переваги публічної хмари з аспектами безпеки приватної хмари. [6]
- Квантові обчислення дозволяють здійснювати аналітику в режимі реального часу дуже близько до джерела вбудованих даних IoT. Компанія Google зробила сміливий крок, оприлюднивши цю інформацію прискорити прийняття підприємством « Інтернет речей на межі». [7]
- Технологія нейро- навчання , що забезпечує високопродуктивну обробку бізнес-даних без необхідності в дорогих серверах. Оскільки постачальник хмарних послуг керує усіма обчислювальними ресурсами, власникам бізнесу стає легше "будувати свої хмарні системи". Найбільша перевага безсерверності: хмарний хост виконує "фрагменти коду" без участі розробників[8]
- Контейнери даних легко переносять програми та робоче навантаження між двома різними налаштуваннями хмар. [9] , якщо загальне припущення полягає в тому, що управління контейнерами та використання контейнерних технологій - це дві різні бізнес -практики,

то впровадження хмарних сервісів може збільшитися за допомогою сервісі Amazon EKS, Microsoft Azure AKS або Google GKE, які активно використовують концепції контейнерних данних [10]

- Огляд нових технологій для хмар. Штучний інтелект, крайова аналітика, платформа AI як сервіс (PaaS) та аналіз графіків сигналізують про появу багатохмарного середовища, що охоплює різні хмарні інфраструктури для обміну робочим навантаженням, програмами та технологічними ресурсами. [11]

1.4 Перегляд сучасних тенденцій в архітектурі хмарних сервісів та їх кібернетичної безпеки.

Згідно з аналізом тенденцій 2021 року [12] хоча такі технології, як «безсерверні», були спеціально створені для хмари, ці технології поступово перетворюють світ корпоративних обчислень. Великою перевагою безсерверного середовища є те, що всі технологічні проблеми в управлінні обчислювальними системами вирішуються постачальником послуг.

Джерело описує колекцію нових технологій для хмари, одна з яких пропонована Amazon [13] -пропозиція сервісу кібернетичної безпеки з підтримкою штучного інтелекту для аналізу даних кібербезпеки. Ще одна технологія штучного інтелекту, яка збирається вийти на хмарне середовище,- це система підтримки прийняття рішень, що активується голосом (DSS), що стимулює продажі та маркетингові функції, та може значно вдосконалити державні сервіси цифрових послуг.

Нещодавно « Загальний регламент захисту даних» (GDPR) ЄС стимулював розвиток технологій безпеки для порушень даних у хмарі. Оскільки невідповідність призводить до серйозних штрафів для підприємств, фахівці з хмарної безпеки стежать за тим, щоб найвищі технології шифрування та захисту паролів були впроваджені для вищого управління на рівні підприємства. Найближчими днями хмарні послуги матимуть безліч технологічних функцій, доступних за низькою вартістю.

Декілька аспектів містить детальне обговорення поточного стану індустрії хмарних послуг цим випуском новин, усі хмарні послуги, такі як інфраструктура як служба (IaaS), програмне забезпечення як послуга (SaaS) та платформа як послуга (PaaS), швидше за все, завоюють популярність у найближчі роки, оскільки вони дозволяють своїм клієнтам масштабні бізнес - послуги з певним ступенем контролю.

Ще одна незаперечна перевага хмарних послуг-це доступна ціна, яка спокушає досі непосвячені підприємства досліджувати керований даними бізнес-менеджмент. Згідно з «Дослідженям промислового використання» [14] ринок хмарних послуг досягне 555 мільярдів доларів до 2020 року з 209,9 мільярда доларів у 2014 році - зростаючи на рівні 17,6 відсотка між 2014 та 2021 роками".

Обчислення та зростання гіперконвергентних рішень хмарному середовищі з технологіями та "центрами мікроданих та локальними центрами обробки даних". Ця тенденція вказує на те, що "очікується, що ринок крайніх обчислювальних технологій зросте на 35 % протягом року, досягнувши 33,75 млрд доларів до 2023 року", що відображено у всіх концептуальних засадах розвитку цифрової громади та суспільства.

Це розповсюдження комбінованих хмарних сервісів викликають відбудову нових механізмів кібернетичної та інформаційної безпеки особливо це стосується авторизації та автентифікації.

1.5 Проблеми пов‘язані з розвитком хмарних сервісів

Розглянемо проблеми які виникають, та придивимось до методології реалізації механізмів автентифікації та авторизації хмарних сервісів:

Статистичний аналіз користування послугами в хмарі :

20% IT -фахівців мають повний доступ до критичних даних у загальнодоступних хмарах

Компанії мають низьку видимість свого публічного хмарного середовища, а інструментів та даних, наданих хмарними провайдерами, недостатньо.

Відсутність можливостей демонстрації сервісу може спричинити різноманітні проблеми, включаючи неможливість відстежувати або діагностувати проблеми з продуктивністю додатків, неможливість моніторингу та виконання відповідно до угод про рівень обслуговування, а також затримки у виявленні та усуненні вразливостей та зловживань безпеки. Опитування "Стан хмарного моніторингу", проведене компанією Ixia, було проведено компанією "Розмірне дослідження" та опитано 338 IT -фахівців в організаціях з різних розмірів та галузей у всьому світі.

Основні висновки включають:

- 87% респондентів висловили побоювання, що відсутність хмарності підвищує загрози безпеці їх організації
- 95% респондентів сказали, що проблеми з відмовлю від хмарних сервісів змусили їх зіткнутися з проблемою роботи програми або мережі
- 38% назвали недостатня використання хмарних сервісів ключовим фактором перебоїв у застосуванні, а 31% - відключення мережі

Це опитування дає зрозуміти, що особи, відповідальні за гібридні IT- середовища, стурбовані своєю нездатністю повністю бачити та реагувати на те, що відбувається у їхніх мережах, особливо у міру того, як критично важливі для бізнесу програми мігрують на віртуалізовану інфраструктуру»[15]

Склад гібридної хмари спонукає організації шукати додаткові засоби безпеки

Оскільки все більше організацій охоплюють гібридну хмару - більше ніж 50 відсотків заявляють про налаштування гібридної хмари - і без сервера, якою зараз користується майже третина організацій, їм не вистачає інструментів (рис.1.1)

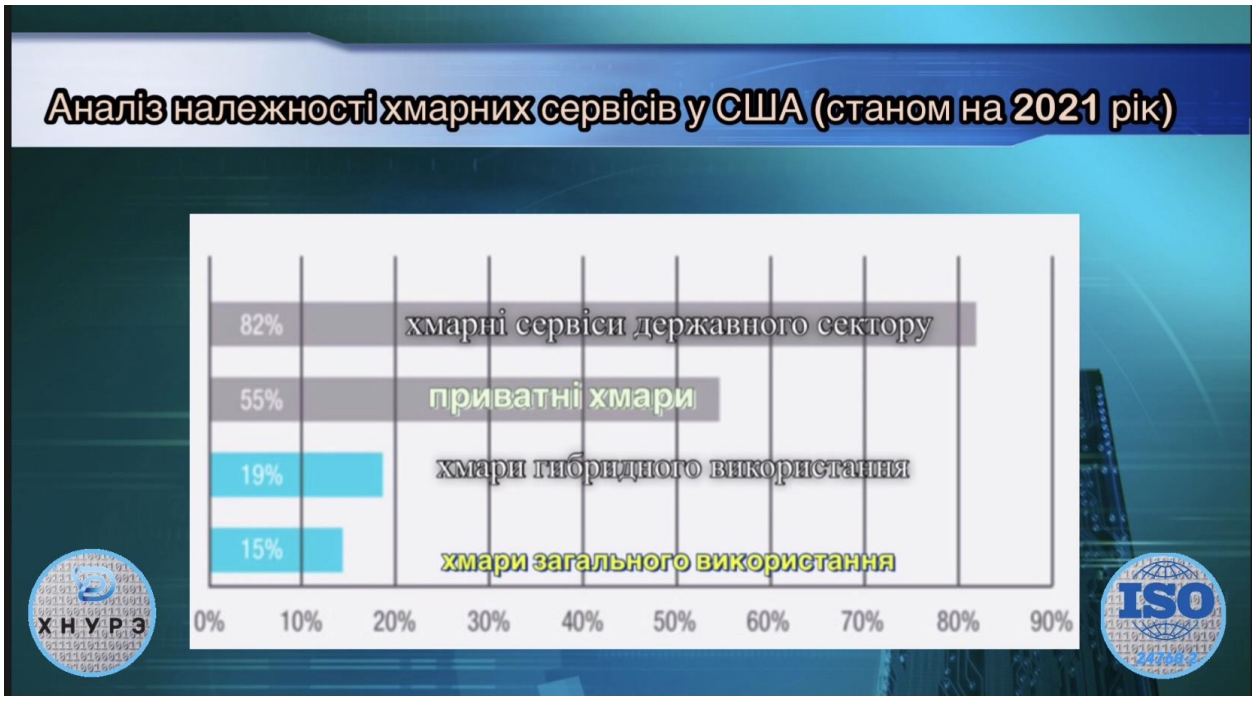


Рисунок 1.1 Аналіз належності хмарних сервісів у США

75 відсотків респондентів очікують, що в наступному році кількість інструментів безпеки, на які вони спираються, збільшиться, тоді як більше половини користувачів все ще налаштовують політики безпеки вручну. Отримана складність може уповільнити важливі бізнес -функції за відсутності інтегрованого підходу безпеки до розподілених хмарних середовищ. Доповідь Alcide, проведена у серпні 2018 року спільно з Informa Engage, підкріплює ідею про те, що нова практика та технології порушують традиційну практику безпеки, з висновками, зокрема:

Складність хмар зростає, а гібридна хмара стала новою інфраструктурою. Хоча віртуальні послуги залишаються найпоширенішим середовищем хмарних обчислень (83%), контейнери (37%), безсерверні послуги (28%) та сервісні мережі (21%) набирають популярність.

Гібридні та мультіхмарні рішення зараз складають більше трьох чвертей усіх конфігурацій (77%).

У міру зростання складності хмарної інфраструктури безпека стає спільною відповідальністю DevOps. Менше половини організацій (45%) зараз мають спеціальну групу безпеки, відповідальну за хмару, а 35% усіх організацій зараз використовують або команду DevOps або спеціальну команду DevSecOps для безпеки (рис.1.2)

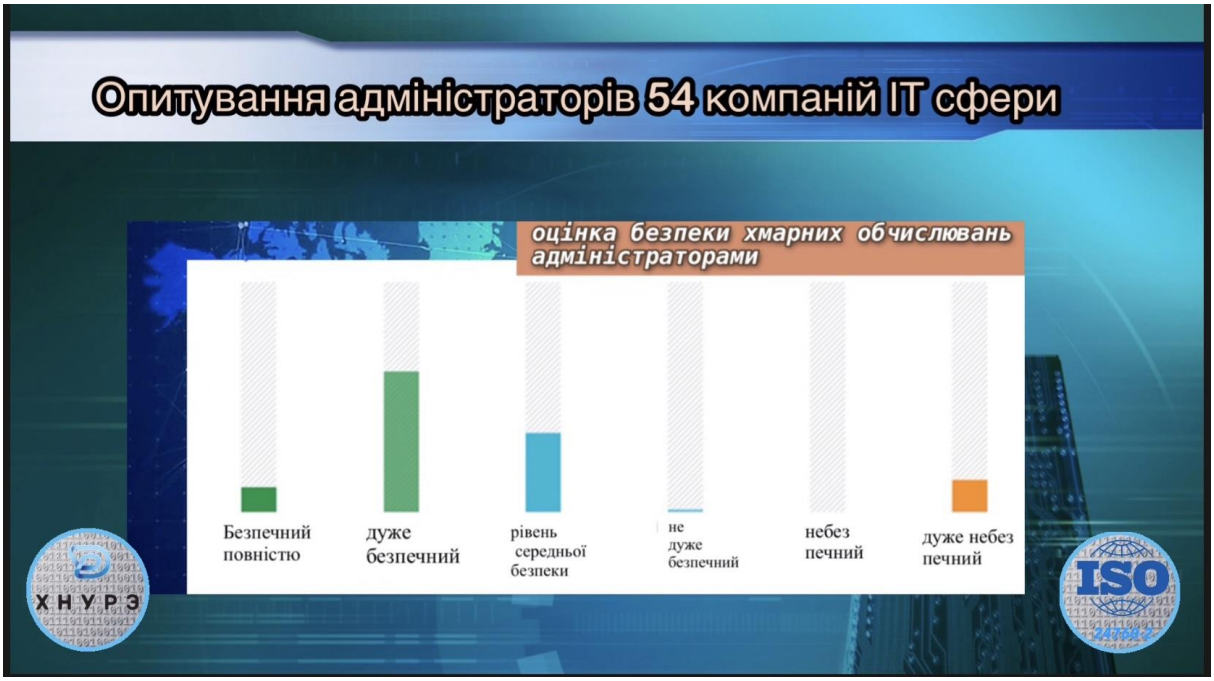


Рисунок 1.2 Опитування адміністраторів

Безсерверна робота у виробництві; Незважаючи на деякі проблеми безпеки, більшість (57%) безсерверних користувачів наразі використовують його як у виробництві, так і в процесі розробки. Більшість, які зараз використовують безсерверні програми, мають високий ступінь впевненості у його безпеці, тоді як третина (32%) висловлюють невпевненість у безпеці свого середовища.

Склад гібридної хмари спонукає команди Dev, Sec та Ops шукати більше інструментів для захисту своїх розподілених середовищ

Понад дві третини (75%) очікують збільшення кількості інструментів, що використовуються, протягом наступних дванадцяти місяців-при цьому ніхто не очікує відмови від використання будь-яких інструментів.

Третина організацій, що звітують, використовують більше п’яти інструментів для безпеки хмар. Поширення хмарних засобів безпеки залишає підприємство вразливим, що вказує на необхідність інтелектуальної автоматизації політики інформаційної безпеки.

Більше половини (60%) організацій покладаються на ручні конфігурації своїх програм, тоді як майже всі організації (90%) покладаються на кількох осіб для налаштування та встановлення правил політики інформаційної безпеки. Відсутність мониторингу може призвести до занападення продуктивності додатків, втрати даних клієнтів та невизначених загроз безпеці, може мати серйозні наслідки для загального успіху бізнесу в організації".

1.6 Мониторінг вразливостей хмарних сервісів

Глобальний та гібридний хмарний моніторинг вразливостей відстежує традиційні центри обробки даних.(рис1.3)

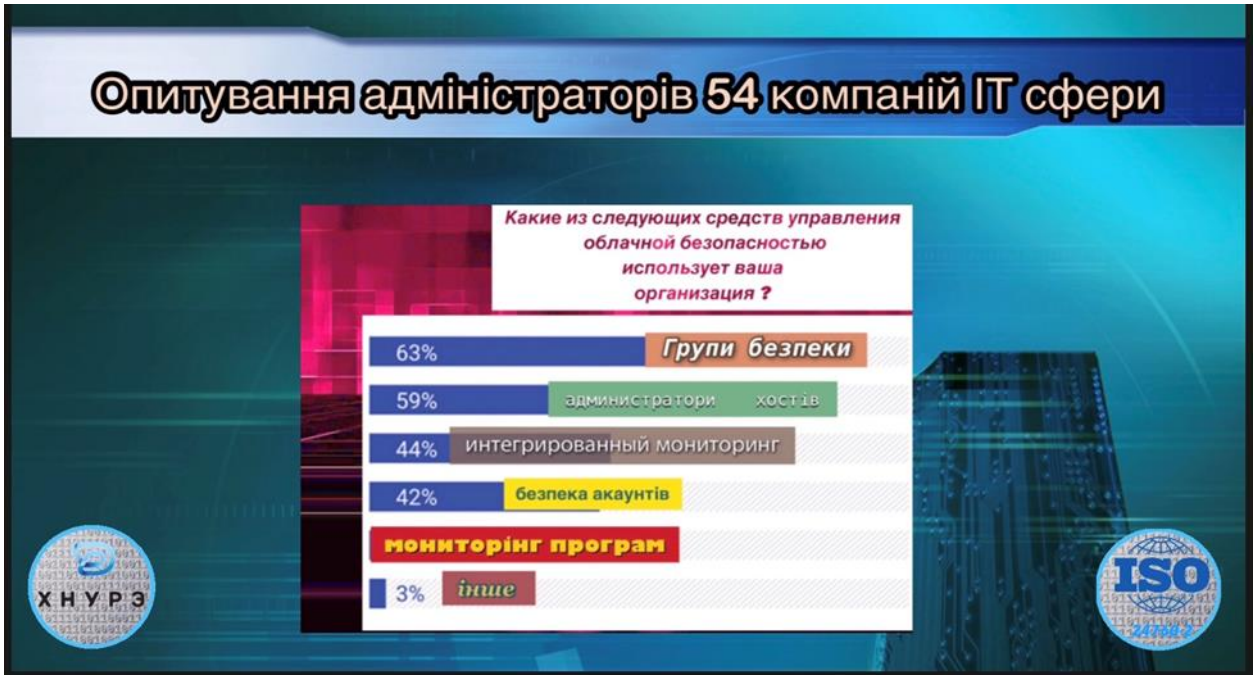


Рисунок 1.3 Опитування адміністраторів

Дані, виявлені IT -спеціалістами, показали, що хмарні провайдери не забезпечують необхідного рівня контролю

- Середовища загальнодоступних хмар важко контролювати : Менше 20% IT -фахівців повідомили, що вони мали повний, своєчасний доступ до пакетів даних у загальнодоступних хмарах. У приватних хмарах ситуація краща: 55% повідомляють про належний доступ. У локальних центрах обробки даних 82% мають необхідну видимість.
- Мониторинг на рівні пакетів має вирішальне значення для контролю : 86% респондентів зазначили, що доступ важливий для контролю продуктивності мережі та додатків, а 93% заявили, що він важливий для безпеки.

Рішення для моніторингу покращують контроль, управління продуктивністю мережі та безпеку

Майже всі респонденти (99%) виявили прямий зв'язок між загальною видимістю мережі та цінністю бізнесу. Пропоновані три найкращі переваги(рис.1.4) :

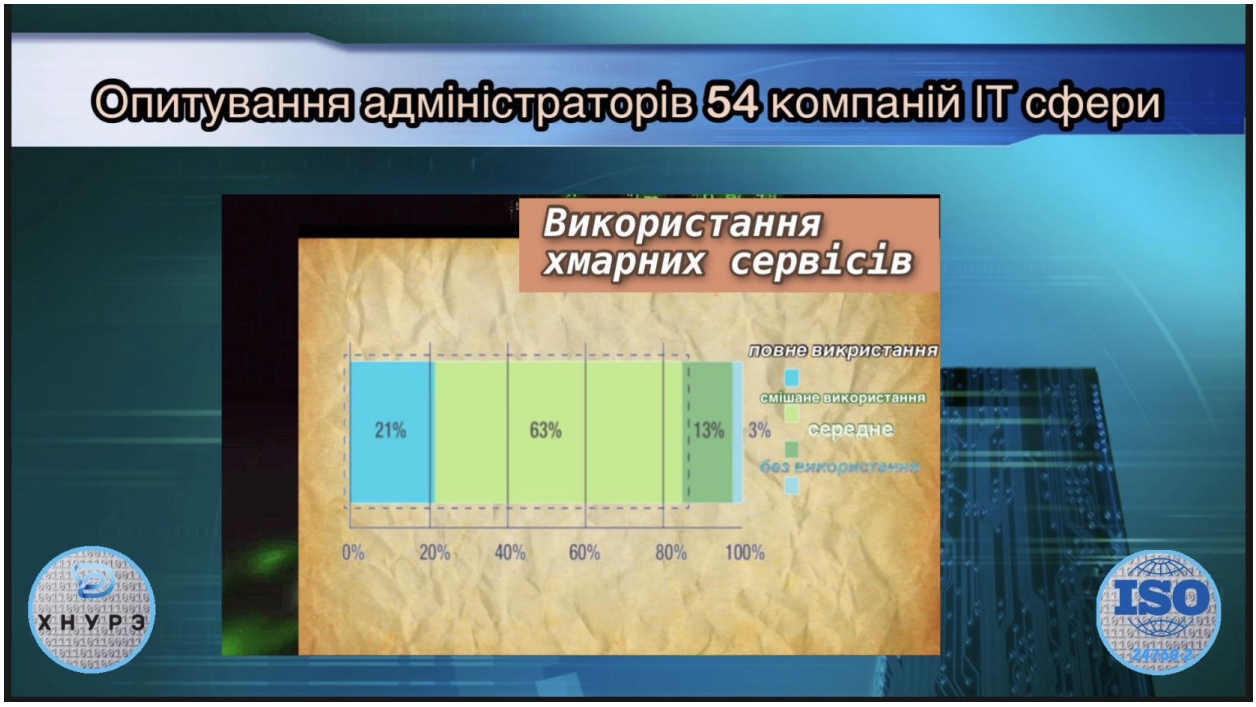


Рисунок 1.4 Опитування адміністраторів

1) Моніторинг та забезпечення продуктивності програми (60%)
2) Увімкнення ідентифікації загрози (59%)
3) Визначення «показників компромісу» безпеки (57%)

Опитування також показало, що видимість має вирішальне значення для моніторингу продуктивності хмар, а також перевірки продуктивності додатків до розгортання хмари:

Передбачення продуктивності - ключовий виклик . 87 % користувачів хмари важко передбачити продуктивність додатків у хмарі.[16]

1.7 П’ять способів керування авторизацією в хмарі

В даний час швидко включені організації, що дозволяє їм зберігати великі обсяги даних і додатків з більш високою безвідмовної роботи і зниження витрат, в той же час, вводячи нові виклики безпеки.

Однією з найбільш помітних проблем є управління особистими даними та авторизація. З початку хмарних обчислень методи авторизації в хмарі перетворилися на нові моделі, які визнають безліч різноманітних послуг, які тепер об’єднуються, щоб сформувати мережу компанії.

Ці підходи враховують зростаючу кількість сліпих місць безпеки та слабких місць у хмарному середовищі. Замість того, щоб з'єднуватись дротом у межах корпоративної мережі, більшість цих нових послуг відкриті для Інтернету, розширюючи поверхню атаки інфраструктури компанії. Ось п’ять ключових подій, які слід розглянути для управління авторизацією в хмарі.

Централізоване управління та розподілені послуги

У традиційному локальному середовищі всіх користувачів зазвичай обслуговував єдиний сервер, який обслуговував би кожну програму, незалежно від того, надавати чи забороняти доступ. У хмарному середовищі кожна служба має свій власний набір дозволів та ідентифікаційних даних, а також власний механізм авторизації та автентифікації для їх підтримки та

застосування. Це значно ускладнює налаштування та відкриває низку проблем помилок конфігурації , що призводить до хмарних атак.

Послуги з авторизації

Для того, щоб керувати користувачами на єдиній платформі, зазвичай використовується одна зовнішня служба авторизації. Ви надаєте облікові дані служби авторизації обліковому запису, який може створювати тимчасові ролі або керувати вашими обліковими записами в одному хмарному сервісі, яким ви користуєтесь. Завдяки цьому користувачів можна визначити на одній платформі, але постачальнику ідентифікаційних даних потрібно довіряти, щоб він не виконував шкідливих дій, а коли це станеться, може бути важче відстежити, звідки ці дії виникли.

Методи хмарної авторизації різні, включаючи MAC - де кожен додаток володіє індивідуальними дозволами доступу, DAC - де кожен додаток запитує дозволи від зовнішньої програми дозволів, RBAC - де служба авторизації володіє ролями з різними привілеями у хмарній службі та ABAC - де доступ базується на атрибутах та політиці запиту.

Статистичний аналіз кіберінциндентів хмарних сервісів (рис1.5):

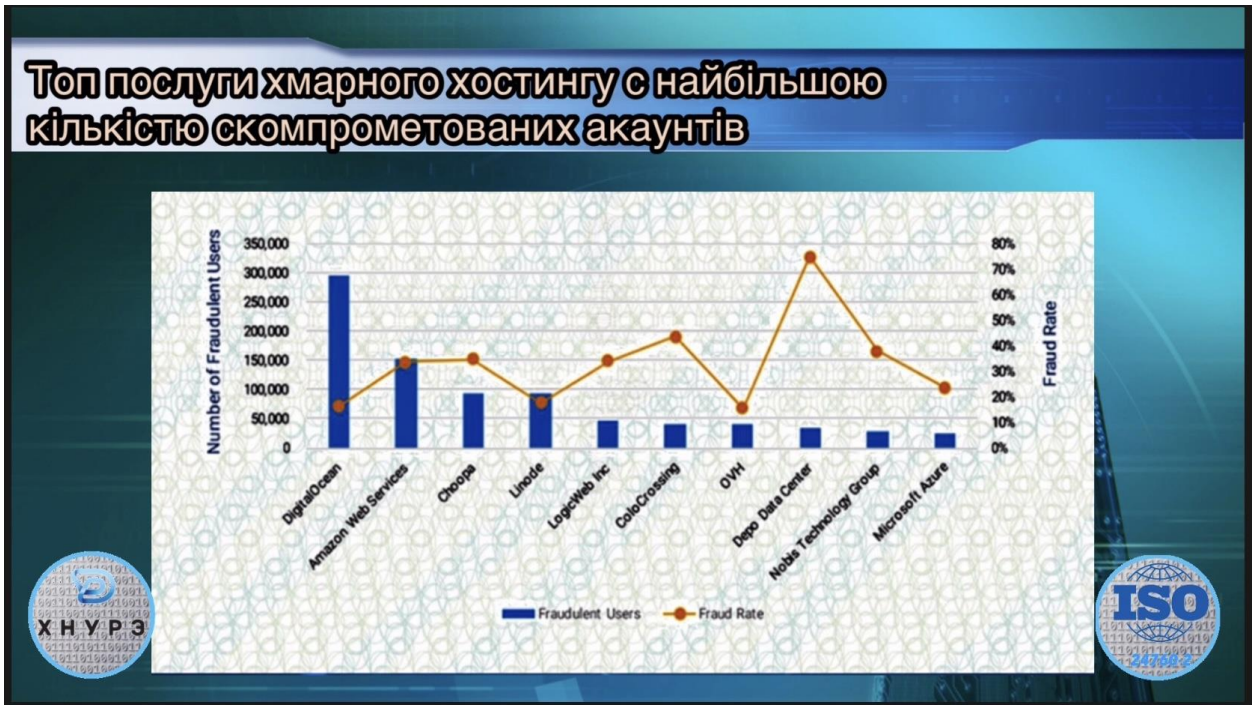


Рисунок 1.5. Топ послуги хмарного хостінгу

Для деяких хмарних сервісів більше 75% облікових записів використовуються хакерами

Дослідники виявили, що 21,57% відсотків облікових записів, що походять із діапазонів IP -адрес хмарного сервісу, є шахрайськими. Шкідливі облікові записи у вісім разів частіше виникають через хмарні сервіси, ніж звичайні користувачі. Насправді, деякі хмарні служби та центри обробки даних можуть мати більше 75% шахрайських облікових записів.

Звіт щодо індексу шахрайства DataVisor за 2 квартал 2020 року - це щоквартальна оцінка типів та методів нападів на хмарні сервіси у фінансових службах. Поточний звіт використовує інформацію, зібрану DataVisor у період з квітня по червень 2021 року, аналізуючи 1,1 мільярда активних облікових записів користувачів; 1,5 млн. Доменів електронної пошти; 231 000 типів пристроїв; та 562 провайдерів хмарного хостингу та центрів обробки даних, серед інших показників

1.8 Методики захисту хмарних сервісів від вразливостей

Добре продумана та керована присутність контролю у хмарних мережах є обов’язковою умовою для більшості компаній , але н потенційні наслідки атаки, спрямованої можуть бути критичними. Дата центри все частіше сприймаються як об‘єкт нападу , забезпечуючи платформу для складних кампаній впливу, які проводяться національними державами , різними хакерськими групами, щоб донести своє повідомлення , а зловмисники прагнуть інших користувачів вразити на персональні данні або крипто валюту . Фішери видають себе за великі британські установи у Twitter. Клієнти банків Великобританії стають мішенню фішерів, які видають себе за обліковий запис служби підтримки клієнтів банків у Twitter, попереджає Proofpoint. Фішери зазвичай вибирають варіанти назви законних облікових записів і повторюють їх зовнішній вигляд, а також вводяться, коли користувач

ставить запитання до законного облікового запису. У наведеному вище прикладі підроблений обліковий запис - @BarclaysUKHelp, а законний - @BarclaysHelpUK. Фішер, що комплектує підроблений рахунок, відповідає та направляє користувача на фішинг -сайт, який дуже нагадує власну сторінку входу банку. Зайве говорити, що користувачі, які вводять свої облікові дані в Інтернет -банкінгу на цей підроблений сайт, фактично передають їх шахраям.

Іноді шахрайство не закінчується, і жертв просять ввести додаткову особисту та фінансову інформацію. Пізніше ця інформація буде використовуватися шахраями для обходу заходів безпеки банків та доступу до рахунку жертв.

Користувачам часто кажуть, що слід остерігатися небажаних повідомлень. Цей метод фішингу є високоефективним, оскільки користувач вже очікує відповіді від акаунта банку в Twitter і просто припускає, що отримане повідомлення надходить від правильного. Звичайно, фішери роблять все можливе, щоб не викликати жодних підозр За даними компанії, фішинг у соціальних мережах зріс більш ніж на 100% між 2 -м та 3 -м кварталами 2016 року. Користувачам рекомендується не занурюватись у самовдоволення через неформальний характер розмов у Twitter - повідомлення, отримані через платформу мікроблогів, можуть бути такими ж небезпечними, як шкідливі електронні листи чи SMS. Також добре пам’ятати, що офіційні облікові записи часто мають біля свого імені синю позначку «галочка». Якщо ні, виконайте короткий пошук у Twitter, щоб побачити, чи з’являються інші облікові записи, і якщо вони з’являються, уважно оцініть кожен із них та відсійте підробки. Соціальні медіа не зникають, вони будуть продовжувати розвиватися та трансформуватися. У всякому разі, поява нових технологій співпраці прискорюється, а поряд з ними з’являються нові ризики. Вплив успішної атаки на різні цифрові канали можна порахувати мільйонами доларів з точки зору репутації та/або втрати цін на акції, крадіжки, витоків інтелектуальної власності-не кажучи вже про невизначені наслідки геополітичних результатів .З усіх цих причин вважається, що рішення для

захисту цифрових медіаканалів стануть повсюдними, як і було і залишається антивірусне програмне забезпечення, та кріптозахист.Єдина платформа для захисту цифрових та соціальних каналів Платформа SaaS Cyber SafeGuard із широким охопленням каналів (соціальні медіа, мобільні додатки, мережі співпраці, магазини додатків тощо), вдосконаленими алгоритмами штучного інтелекту та машинним навчанням була розроблена для виявлення загроз для всіх цифрових каналів, що належать організації та захищатися від них.

Постановка на карантин шкідливого програмного забезпечення, спам та фішинг, які мають місце у цифрових та соціальних облікових записах і використовуються для отримання доступу до організації. Захист облікових записів від злому облікових даних. Але, найголовніше, наша платформа адаптована до нових ризиків. Наприклад: нещодавно генеральний директор клієнта був мимоволі залучений до акційної схеми «прокачуй-скидай», яка діяла в Інтернеті, темній мережі та соціальній мережі. Це новий тип загрози та кризи у соціальних мережах, яку наша платформа сприяла вирішенню ».

Виклики, про які слід пам’ятати

Шукаючи рішення для мінімізації ризиків у соціальних мережах, організації повинні пам’ятати про конфіденційність працівників, використання неспецифічних технологічних рішень і повинні думати про те, щоб масштабно реагувати на кількість попереджень. Співробітники вважають соціальні комунікації чутливим питанням, і вони не обов’язково хочуть, щоб організація діяла як« Великий брат », тому вам потрібна система, яка лише вмикається і дає співробітникам уявлення про ризики нападу, з якими вони стикаються під час водночас поважаючи їхнє приватне життя. Існують технології, політика та рішення для моніторингу, які можуть допомогти захистити від соціальних та цифрових ризиків, але жодна з них не є всеосяжною, деякі неефективні, а деякі не можуть масштабуватися - вони просто не можуть обробити всю інформацію та робочий процес усіх соціальні та цифрові канали, які належать організації та не можуть негайно вживати заходів для придушення кожного ризику згідно із заздалегідь налаштованими

правилами (при цьому уникаючи хибнопозитивних результатів). Атаки відбуваються в режимі реального часу, і їм потрібна відповідь у режимі реального часу-сповіщення без дій безглузді",-зазначає він.

1.9 Поради організаціям з використання CS

Для організацій з багатою присутністю у соціальних мережах, які не мають додаткової безпеки, - це комплексний підхід до його посилення стандартів інформаційної безпеки.

Перший крок - інвентаризувати на глобальній основі всі існуючі цифрові активи компанії, які потенційно піддаються ризику. Як тільки є мониторинг поверхні атаки, аналіз її на наявність потенційних уразливостей. Озброївшись цим розумінням, спершу створіть план вирішення проблем високого ризику. На другому етапі перейдіть до захисту своїх соціальних та цифрових активів, використовуючи рішення безпеки для вирішення ризиків, виявлених на першому етапі, а також будь -яких нових загроз. Нарешті, змоделюйте атаки на активи за допомогою соціальних каналів та повідомте про результати, а потім розширіть захисний слід за необхідності ».[17]

Найбільша кількість шахрайських атак - у США та Китаї. Більше 21% фейкових акаунтів, націлених на онлайн та фінансові послуги, походять із США, а 17% - з Китаю. У атаках, націлених на північноамериканські онлайн - сервіси, більше 45% нападів було здійснено в США (рис. 1.6)

Рисунок 1.6 Співвідношення фейкових та справжніх аккаунтів

Цікаво, що злочинні групи залучають різних постачальників хмарних послуг залежно від атаки. Шахраї, націлені на соціальні платформи, значною мірою використовують веб -служби Amazon, тоді як шахраям, націленим на мобільні додатки та фінансові послуги, віддають перевагу DigitalOcean.

Скоординовані атаки - група шахрайських облікових записів, контрольованих одним і тим же зловмисником - представляють більшість шахрайських дій як у соціальних платформах, так і у фінансових службах.Більше 90% реєстрації фейкових акаунтів у соціальних платформах пов’язані з скоординованими атаками; у фінансовому секторі більше 40% шахрайства з додатками походить від скоординованих атак. Хоча більшість шахрайських атак трапляється менше ніж через день після створення облікових записів, деякі акаунти "спальних клітин" можуть чекати місяцями або роками, перш ніж їх використовувати. В середньому шахрайські акаунти інкубуються 35 днів перед атакою.

«Звіт за індекс шахрайства DataVisor за цей квартал демонструє, що посилення впровадження хмари має небажані наслідки для фінансового благополуччя онлайн-бізнесу»,-сказав Інгліан Се, генеральний директор DataVisor. [18]

1.10 Організаційні тези політики безпеки хмарних сервісів.

Кожен хманий сервіс CS має власний набір інструментів, дозволів, формату журналу та інтерфейсу, що робить безпеку новою проблемою для кожної програми. Важливо звернути увагу на відмінності між хмарними сервісами та вибрати правильний, виходячи з ваших потреб. Переконайтеся, що ви завжди можете сказати, хто і з якої причини отримує доступ до ваших конфіденційних даних, і що кожен доступ надходить із законного джерела.

Нульова довіра

Архітектура нульової довіри базується на припущенні, що жодній службі, серверу, ролі чи клієнту у вашій мережі не можна довіряти. Завжди двічі перевіряйте запити на доступ до конфіденційних даних, застосовуйте МФА, відстежуйте зміни в поведінці та впроваджуйте модель принципу найменшого привілейованого. Якщо ви можете визначити, як повинен поводитися кожен користувач, і до яких даних він має доступ, ви знаєте, як відстежувати цих користувачів.

Користувачів API слід обмежити відповідно до пристрою -виробника, а також відстежуючи їх моделі поведінки, а привілейовані API повинні обмежуватися для роботи лише з внутрішньої мережі компанії. Нарешті, користувачі повинні постійно проходити аутентифікацію за допомогою МЗС та контролювати їх за допомогою антивірусного програмного забезпечення.

Безперервна авторизація

Витік облікових даних може статися де завгодно, від зламаного персонального комп’ютера до сервера баз даних. Тому на кожному кроці доступу до секретної інформації користувачеві потрібно

авторизуватись. Якщо, наприклад, використовується зовнішня служба авторизації, і ця служба має надійний обліковий запис у веб-програмі, ця веб-програма повинна забезпечити, щоб надійний обліковий запис використовувався службою, а не людиною посередині.

Коли веб -сервер запитує доступ до секретної інформації, він повинен надходити із законного потоку, а не лише від когось із оболонкою на машині. Раптова зміна кількості підключених пристроїв або використання рідко використовуваного виклику API може свідчити про компрометацію облікових данних . Згідно з даними виявлення облікових даних компанії Blueliv, з початку 2018 року кількість компрометованих облікових даних, виявлених в Європі та Росії, збільшилася на 39% порівняно з аналогічним періодом 2017 року (січень-травень). Насправді в Європі та Росії зараз проживає половина жертв крадіжки облікових даних у світі (49%). У цьому подкасті Патрик Пілат, керівник відділу інженерії та розвідки кіберзагроз у Blueliv, розповідає про звіт та ілюструє, як це вражаюче зростання успіху кіберзлочинців свідчить про те, що індустрія крадіжки облікових даних зростає в Європейському регіоні як у сфері інновацій, так і в масштабах В екосистемі кіберзлочинності зростає індустрія, зосереджена на отриманні дійсних облікових даних для входу за допомогою декількох механізмів та інструментів. Сьогодні ці інструменти можна недорого придбати на підземних ринках, у темних мережах та на форумах. І не обов’язково бути досвідченим кіберзлочинцем, щоб розпочати атаку. Згідно з нашими даними про виявлення облікових даних, з початку 2018 року до кінця травня спостерігалося 39 - відсоткове збільшення кількості скомпрометованих облікових даних, які ми виявили в Європі та Росії, порівняно з тим же періодом 2017 року. Фактично, спостереження Blueliv роблять висновок, що Європа та Росія складають половину світових жертв крадіжки грамот.Ми також виявили, що коли ми видалимо Росію з набору даних, показник зростання європейських жертв крадіжок зросте до 62 відсотків. Ці показники європейського зростання, які ми відстежуємо, на диво вищі, ніж у Північній Америці, яка за цей період

зафіксувала скорочення майже наполовину. Ми вважаємо, що ці показники успіху в кіберзлочинності означають, що індустрія крадіжки облікових даних зростає в європейському регіоні як в інноваційній сфері, так і в масштабах. Ми вважаємо, що на це є кілька причин.По -перше, наразі в Європі розповсюджується більше кампаній з викрадення даних. Ми також бачимо, що ми використовуємо більшість сервісів в Інтернеті, ніж будь -коли раніше, таких як біржі криптовалют та інші послуги, такі як ігри чи навіть азартні ігри. Просто поганих хлопців можна монетизувати більше.Ми також бачили тенденції, що свідчать про те, що APT, які вже добре відомі за обмін інформацією в Інтернеті для цілеспрямованих атак, продовжують свою співпрацю швидкими темпами (рис 1.7). У звіті ми також вказуємо на те, що відбулося поширення дешевих наборів шкідливих програм, доступних для використання менш кваліфікованими зловмисниками.

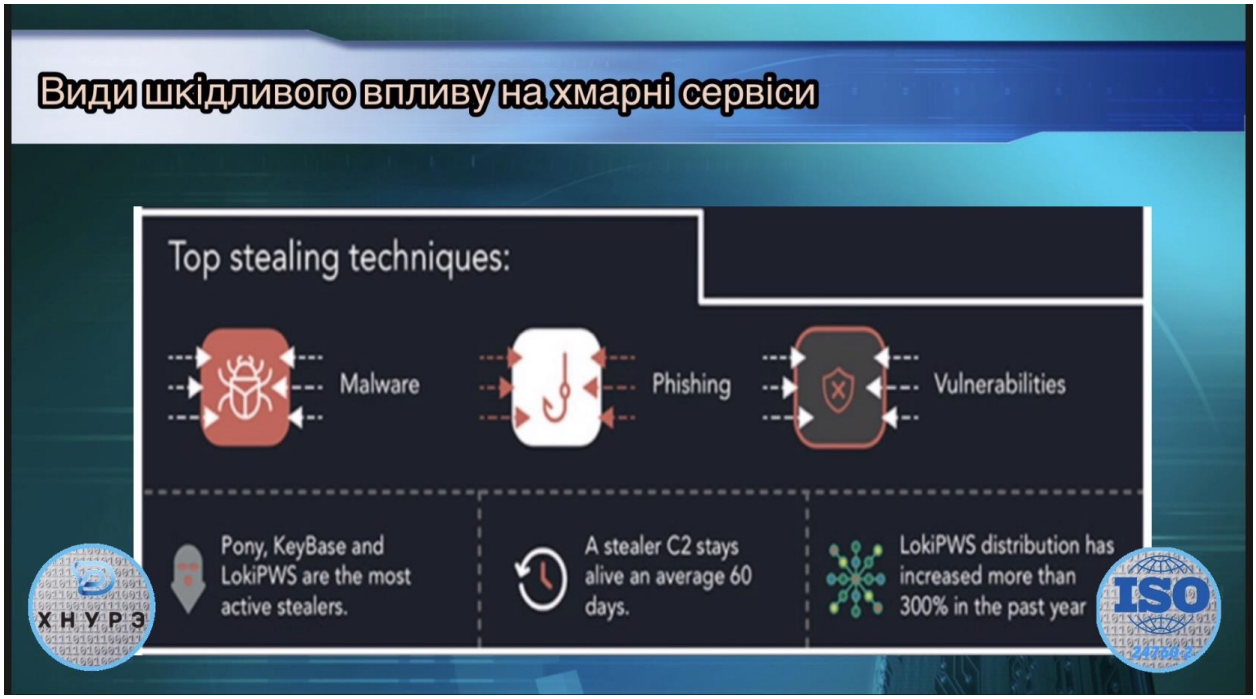


Рисунок 1.7 Види шкідливого впливу на хмарні сервіси

Ми також виділяємо деякі прайс -листи облікових даних. Наприклад, вкрадені облікові дані для сайту електронної комерції можна придбати

приблизно за 9 доларів, при цьому облікові дані банківського рахунку змінюються за ціною залежно від залишку на рахунку. Вони можуть заробити до двадцяти п’яти тисяч доларів за один рахунок, на якому, наприклад, розміщено півмільйона доларів. Для того, щоб суб’єкт загрози отримав доступ до організації та завдав хаосу, потрібна лише одна хороша облікова інформація. Отже, ми були стурбовані тим, що у нашому регіоні спостерігаються значні темпи зростання крадіжок облікових даних. у більшості випадків мотивація компромісу облікових даних - фінансова - від шантажу до викупу, продажу конфіденційної інформації до шахрайства. Кінцевою метою зазвичай є отримання прибутку від атаки. Це може бути через вимагання чи шантаж, шпигунство або заподіяння репутації шкоди, або через низку інших причин, які ми детально досліджуємо у звіті.

Зрештою, будь -яка організація, яка володіє цінними даними, перебуває під загрозою, тому вона повинна вживати відповідних заходів для свого захисту. Отже, які різні заходи можуть вжити організації для запобігання та пом'якшення наслідків крадіжки облікових даних? Що ж, є деякі ключові речі, які, на нашу думку, організації повинні вилучити з цього звіту. Як і у багатьох аспектах кібербезпеки, освіта є ключовою для пом'якшення атак. Люди в будь -якій організації повинні розцінювати будь -які запити на отримання повноважень як винні, доки не доведено їх невинуватість. Кінцеві користувачі завжди найслабші, а також найсильніша ланка у ланцюжку. Людський дотик, доповнений інформацією про загрози, є найкращим способом захисту організації. Насправді, оперативна розвідка дозволяє організаціям блокувати потенційні вторгнення на рівні брандмауера. Це допомагає забити отвори, перш ніж зловмисник зможе проникнути. Ця безперервна кібергігієна в організації запобігає атакам і пом'якшує наслідки атаки, коли це відбувається. Це змушує групи IT -безпеки своєчасно виявляти джерела порушень та виправлення вразливостей, проводячи постійне тестування на проникнення, вправи з командного об’єднання тощо. Тепер організації завжди повинні пам’ятати, що чим свіжіші облікові дані, (рис1.8) тим більша

ймовірність їх ефективного використання кіберзлочинцями. З іншого боку, чим раніше компромісні дані будуть захищені, тим швидше групи безпеки зможуть виправити ситуацію. Отже, наявність надто свіжої облікової інформації часто надзвичайно важливо. Дуже раннє виявлення скомпрометованих облікових даних, не більше ніж через кілька днів після того, як вони були скомпрометовані, може значно зменшити наслідки крадіжки

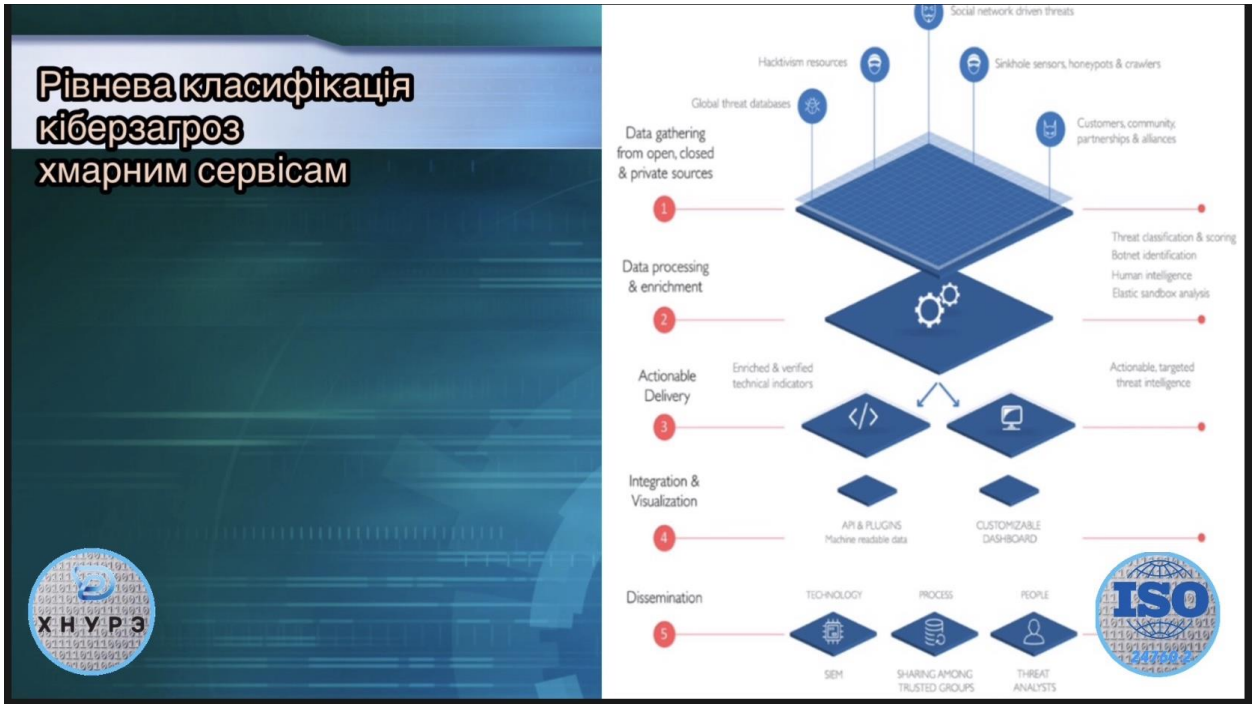


Рисунок 1.8 Рівнева класифікація кіберзагроз

Висновки хмарні сервіси мають багато вразливостей зокрема протоколи авторизації та автентифікації повинні підлягати підвищеному криптозахисту , що знизить вірогідність негативного впливу від кіберзлочинців.

2 ВДОСКОНВЛЕННЯ КРИПТОАЛГОРИТМІВ АВТОРИЗАЦІІ ТА АВТЕНТИФІКАЦІІ РОЗПОДІЛЕННОГО ДОСТУПУ ДО ХМАРНИХ СЕРВІСІВ ЗА ДОМОГОЮ АЛГОРИТМУ ЦИФРОВОГО ПІДПИСУ ЕЛИПТИЧНОІ КРИВОІ.

2.1 Пояснення сутності криптоалгоритму на еліптичних кривих та його переваги у механізмах автентифікації та авторизації хмарних сервісів.

Існує дві принципово різні схеми автентифікації: симетричні системи, які покладаються на секретні ключі, якими користуються хост та автентифікатор, та асиметричні системи, такі як алгоритм цифрового підпису з еліптичною кривою (ECDSA), які покладаються на приватний ключ в автентифікаторі та відкритий ключ, який хост використовує для перевірки автентифікатора. У відкритих системах, де сторонні особи мають бути автентифіковані, управління та захист секретних ключів може бути проблемою. Тут ECDSA пропонує необхідну гнучкість. У цьому розділі представлено концепцію ECDSA, її математичну основу та показано, як метод може бути успішно застосований на практиці.

Понад 15 років автентифікація SHA-1 використовувалася для захисту інтелектуальної власності (IP) від підробки та незаконного копіювання. Але зараз, коли обробка інформації просунулася вперед, інженери хочуть ще більш високого рівня безпеки. Сьогодні безпечний аутентифікатор та захищені мікросхеми співпроцесора реалізують аутентифікацію SHA-256. Ця технологія забезпечує передову фізичну безпеку для забезпечення неперевершеного недорогого захисту IP, запобігання клонуванню та периферійної автентифікації.

2.2.Безпечна система автентифікації

Впровадження безпечної системи автентифікації вимагає зв’язування хост -системи з датчиком/периферійним модулем. На малюнку 1 показаний захищений аутентифікатор алгоритма безпечного хешировання (256 бит) плюс захищений співпроцесор SHA-256. Хост спілкується з автентифікатором та співпроцесором по шині I²C.(рис2.1)

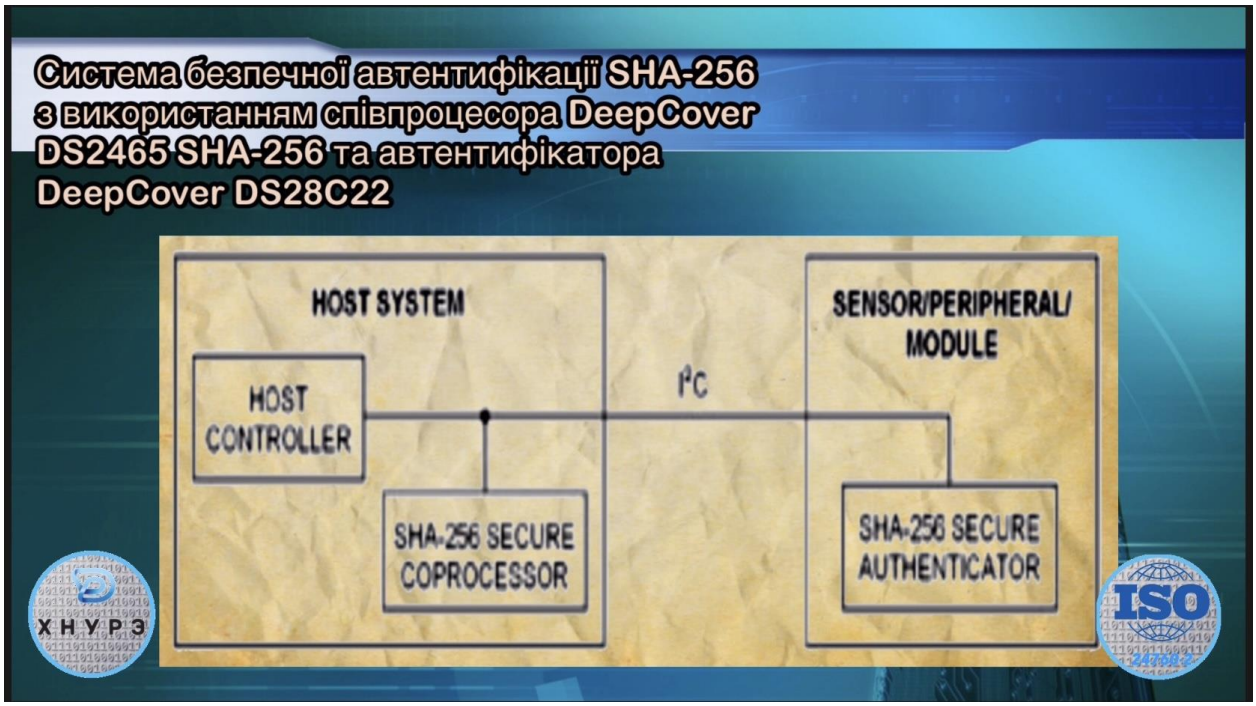


Рисунок 2.1 Система безпечної автентифікації SHA-256 з використанням співпроцесора DeepCover DS2465 SHA-256 та автентифікатора DeepCover DS28C22

*2.2.*1 Захищений аутентифікатор SHA-256

В цій системі підтримує розмір завдання 256 біт і передає 256-бітний секрет. Наприклад, автентифікатор на малюнку 1 є ведомою I²C з унікальним 64-розрядним ідентифікатором ПЗУ, який служить основним елементом даних для обчислень автентифікації. Розробник системи може розділити 3-Кбітну EEPROM користувача на зони з відкритим (незахищеним) доступом,

області, де майстер повинен аутентифікувати себе для доступу до запису, та області, де доступ для читання та запису передбачає шифрування даних. Шифрування можна поєднати з автентифікацією для подальшого підвищення безпеки даних. Таблиця 1 показує доступні режими захисту. За замовчуванням система не має захисту, якщо не активовано RP, WP, EM, AP та EP. Захист є накопичувальним.

Таблиця 1: Варіанти захисту автентифікатора

RP	Захист від читання. Якщо активовано, дані доступні лише для внутрішнього використання, наприклад, як секрет.
WP	Захист від запису. Якщо активовано, дані неможливо змінити.
EM	Режим емуляції EPROM. Якщо активовано, окремі біти можна змінити лише з 1 на 0.
AP	Захист автентифікації. Якщо активовано, доступ до запису в пам'ять потребує майстер -автентифікації.
EP	Захист шифрування. Якщо активовано, дані шифруються на шляху до контролера хосту та надсилаються до захищеного автентифікатора для доступу до запису.

2.2.2 Захищений співпроцесор SHA-256

Захищений співпроцесор SHA-256 на рис. 1 звільняє хост-процесор від виконання обчислень SHA-256 і вбудовує захищену пам'ять, яка надійно зберігає головний секрет. Додаткова пам'ять виділяється для зберігання та захисту інших елементів даних, що використовуються для обчислення унікальних підпорядкованих секретів. З точки зору хоста, безпечний співпроцесор SHA-256 виглядає як 256-байтова пам'ять для читання/запису з

певними регіонами (елементами даних), призначеними для спеціальних цілей.

2.2.3 Логістика безпеки.

Захист на основі SHA спирається на коди автентифікації повідомлень (MAC), обчислені з відкритих даних та секрету. Щоб перевірити справжність, обидві сторони (тобто ведучий чи співпроцесор та автентифікатор) повинні знати таємницю, яку ніколи не можна розкривати. Крім того, для максимальної безпеки секрет кожного аутентифікатора має бути унікальним. Таким чином, безпека всієї системи не зачіпається, якщо таємниця єдиного автентифікатора коли -небудь порушується.

На перший погляд, ці вимоги можуть здатися неможливими. Однак є просте рішення: обчислити секрет із відомих «інгредієнтів» та встановити його у безпечний автентифікатор у надійному/контрольованому виробничому середовищі. Інгредієнти для унікальної таємниці є майстер-таємницею; дані зв'язування; часткова таємниця; ідентифікатор ПЗУ захищеного автентифікатора; та заповнення/форматування ("інші дані"). Малюнок 2 ілюструє процес. Хоча інгредієнти виявляються в певний момент часу, наприклад, у надійному виробничому середовищі, обчислена таємниця ніколи не розкривається і завжди залишається прихованою (рис2.2)

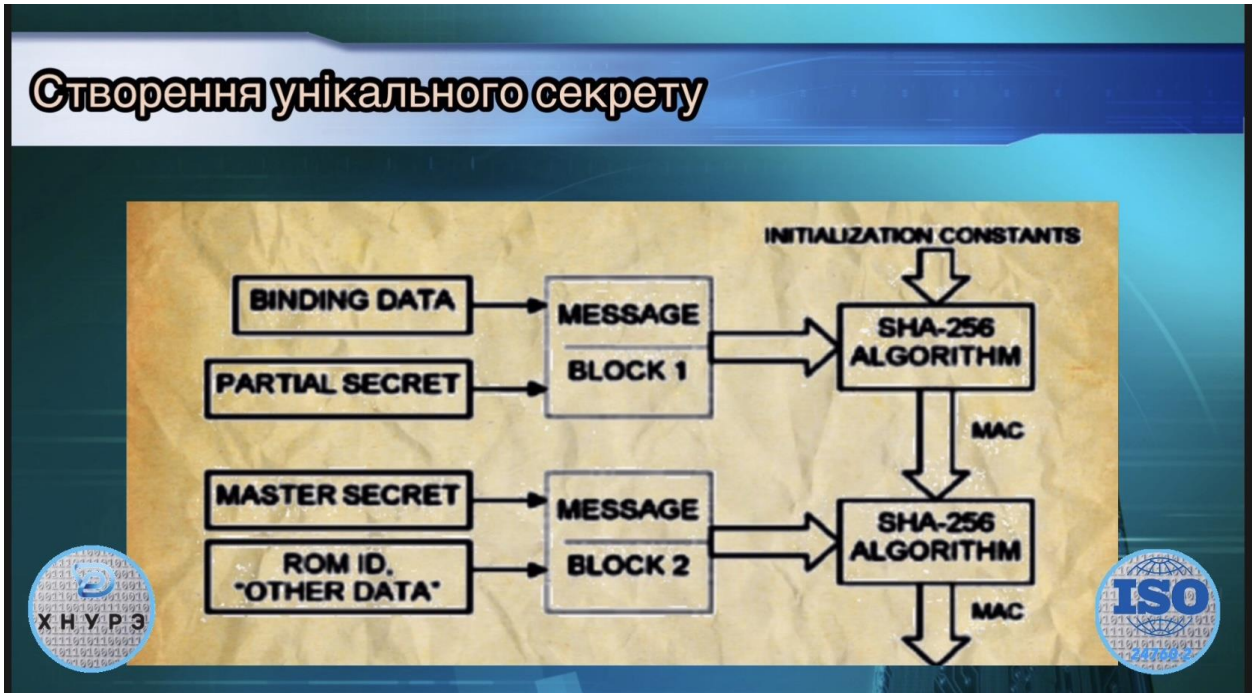


Рис. 2.2 Створення унікального секрету.

З міркувань безпеки та простору для зберігання унікальні секрети всіх захищених пам'ятей в системі не можна зберігати у захищеному співпроцесорі або на хості. Натомість співпроцесор зберігає *лише* основний секрет та дані прив’язки в захищеному розділі пам’яті. Частковий секрет - це системна константа, яка може бути закодована в прошивці головного процесора і відкрито передана. Після прочитання ідентифікатора ПЗУ автентифікатора співпроцесор може обчислити унікальний секрет, як показано на рис. 2. Оскільки аутентифікатор та співпроцесор тепер ділиться унікальним секретом, система готова до роботи.

2.2.4 Аутентифікація виклику та відповіді

Основна мета захищеного автентифікатора - надати доказ того, що об'єкт, до якого він прикріплений, є справжнім. Симетрична автентифікація на основі ключів використовує секретний ключ та дані (повідомлення), що підлягають автентифікації, як вхідні дані для обчислення MAC. Хост виконує ті ж обчислення, використовуючи очікуваний секрет і ті ж дані

повідомлення; потім він порівнює свою версію MAC з версією, отриманою від безпечного автентифікатора. Якщо обидва результати MAC ідентичні, захищений автентифікатор є частиною системи.

У цій системі автентифікації SHA-256 повідомлення являє собою комбінацію виклику хосту та елементів даних, що зберігаються в безпечному аутентифікаторі. Дуже важливо, щоб виклик ґрунтувався на випадкових даних. Незмінний виклик відкриває двері для повторення атак за допомогою дійсного статичного MAC, який записується та відтворюється замість MAC, який миттєво обчислюється.

Захищений автентифікатор обчислює MAC із завдання; її секрет; дані пам’яті; та додаткові дані, які разом складають повідомлення (рис. 3). Якщо безпечний автентифікатор може створити дійсний MAC для будь -якого виклику, можна з упевненістю припустити, що він знає секрет і, отже, може вважатися справжнім (рис 2.3)

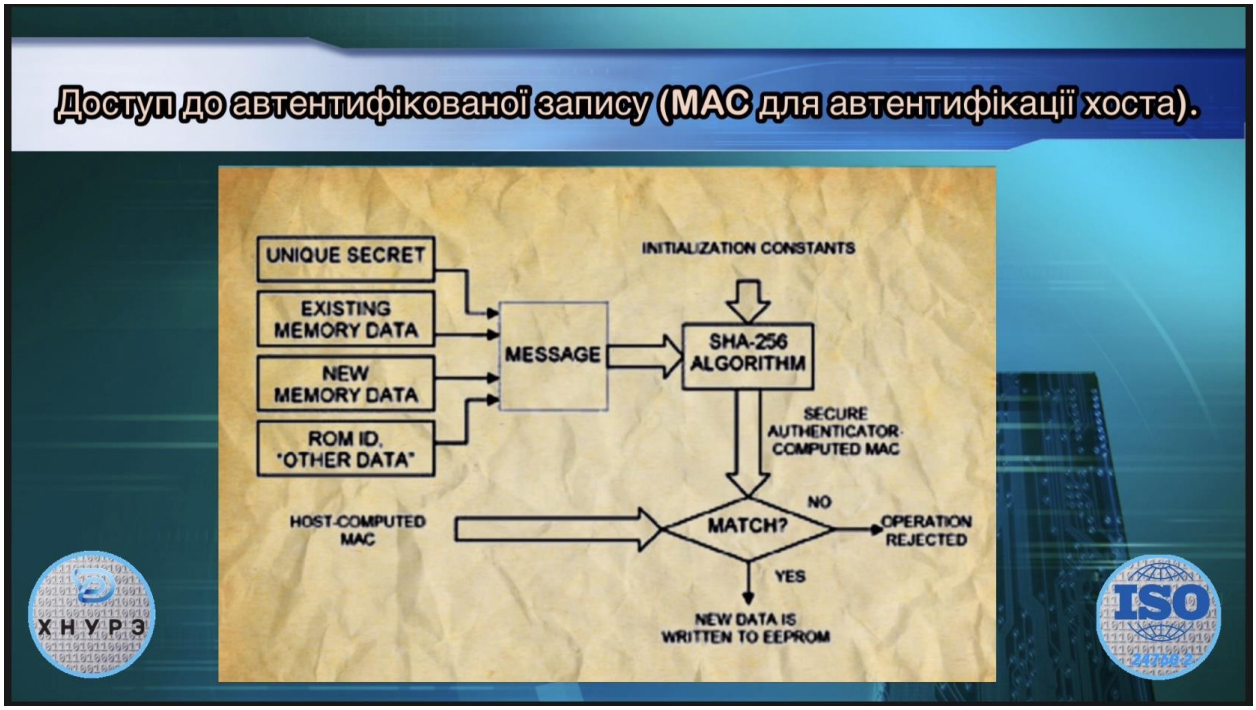


Рис. 2.3 Обчислення MAC для автентифікації виклику та відповіді.

2.2.5 Захист даних (автентифікована запис)

Крім підтвердження автентичності, дуже бажано знати, що дані, що зберігаються в захищеному аутентифікаторі, можна довіряти. Для цього деякі або всі EEPROM у захищеному автентифікаторі можуть бути захищені для (рис 2.4) автентифікації.

Рис. 2.4 Доступ до автентифікованої запису (MAC для автентифікації хоста).

Якщо активовано захист автентифікації, доступ до запису в пам'ять вимагає, щоб хост представив доказ своєї автентичності, надавши MAC для автентифікації хоста безпечному автентифікатору (мал. 4). MAC для автентифікації хоста обчислюється з нових даних пам'яті; наявні дані пам’яті; унікальний секретний секретний аутентифікатор плюс ідентифікатор ПЗУ; та інші дані, які разом складають повідомлення. Захищений аутентифікатор обчислює MAC таким же чином.

Справжній хост відтворив секрет безпечного автентифікатора і може створити дійсний MAC із доступом до запису. Отримуючи MAC від хоста, захищений автентифікатор порівнює його з власним результатом. Дані

записуються в EEPROM, лише якщо обидва MAC збігаються. Області пам'яті користувача, захищені від запису, не можна змінювати, навіть якщо MAC правильний.

2.2.6 Захист даних зашифроване читання та запис

Приклад чіпа, який ми використовуємо, захищеного аутентифікатора DS28C22, може виходити за межі загальних аутентифікаторів SHA-256, де секрет ніколи не розкривається, і може бути налаштований таким чином, що він навіть не відкриває свої дані пам'яті під час доступу до читання та запису в пам'яті. Цей посилений захист досягається за допомогою шифрування даних під час транзитування

Шифрування з доступом до запису використовує одноразову клавіатуру (OTP), яка обчислюється з набору шифрування, що надається хостом; секрет безпечного автентифікатора; частина ідентифікатора ROM аутентифікатора; та інші дані (дані про заповнення, форматування та адресу даних). Як показано на рис. 5, ці елементи даних утворюють повідомлення, яке обробляється за алгоритмом SHA-256. Отриманий код автентифікації повідомлення - це OTP. Хост XOR надсилає нові дані пам’яті з відповідними даними в OTP, перш ніж надсилати їх автентифікатору. Аутентифікатор знову виконує XOR, відновлюючи вихідні дані, які потім запрограмовані на EEPROM користувача. Хост надає насіння шифрування, яке має бут випадковим числом. Таким чином, навіть якщо хост записує одні і ті ж дані знову і знову комусь, хто підслуховує шину I²C (рис2.5)

Рис. 2.5. Доступ до шифрованого запису.

Шифрування доступу для читання дуже схоже на шифрування для доступу до запису. Хоча елементи даних повідомлення, по суті, однакові, існують відмінності в «інших даних», які спричиняють, що OTP для доступу для читання відрізняється від OTP для запису, навіть якщо інші інгредієнти ідентичні. Як показано на мал. 6, захищений автентифікатор бере дані з пам’яті користувача, XOR їх передає за допомогою OTP і робить їх доступними для читання для хоста. Потім хост виконує XOR, використовуючи свою версію OTP. Якщо хост може обчислити секрет безпечного автентифікатора та OTP, що використовується для шифрування, крок XOR успішно розшифровує дані. Знову ж таки, хост надає насіння шифрування, яке має бути випадковим числом. Тепер навіть якщо хост неодноразово читає ті самі дані, щоб хтось підслуховував шину I^2C, дані завжди виглядають інакше.(рис2.6)

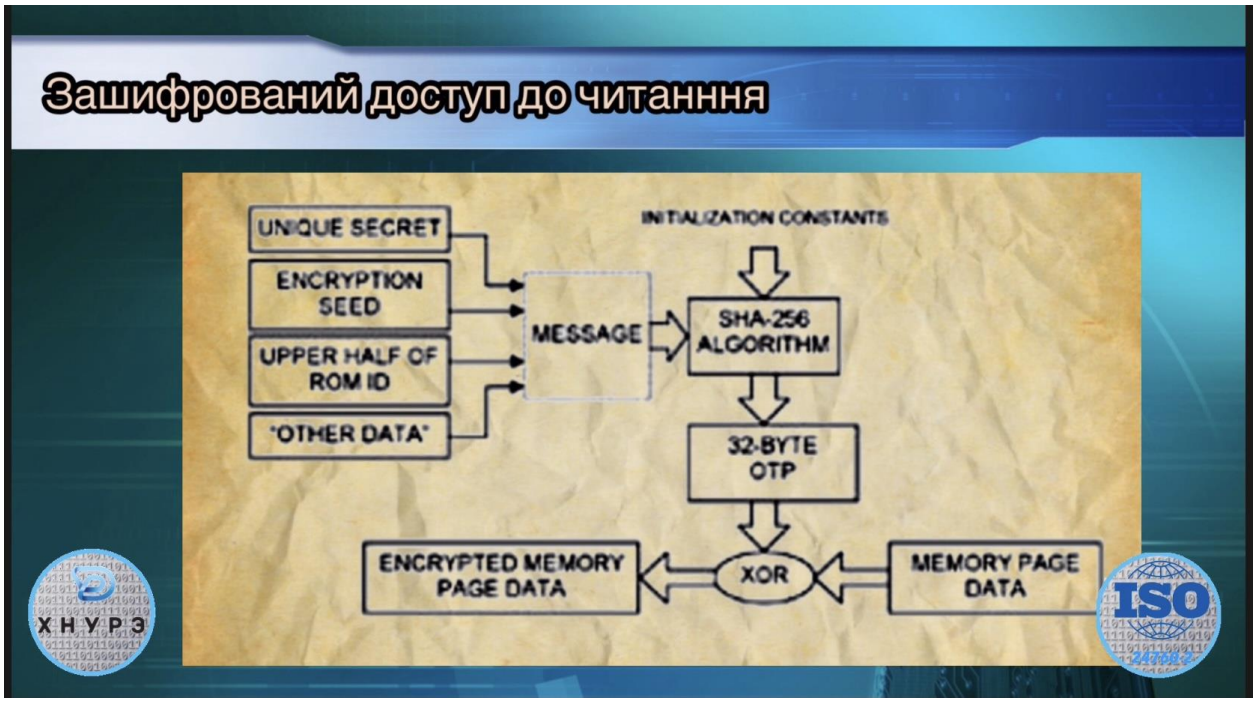


Рис 2. 6. Зашифрований доступ для читання.

Зашифроване записування не перешкоджає запису в пам'ять хост - процесору, який не знає секрету безпечного автентифікатора. Однак фактично записані дані в пам’ять не принесуть ніякої користі. Слід визнати, що можна було зловмисно витерти пам’ять і таким чином поставити під загрозу автентифікатор. Щоб цього не сталося, області пам'яті, налаштовані для шифрування, повинні бути захищені від запису після початкового запису або захищені автентифікацією, щоб дозволити зміни. Тоді лише справжній хост може змінити дані пам’яті.

Зашифрований автентифікований доступ до запису складається з двох кроків. На першому кроці хост шифрує нові дані, як на малюнку 5, а потім надсилає їх у захищений автентифікатор. На другому етапі хост обчислює MAC для автентифікації запису, як на малюнку 4, а потім надсилає його до захищеного автентифікатора. На відміну від автентифікованого запису без шифрування, тепер MAC обчислюється як із наявних розшифрованих даних пам’яті, так і із зашифрованих нових даних пам’яті.

2.2.7 Таємний захист

Секрет безпечного аутентифікатора та головний секрет безпечного співпроцесора читаються захищеними апаратним забезпеченням. При бажанні секрет можна захистити від запису, що запобігає втручанню в дані автентифікатора шляхом заміни невідомого секрету відомим секретом. Після встановлення дані зв'язування, які зазвичай зберігаються в пам'яті співпроцесора, слід читати захищеними. Цей рівень захисту діє до тих пір, поки співпроцесор та автентифікатор налаштовані для застосування на надійній виробничій площадці.

2.2.8 Безпека DeepCover

Розгортання технологій DeepCover від Maxim Integrated забезпечує найсильніший доступний захист від будь-яких атак на рівні смерті, які намагаються виявити секретний ключ. Технології DeepCover включають численні схеми для активного моніторингу подій на рівні штампа, передові методи маршрутизації та компонування штампа, а також додаткові фірмові методи боротьби зі складними можливостями зловмисників.

2.2.9. Двонаправлена автентифікація

Захищений автентифікатор у прикладі системи підтримує як перевірку автентичності та відповіді, так і автентифіковані записи (автентифікація хоста). Вся пам'ять користувача може бути використана для автентифікації виклику та відповіді. Двонаправлена автентифікація застосовується до областей пам'яті, налаштованих для безпечного зберігання даних (автентифікована запис). Шифрування даних не перешкоджає автентифікації виклику та відповіді. MAC для автентифікації завжди обчислюється з незашифрованих даних у EEPROM користувача. [19]

Врироб гикам необхідно захищати свою продукцію продукцію від підроблених компонентів, які компанії з післяпродажного обслуговування намагатимуться впровадити у ланцюжок поставок OEM. Безпечна автентифікація забезпечує надійне електронне рішення для вирішення цієї загрози.

Традиційно системи автентифікації спиралися на симетричні алгоритми, такі як алгоритми безпечного хешування [1]які вимагають секретних ключів. Однак управління та захист секретних ключів може бути складним. Бажаною альтернативою цій логістичній проблемі є криптографія з еліптичною кривою (ECC), де всі пристрої -учасники мають пару ключів, які називаються «приватний ключ» та «відкритий ключ». Приватний ключ використовується автором для підписання повідомлення, а одержувач використовує відкритий ключ ініціатора для перевірки справжності підпису. Якщо повідомлення буде змінено на шляху до одержувача, перевірка підпису буде невдалою, оскільки вихідний підпис недійсний для зміненого повідомлення. Стандарт цифрового підпису (DSS), виданий Національним інститутом стандартів і технологій (NIST), визначає відповідні еліптичні криві, обчислення пар ключів та цифрові підписи. [2] У цій статті обговорюється концепція алгоритму цифрового підпису еліптичної кривої (ECDSA) та показано, як цей метод можна використовувати на практиці.

2.3Еліптичні криві

Багато читачів можуть пов'язувати термін «еліптичний» з конічними розділами з далеких шкільних днів. Еліпсис-це окремий випадок загального рівняння другого ступеня $ax^2 + bxy + cy^2 + dx + ey + f = 0$. Залежно від значень параметрів від a до f, отриманий графік може бути колом, гіперболою, або парабола. Криптографія з еліптичною кривою використовує рівняння третього ступеня.

DSS визначає два види еліптичних кривих для використання з ECC: псевдовипадкові криві, коефіцієнти яких генеруються на підставі вихідної криптографічної хеш-функції; та спеціальні криві, коефіцієнти та поле, що лежить в їх основі, були обрані для оптимізації ефективності операцій з еліптичною кривою. Псевдовипадкові криві можна визначити над простими полями GF (p), а також над двійковими полями GF (2m).

Просте поле - це поле GF (p), яке містить просте число елементів p. Елементами цього поля є цілі числа за модулем p; арифметика поля реалізована з точки зору арифметики цілих чисел за модулем p. Відповідна еліптична крива має вигляд $y^2 = x^3 + ax + b$. На рисунку 1 показаний приклад еліптичної кривої в дійсній області та над основним полем за модулем 23. Загальною характеристикою є вертикальна симетрія.(2.7)

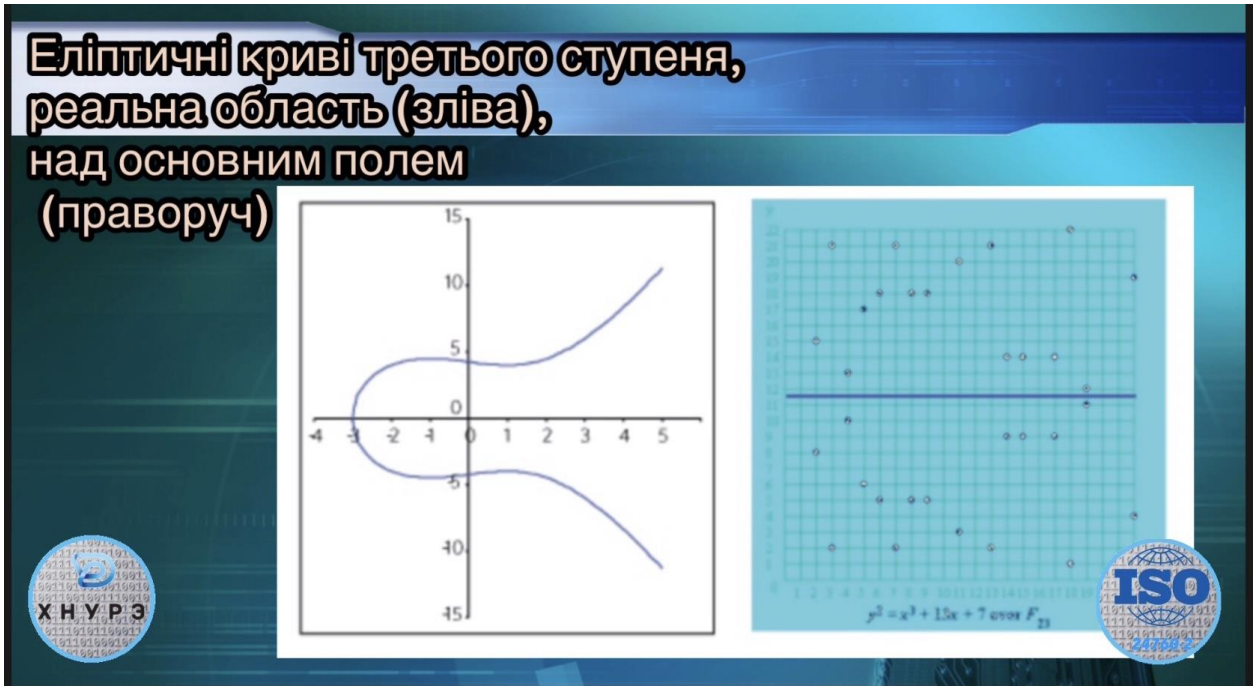


Рисунок 2.7. Еліптичні криві третього ступеня, реальна область (зліва), над основним полем (праворуч).

Двійковим полем є поле GF (2 м), яке містить елементи 2 м для деякого м (так званий ступінь поля). Елементами цього поля є бітові рядки довжиною m; арифметика поля реалізована з точки зору операцій над бітами. Відповідна еліптична крива має вигляд $y^2 + xy = x^3 + ax^2 + b$.

Хоча існує практично необмежена кількість можливих кривих, які відповідають рівнянню, лише невелика кількість кривих має значення для ECC. Ці криві згадуються як еліптичні криві, рекомендовані NIST, у публікації FIPS 186. Кожна крива визначається своїм назвою та набором параметрів домену, який складається з простого модуля p, першого порядку

n, коефіцієнта a, коефіцієнта b та x і y координати базової точки G (x, y) на кривій. Таблиця 1 , наприклад, показує параметри області кривої P-192, яка є псевдовипадковою кривою над простим полем. Додаткові приклади див. У посиланні 2. Цифрова частина назви кривої вказує довжину приватного ключа в бітах. Розмір відкритого ключа та цифрового підпису вдвічі перевищує довжину приватного ключа.

Таблиця 1. Параметри домену кривої P-192

Назва параметра	Позначення	Цінність
Основний модуль c	Десятковий	6277101735386680763835789423207666416083908700390324961279
	Шестигранна	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFF
Головне замовлення n	Десятковий	6277101735386680763835789423176059013767194773182842284081
	Шестигранна	FFFFFFFF FFFFFFFF FFFFFFFF 99DEF836 146BC9B1 B4D22831
Коефіцієнт a	Десятковий	-3 (так само, як p - 3)
	Шестигранна	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFC
Коефіцієнт b	Шестигранна	64210519 E59C80E7 0FA7E9AB 72243049 FEB8DEEC C146B9B1
x координата базової точки G (x, y)	Шестигранна	188DA80E B03090F6 7CBF20EB 43A18800 F4FF0AFD 82FF1012
y координата базової точки G (x, y)	Шестигранна	07192B95 FFC8DA78 631011ED 6B24CDD5 73F977A1 1E794811

2.8.1 Математична довідка

Криптографія з еліптичною кривою включає скалярів та точки. Як правило, скаляри представлені малими літерами, тоді як точки представлені великими літерами, як у таблиці 1. Для скалярів визначено три числові операції: додавання (+), множення (*) та інверсія ($^{-1}$). Для точок існує дві числові операції: додавання (+) і множення (×). Хоча символ «+» використовується для

скалярів і точок, додавання точки відповідає іншим правилам, ніж скалярне додавання. Ці операції застосовуються до кривих над простими полями, а також до кривих над двійковими полями. Алгебраїчні формули для виконання цих обчислень наведені у посиланні 3.

Обчислення, необхідні для автентифікації ECDSA, - це створення пари ключів (приватний ключ, відкритий ключ), обчислення підпису та перевірка підпису. Відповідні рівняння зустрічаються в публічній літературі. [2], [3], [4] На жаль, різні автори використовують власні умови, що ускладнює дотримання їх пояснень. Щоб подолати цю прогалину, сюди включаються рівняння, чітко дотримуючись наведених вище умов.

2.3.1 Генерація пари ключів

Перш ніж аутентифікатор ECDSA зможе працювати, йому потрібно знати його приватний ключ. Відкритий ключ походить від приватного ключа та параметрів домену. Пара ключів повинна знаходитися в пам’яті автентифікатора. Як зрозуміло з назви, приватний ключ недоступний із зовнішнього світу. Навпаки, відкритий ключ має бути відкритим для читання. (рис2.8) ілюструє генерацію пари ключів.

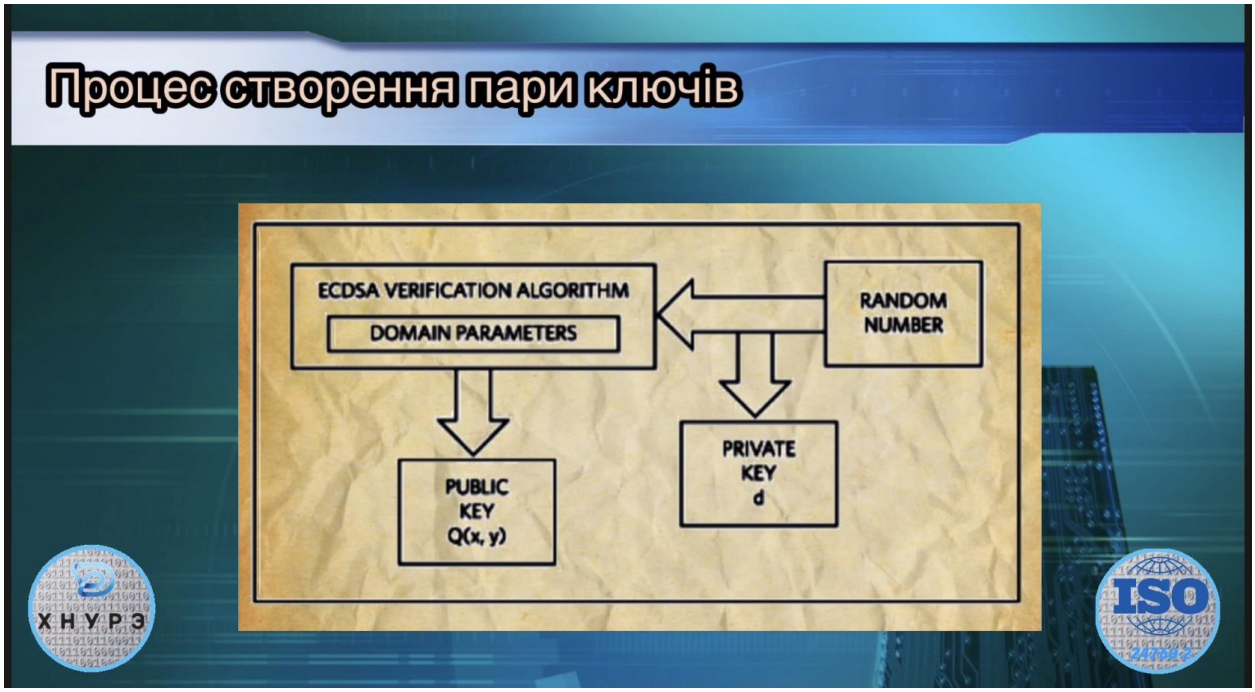


Рисунок 2.8 Процес створення пари ключів.

Генератор випадкових чисел запускається і після завершення операції видає числове значення, яке стає приватним ключем d (скаляром). Далі відкритий ключ Q (x, y) обчислюється відповідно до рівняння 1 за допомогою множення точок:

$$Q(x, y) = d \times G(x, y) \qquad \text{(Рівняння 1)}$$

Розрахунок підпису

Цифровий підпис дозволяє одержувачу повідомлення перевірити справжність повідомлення за допомогою відкритого ключа автентифікатора. Спочатку повідомлення зі змінною довжиною перетворюється на дайджест повідомлень фіксованої довжини h (m) за допомогою алгоритму захищеного хешування. [1] Захищений хеш має такі відмінні властивості: 1) незворотність - обчислювально неможливо визначити повідомлення з його дайджесту; 2) опір зіткненню - недоцільно знайти більше одного повідомлення, яке створює даний дайджест; і 3) високий ефект лавини - будь -яка зміна повідомлення спричиняє значну зміну дайджесту.

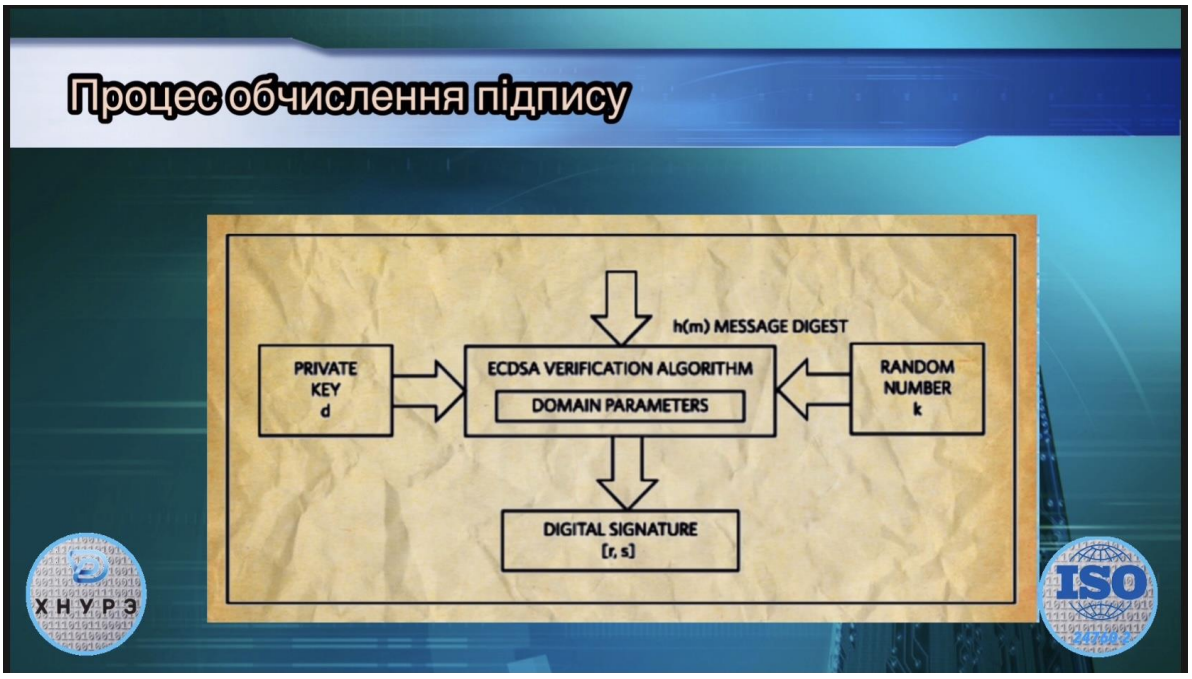


Рис 2.9. Процес обчислення підпису.

Після обчислення дайджесту повідомлення активується генератор випадкових чисел, щоб забезпечити значення k для розрахунків еліптичної кривої. (рис2.9) .

Підпис складається з двох цілих чисел, r і s. Рівняння 2 показує обчислення r з випадкового числа k та базової точки G (x, y):

$$(x1, y1) = k \times G(x, y) \bmod p$$
$$r = x1 \bmod n \qquad \text{(Рівняння 2)}$$

Щоб бути дійсним, r має відрізнятися від нуля. У рідкісному випадку, коли r дорівнює 0, необхідно створити нове випадкове число, k, і r потрібно знову обчислити. Після успішного обчислення r обчислюється s відповідно до рівняння 3 за допомогою скалярних операцій. Вхідними даними є дайджест повідомлення h (m); приватний ключ d; r; і випадкове число k:

$$s = (k^{-1} (h(m) + d * r) \bmod n \qquad \text{(Рівняння 3)}$$

Щоб бути дійсним, s має відрізнятися від нуля. Якщо s дорівнює 0, необхідно створити нове випадкове число k, і r і s потрібно знову обчислити.

2.8.3 Перевірка підпису

Перевірка підпису є аналогом обчислення підпису. Його мета - перевірити справжність повідомлення за допомогою відкритого ключа автентифікатора. Використовуючи той самий алгоритм безпечного хешування, що і на етапі підпису, обчислюється дайджест повідомлень, підписаний автентифікатором, який разом із відкритим ключем Q (x, y) та компонентами цифрового підпису r та s призводить до результату (рис 2.10) ілюструє процес.

Рівняння 4 показує окремі етапи процесу перевірки. Вхідними даними є дайджест повідомлення h (m), відкритий ключ Q (x, y), компоненти підпису r і s та базова точка G (x, y):

$$w = s\text{-}1 \bmod n$$
$$u1 = (h(m) * w) \bmod n$$
$$u2 = (r * w) \bmod n \qquad \text{(Рівняння 4)}$$
$$(x2, y2) = (u1 \times G(x, y) + u2 \times Q(x, y)) n$$

Перевірка пройшла успішно ("проходить"), якщо x2 дорівнює r, тим самим підтверджуючи, що підпис дійсно обчислювався за допомогою приватного ключа

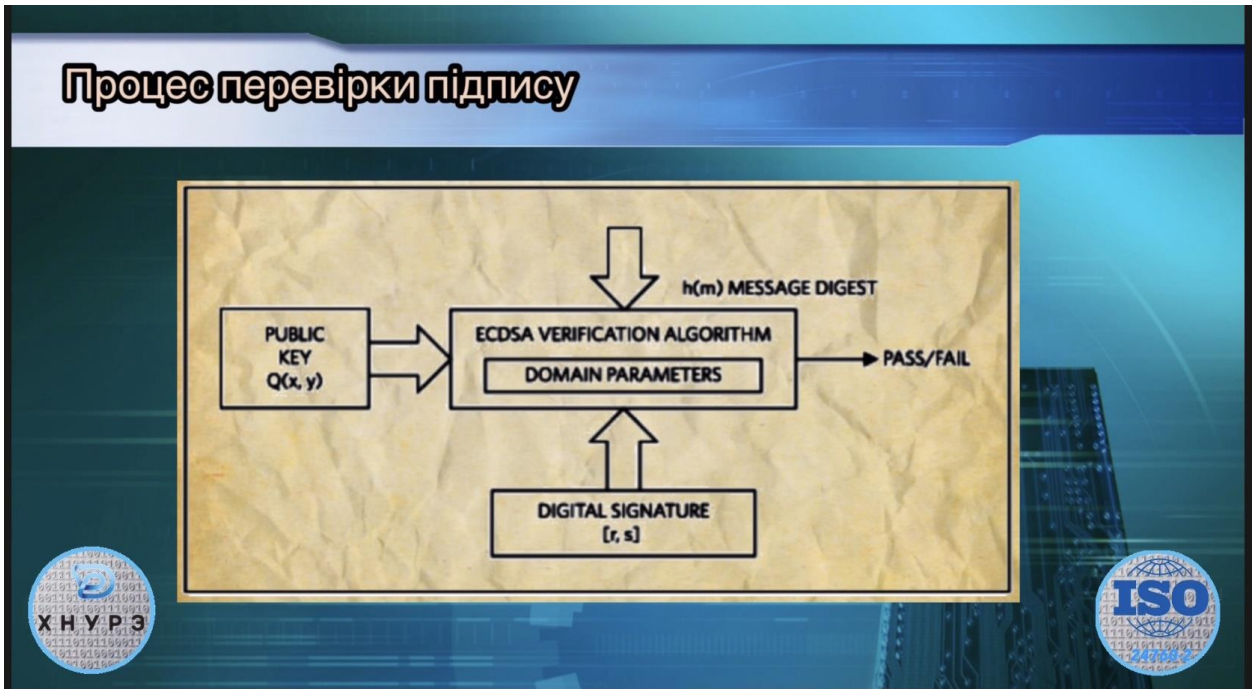


Рисунок 2.10 Процес перевірки підпису.

.

2.3.2 Конфігурація обладнання

Впровадження безпечної системи автентифікації вимагає зв’язування хост -системи з периферійним модулем. Хост -контролер спілкується з автентифікатором по послідовній шині. Можна вибрати будь -який тип автобуса. Одиночний штифт інтерфейсу 1-Wire ® плюс опорний сигнал заземлення (без годинника, без V_{CC}) є особливо привабливим, оскільки він мінімізує складність з'єднання, спрощує конструкцію і таким чином знижує вартість. Новим на малюнку 5 є системний відкритий ключ та системна константа на стороні хоста, а також ідентифікатор пристрою# та сертифікат відкритого ключа на периферійній стороні.(рис 2.11)

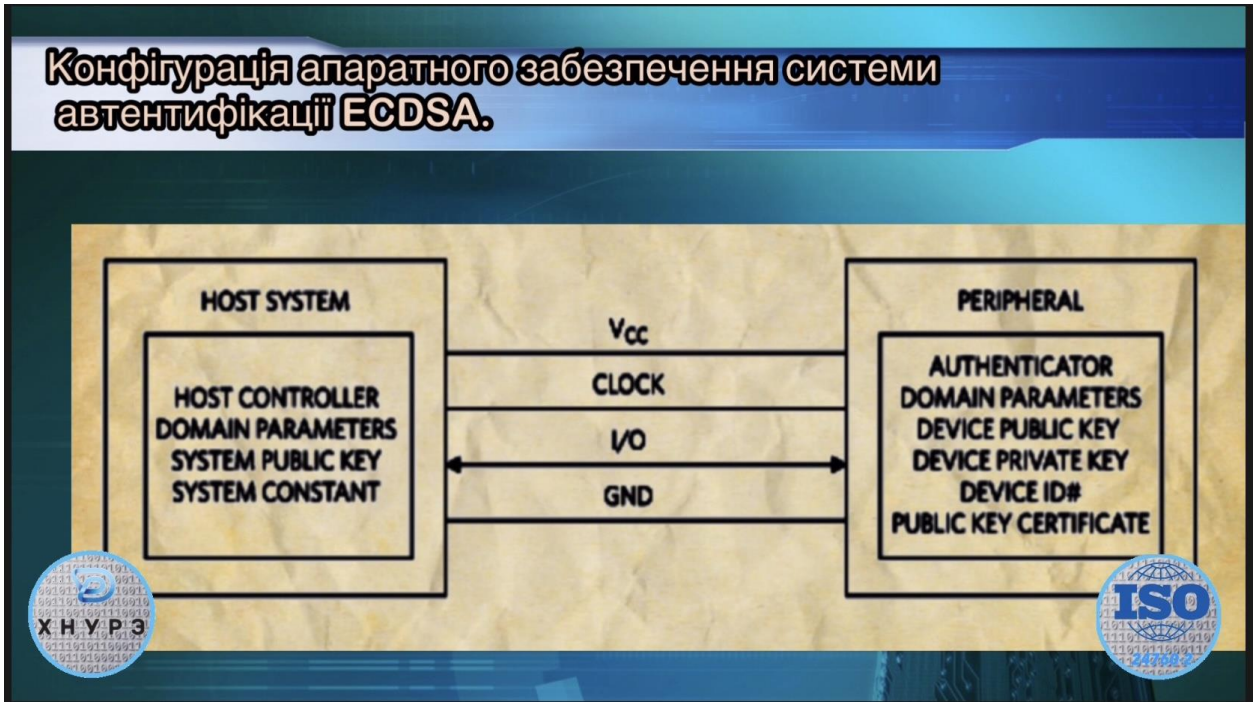


Рисунок 2.11 Конфігурація апаратного забезпечення системи автентифікації ECDSA.

2.3.3 Налаштування автентифікатора

Перш ніж аутентифікатор можна використовувати у програмі, його потрібно налаштувати. Першим кроком є обчислення та встановлення пари ключів (див. Малюнок 2). Пара ключів може бути обчислена зовні, а потім записана в автентифікатор. Крім того, автентифікатор може включати функціональний блок, який виконує цей крок за зовнішньою командою. Щоб запобігти несанкціонованим змінам, пару ключів потрібно захистити від запису.

Додаток може вибирати між двома сценаріями використання. У сценарії 1 усі автентифікатори запрограмовані на одну і ту ж пару ключів. У цьому випадку всі хости в системі знають дійсний відкритий ключ. Будь -який автентифікатор з таким відкритим ключем вважається учасником програми. Для перевірки самого автентифікатора не потрібні додаткові засоби.

У сценарії 2 кожен аутентифікатор має свою власну унікальну пару ключів. У цьому випадку успішна перевірка підписів не дає доказів того, що певний пристрій автентифікації також є учасником певної програми, тобто “системи”. Зв’язування автентифікатора з системою вимагає введення сертифіката, який обчислюється як підпис із відкритого ключа автентифікатора, унікального ідентифікатора пристрою автентифікатора, системної константи та системного приватного ключа. Малюнок 6показує обчислення сертифіката, оскільки це може бути виконано системою управління ключами, також відомою як "орган сертифікації". Два компоненти сертифіката, cr та cs, потім зберігаються в пам’яті автентифікатора та захищені від запису. На цьому налаштування автентифікатора завершено. Зауважте, що у сценарії 2 хост -система повинна знати як системний відкритий ключ, так і системну константу для перевірки дійсності відкритого ключа автентифікатора у програмі.(рисунок 2.13)

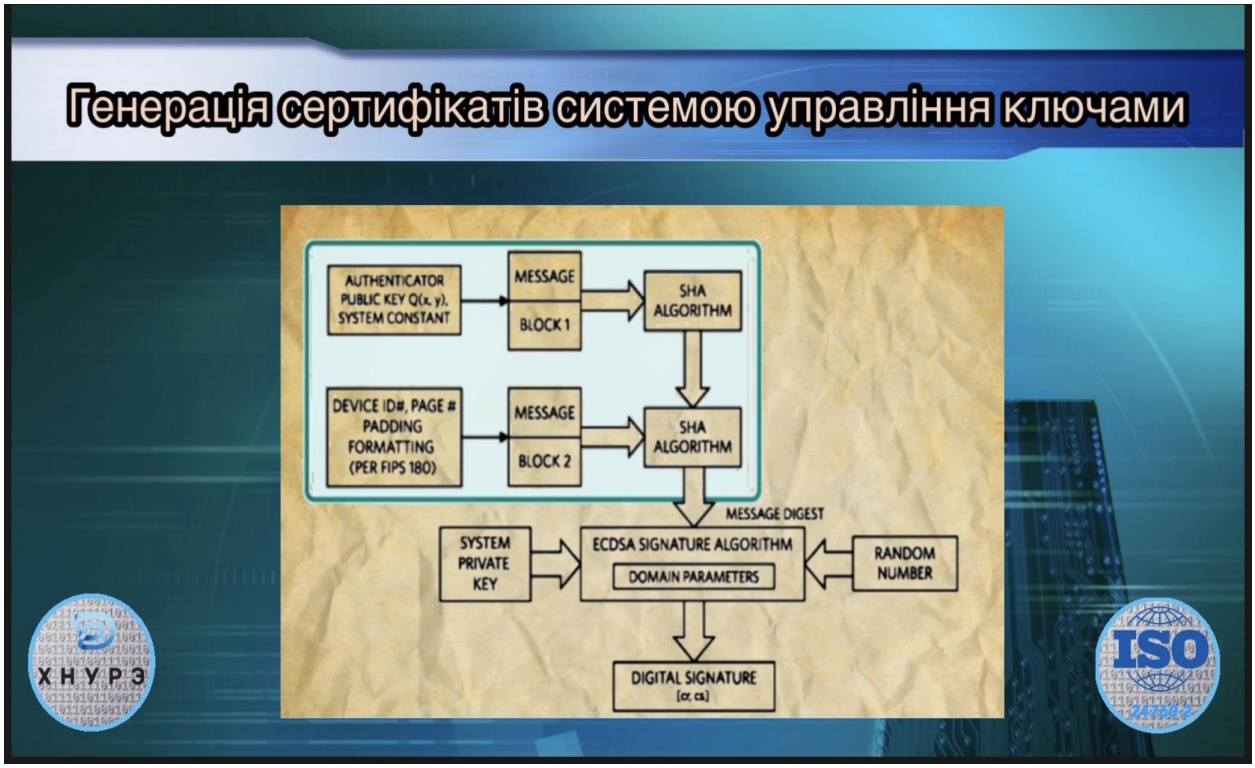


Рисунок 2.13. Генерація сертифікатів системою управління ключами.

Інфраструктура, що підтримує управління сертифікатами, називається інфраструктурою відкритого ключа. За допомогою такої інфраструктури можна створювати сертифікати та надавати засоби для їх перевірки. Ще однією перевагою такої інфраструктури є можливість підтримки товарів, вироблених третіми сторонами або субпідрядниками. Якщо припустити, що субпідрядник виготовив товари із вбудованими автентифікаторами ECDSA і що кожен аутентифікатор має свою власну статистично унікальну пару ключів, то підписання їх відкритого ключа для створення сертифіката змушує їх приєднатися до системи.

2.3.4 Автентифікація розгорнутого периферійного пристрою

По -перше, аутентифікатор включається (кроки 1, 2). Потім хост отримує ідентифікатор пристрою аутентифікатора і читає відкритий ключ та сертифікат (кроки 3–7). Тепер хост виконує алгоритм перевірки підписів сертифіката (Крок 8, Малюнок 8). Якщо результатом є "pass", відкритий ключ дійсний у системі. Якщо результат “невдалий”, автентифікатор не належить до системи; хост може пропустити кроки 9-12 і негайно вимкнути аутентифікатор (кроки 13–15) (рис 2.14)

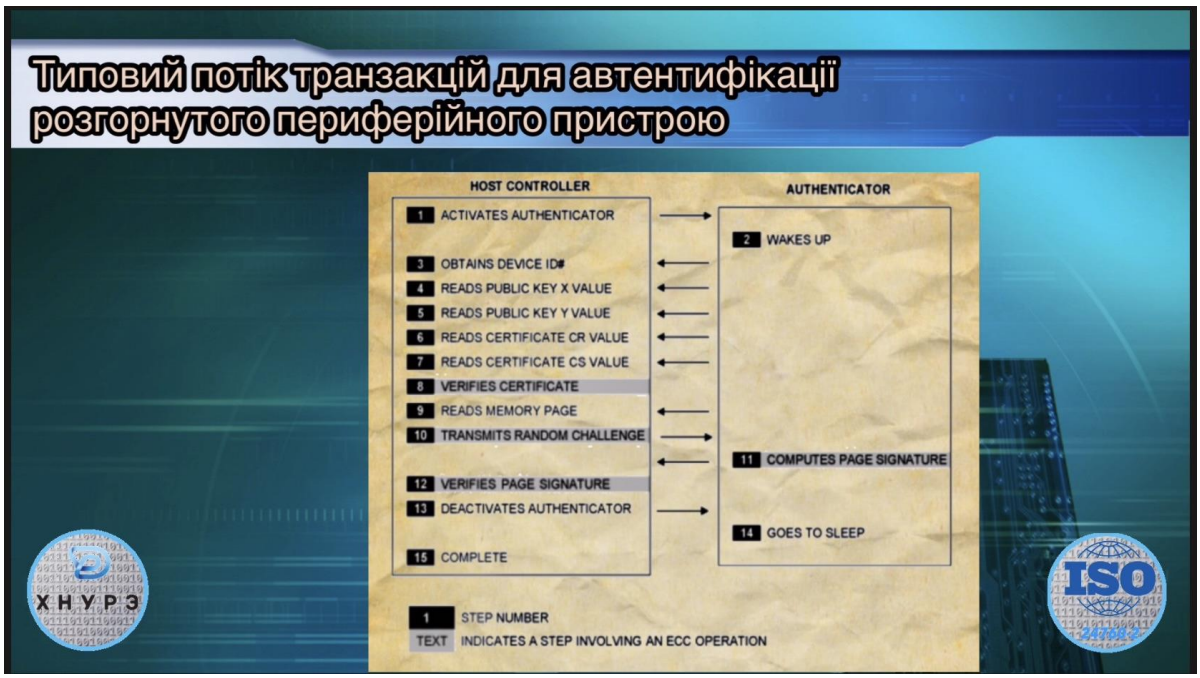


Рисунок 2.14 Типовий поток транзакцій для автентифікації розгорнутого периферійного пристрою.

Знання того, що відкритий ключ автентифікатора дійсний у системі, не гарантує, що хост спілкується з справжнім автентифікатором. Дані, які використовуються досі, також могли надходити з емулятора, який намагається виконати атаку повтору. Щоб визначити, чи автентифікатор на периферійному пристрої справжній, ведучий читає одну зі сторінок пам'яті аутентифікатора (крок 9), надсилає аутентифікатору випадковий виклик (крок 10) і вказує йому обчислити підпис. Повідомлення складається з даних сторінки пам’яті, завдання, ідентифікатора пристрою #, сторінки № плюс відступування та форматування. На малюнку 9 показано, як автентифікатор ECDSA обчислює підпис. Підпис обчислюється в режимі реального часу за допомогою апаратного двигуна ECDSA автентифікатора. Два компоненти підпису r і s надсилаються на хост (крок 11) для перевірки. Зауважте, що обчислення підпису включає приватний ключ автентифікатора та випадкове число. Отже, навіть якщо завдання залишається незмінним, наступні обчислення підписів забезпечують різні значення підпису Тепер з усіма необхідними даними, включаючи підпис, хост обчислює дайджест повідомлення та виконує алгоритм перевірки підпису для підпису . Якщо результат "пройти", автентифікатор перевіряється як справжній. Якщо результат “невдалий”, пара ключів в автентифікаторі недійсна, і хост відхиляє периферійні пристрої.

2.3.5 Доступна безпека автентифікації відкритого ключа з еліптичною кривою

Стандарт цифрового підпису був спочатку випущений в 1994 році, і протягом тривалого часу автентифікація ECDSA була переважно предметом теоретичних досліджень. Ця ситуація нещодавно змінилася з такими продуктами, як Maxim DeepCover ® Secure Authenticator DS28E35 , перший автентифікатор ECDSA з 1-дротовим інтерфейсом і 1Kbit користувальницькою EEPROM. Рішення безпеки, вбудовані в DeepCover, приховують конфіденційні дані під кількома рівнями розширеної фізичної безпеки, щоб забезпечити максимально безпечне зберігання ключів. DS28E35 реалізує ECC, використовуючи псевдовипадкову криву над основним полем відповідно до

рівняння $y^2 = x^3 + ax + b$ з використанням параметрів області кривої P-192 (табл.1). Пристрій може самостійно обчислити, встановити та заблокувати пару приватних/відкритих ключів; вона не потребує сторонньої допомоги. Для зберігання та блокування сертифіката відкритого ключа виділяється окремий простір пам'яті. DS28E35 також має одноразово настроюваний, енергонезалежний 17-розрядний лічильник зменшення по команді. Цей лічильник можна використовувати для відстеження терміну служби периферійного пристрою, в який вбудований DS28E35. Кожен пристрій має власний гарантований унікальний 64-розрядний ідентифікатор пристрою# заводський, запрограмований у чіп. Як показано вище, ідентифікатор пристрою# є основним вхідним параметром для криптографічних операцій. Простота інтерфейсу 1-Wire (використовуючи лише введення-виведення та GND полегшує використання DS28E35 у широкому спектрі програм. Як опція послуги з доданою вартістю, налаштування пристрою (пара ключів, сертифікат), включаючи програмування пам’яті користувача та ініціалізацію лічильника, може виконуватись захищеною фабричною службою Максима. Ця послуга є безпечним методом налаштування деталей перед відвантаженням у ланцюжок поставок OEM. Таким чином, це виключає можливість розкриття конфіденційних даних та розвантажує необхідні ключові системи управління та зусилля.

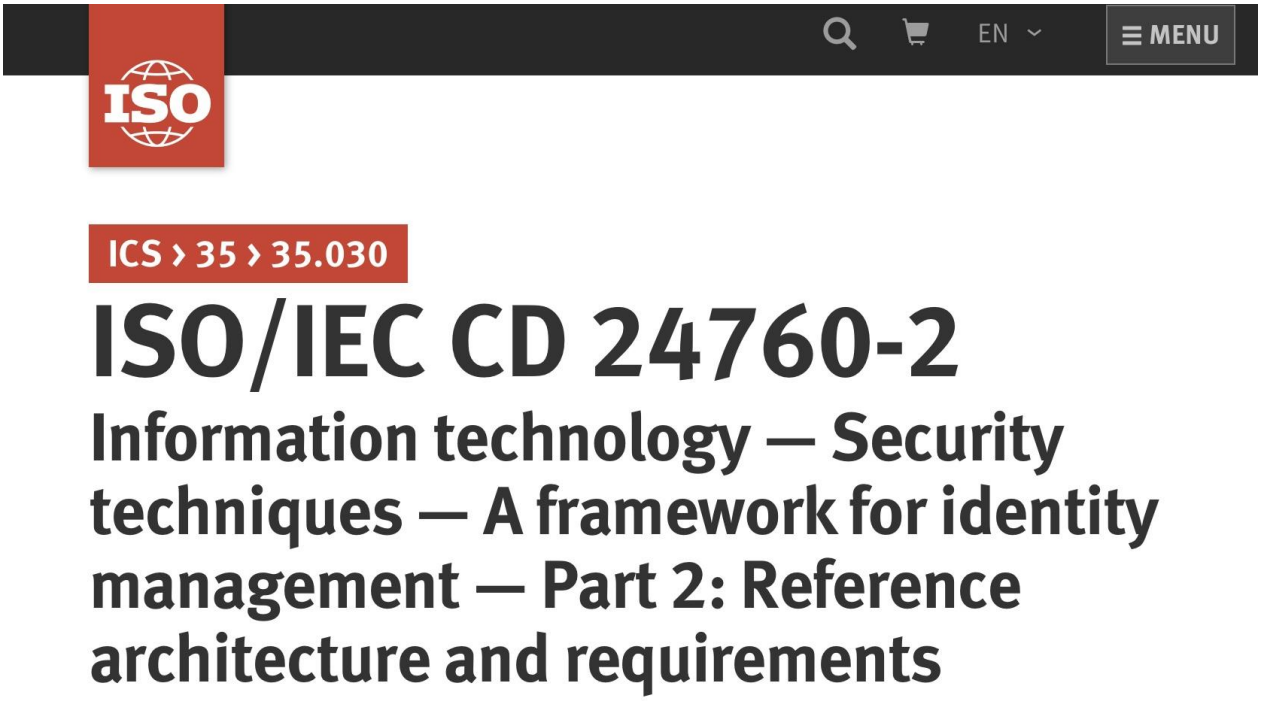
Висновок : Основна перевага ECDSA полягає в тому, що сторона, яка автентифікує периферійне обладнання, звільняється від обмежень для безпечного зберігання секрету. Сторона автентифікації може автентифікуватися завдяки відкритому ключу, який можна вільно розповсюджувати. Схеми автентифікації, такі як вбудовані рішення безпеки DeepCover від Maxim, допомагають спростити впровадження надійних методів автентифікації виклик-відповідь, які складають основу більш ефективної безпеки додатків. Автентифікатори ECDSA також спрощують автентифікацію товарів від третіх сторін або субпідрядників.

3 ДОСЛІДЖЕННЯ МОДЕЛЕЙ ТА МЕТОДІВ АВТОРИЗАЦІЇ ДОСТУПУ В ІТС

3.1 Аналіз недоліків протоколів безпеки хмарних сервісів

Проведені дослідження протоколів безпеки хмарних сервісів дозволили виявити певні недоліки при формуванні ключів авторизації доступу. Виявлені недоліки обумовлюють об’єктивно існуюче протиріччя, коли необхідні властивості схеми автентифікації та авторизації не забезпечуються застосовуваними механізмами, що створює передумови для несанкціонованого перехвату переданих даних, неавторизованого доступу до різних даних , порушень, що пов’язані з хибною автентифікацією пристроїв та користувачів системи, порушень або виходу за встановлені режими роботи комунікаційних пристроїв та окремих елементів системи. Виявлене протиріччя обумовлює актуальність наукового дослідження моделей та методів авторизації доступу для підвищення безпеки безпроводових телекомунікаційних систем та мереж.

В цьому розділі проводяться дослідження протоколів автентифікації та авторизації доступу в безпроводових телекомунікаційних системах та мережах відповідно до специфікації міжнародних стандартів ISO/IEC 24760-2:2021.



Розробляється математична модель авторизації та автентифікації доступу до хмарних сервісів, в якій враховуються колізійні властивості формованих ключів авторизації для оцінки безпеки хмарних сервісів. Проводяться експериментальні дослідження властивостей застосовуваної функції генерації ключів авторизації та оцінюється рівень забезпечуваної безпеки. Отримані результати досліджень дозволили встановити певні недоліки застосовуваного методу авторизації та автентифікації, для усунення яких пропонується удосконалений метод, який відрізняється використанням генераторів псевдовипадкових послідовностей максимального періоду, що за рахунок забезпечення потрібних колізійних властивостей формованих ключів авторизації дозволяє підвищити безпеку хмарних сервісів.

3.2 Дослідження протоколів автентифікації та авторизації доступу в CS та ISO/IEC 24760

Для вирішення задач автентифікації та авторизації в CS , які побудовано відповідно до специфікації міжнародних стандартів серії ISO/IEC 24760,

використовуються засоби протоколу EAP (Extensible Authentication Protocol), криптографічного протоколу RSA (Rivest, Shamir і Adleman), а також засоби протоколу управління ключами PKM (Privacy and Key Management protocol) для безпечного розподілу ключової інформації.

Протоколи автентифікації і авторизації, які використовуються в CS, призначено для забезпечення вимог сервіс-провайдерів (IPS) та користувачів. З одного боку, автентифікація дозволяє встановити достовірність користувача . За допомогою процедури авторизації сервіс-провайдер ISP встановлює відповідність між автентифікованим користувачем та переліком доступних йому сервісів. Таким чином, сервіс-провайдери можуть бути упевнені в тому, що доступ до хмарного сервісу буде надано тільки їх клієнтам, і що вони використовуватимуть тільки ті сервіси, за які сплатили. З іншого боку, підрівень безпеки стандартів ISO/IEC 24760-2:2021 задовольняє основним вимогам користувачів, а саме, вимоги в конфіденційності і цілісності даних, що передаються в мережі, а також в тому, що клієнт завжди зможе дістати доступ до сплачених ним сервісів.

Згідно специфікації ISO/IEC 24760-2:2021 у якості автентифікатора AC найчастіше виступає спеціальна служба автентифікації всередині ASN (Access Service Network). Повідомлення між користувачем та хмарою передаються відповідно до протоколу PKM за допомогою PKM-REQ, PKM-RSP. БС і автентіфікатор обмінюються інформацією відповідно до протоколу Authentication Relay Protocol. Автентіфікатор зв'язується з сервером AAA, розташованим в домашній мережі CSN (Connectivity Service Network), за допомогою протоколу RADIUS (Remote Authentication in Dial In User Service).

Протокол управління PKM контролює всі компоненти підрівня безпеки і, фактично, визначає загальну схему автентифікації та авторизації доступу.

Розглянемо схему автентифікації та авторизації доступу в типовій інформаційно технічній системі, побудованої відповідно до специфікації міжнародних стандартів серії ISO/IEC 24760-2:2021 дослідимо основні компоненті та застосовувані перетворення, які визначають послідовність дій,

яку потрібно виконати для вирішення задач автентифікації та авторизації доступу.

3.3 Дослідження протоколу автентифікації та авторизації доступу відповідно до специфікації PKMv1

Схема автентифікації та авторизації доступу відповідно до специфікації PKMv1 в інформаціно технічній системі, побудованої за ISO/IEC 24760-2:2021, наведена на рис. 2.1. Відповідно до цієї схеми використовується така послідовність передачі службових повідомлень.

На першому етапі користувач посилає до хмарного сервісу повідомлення Authentication Information. Воно містить цифровий сертифікат X.509, закладений в кінцевий пристрій користувача виробником або сторонньою організацією. Сертифікат містить також MAC-адресу Користувача і її відкритий ключ шифрування. Сам користувач (AC) , відповідно має секретний ключ, який відповідає цьому переданому відкритому ключу (рис3.1)

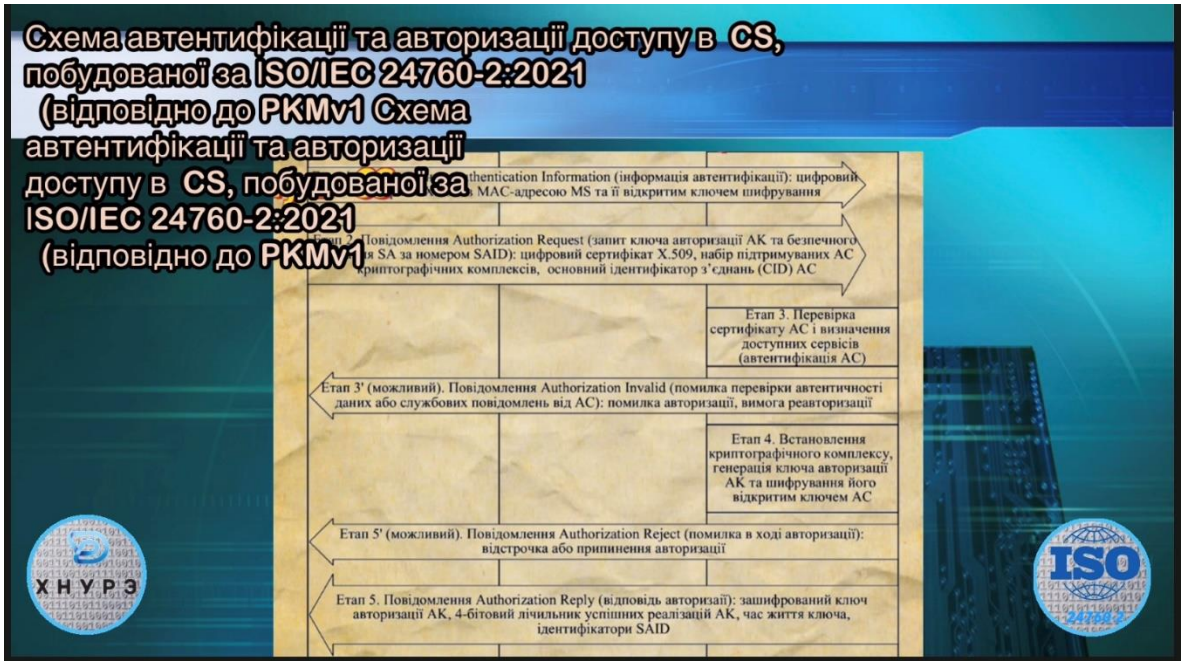


Рисунок 3.1 – Схема автентифікації та авторизації доступу в CS, побудованої за ISO/IEC 24760-2:2021 (відповідно до PKMv1)

Відразу після надсилання повідомлення Authentication Information AC посилає повідомлення Authorization Request, в якому запрошує у БС загальний ключ авторизації (Authorization Key, AK), а також запрошує встановлення безпечного з'єднання (Security Association, SA). За визначенням, яке використовується у специфікації стандартів серії ISO/IEC 24760-2:2021, під безпечним з'єднанням розуміється сукупність інформації, яка дозволяє здійснювати безпечний обмін даними між користовачем та хмарним сервісом. Зокрема, до інформації SA відноситься використовуваний криптографічний комплекс, вектори ініціалізації, ключі TEK і час їх життя. Як вже було відмічено, час життя TEK обмежений, і для постійного підтримування SA AC доводиться отримувати нові ключі через певні проміжки часу.

Безпечне з'єднання SA визначається своїм номером SAID (Security Association Identifier). Цей номер, разом з AK, AC запрошує у БС в повідомленні Authorization Request. Повідомлення містить наступну інформацію:

- цифровий сертифікат X.509;
- набір підтримуваних AC криптографічних комплексів;
- основний ідентифікатор з’єднань (Connection Identifier, CID) AC, який, у разі позитивної відповіді від БС, буде привласнений SAID.

На стороні NAP (Network Access Provider) і NSP (Network Service Provider) здійснюється перевірка сертифікату AC і визначення доступних цій AC сервісів, тобто відбувається авторизація.

Далі БС встановлює загальний з AC підтримуваний криптографічний комплекс, генерує AK, шифрує його відкритим ключем AC і посилає їй повідомлення Authorization Reply, що містить:

- зашифрований ключ авторизації AK;
- 4-бітовий лічильник успішних реалізацій AK;
- час життя ключа;
- ідентифікатори SAID, які БС надає AC для встановлення одного або декілька безпечних з’єднань SA.

У разі виникнення помилок в ході авторизації БС надсилає АС повідомлення Authorization Reject, в якому БС може вимагати від АС або відстрочити спроби авторизації, або припинити ці спроби зовсім (якщо неможливо визначити виробника АС, або не вдається перевірити її цифровий сертифікат, або не представляється можливим погоджувати криптографічний комплекс і т. д.).

Ключ авторизації АК має обмежений термін життя, тому АС (як і БС) повинна періодично оновлювати АК, посилаючи запити Authorization Request. Для того, щоб безпечне з'єднання SA не уривалася на час зміни ключів, АС повинна зберігати одночасно два ключа авторизації АК - поточний і новий, причому такі, що перекривають один одний наполовину за часом дії. Як тільки закінчується термін дії поточного ключа авторизації АК, АС переходить на новий АК (який стає поточним) і посилає Authorization Request для отримання нового АК.

Якщо на стороні БС відбудеться помилка перевірки автентичності даних або службових повідомлень від АС (тобто при підозрі на дію зловмисника), БС може надіслати АС повідомлення Authorization Invalid з вимогою реавторизації.

3.4 Дослідження протоколу автентифікації та авторизації доступу відповідно до специфікації PKMv2

Відповідно до специфікації PKMv2 можливі три схеми автентифікації та авторизації [20]:

- із застосуванням алгоритму RSA (одностороння автентіфікция АС);
- із застосуванням протоколу EAP (двостороння автентифікація: АС і БС);
- комбінація алгоритмів RSA і протоколу EAP (двостороння автентифікація: АС і БС).

Перша схема автентифікації та авторизації (із застосуванням схеми RSA) ідентична розглянутій вище схемі в протоколі PKMv1.

Схеми автентифікації та авторизації із застосуванням протоколу EAP та комбіновані схеми із алгоритмом RSA і протоколом EAP мають спільну загальну конструкцію із двома фазами: фаза EAP і фаза так званого потрійного рукостискання (3-way handshake). Загальна схема автентифікації та авторизації доступу в телекомунікаційній системі, побудованої за IEEE 802.16e (відповідно до PKMv2) зображена на рис. 2.2 [22].

Позначення, використані на рис. 2.2, відповідають схемі авторизації в типовій системі стандарту ISO/IEC 24760-2:2021,

- MS - мобільна станція;
- BS - базова станція;
- AAA - сервер автентифікації, авторизації та обліку.

Перша автентифікація EAP є автентифікацією пристроїв, друга автентифікація EAP є автентифікацією користувачів, що виконується після успішного виконання першої автентифікації EAP.

На першому етапі при необхідності автентифікації пристроїв базова станція (BS) передає запит імені EAP («EAP-REQUEST/IDENTITY») на мобільну станцію (MS), запрошуючи автентифікацію EAP.

На другому етапі, після обміну повідомленнями EAP між мобільною станцією (MS) і базовою станцією (BS) за допомогою протоколу розподілу ключів секретності (PKM)_EAP_TRANSFER в системі IEEE 802.16e, базова станція (BS) передає запит імені EAP («PKM_EAP/EAP-REQUEST/IDENTITY») на мобільну станцію (MS). Мобільна станція (MS) відповідає передачею відповіді з ім'ям EAP («PKM_EAP/EAP-RESPONSE/IDENTITY») (рис 3.1)

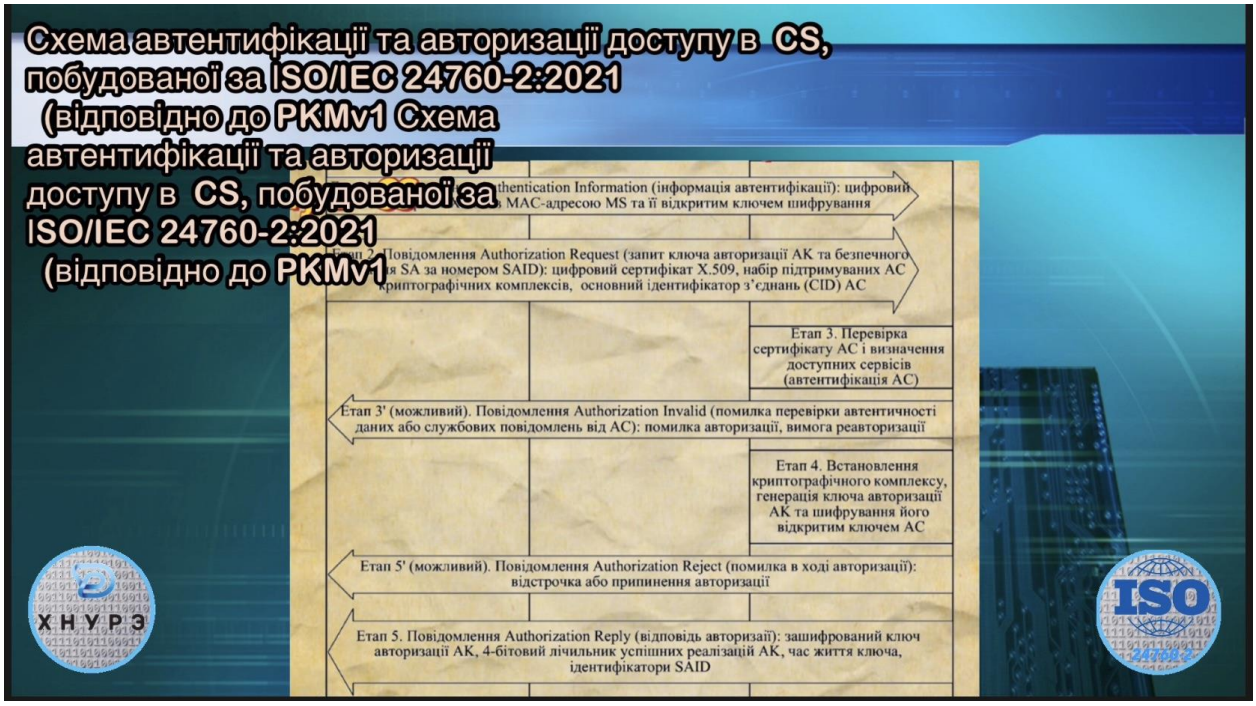


Рисунок 3.1 Схема авторизаціі та автентифікаціі доступу в CS

На третьому етапі базова станція (BS) передає запит імені EAP («PKM_EAP-EAP-RESPONSE/IDENTITY») на сервер автентифікацій, авторизації і обліку (AAA). Базова станція (BS) і сервер аутентифікацій, авторизації і обліку (AAA) обмінюються повідомленнями EAP за допомогою повідомлень протоколу служби дистанційної автентифікації користувачів. Відповідно до цього базова станція (BS) передає відповідне повідомлення («RADIUS ACCESS REQEST/IDENTITY») на сервер автентифікацій, авторизації і обліку (AAA).

На четвертому етапі сервер автентифікацій, авторизації і обліку (AAA) виконує автентифікацію пристроїв на мобільній станції (MS) за допомогою автентифікації повідомлень PKM_EAP з використанням протоколу захисту транспортного рівня (EAP-TLS), протоколу захисту транспортного рівня з використанням передвстановленого загального ключа (EAP-TLSPSK), протоколу для автентифікації і узгодження ключів (EAP-AKA) або протоколу EAP-PSK. В результаті автентифікації пристроїв, на п'ятому та шостому

етапах, сервер автентифікацій, авторизації і обліку (AAA) і мобільна станція (MS) спільно отримують майстер-ключ сеансу (MSK).

На сьомому етапі сервер автентифікацій, авторизації і обліку (AAA) передає повідомлення «RADIUS ACCEPT» як повідомлення «EAP-SUCCESS» на базову станцію (BS). Це повідомлення «RADIUS ACCEPT» включає майстер-ключ сеансу (MSK).

На восьмому етапі базова станція (BS) передає повідомлення «PKM_EAP/EAP-SUCCESS» на мобільну станцію (MS), повідомляючи про успішну автентифікацію EAP.

На дев'ятому та десятому етапах мобільна станція (MS) і базова станція (BS) формують ключ цілісності EAP (EIK) і парний майстер-ключ (PMK) з мастер-ключа сеансу (MSK) в процесі автентифікації пристроїв. Ключ цілісності EAP (EIK), сформований в процесі автентифікації пристроїв, використовується для захисту повідомлень EAP, що передаються в процесі другої автентифікації EAP, тобто автентифікації користувачів.

На одинадцятому етапі, при необхідності автентифікації користувачів, в процесі автентифікації користувачів базова станція (BS) передає повідомлення «PKM_EAP/EAP-REQUEST/IDENTITY» на мобільну станцію (MS). На дванадцятому етапі мобільна станція (MS) відповідає передачею повідомлення «PKM_EAP/EAP-RESPONSE/IDENTITY».

На тринадцятому етапі базова станція (BS) перетворює повідомлення «PKM_EAP/EAP-RESPONSE/IDENTITY» у форму повідомлення «RADIUS ACCESS REQUEST/IDENTITY» і передає його на сервер автентифікацій, авторизації і обліку (AAA).

На чотирнадцятому етапі сервер автентифікацій, авторизації і обліку (AAA) виконує автентифікацію користувачів на мобільній станції (MS) за допомогою аутентифікації повідомлень PKM_EAP з використанням протоколу аутентифікації EAP-MD5 або EAP-MSCHAPV2. На відміну від автентифікації пристроїв, ніякий додатковий майстер-ключ сеансу (MSK) не

формується, навіть в тому випадку, якщо автентифікація користувачів завершена.

Тим часом, на п’ятнадцятому етапі, базова станція приймає повідомлення «RADIUS ACCEPT» та на шістнадцятому етапі передає повідомлення «PKM_EAP/EAP-SUCCESS» на мобільну станцію (MS).

На шістнадцятому та сімнадцятому етапах мобільна станція (MS) і базова станція (BS) формують ключ авторизації (AK) з використанням парного мастер-ключа (PMK).

Таким чином, в процесі автентифікації EAP системи зв'язку за стандартом ISO/IEC 24760-2:2021 , майстер-ключ сеансу (MSK) формується в процесі першої автентифікації EAP.

Далі базова станція (BS) (див. рис. 2.2) приймає майстер-ключ сеансу (MSK), сформований в процесі першої автентифікації EAP, тобто автентифікації пристроїв, з сервера автентифікації, авторизації і обліку (AAA), а потім формує ключ цілісності EAP (EIK) і парний майстер-ключ (PMK) з використанням мастер-ключа сеансу (MSK). Зокрема, базова станція (BS) формує ключ цілісності EAP (EIK) і парний майстер-ключ (PMK) із заздалегідь певною кількістю бітів, наприклад 160-бітовий ключ цілісності EAP (EIK) і 160-бітовий парний майстер-ключ (PMK), за допомогою усікання мастер-ключа сеансу (MSK).

Таким чином, проведенні дослідження протоколів автентифікації та авторизації підключень в сучасних хмарних сервісах дозволили встановити, що основними застосовуваними механізмами є протоколи RSA та/або EAP із певними функціями розподілу ключів. Їх використання дозволяє провести односторонню (АС) або двосторонню (АС і БС) автентифікацію та створити відповідну ієрархію ключів авторизації безпроводового доступу. Саме властивості формованих ключів авторизації і визначають рівень безпеки телекомунікаційних систем і мереж при наданні безпроводового доступу.

Для врахування певних властивостей формованих ключів авторизації при оцінці безпеки телекомунікаційних систем та мереж в кваліфікаційній роботі

пропонується математична модель авторизації та автентифікації безпроводового доступу.

3.5 Розробка математичної моделі авторизації та автентифікації хмарного сервісу

Для формалізованого опису всіх етапів автентифікації та авторизації безпроводового доступу в сучасних телекомунікаційних системах та мережах, які побудовано відповідно до специфікації міжнародних стандартів серії ISO/IEC 24760-2:2021, будемо використовувати наступні позначення:

- pre-PAK – головний ключ авторизації (pre-Primary Authorization Key), який отримано в результаті виконання протоколу автентифікації та авторизації із застосуванням алгоритму RSA;
- EIK – ключ цілісності (EAP Integrity Key for authenticating Authenticated EAP message), який формується із застосуванням спеціальної функції Dot16KDF, та який призначено для забезпечення цілісності та автентичності переданих даних протоколу EAP;
- PAK – первинний ключ авторизації (Primary Authorization Key), який формується із застосуванням спеціальної функції Dot16KDF, та який призначено для формування ключа авторизації AK (Authorization Key);
- MSK – майстер-ключ сеансу (Master Session Key), який формується в процесі автентифікації EAP та призначений для формування парного майстер ключа PMK (Pairwise Master Key);
- PMK – парний майстер-ключ, який формується із застосуванням спеціальної функції Dot16KDF, та який призначено для формування ключа авторизації AK;
- Dot16KDF - спеціальна функція, яка призначена для для формування псевдовипадкових послідовностей, які використовуються у якості ключів різного призначення, в тому числі, і для формування ключа авторизації AK;

- SSID – ідентифікатор мобільної станції, для якої виконана автентифікація EAP;
- BSID – ідентифікатор базової станції;
- AK – ключ авторизації, який надає права авторизованого доступу та із застосуванням якого формується решта ключів, в тому числі ключів шифрування трафіку TEK (Traffic Encryption Key).

Основною функцією, яка застосовується під час формування ключів авторизації, є спеціальна функція

Dot16KDF(key, astring, keylength),

аргументами якої є наступні значення:

- key – секретний ключ, який ініціює функцію Dot16KDF, тобто задає конкретне правило її обчислення;
- astring – значення, яке подається на вхід функції Dot16KDF у якості відкритого параметру, тобто параметру, на який не накладається вимага секретності;
- keylength – несекретний параметр, який визначає бітову довжину виходу перетворення, тобто бітову довжину значення функції Dot16KDF за введеними key та astring.

Конкретна реалізація обчислення функції Dot16KDF залежить від певних налаштувань і може бути побудована одним із сучасних криптографічних алгоритмів. Зокрема, за специфікацією протоколів безпеки стандартів серії IEEE 802.16 у якості базового криптографічного алгоритму пропонується використовувати блокове симетричне шифрування AES (наприклад, в режимі CMAC), алгоритм якого стандартизовано в федеральному стандарті США FIPS-197. Допускається також застосування алгоритму ключового ґешування HMAC із використанням стандартизованої функції SHA.

Таким чином, у разі застосування алгоритму блокового симетричного шифрування правило обчислення функції Dot16KDF визначається наступним чином [ ]:

```
Dot16KDF(key, astring, keylength)
{
result = null;
Kin = Truncate (key, 128);
for (i = 0;i <= int((keylength-1)/128); i++) {
result = result | CMAC(Kin, i | astring | keylength);
}
return Truncate (result, keylength);
}
```

Функція Truncate(x, y) повертає у найправіших бітів послідовності x, відповідно y не перевищує бітову довжину x.

У разі застосування HMAC правило обчислення Dot16KDF визначається наступним чином [ ]:

```
Dot16KDF(key, astring, keylength)
{
result = null;
Kin = Truncate (key, 160);
For (i=0; i <= int( (keylength-1)/160 ); i++) {
result = result | SHA-1( i| astring | keylength | Kin);
}
return Truncate (result, keylength);
```

При авторизації із використанням алгоритму RSA правило формування ключів цілісності EIK та первинних ключів авторизації PAK із застосуванням спеціальної функції Dot16KDF за визначеними (наперед заданими) ідентифікаторами мобільної та базової станції та головним ключем авторизації pre-PAK задається наступним математичним виразом:

$$EIK \mid PAK = Dot16KDF(pre\text{-}PAK, SSID \mid BSID \mid \text{“EIK+PAK”}, 320), \quad (3.1)$$

де x | y – є конкатенацією бітових послідовностей x та y, тобто, якщо бітову довжину keylength значення функції Dot16KDF задано у 320 бітів, тоді бітові

довжини ключа цілісності EIK та первинного ключа авторизації PAK дорівнюють 160 бітів кожна.

При застосуванні для авторизації алгоритму RSA правило формування ключів авторизації безпроводового доступу визначається за наступним виразом:

$$AK = Dot16KDF (PAK, SSID | BSID | “AK”, 160). \quad (3.2)$$

Таким чином, при використанні алгоритму RSA відбувається встановлення первинного, загального для БС і АС ключового матеріалу - головного ключа AK (pre-Primary AK, pre-PAK). За допомогою Dot16KDF з pre-PAK формується 160-бітовий PAK, з якого, у свою чергу, за допомогою Dot16KDF генерується AK. Ієрархія ключів у разі RSA-авторизації (рис 3.3)

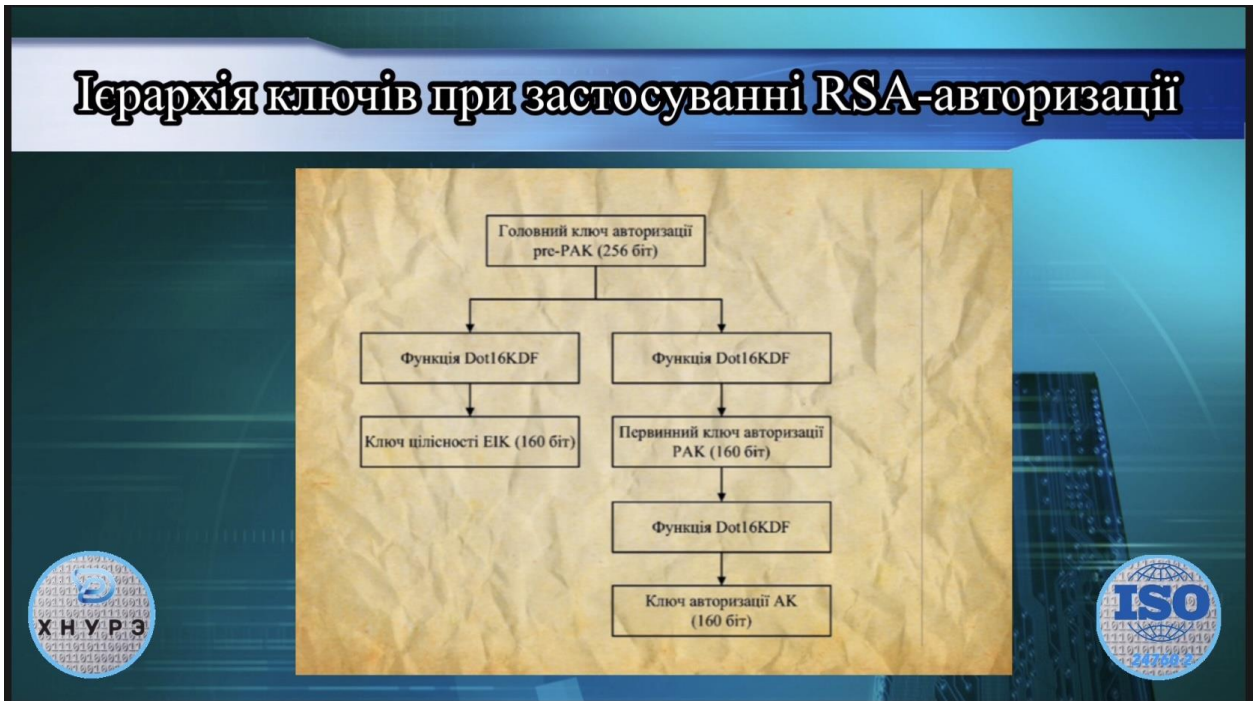


Рис. 3.3 – Ієрархія ключів при застосуванні RSA-авторизації

Таким чином, алгоритм формування ключа авторизації AK подамо такою послідовністю кроків:

Крок 1. Введення головного ключа авторизації pre-PAK;

Крок 2. Формування ключа цілісності EIK та парного ключа авторизації PAK за виразом (3.1);

Крок 3. Формування ключа авторизації AK за виразом (3.2);

Крок 4. Вивід сформованого ключа авторизації AK.

Основні властивості формованих ключів авторизації AK визначаються таким чином певними властивостями головного ключа авторизації pre-PAK та спеціальної функції Dot16KDF.

При авторизації із використанням алгоритму EAP правило формування ключів цілісності EIK та парних майстер ключів із застосуванням функції Dot16KDF за визначеними (наперед заданими) ідентифікаторами мобільної та базової станції та майстер-ключем сеансу MSK задається наступним математичним виразом:

$$EIK \mid PMK = truncate\ (MSK, 320)\ . \qquad (3.3)$$

Наступний вираз задає правило формування ключів авторизації безпроводового доступу із використанням алгоритму EAP:

$$AK = Dot16KDF(PMK, SSID \mid BSID \mid\ \text{“AK”}, 160)\ . \qquad (3.4)$$

Таким чином, при використанні EAP-авторизації, первинним, загальним для БС і АС ключовим матеріалом є 512-бітовий майстер-ключ сеансу MSK (див. рис. 3.2). Шляхом скорочення MSK до 160 битів АС і автентифікатор отримують парний майстер-ключ PMK. Після цього з PMK за допомогою функції Dot16KDF генерується AK, а для PMK встановлюється час життя, до закінчення якого повинна бути проведена реавтентіфікація. Інакше, автентифікація проводиться спочатку. Ієрархія ключів у разі EAP-авторизации представлена на рис. 3.4

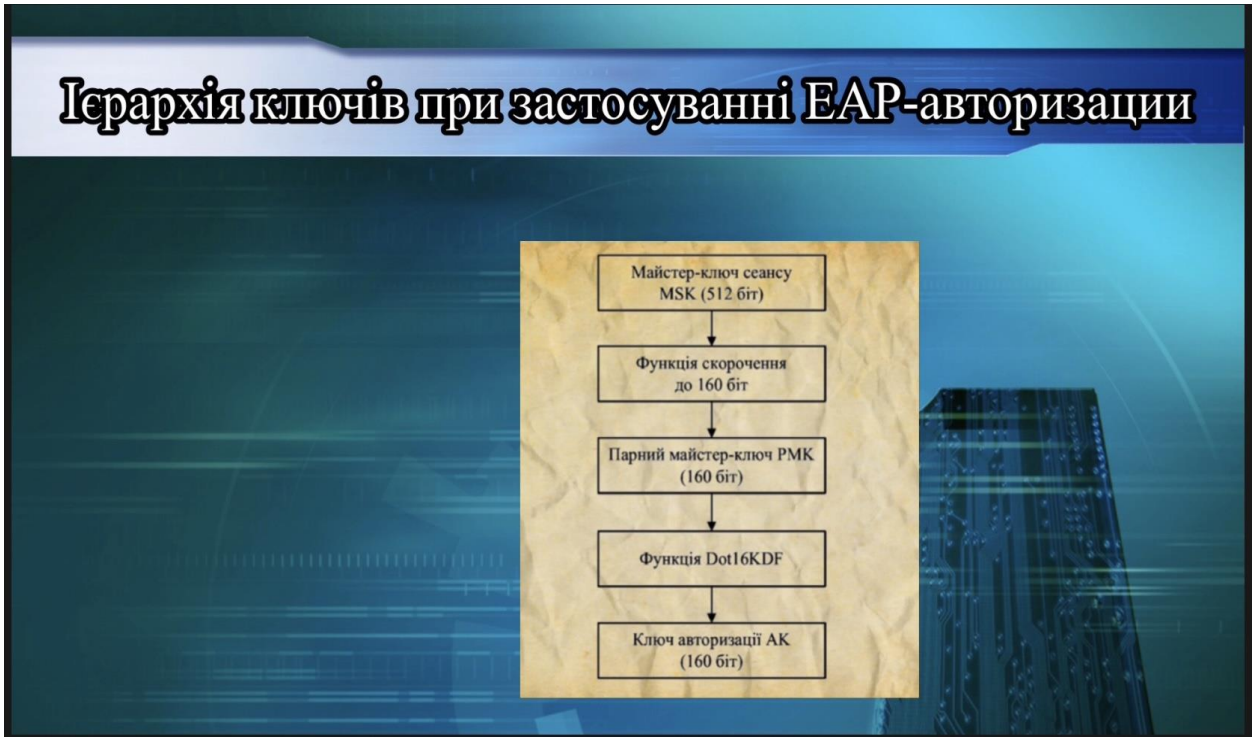


Рис. 3.4 – Ієрархія ключів при застосуванні EAP-авторизации

Алгоритм формування ключа авторизації AK при застосуванні протоколу EAP подамо такою послідовністю кроків:

Крок 1. Введення майстер-ключа сеансу MSK;

Крок 2. Формування парного ключа майстер-ключа PMK за виразом (3.3);

Крок 3. Формування ключа авторизації AK за виразом (3.4);

Крок 4. Вивід сформованого ключа авторизації AK.

Таким чином, основні властивості формованих ключів авторизації AK визначаються певними властивостями майстер-ключа сеансу MSK та спеціальної функції Dot16KDF.

При сумісному використанні RSA і EAP проводяться обидві процедури авторизації, які описані вище. За допомогою pre-PAK також створюється 160-бітовий ключ EIK для автентифікації повідомлень EAP. В результаті AC володіє як PAK, так і PMK, з яких за допомогою функції Dot16KDF генерується AK.

$$AK = Dot16KDF\ (PAK \oplus PMK,\ SSID \mid BSID \mid \text{“AK”},\ 160). \qquad (3.5)$$

Ієрархія ключів у разі RSA-EAP-авторизації представлена на (рис 3.5)

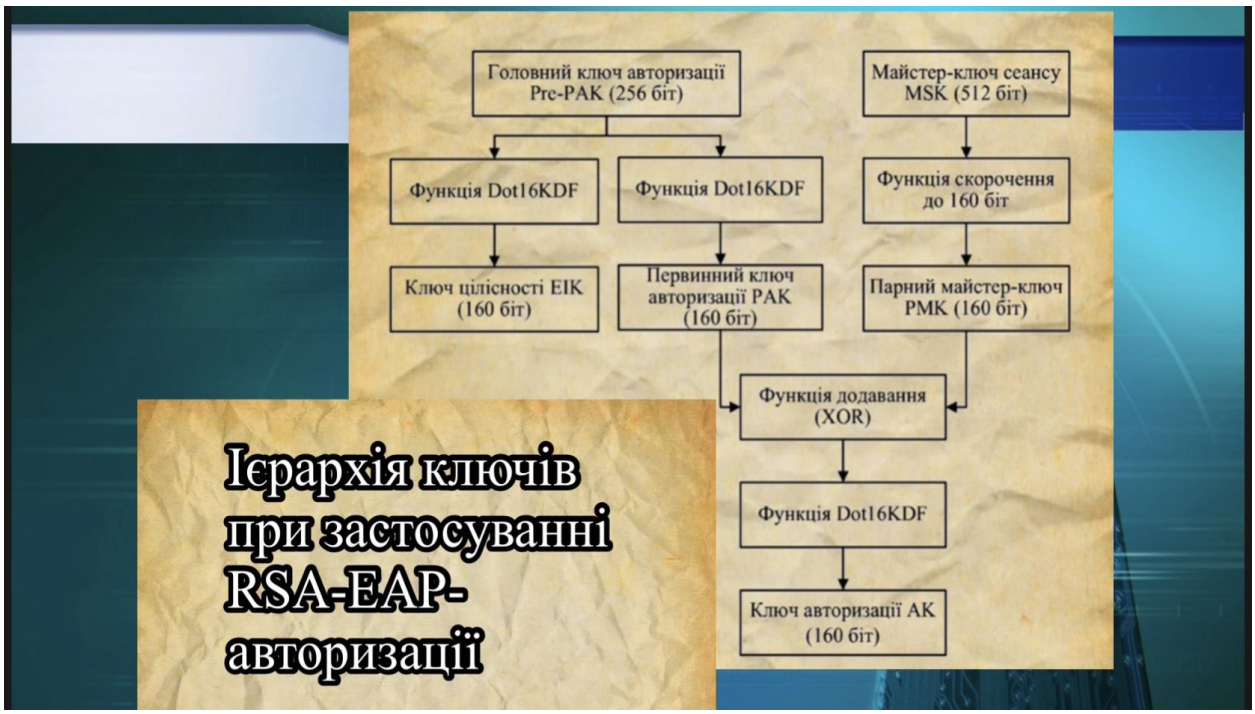


Рисунок 3.5 Ієрархія ключів при застосуванні RSA-EAP-авторизації

Алгоритм формування ключа авторизації AK при сумісному застосуванні протоколу EAP та алгоритму RSA подамо такою послідовністю кроків:

Крок 1. Введення головного ключа авторизації pre-PAK та майстер-ключа сеансу MSK;

Крок 2. Формування ключа цілісності EIK та парного ключа авторизації PAK за виразом (2.1);

Крок 3. Формування парного ключа майстер-ключа PMK за виразом (3.3);

Крок 4. Формування ключа авторизації AK за виразом (3.5);

Крок 5. Вивід сформованого ключа авторизації AK.

Властивості формованих ключів авторизації АК визначаються у цьому випадку певними властивостями головного ключа авторизації pre-PAK майстер-ключа сеансу MSK та спеціальної функції Dot16KDF.

В пропонованій математичній моделі авторизації та автентифікації безпроводового доступу для оцінки безпеки телекомунікаційних систем та мереж враховуються колізійні властивості формованих ключів авторизації АК. Для вирішення цієї задачі використаємо такі припущення:

- введений головний ключ авторизації pre-PAK та/або майстер-ключ сеансу MSK було сформовано випадково, рівноймовірно та незалежно один від одного;
- спеціальна функція Dot16KDF побудована із застосуванням криптографічно стійкого алгоритму, наприклад, алгоритму AEC та/або HMAC;
- ідентифікатори мобільної SSID та базової BSID станції, які використовуються як аргумент функції Dot16KDF, сформовано відкритим способом (без збереження в таємниці цих ідентифікаторів).

Введені припущення повністю відповідають основним положенням, які викладено в специфікації стандартів серії IEEE 802.16. При цьому, перше та друге припущення задовольняє виконанню вимог щодо забезпечення ймовірнісно-часових та статистичних властивостей ключів авторизації АК доступу:

- ймовірність викриття $P_{\hat{A}}$ правила їх формування АК визначається криптографічними властивостями функції Dot16KDF, яка за умови застосування криптографічно стійкого алгоритму із випадковим, рівноймовірним та незалежним один від одного введеним ключем ініціації (головним ключем авторизації pre-PAK та/або майстер-ключем сеансу MSK) визначається за нижньою межею, тобто $P = 2^{-160}$;
- безпечний час $\grave{O}_{\acute{A}}$ функціонування ключів авторизації АК, який як зворотна величина до ймовірності $P_{\hat{A}}$ викриття із врахуванням

обчислювальних можливостей зловмисника буде дорівнювати $\grave{O}_{\acute{A}} = \frac{2^{160}}{\gamma \cdot \Psi}$. Якщо припустити, що зловмисник володіє надпотужними обчислювальними можливостями, тобто, наприклад, може виконувати 10^{15} переборів ключів авторизації АК за секунду (обчислювальні потужності всього світу менші за цю оцінку), тоді $\grave{O}_{\acute{A}} > 10^{25}$ років, що значно більше ніж термін життя ключів авторизації доступу;

– статистичні властивості формованих ключів авторизації доступу визначаються статистичними властивостями вихідних послідовностей функції Dot16KDF, яка за умови застосування криптографічно стійкого алгоритму із випадковим, рівноймовірним та незалежним один від одного введеним ключем ініціації (головним ключем авторизації pre-PAK та/або майстер-ключем сеансу MSK) є статистично безпечним генератором псевдовипадкових послідовностей.

Втім, зазначені позитивні ймовірнісно-часові та статистичні властивості ключів авторизації доступу, які формуються із використанням спеціальної функції Dot16KDF, не гарантують виконання вимог щодо до ймовірності збігу $P_{\c{C}}$ ключів авторизації доступу АК.

Пропонована математична модель дозволяє врахувати колізійні властивості формованих ключів авторизації для оцінки безпеки безпроводових телекомунікаційних систем та мереж наступним чином.

Позначимо через

$$K_1, K_2, \ldots, K_n \tag{3.6}$$

та

$$K'_1, K'_2, \ldots, K'_n \tag{3.7}$$

послідовність випадково, рівноймовірно та незалежно один від одного введених ключів ініціації, тобто головних ключів авторизації pre-PAK та майстер-ключів сеансу MSK, відповідно.

Позначимо також через

$$AK_1, AK_2, \ldots, AK_n \qquad (3.8)$$

послідовність формованих за розглянутими вище схемами ключів авторизації доступу.

У разі застосування RSA-авторизації кожен з ключів авторизації доступу визначається наступною функцією:

$$AK_i = \text{Dot16KDF}\ (PAK_i, SSID \mid BSID \mid \text{“AK”}, 160), \qquad (3.9)$$

де

PAK_i = Truncate (Dot16KDF(K_i, SSID | BSID | “EIK+PAK”, 320), 160)

є і-м первинним ключем авторизації, який сформовано відповідно до (3.1).

Таким чином, маємо наступний ланцюг послідовностей головних ключів авторизації K_i, первинних ключів авторизації PAK_i, та ключів авторизації доступу AK_i (рис. 3.6).

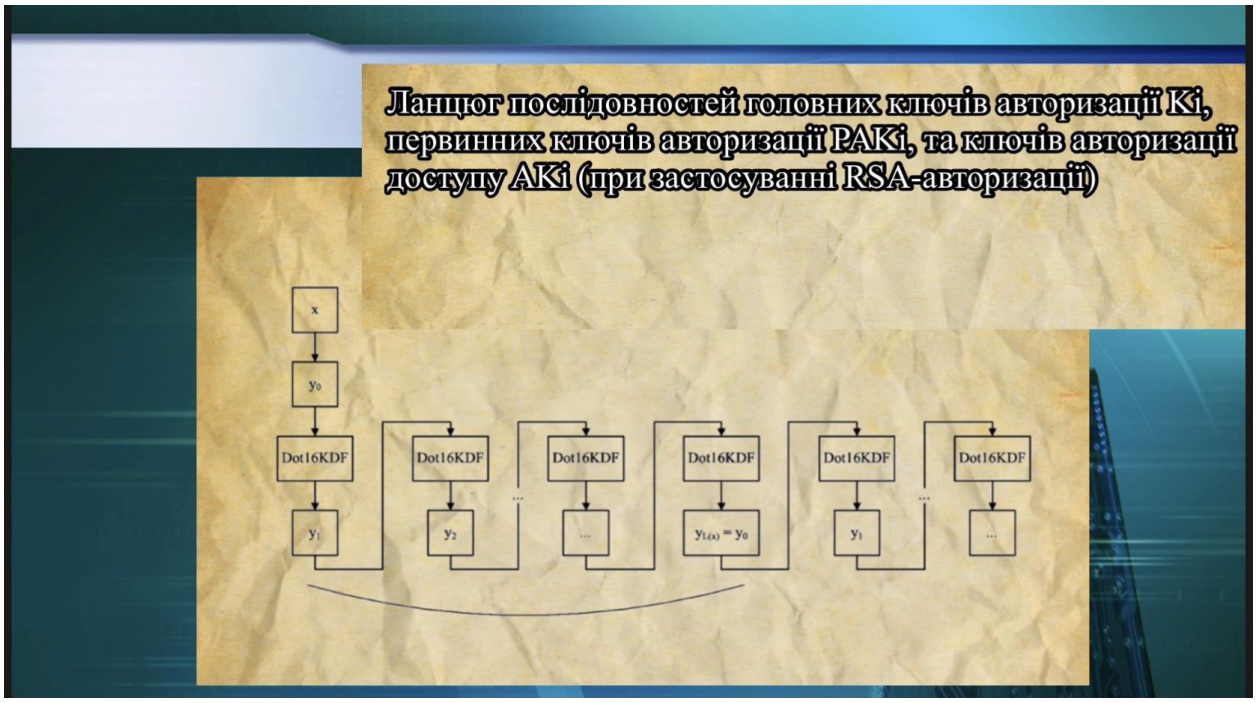


Рисунок 3.6– Ланцюг послідовностей головних ключів авторизації K_i, первинних ключів авторизації PAK_i, та ключів авторизації доступу AK_i (при застосуванні RSA-авторизації)

У разі застосування EAP-авторизації кожен з ключів AK_i авторизації доступу визначається наступною функцією:

$$AK_i = \text{Dot16KDF}\ (PMK_i, SSID \mid BSID \mid \text{“AK”}, 160), \qquad (3.10)$$

де

$$PMK_i = \text{Truncate}\ (\text{Truncate}\ (K'_i, 320), 160)$$

є і-им парний майстер-ключем, який сформовано відповідно до (3.3).

Відповідний ланцюг послідовностей майстер-ключів сеансу K'_i, парних майстер-ключів PMK_i, та ключів авторизації доступу AK_i зображено (рис. 3.7)

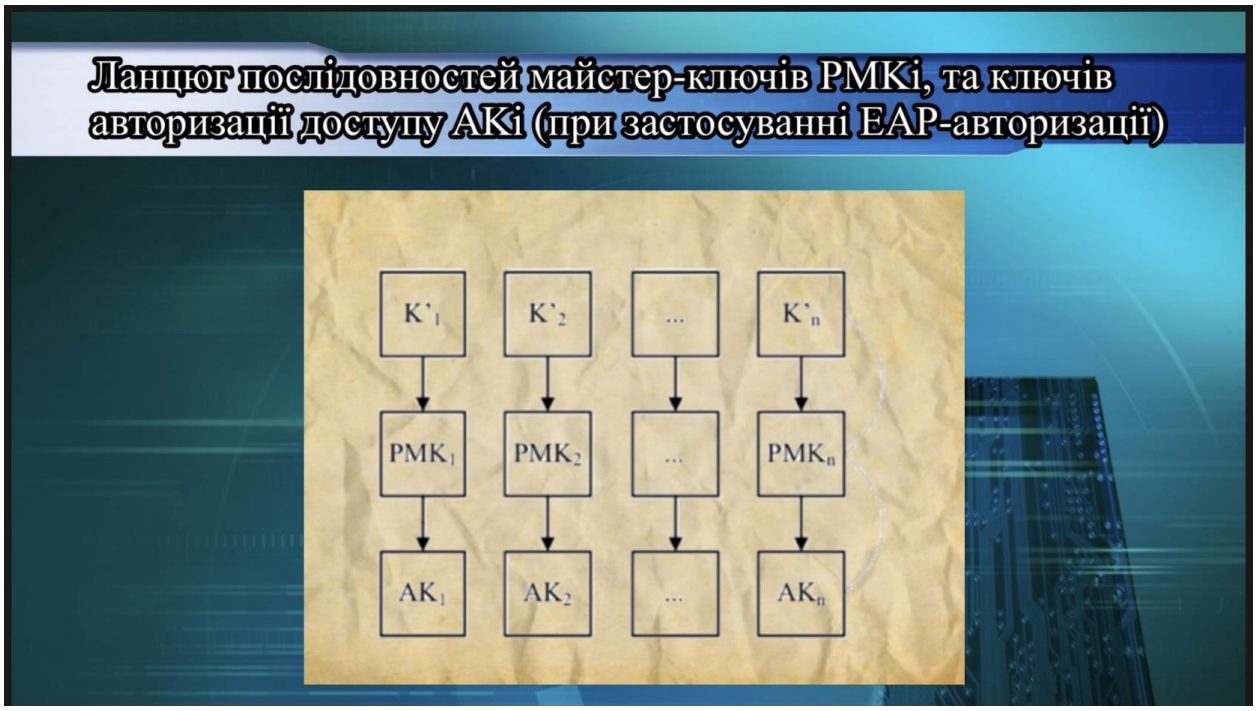


Рис. 3.7 – Ланцюг послідовностей майстер-ключів сеансу K_i, парних майстер-ключів PMK_i, та ключів авторизації доступу AK_i (при застосуванні EAP-авторизації)

У разі сумісного застосування RSA-EAP-авторизації кожен з ключів AK_i визначається наступною функцією:

$$AK_i = \text{Dot16KDF}\ (PAK_i \oplus PMK_i, SSID \mid BSID \mid \text{“AK”}, 160), \qquad (3.11)$$

де

$$PAK_i = \text{Truncate}\ (\text{Dot16KDF}(K_i, SSID \mid BSID \mid \text{“EIK+PAK”}, 320), 160)$$

та

$$PMK_i = Truncate\ (Truncate\ (K'_i, 320), 160)$$

є і-им первинним ключем авторизації та парним майстер-ключем, які сформовано відповідно до (3.1) та (3.3).

Відповідний ланцюг послідовностей головних ключів авторизації K_i, первинних ключів авторизації PAK_i, майстер-ключів сеансу K'_i, парних майстер-ключів PMK_i, та ключів авторизації доступу AK_i зображено на рис 3.8

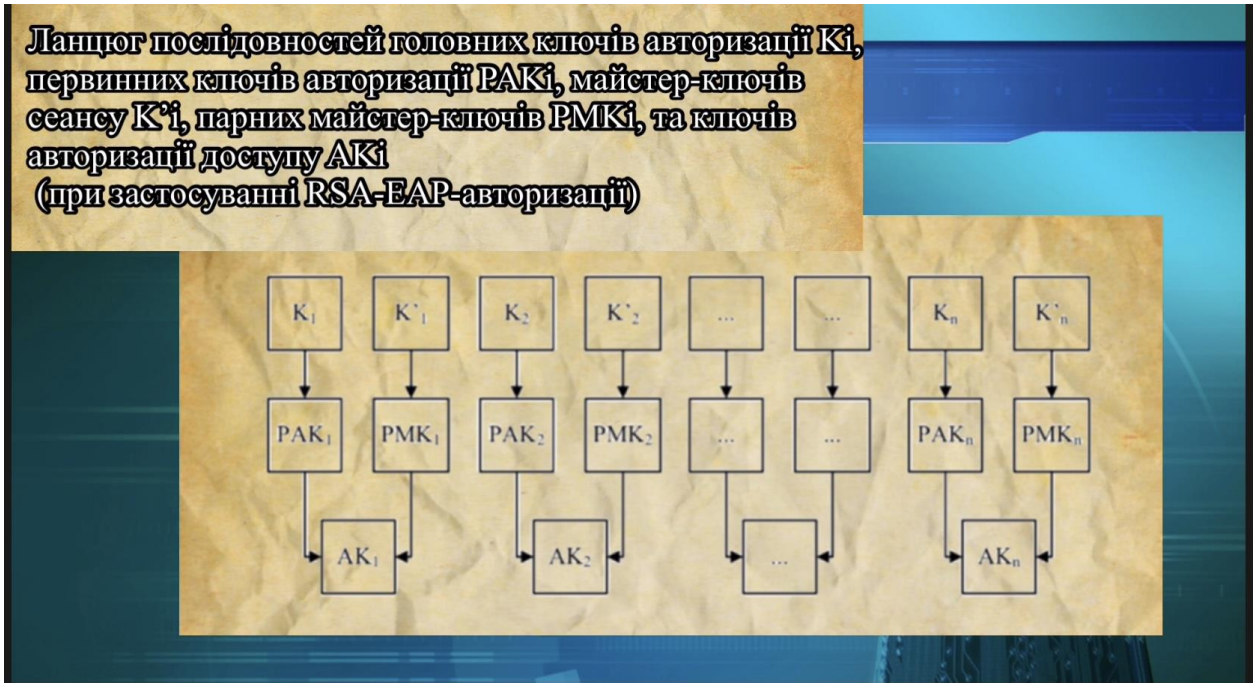


Рисунок 3.8 Ланцюг послідовностей головних ключів

Колізійні властивості формованих ключів авторизації визначаються як за колізійними властивостями послідовностей головних ключів авторизації та/або майстер-ключів сеансу, так і періодичними властивостями вихідних послідовностей функції Dot16KDF. Ці залежності випливають з наступних тверджень.

Твердження 1. У разі виникнення колізії (збігу) головних ключів авторизації та/або майстер-ключів сеансу формовані ключі авторизації доступу будуть також повторюватися, тобто буде виникати їхня колізія (збіг).

Доказ.

Припустимо, що деякі елементи з послідовності (2.6) та/або послідовності (2.7) повторюються, тобто для деяких i та j при $i \neq j$ виконується рівність:

$$K_i = K_j$$

та/або

$$K'_i = K'_j,$$

тобто відбувається колізія (збіг) окремих головних ключів авторизації та/або майстер-ключів сеансу.

Використовуючи формули (3.10) – (3.11) запишемо відповідні рівняння для різних випадків застосування схеми авторизації:

– у разі SA-авторизації

$$AK_i = \text{Dot16KDF (Truncate (Dot16KDF}(K_i, \text{SSID} \mid \text{BSID} \mid \text{“EIK+PAK”}, 320), 160), \text{SSID} \mid \text{BSID} \mid \text{“AK”}, 160),$$

$$AK_j = \text{Dot16KDF (Truncate (Dot16KDF}(K_j, \text{SSID} \mid \text{BSID} \mid \text{“EIK+PAK”}, 320), 160), \text{SSID} \mid \text{BSID} \mid \mid \text{“AK”}, 160);$$

– у разі EAP-авторизації

$$AK_i = \text{Dot16KDF (Truncate (Truncate (K'}_i, 320), 160), \text{SSID} \mid \text{BSID} \mid \text{“AK”}, 160),$$

$$AK_j = \text{Dot16KDF (Truncate (Truncate (K'}_j\ 320), 160), \text{SSID} \mid \text{BSID} \mid \text{“AK”}, 160);$$

– у разі RSA-EAP-авторизації

$$AK_i = \text{Dot16KDF (Truncate (Dot16KDF}(K_i, \text{SSID} \mid \text{BSID} \mid \text{“EIK+PAK”}, 320), 160) \oplus \text{Truncate (Truncate (K'}_i, 320), 160), \text{SSID} \mid \text{BSID} \mid \text{“AK”}, 160),$$

$$AK_j = \text{Dot16KDF (Truncate (Dot16KDF}(K_j, \text{SSID} \mid \text{BSID} \mid \text{“EIK+PAK”}, 320), 160) \oplus \text{Truncate (Truncate (K'}_j, 320), 160), \text{SSID} \mid \text{BSID} \mid \text{“AK”}, 160).$$

Аргументи функції Dot16KDF в правій частині кожного з математичних виразів при будь якій схемі авторизації є тотожними, тобто при $i \neq j$, якщо

виконується рівність $K_i = K_j$ та/або $K'_i = K'_j$ завжди виконуються наступні рівності:

– у разі SA-авторизації

$$AK_i = \text{Dot16KDF}(PAK_i, SSID \mid BSID \mid \text{“AK”}, 160) =$$
$$= \text{Dot16KDF}(PAK_j, SSID \mid BSID \mid \mid \text{“AK”}, 160) = AK_j;$$

– у разі EAP-авторизації

$$AK_i = \text{Dot16KDF}(PMK_i, SSID \mid BSID \mid \text{“AK”}, 160) =$$
$$= \text{Dot16KDF}(PMK_j, SSID \mid BSID \mid \text{“AK”}, 160) = AK_j;$$

– у разі RSA-EAP-авторизації

$$AK_i = \text{Dot16KDF}(PAK_i \oplus PMK_i, SSID \mid BSID \mid \text{“AK”}, 160) =$$
$$= \text{Dot16KDF}(PAK_j \oplus PMK_j, SSID \mid BSID \mid \text{“AK”}, 160) = AK_j.$$

Практично це означає, що у разі виникнення колізії (збігу) головних ключів авторизації та/або майстер-ключів сеансу формовані ключі авторизації доступу будуть також повторюватися, тобто буде виникати їх колізія (збіг).

Твердження доведено.

Таким чином, як випливає з сформульованого та доведеного твердження, послідовність ключів авторизації доступу, які формуються розглянутим вище способом, буде мати кількість колізій (збігів ключів) не менше ніж кількість збігів в послідовностях введених головних ключів авторизації та/або майстер-ключів сеансу. З цього слідує наступний, важливий з погляду рівня забезпечуваної безпеки безпроводових телекомунікаційних систем і мереж висновок: процедура введення головних ключів авторизації та/або майстер-ключів сеансу в існуючій схемі формування ключів авторизації доступу повинна передбачати контроль їхньої неповторності, що забезпечить відсутність певних колізій (збігів), викликаних наявністю колізій послідовностей ключів (3.6) та/або (3.7).

Припустимо, що сформульована умова виконується, тобто введені головні ключі авторизації та/або майстер-ключі сеансу сформовано так, що вони не збігаються протягом визначеного терміну часу, тобто виконується

вимога щодо відсутності колізій в послідовностях (3.6) та/або (3.7). Тоді колізійні властивості формованих ключів авторизації визначаються періодичними властивостями вихідних послідовностей функції Dot16KDF за наступним твердженням.

Твердження 2. При відсутності колізій (збігів) головних ключів авторизації та/або майстер-ключів сеансу формовані ключі авторизації доступу будуть збігатися не частіше, ніж довжина періоду вихідної послідовності застосовуваної функції Dot16KDF.

Доказ.

Збіг формованих ключів авторизації доступу буде виникати тоді, коли вихідні значення функції Dot16KDF, яку ініційовано різними головними ключами авторизації та/або майстер-ключами сеансу, співпадуть, тобто, коли виникне така подія:

$$AK_i = AK_j,$$

де

– у разі SA-авторизації $K_i \neq K_j$ і

AK_i = Dot16KDF (Truncate (Dot16KDF(K_i, SSID | BSID | “EIK+PAK”, 320), 160), SSID | BSID |“AK”, 160),

AK_j = Dot16KDF (Truncate (Dot16KDF(K_j, SSID | BSID | “EIK+PAK”, 320), 160), SSID | BSID | | “AK”, 160);

– у разі EAP-авторизації $K'_i \neq K'_j$ і

AK_i = Dot16KDF (Truncate (Truncate (K'_i, 320), 160), SSID | BSID | “AK”, 160),

AK_j = Dot16KDF (Truncate (Truncate (K'_j 320), 160), SSID | BSID | “AK”, 160);

– у разі RSA-EAP-авторизації $K_i \neq K_j$, $K'_i \neq K'_j$ і

AK_i = Dot16KDF (Truncate (Dot16KDF(K_i, SSID | BSID | “EIK+PAK”, 320), 160) ⊕ Truncate (Truncate (K'_i, 320), 160), SSID | BSID | “AK”, 160),

AK_j = Dot16KDF (Truncate (Dot16KDF(K_j, SSID | BSID | “EIK+PAK”, 320), 160) ⊕ Truncate (Truncate (K'_j, 320), 160), SSID | BSID | “AK”, 160).

Позначимо вихід функції Dot16KDF, яку ініційовано вектором x, символом y:

$$y = \text{Dot16KDF}(x, \text{astring}, \text{keylength}),$$

а довжину періоду вихідних послідовностей y_i функції Dot16KDF як L(x), де кожне значення y_i формується із застосуванням рекурентного співвідношення

$$y_i = \text{Dot16KDF}(y_{i-1}, \text{astring}, \text{keylength}),\ y_0 = x,\ i = 1, \ldots, n. \quad (3.12)$$

Припустимо, що функція Dot16KDF не є тотожністю (це найбільш вірогідно, оскільки ця функція будується із застосуванням криптоалгоритмів і тотожність тут еквівалентна рівності вихідного значення і введеного ключа). Таким чином видно, що подія $y_i = y_j$ при $i \neq j$ буде виникати не частіше, ніж за довжину періоду вихідних послідовностей y_i, тобто не менш ніж за L(x) рекурентних перетворень за виразом (3.12).

Таким чином, при відсутності колізій (збігів) головних ключів авторизації та/або майстер-ключів сеансу формовані ключі авторизації доступу АК будуть збігатися не частіше, ніж довжина періоду L(x) вихідної послідовності y_i застосовуваної функції Dot16KDF.

Твердження доведено.

З сформульованого та доведеного ствердження випливають наступні, важливі в прикладному значенні, висновки:

- довжини періодів вихідних послідовностей застосовуваної функції Dot16KDF при кожному введеному головному ключі авторизації та/або майстер-ключі сеансу повинні бути максимізовані;
- ймовірність збігу ключів авторизації визначається через довжину періодів вихідних послідовностей застосовуваної функції Dot16KDF.

Найбільшу практичну цінність має другий висновок, бо він надає можливість для точного визначення основного показника безпеки телекомунікаційних систем та мереж пов’язаного із забезпеченням автентифікації та авторизації безпроводового доступу. Оцінки кількості збігів ключів авторизації доступу та відповідної ймовірності збігу дає наступне твердження.

Твердження 3. При відсутності колізій (збігів) головних ключів авторизації та/або майстер-ключів сеансу кількість збігів ключів авторизації

доступу визначається через співвідношення максимального періоду при заданій довжині вектору ініціації та довжини періоду вихідної послідовності застосовуваної функції Dot16KDF. Ймовірність збігу визначається зворотною величиною до довжини періоду вихідної послідовності.

Доказ.

Позначимо через $L_{max}(x)$ максимальний період послідовності значень y_i при заданій довжині вектору ініціації x.

Відповідно до твердження 2 формовані ключі авторизації доступу будуть збігатися не частіше, ніж довжина періоду вихідної послідовності застосовуваної функції Dot16KDF, тобто подія $y_i = y_j$ при $i \neq j$ буде виникати не частіше, ніж через L(x) рекурентних перетворень за виразом (2.12). Практично це означає, що з $L_{max}(x)$ можливих ненульових векторів ініціації кожен L(x)-ий вектор може призводити до збігу вихідних векторів функції Dot16KDF, тобто колізія (збіг) ключів авторизації доступу буде виникати не більше $L_{max}(x)/L(x)$ разів. Якщо вектори ініціації обираються випадково, рівноймовірно та незалежно один від одного, тоді ймовірність того, що виникне збіг ключів авторизації доступу буде визначатися через співвідношення кількості збігів до максимального періоду, тобто

$$P_Ç \le \frac{L_{max}(x)}{L(x)} / L_{max}(x) = \frac{1}{L(x)}. \qquad (3.13)$$

Твердження доведено.

Сформульоване та доведене твердження має важливий наслідок.

Наслідок твердження 3. Для виконання нижньої межі ймовірності збігу ключів авторизації необхідно забезпечити максимальний період вихідних послідовностей функції Dot16KDF.

Доказ.

Використовуючи результат твердження 3 і формулу (3.13) маємо

$$P_Ç \le \frac{1}{L(x)}.$$

Якщо забезпечується максимальний період формованих вихідних послідовностей маємо

$$P_{Ç} \le \frac{1}{L_{max}(x)} = 2^{-len(x)} \qquad (3.14)$$

де під len(x) розуміється бітова довжина вектору ініціації x.

Наслідок доведено.

Сформульовані та доведені твердження і їх наслідок разом із введеною формалізацією процесу формування ключів авторизації доступу у сукупності складають **перший науковий результат**, який отримано в дисертаційній роботі, а саме: вперше розроблено математичну модель авторизації та автентифікації безпроводового доступу, в якій враховуються колізійні та періодичні властивості формованих ключів авторизації для оцінки безпеки безпроводових телекомунікаційних систем та мереж.

Проведені дослідження із використанням запропонованої математичної моделі дозволяють обґрунтувати наступні вимоги до схеми формування ключів авторизації доступу:

- вхідні послідовності (наприклад, головні ключі авторизації та/або майстер-ключі сеансу), які використовуються у якості векторів ініціації функції генерації ключів авторизації доступу (наприклад, функції Dot16KDF) не повинні мати колізій (збігів), тобто схема їх вводу повинна передбачати певний контроль;
- реалізація функції генерації ключів авторизації доступу (наприклад, функції Dot16KDF) повинна забезпечувати максимальний період формованих послідовностей.

Виконання сформульованих вимог дозволить забезпечити потрібні ймовірнісно-часові показники формованих ключів авторизації доступу для підвищення безпеки безпроводових телекомунікаційних систем і технологій. Навпаки, невиконання сформульованих вимог гарантовано призведе до колізії (збігу) формованих ключів авторизації доступу із зниженням рівня

забезпечуваної безпеки, так як це створює передумови для порушення авторизації безпроводового доступу.

Для оцінки рівня забезпечуваної безпеки телекомунікаційних систем і мереж при автентифікації та авторизації безпроводового доступу перевіримо виконання сформульованих вище вимог шляхом дослідження колізійних властивостей вихідних послідовностей застосованої функції Dot16KDF.

3.6 Генерація ключів авторизації доступу та оцінка рівня забезпечуваної безпеки

Ключі авторизації доступу в безпроводових телекомунікаційних системах і мережах, побудованих у відповідності до специфікації міжнародних стандартів серії IEEE 802.16, формуються із застосуванням спеціальної функції Dot16KDF. Ця функція реалізується за допомогою сучасних криптографічних алгоритмів, найпоширенішим з яких є стандарт симетричного шифрування США FIPS-197 AES (Advanced Encryption Standard). Проведемо експериментальні дослідження колізійних властивостей застосовуваної функції генерації ключів авторизації доступу, що реалізується за допомогою FIPS-197, оцінимо рівень забезпечуваної безпеки телекомунікаційних систем і мереж при наданні безпроводового доступу.

Метою оцінки колізійних властивостей функції генерації ключів авторизації доступу є підрахунок числа збігів формованих послідовностей на виході функції генерації у разі ініціації її різними векторами (різними головними ключами авторизації та/або майстер-ключами сеансу в залежності від застосовуваного методу авторизації).

У разі відсутності збігів (колізії) формованих послідовностей для всієї множини векторів ініціації буде забезпечено найвищий рівень безпеки телекомунікаційних систем і мереж при наданні безпроводового доступу. У цьому випадку ймовірність збігу $P_{Ç}$, як основний показник оцінки безпеки

безпроводового доступу, буде найменша і може бути оцінена за нижньою межею $P_{Ç} \le 2^{-n}$, де n - бітова довжина формованих ключів авторизації.

У разі наявності збігів (колізії) формованих послідовностей для всієї множини векторів ініціації рівень безпеки телекомунікаційних систем і мереж при наданні безпроводового доступу буде зменшено. Показник оцінки безпеки безпроводового доступу може бути оцінено через відношення максимальної кількості збігів δ до потужності множини формованих ключів авторизації доступу, тобто $P_{Ç} \le \delta / 2^{n}$. Нажаль провести дослідження з підрахунку кількості збігів δ для застосовуваної функції формування ключів авторизації неможливо з причини великої потужності множини векторів ініціації та множини вихідних послідовностей.

Для проведення експериментальних досліджень колізійних властивостей формованих ключів авторизації доступу та оцінки рівня забезпечуваної безпеки пропонується застосувати принцип масштабованості, що полягає в заміні об'єкту досліджень його зменшеною моделлю. З цією метою в роботі застосована зменшена (міні) модель шифру AES (mini-AES) [29], її програмна реалізація, а також запропонована методика статистичних досліджень колізійних властивостей.

Застосування зменшених моделей використовуваних шарів перетворень дозволяє, зберігши алгебраїчну структуру початкового алгоритму, проводити дослідження основних показників його ефективності. Цей похід широко використовується на сьогоднішній день при дослідженні криптографічних властивостей блокових симетричних шифрів. Так, наприклад, в роботах [ ] розроблені зменшені моделі кріптоалгорітмов AES, Camelia, ADE, Лабіринт, Калина, Мухомор і ін., використання яких дозволило експериментально досліджувати диференціальні і лінійні властивості відповідних шифрів, оцінити їх стійкість до атак диференціального і лінійного криптоаналізу. Комі того, на основі аналізу зменшених моделей в роботах запропоновано підхід до оцінки ефективності блокових симетричних шифрів

у вигляді обчислювальних витрат, потрібних для досягнення шифром асимптотичних характеристик випадкової підстановки.

Обґрунтування основних елементів зменшеної моделі AES (mini-AES) найбільш докладно наведено в роботах [30], її спрощений опис наведено в додатку А. Зменшена модель mini-AES реалізує відображення 16-бітних вхідних векторів в 16-бітні вихідні вектори (замість 128 бітних векторів входу і виходу для повної версії алгоритму AES). Таким чином застосовуване масштабування дозволяє провести експериментальні дослідження колізійних властивостей функції генерації кодів автентифікації та отримати оцінку рівня безпеки телекомунікаційних систем та мереж при наданні безпроводового доступу.

Позначимо множину вхідних елементів, що ініціюють зменшену модель функції генерації символом X, потужність цієї множини відповідно до наведеного опису mini-AES в додатку А визначається як $|X| = 2^{16}$. Множина X є зменшеною моделлю множини векторів ініціації «key», що застосовується до повної версії функції Dot16KDF(key, astring, keylength) для генерації ключів авторизації доступу, тобто множини головних ключів авторизації та/або майстер-ключів сеансу в залежності від застосовуваного методу авторизації.

Позначимо множину аргументів зменшеної моделі функції генерації символом Y, $|Y| = 2^{16}$. Ця множина є зменшеною моделлю множини векторів «astring» повної версії функції Dot16KDF(key, astring, keylength).

Позначимо множину значень зменшеної моделі функції генерації символом Z, $|Z| = 2^{16}$. Ця множина є зменшеною моделлю множини значень повної версії функції АК = Dot16KDF(key, astring, keylength), тобто множини формованих ключів АК авторизації доступу.

Оцінку колізійних властивостей проводитимемо в середньостатистичному сенсі. Іншими словами, при постановці експерименту використовуватимемо обмежений набір аргументів $y_i \in Y$ функції генерації і відповідних ним образів $z_i \in Z$, розглядаючи відповідні результати як вибірку

з генеральної сукупності. Оцінювати будемо число різних векторів ініціації з повної множини X, що приводять до збігу формованих образів для заданого аргументу $y_i \in Y$. Метою кожного іспиту є оцінка максимуму δ_i, $i = 1, ..., N$ кількості збігів формованих образів для вхідних аргументів.

Максимальну кількість збігів δ будемо оцінювати як середнє арифметичне $\bar{\delta}$ спостережуваних максимальних значень для вибірки з N значень δ_i:

$$\bar{\delta} = \frac{1}{N}\sum_{i=1}^{N}\delta_i ,$$

де кожне δ_i розраховується як максимальне значення кількості збігів образів для набору з N' заданих аргументів.

Дисперсію оцінимо за формулою

$$\bar{D} = \frac{1}{N-1}\sum_{i=1}^{N}(\delta_i - \bar{\delta})^2 .$$

Через центральну граничну теорему теорії ймовірності при великих значеннях кількості реалізацій N середнє арифметичне матиме розподіл, близький до нормального з математичним очікуванням

$$m \approx \bar{\delta}$$

і середнім квадратичним відхиленням

$$\sigma \approx \frac{\bar{\sigma}}{\sqrt{N}},$$

де $\bar{\sigma} = \sqrt{\bar{D}}$ – середнє квадратичне відхилення оцінюваного параметра.

При цьому ймовірність того, що оцінка $\bar{\delta}$ відхилиться від свого математичного очікування менше ніж на ε (довірча ймовірність), дорівнює

$$P(|\bar{\delta} - m| < \varepsilon) \approx 2\hat{O}\left(\frac{\varepsilon}{\sigma}\right),$$

де $\hat{O}(x)$ – функція Лапласа, яка визначається виразом

$$\hat{O}(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-\frac{t^2}{2}} dt.$$

Отримані результати експериментальних досліджень зведено у таблицю 3.1

Таблиця 3.1 – Результати експериментальних досліджень ймовірності збігу ключів авторизації безпроводового доступу

	$\bar{\delta}$	$\overline{D}$	σ	$P(\lvert\bar{\delta} - m\rvert < \varepsilon)$
$\varepsilon = 0{,}3$	6,68	0,418	0,065	0,999
$\varepsilon = 0{,}2$				0,998
$\varepsilon = 0{,}1$				0,876

Отримані результати експериментальних досліджень колізійних властивостей зменшеної моделі функції формування ключів авторизації доступу показують, що застосовувані перетворення не дозволяють забезпечити високі показники безпеки телекомунікаційних систем і мереж при наданні безпроводового доступу. Емпірична оцінка ймовірності збігів ключів авторизації доступу більша за прогнозована в понад 6 разів: для зменшеної моделі нижня оцінка ймовірності збігу дорівнює $P_Ç = 2^{-16}$, отримані емпіричні значення дають оцінку $P_Ç \le 6{,}68 / 2^{16}$ і ця оцінка отримана із дуже високою вірогідністю. Дійсно, при точності $\varepsilon = 0{,}1$ вірогідність отриманої оцінки дорівнює $P(\lvert\bar{\delta} - m\rvert < \varepsilon) \approx 0{,}876$, а вже при точності $\varepsilon = 0{,}3$ вірогідність отриманої оцінки дорівнює $P(\lvert\bar{\delta} - m\rvert < \varepsilon) \approx 0{,}999$. Отже, невідповідність колізійних властивостей прогнозованим значенням у застосовуваної схеми формування ключів авторизації доступу слід вважати емпірично доведеною. З погляду на результати доведених вище тверджень це зниження основного показника безпеки безпроводового доступу пов’язане з невиконанням вимоги

максимального періоду формованих послідовностей, які застосовуються у якості ключів авторизації сучасних телекомунікаційних систем і мереж.

Таким чином, проведені експериментальні дослідження дозволили встановити певні недоліки застосовуваного методу авторизації та автентифікації безпроводового доступу. Застосовувана функція генерації ключів авторизації доступу не забезпечує виконання вимог щодо максимального періоду формованих послідовностей. Відповідні ключі авторизації можуть збігатися, що створює передумови для порушень встановленого режиму авторизації та автентифікації і відповідного зниження безпеки телекомунікаційних систем та мереж.

Для усунення виявлених недоліків в дисертаційній роботі пропонується удосконалений метод авторизації та автентифікації безпроводового доступу, який відрізняється від відомих використанням генераторів псевдовипадкових послідовностей максимального періоду, що за рахунок забезпечення потрібних колізійних властивостей формованих ключів авторизації дозволяє підвищити безпеку телекомунікаційних систем та мереж.

3.7 Удосконалення методу авторизації та автентифікації доступу для підвищення безпеки хмарних сервісів

У якості основи при розробці удосконаленого методу авторизації та автентифікації безпроводового доступу використано відомий та розглянутий вище метод, який полягає в комплексному застосуванні процедур та операцій організаційного та технічного характеру із створення встановленого режиму авторизації та автентифікації для підвищення безпеки телекомунікаційних систем та мереж.

Основним відмінним елементом удосконаленого методу є застосування генераторів псевдовипадкових послідовностей максимального періоду для формування ключів авторизації доступу, тобто замість спеціальної функції Dot16KDF, колізійні властивості якої є незадовільними, пропонується

використовувати більш досконалу функцію генерації послідовностей. Застосування генераторів псевдовипадкових послідовностей максимального періоду за рахунок забезпечення потрібних колізійних властивостей формованих ключів авторизації дозволяє підвищити безпеку телекомунікаційних систем та мереж.

Структурна схема удосконаленого методу представлена на рис. 2.10, на якому наведено сукупність процедур і функцій відомого методу та введені нові елементи, які виділені жирним шрифтом.

Удосконалений метод авторизації та автентифікації безпроводового доступу складається з наступних елементів:

- процедур та операцій передачі даних, які будуються із використанням методів та засобів телепередачі даних і стандартизованих телекомунікаційних протоколів;
- процедур та операцій організації безпечних з’єднань, які будуються із використанням методів та засобів симетричної криптографії та певних механізмів безпечного з’єднання, які налаштовуються, зокрема, за встановленим криптографічним комплексом, із визначеними векторами ініціації, секретними ключами та часом їх життя, тощо;
- процедур та операцій організації автентифікації користувачів та пристроїв, які будуються із використанням методів та засобів асиметричної криптографії, інфраструктури відкритих ключів, цифрових сертифікатів, тощо, та відповідних протоколів автентифікації та авторизації, зокрема RSA-авторизації, EAP-авторизації та сумісної RSA-EAP-авторизації;
- процедур та операцій формування ключів авторизації доступу, які будуються із використанням методів та засобів (генераторів) псевдовипадкових послідовностей із застосуванням удосконалених механізмів, а саме:

1) процедур контролю векторів ініціації для виконання першої сформульованої вимоги щодо відсутності колізій (збігів) в вхідних послідовностях;
2) безпечних генераторів послідовностей максимального періоду для виконання другої сформульованої вимоги щодо періодичних властивостей ключів авторизації (рис 3.9)

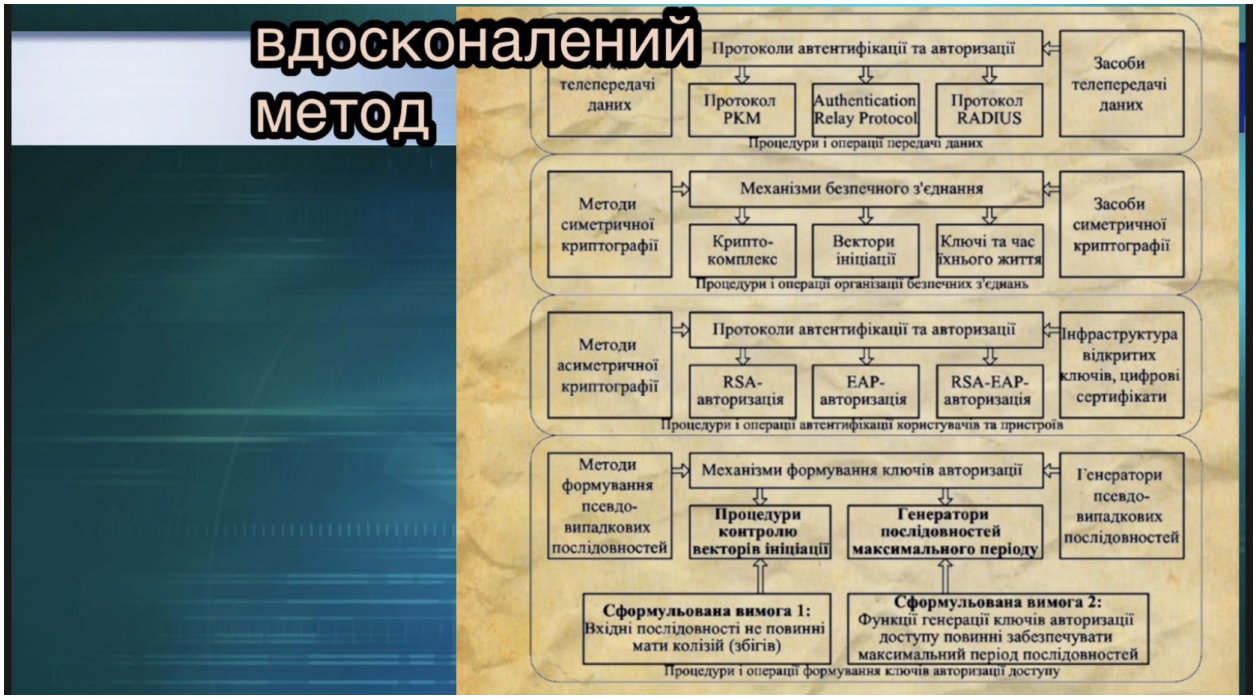


Рис. 3.9 – Структурна схема вдосконаленого методу авторизації та автентифікації доступу для підвищення безпеки CS

Запропоновані процедури контролю векторів ініціації реалізуються шляхом введення до функції генерації ключів авторизації доступу додаткового параметра і (аргументу функції генерації), який визначається за порядковим номером ключа авторизації. Таким чином, для кожного наступного виклику функції генерації використовується унікальний номер, що і забезпечує виконання першої вимоги стосовно відсутності колізій (збігів) в вхідних послідовностях.

При застосуванні для авторизації алгоритму RSA правило формування ключів авторизації безпроводового доступу пропонується визначати за наступним виразом:

AK = Generator (Hash (PAK | SSID | BSID), i, 160),

де Generator(x, y, z) – функція формування псевдовипадкових послідовностей максимального періоду яку ініційовано вектором x та яка повертає y-й блок вихідної послідовності довжини z біт;

Hash (x) – функція безпечного ґешування вектору x;

i – порядковий номер ключа авторизації, тобто номер виклику функції Generator(x, y, z) для заданих (встановлених) SSID та BSID.

Правило формування ключів авторизації безпроводового доступу із використанням алгоритму EAP пропонується визначати за наступним виразом:

AK = Generator (Hash (PMK | SSID | BSID), i, 160).

При сумісному використанні RSA і EAP авторизації правило формування ключів AK пропонується визначати за наступним виразом:

AK = Generator (Hash (PAK | PMK | SSID | BSID), i, 160).

Удосконалений метод авторизації та автентифікації безпроводового доступу становить **другий науковий результат**, отриманий в дисертаційній роботі. Цей метод відрізняється від відомих, перш за все, використанням генераторів псевдовипадкових послідовностей максимального періоду (додатково введена функція Generator(x, y, z)). Це дозволяє за рахунок забезпечення потрібних колізійних властивостей формованих послідовностей позбавитися збігів ключів авторизації і шляхом зменшення ймовірності збігів до нижньої межі $P_{\text{Ç}} = 2^{-n}$, де n - бітова довжина формованих ключів авторизації, підвищити безпеку телекомунікаційних систем та мереж.

Перспективним напрямком подальших досліджень є аналіз відомих методів формування псевдовипадкових послідовностей та обґрунтування шляхів побудови безпечних генераторів із забезпеченням максимального періоду формованих ключів авторизації доступу.

4 РЕАЛІЗАЦІЯ МЕТОДУ ПОБУДОВИ ПСЕВДОВИПАДКОВИХ КЛЮЧІВ АВТОРИЗАЦІЇ ДОСТУПУ

4.1 Програмно-апаратна платформа макету локального хмарного сервісу.

Raspberry Pi B має низку позитивних властивостей , що визначають його приемним для моделювання та технологічних іспитів .

Raspberry Pi знайшов свій шлях на ринку комп'ютерів для любителів, але він також дуже спроможний для інших технологічних та спеціальних потреб. Надзвичайно низьке енергоспоживання, малий форм-фактор, відсутність шуму, твердотільний накопичувач та інші функції роблять його привабливим рішенням для невеликого та легкого хмарного сервера (рис 4.1)

Рисунок 4.1 Зовнішній вигляд Paspberry PI4

Під час лабораторних іспитів з Raspberry Pi (версія B) під керуванням різних дистрибутивів GNU/Linux, виявилась низка переваг:

1) Споживання електроенергії - Pi споживає близько п'яти-семи ват електроенергії. Це приблизно одна десята того, що може використовувати порівнянна повнорозмірниц сервер.. Оскільки сервери працюють постійно, економія електроенергії може дійсно збільшитися. Базовий комплект Pi (плата Pi, корпус і блок живлення) окупиться приблизно за рік економії електроенергії, якщо його залишити працювати 24x7x365. У підсумку я отримав базовий комплект CanaKit (ASIN # B00DG9D6IK), який дуже доступний і якісний. Важливий економічний показник.
2) Без рухомих частин – Pi використовує SD-карту для зберігання, яка має високу бистродію і не має рухомих частин. Тут також немає вболівальників та інших речей, про які можна було б казати як технологічні недоліки . SD-карта класу 10 зазвичай є найкращою в порівнянні з картами нижчого класу, але це в основному вплине на час завантаження лише там, де найбільше вводу-виводу.
3) Малий форм-фактор - Pi (з футляром). Порівнянна повно. Це означає, що Pi також можна інтегрувати всередину пристроїв та створювати мульті системи.
4) Низький рівень шуму - Pi не має механічних приладів.
5) Індикатори стану - на материнській платі Pi є кілька індикаторів стану. За допомогою чіткого регістра ви можете побачити активність NIC, дисковий ввод-вивод, стан живлення тощо.
6) Можливості розширення. Існує безліч пристроїв, доступних для Pi, за дуже доступними цінами. Усе від плати вводу/виводу (GPIO) до камери. Pi має два порти USB, однак, підключивши USB-концентратор з живленням, можна додати більше пристроїв.Цедозволить на макеті використовувати будь які прилади.
7) Вбудована графіка з підтримкою HDMI . Порт дисплея на Pi є HDMI і може працювати з роздільною здатністю до 1920×1200, що добре, наприклад, для того, щоб підключити Pi до відеопрогравача. Є деякі

конвертори, які можуть конвертувати в VGA для зворотної сумісності. Список HDMI перетворювачі VGA можна знайти тут . У підсумку я використав кабель Sanoxy HDMI-VGA (ASIN # B0088K7QUQ), який досі добре працював. Що значно полегшує налаштування програмного забезпечення.

8) Доступна ціна – у порівнянні з іншими подібними альтернативами, Pi (версія B) пропонує найкращі характеристики за ціною. Це один з небагатьох пристроїв у своєму класі, який пропонує 512 МБ оперативної пам'яті.
9) Соціальне значенн -RB має підтримку спільноти. Підтримку можна отримати досить легко для обладнання та/або програмного забезпечення GNU/Linux, яке працює на Pi в основному на форумах користувачів, залежно від використовуваного дистрибутива GN/Linux.
10) Можливість вдосконалення – Pi можна збільшити швидкість обробки інформації, якщо є проблеми з продуктивністю використовуваної програми, але це на ризик користувача.
11) Різноманітне використання. Наявність пам'яті на картці SD дозволяє легко обмінюватися іншими картами SD з іншими дистрибутивами GNU/Linux, щоб швидко та легко змінити функціональність Pi. Якщо ви хочете налаштувати Pi для роботи як сервер, щоб перевірити його, то пізніше спробуйте щось інше, просто поміняйте SD-карту, і все готово. Використовуючи команду «dd» на комп'ютері GNU/Linux, можна створити резервну копію SD-карти, а потім відновити її, якщо потрібно (рис 4.2)

Рисунок 4.2 Зовнішній вигляд у корпусі.

Недоліки Пі

З усіма позитивними сторонами Pi, є кілька пунктів, які є Чоп і незначними, але недоліками:

1) Архітектура ARM. Хоча ARM є високоефективною та малопотужною архітектурою, вона не є x86, і тому будь-які двійкові файли, скомпільовані для роботи на x86, не можуть працювати на Pi. Позитив в тому, що всі дистрибутиви GNU/Linux були зібрані для архітектури ARM, і постійно з'являються нові. Існує дуже мало програм, які абсолютно потребують x86. Єдина проблема, яку я виявив, це Wine, який запускає програми Windows. На жаль, Win не працює на Pi, лише на останніх моделях
2) Оперативна пам'ять не підлягає оновленню - основні компоненти Pi припаяні до материнської плати, включаючи оперативну пам'ять, яка становить 512 МБ. Хоча це не проблема, оскільки GNU/Linux може легко працювати на цьому. Я виявив, що Pi використовує близько 100

МБ оперативної пам’яті, працюючи як невеликий сервер (це без запуску X11). (рис. 4.3)

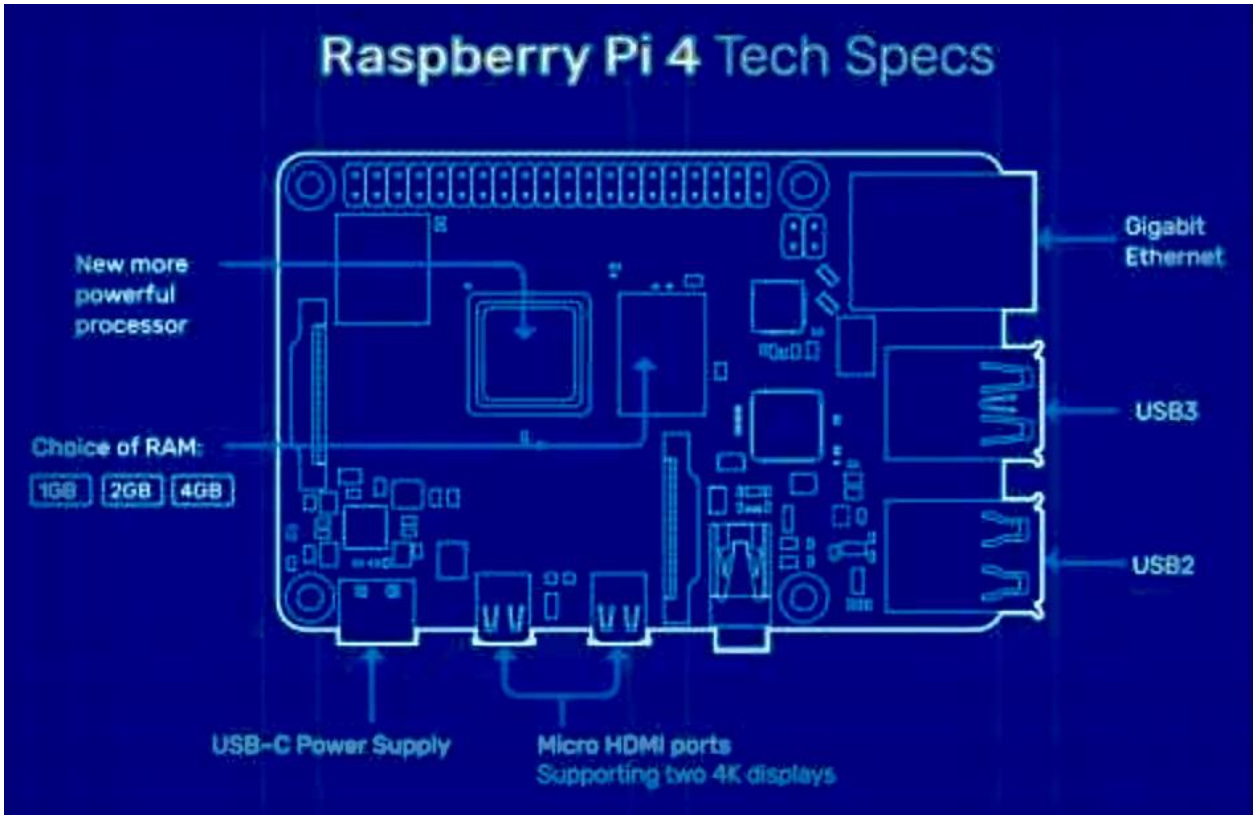


Рисунок . 4.3 Схема підключення

4.2 Програмне забезпечення локального хмарного сервісу

Комп’ютер Linux Raspberry Pi спровокував революцію в кодуванні. Pi працює під керуванням GNU/Linux та варіантів подібних операційних систем. Windows — не встановлюється на данной архітектурі , у Windows занадто багато технічних проблем із запуском на Pi, тому Windows було визнано непрактичним на Pi.

Приємними для організації макету на хмарному сервері Red Hat GNU/Linux. Отже, тако потрібно вказати що RedSleeve— це варіант Red Hat Enterprise/CentOS, який працює на Pi.(рис 4.4)

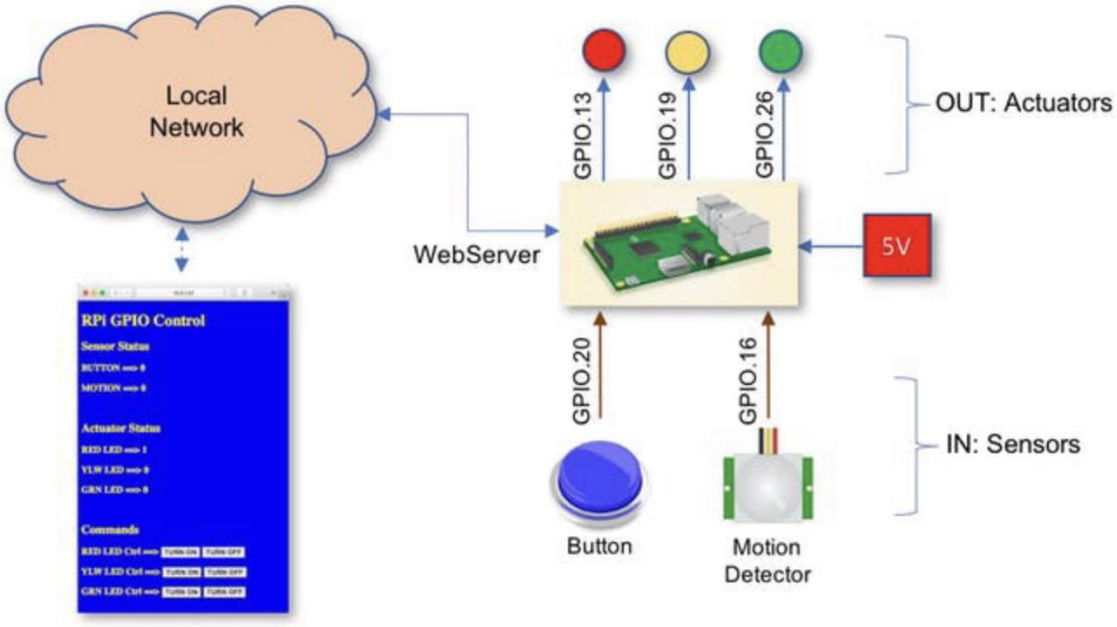


Рисунок 4.4 Реалізація в хмарному сервісі

Дистрибутив RedSleeve містить більшість бінарних файлів, які доступні в звичайних CentOS на базі x86 і Red Hat Enterprise Linux. За допомогою RedSleeve Pi може стати DNS-сервером, файловим сервером, веб-сервером, брандмауером, кластером або будь-яким іншим, що ви виберете, що може працювати без використання максимальної оперативної пам’яті. Одноцільовий або багатоцільовий сервер цих чи інших типів, ймовірно, не буде проблемою з пам’яттю при невеликому використанні. Програми, які інтенсивно витрачають пам’ять, як правило, стають проблемою з настільним комп’ютером X11 і запущеними програмами кінцевого користувача.

Сьогодні віртуалізація дуже популярна, тому деякі можуть сказати, що вартість розгортання віртуальної машини значно вище , ніж використання Raspberry Pi. Але розрахунок енергоспоживання вашого гіпервізора надає відмінності, щоб побачити, який метод насправді коштує менше. Іноді необхідна фізичний пристрій або фізична сегментація, або уникнення великих

витрат на запуск повноцінного гіпервізора є фактором, і саме тут корисне використання Pi.

Pi — Linux орієнтований , тому технічно він може робити все, що може робити будь-який комп'ютер Linux, наприклад, запускати електронну пошту та веб- сервери , діяти як мережеве сховище або працювати як VPN. Є низка проектів, створених спеціально для Raspberry Pi: він використовується , у навчанні кодувати , його можливо перетворити його на ігрову консоль DIY, використовувати як медіа-иентр. підключений до телевізора, створити IP камеру., перетворити прилад на розумний в IoT.

Доцільно використовувати Pi для імітації готової технології, яка є способом дізнатися, як працюють повсякденні технології. Це майже ніколи не є найпростішим або найефективнішим варіантом, але це може бути цікавим способом опанувати нові навички.

На RBPI можливо створити свій власний голосовий помічник, схожий на Aiexa (але зосереджений на конфіденційності), бездротову точку доступу , пристрій, схожий на Chromecast, приймач AirPlav для потокової передачі музики і навіть свою власну хмарну службу синхронізації файлів .

Багато компаній пропонують периферійні пристрої, орієнтовані на Raspberry Pi, які значно полегшують виконання неможливих проектів, тому що вам не доведеться витрачати час на з'ясування основних речей, як-от додати йому сенсорний екран. Ви просто купуєте річ, підключаєте її до Pi і починаєте робити щось круте.

Є багато точок входу з Raspberry Pi, залежно від того, який тип проекту ви хочете почати першим, але рекомендується CanaKit Raspberry Pi 4 Starter Kit (2 eel якщо ви не зовсім впевнені, що ви будете робити з це. Таким чином, у вас є все необхідне, і ви зможете розширюватися.

Цей комплект включає сам Raspberry Pi 4, блок живлення USB-C, чохол, карту microSD на 32 ГБ, кабель HDMI та кілька інших додаткових аксесуарів. Якщо ви плануєте використовувати Raspberry Pi як комп'ютер, немає кращого

варіанту, ніж комплект персонального комп’ютера Raspberry Pi 400 , який містить Raspberry Pi в компактній клавіатурі та включає мишу, блок живлення, SD- карту, кабель HDMI, і посібник для початківців, тому все, що вам знадобиться, це екран. В іншому випадку вам потрібно буде мати власну мишу , клавіатуру та телевізор або монітор. Якщо ви хочете підключити Pi до таких об'єктів, як датчики, ручки або кнопки, CanaKit's Raspberry Pi 4 Ultimate Київключає Pi разом із макетною платою, стрічковим кабелем, перемичками, світлодіодами, резисторами та кнопковими перемикачами. Якщо ви хочете вибрати власний футляр і карту microSD і вам не потрібні всі довільні кабелі, CanaKit має простіший набір, який включає Pi, блок живлення та пару радіаторів.

Модель PI4 — це корисне оновлення для тих, хто хоче використовувати Raspberry Pi як настільний комп’ютер, для проектів машинного навчання, робототехніки або веб-сервера.

Raspberry Pi потребує операційної системи з метою моделювання хмарного захищеного сервісу . Сьогодні більшість комп’ютерів працює під керуванням Windows або macOS, але Raspberry Pi в основному працює під керуванням Linux, і у вас є багато варіантів . Raspberry Pi Foundation має офіційну операційну систему загального користування під назвою Raspberry Pi OS, яка оптимізована для роботи на Pi. Він включає в себе безкоштовне програмне забезпечення для кодування, офісний пакет і, звичайно, спеціальну версію Minecraft, Raspberry Pi OS тепер навіть включає магазин додатків,щоб спростити завантаження стороннього програмного забезпечення. Кілька інших спеціалізованих операційних систем побудовано на основі конкретних проектів, як-от Recalbox для ретро-ігор або OSMC для медіа-центру.

На відміну від більшості комп’ютерів із вбудованим жорстким диском або SSD- накопичувачем, ОС Pi встановлюється на карту microSD , куди також можна помістити всі свої файли, оскільки плата не містить вбудованої пам’яті (хоча ви також можна завантажуватися із зовнішнього накопичувана).

Ця структура дозволяє вам легко розширювати сховище та перемикатися між різними операційними системами, замінюючи картки microSD. (Це також робить Pi стійким: якщо ви зупините встановлення ОС, ви можете просто перезняти зображення карти на іншому комп’ютері, і ви знову в роботі.)

Якщо ви хочете щось менше, ніж Raspberry Pi 4, або хочете витратити всього 15 доларів, Raspberry Pi Zero 2 W (також доступний з футляром і аксесуарами від CanaKit) — найкращий вибір. Pi Zero 2 W розміром з флешку пам’яті і має один порт USB і порт Mini HDMI. Він працює на тих же операційних системах, що й повнорозмірний Pi, хоча він повільніший, ніж і без того повільний Raspberry Pi 4. У той час як Pi 4 дещо можна використовувати як настільний комп’ютер, Pi Zero 2 W найкраще підходить для одноиільового DIY проекти , такі як крихітний інформаційний дисплей або комічно маленький аркадний кабінет MAME .

Висновок: вищевказане обладнання технологічно підходить для програмного моделювання захищеного сервісу хмар та дата центрів, та не потребує високовартісноі модернізації та можливе його використання у навчанні середньої та молодшої ланки IT спеціалістів.

4.3 Програмно апаратна реалізація протоколу авторизації та автентифікації

Захищений хмарний сервіс реалізований на Python

(скрипти на додатку)

Згідно алгоритму специфічному для пристроїв ARM архітектури.

ВИСНОВКИ

1) Проведенні дослідження протоколів автентифікації та авторизації в сучасних хмарних сервісах дозволили встановити, що основними застосовуваними механізмами є протоколи RSA та/або EAP із певними функціями розподілу ключів. Їх використання дозволяє провести односторонню або двостороннюавтентифікацію та створити відповідну ієрархію ключів авторизації безпроводового доступу. Саме властивості формованих ключів авторизації і визначають рівень безпеки хмарних сервісів при наданні доступу.
2) Для врахування певних властивостей формованих ключів авторизації при оцінці безпеки телекомунікаційних систем та мереж в дисертаційній роботі запропоновано математичну модель авторизації та автентифікації . Пропонована математична модель дозволяє врахувати колізійні та періодичні властивості формованих ключів авторизації для оцінки безпеки нацбільш вразливих механізмів хмарних сервісів .
3) Проведені дослідження із використанням запропонованої математичної моделі дозволили обґрунтувати наступні вимоги до схеми формування ключів авторизації доступу:
    a. вхідні послідовності (наприклад, головні ключі авторизації та/або майстер-ключі сеансу), які використовуються у якості векторів ініціації функції генерації ключів авторизації доступу (наприклад, функції Dot16KDF) не повинні мати колізій (збігів), тобто схема їх вводу повинна передбачати певний контроль колізій;
    b. реалізація функції генерації ключів авторизації доступу (наприклад, функції Dot16KDF) повинна забезпечувати максимальний період формованих послідовностей.
4) Виконання сформульованих вимог дозволяє забезпечити потрібні ймовірнісно-часові показники формованих ключів авторизації доступу

для підвищення безпеки безпроводових телекомунікаційних систем і технологій. Навпаки, невиконання сформульованих вимог гарантовано призведе до колізії (збігу) формованих ключів авторизації доступу із зниженням рівня забезпечуваної безпеки, так як це створює передумови для порушення авторизації безпроводового доступу.

5) Проведені експериментальні дослідження дозволили встановити певні недоліки застосовуваного методу авторизації та автентифікації безпроводового доступу. Застосовувана функція генерації ключів авторизації доступу не забезпечує виконання вимог щодо максимального періоду формованих послідовностей. Відповідні ключі авторизації можуть збігатися, що створює передумови для порушень встановленого режиму авторизації та автентифікації і відповідного зниження безпеки телекомунікаційних систем та мереж.
6) Для усунення виявлених недоліків пропонується удосконалений метод авторизації та автентифікації , який відрізняється від відомих використанням послідовностей максимального періоду, що за рахунок забезпечення потрібних колізійних властивостей формованих ключів авторизації дозволяє підвищити безпеку хмарних сервісів . Перспективним напрямком подальших досліджень є аналіз відомих методів формування псевдовипадкових послідовностей та обґрунтування шляхів побудови безпечних генераторів із забезпеченням максимального періоду формованих ключів авторизації доступу.

<u>В роботі були отримані наступні результати:</u>

1) Проаналізовані існуючі протокол авторизації та автентифікації , їх переваги і недоліки. Було виділено клас найбільш перспективних протоколів на основі еліптичних кривих.
2) Обраний для застосування алгоритм , що використовує еліптичні обчислювання на ланці взаємодії хмара – клієнт . Були вивчені його

можливості, достоїнства і недоліки, детально розглянуто його застосування в процесі авторизації та автентифікації користувачів.

3) Запропонована програмна реалізація на мові Python, придатна для легкої інтеграції в пропонованому макеті ARM архітектури .
4) Розглянуті проблеми розвитку та додання в існуючих стандартах інформаційної безпеки , зокрема в стандарті ISO 24760-2.

ПЕРЕЛІК ДЖЕРЕЛ ТА ПОСИЛАННЯ

1. Веб сто друкованого видання «Форбс»[forbes.com]: [веб сайт] – електронні данні _ Вашингтон 2020 , - режим доступу : https://www.forbes.com/sites/steveandriole/2019/11/20/forrester-research-gets-cloud--computing-trends-right/) (дата звернення 4.12.2020) , «Прогнози 2020: Хмарні обчислення»:
2. Веб сторінка видання «Датаверсіти» - електронні данні Нью Джеррсі США 2021 рік (https://www.dataversity.net/cloud-computing-and-cloud-architecture-trends-in-2020/)(дата звернення 4.12.2021) , «Тенденції хмарних обчислень та хмарної архітектури у 2020 році«
3. Веб сторінка IT видання , електронні данні. Новий Орлеан США 2021 рік https://www.vxchnge.com/blog/different-types-of-cloud-computing (дата звернення (дата звернення 4.13.2021), «Різноманітними види хмарних обчислень.
4. Веб сторінка видання «Датаверсіти» - електронні данні Нью Джеррсі США 2021 рік (https://www.dataversity.net/cloud-computing-challenges-navigating-the-multi-cloud-landscape/) (дата звернення 4.12.2021) Проблеми хмарних обчислень
5. Інформаційна агенція CBN веб-сторінка , електронні данні нью Йорк США 2021 рік (https://www.crn.com/news/cloud/10-emerging-cloud-computing-trends-to-watch-in-2020) (дата звернення 4.12.2021 рік) , назва: « 10 особливостей хмарних обчислень».
6. Веб сторінка видання «Датаверсіти» - електронні данні Нью Джеррсі США 2021 рік електронні данні посилання : ttps://www.dataversity.net/cloud-computing-challenges-navigating-the-multi-cloud-landscape/ (дата звернення 5.12.2021, Проблеми хмарних обчислень.

7. Веб ресурс ТВ каналу CRN , США електронні данні , https://www.crn.com/news/internet-of-things/300107041/google-merges-ai-iot-with-new-chips-and-machine-learning-platform.htm, (дата звернення 5.12.2021), назва Використання хмар в Інтернеті речей.
8. Веб сторінка видання «Датаверсіти» - електронні данні Нью Джеррсі США 2021 рік електронні данні посилання : https://www.dataversity.net/what-is-a-data-container/, (дата звернення 5.12.2021) Визначення поняття контейнер данних.
9. Веб ресурс ТВ каналу CRN , США електронні данні (https://www.crn.com/slide-shows/cloud/300105761/kubernetes-craze-8-hot-offerings-now-on-the-market.htm). (дата звернення 5.12.2021) назва: Кібернетична криза
10. Веб ресурс експертної компанії «Хартнер» Великобританія , Лондон (https://www.gartner.com/en/documents/3956097/hype-cycle-for-cloud-computing-2019) (дата звернення 5.12.2021 року) назва «Гиперцикл Хмариних обчислень».
11. Веб ресурс маркетингової компанії “Amazon” електронні данні (https://aws.amazon.com/ru/guardduty/) дата звернення 5.12.2021 року , назва «Захист аккаунтів».
12. Веб сайт агенства новин “Си про ньюс» електронні данні (https://www.sitepronews.com/2019/06/03/3-recent-developments-in-the-cloud-service-industry/). (дата звернення 5.12.2021), Останні події в хмарних сервісах.
13. Веб ресурс маркетингової агенції «Алиедмаркет», електронні данні (https://www.alliedmarketresearch.com/) (дата звернення 5.12.2021) назва “Маркетінгові досліди»
14. Веб ресурс інформагенції «Веб Хелп секьюріти» електронні данні (https://www.helpnetsecurity.com/2019/03/26/access-critical-data-public-

clouds/) (дата звернення 5.12.2021) назва «Доступ фахівців IT до хмарних сервісів»

15. Веб ресурс інформагенції «Веб Хелп секьюріти» електронні данні (https://www.helpnetsecurity.com/2018/09/20/protect-digital-channels/) (дата звернення 5.12.2021) назва « Як ви захищаєте цифрові канали від кіберзагро
16. Веб ресурс компанії « Електронікпрдукт» США, Нью Йорк електронні данні : (https://www.electronicproducts.com/a-sha-256-master-slave-authentication-system/), (дата звернення 5.12.2021) назва « Агоритм автентифікації SHA-256".
17. Сорока Л. С. Моделі і методи авторизації доступу в безпроводових телекомунікаційних системах / Л С. Сорока, О. О. Кузвецов, Д. L Ірокопович- Ткаченхо.- Дніпропетровськ :Пороги- 2013.-196 с.
18. Проколович-Ткаченко Д. І. Дослідження протоколів автентифікації та авторизації доступу в безпроводових телекомунікаційних системах та мережах / Д І. Прокопович-Ткаченко И Системи озброєння і військова техніка. - 2013. - No 1(33).- С . 119-122.
19. Прокопович-Ткаченко Д. 1. Математична модель авторизації та автентифікації безпроводового доступу в телекомунікаційних системах та мережах / Д І. Прокопович-Ткаченко // Системи обробки інформації —Х .: ХУПС, 2013. — Вип. 5 (112).-С . 97-104.
20. Прокопович-Ткаченко Д. І. Метод формування псевдовипадкових послідовностей максимального періоду із використанням перетворень на еліптичних кривих / Д. І. Прокопович-Ткаченко // Вісник Академії митної служби України. Серія «Технічні науки». - Дніпропетровськ : АМСУ, 2013 - Jfe I.-С . 47-53.
21. Прокопович-Ткаченко Д 1. Прискорене формування псевдовипадкових послідовностей максимального періоду із перетвореннями на еліптичних кривих / Д І. Прокопович-Ткаченко // Системи обробки інформації - Х .: ХУПС, 2013. - Вил. 2 (109). - С. 197-203

22. 6. Прокопович-Ткаченко Д І. Удосконалення методу авторизації та автентяфікації безпроводового доступу для підвищення безпеки телекомунікаційних систем та мереж / Д. І. Прокопович-Ткаченко // Системи озброєння і військова техніка. - 2013. - No 2(34). - С. 124-132.
23. 7. Сорока Л. С. Властивості генераторів псевдовипадковнх послідовностей на еліптичних кривих / Л. С. Сорока, О. О. Кузнецов, Д L Прокопович-Ткаченко // Вісник Академії митної служби України. Серія «Технічні науки». - Дніпропетровськ: АМСУ, 2012 - No 1(47). - С. 5-15.
24. 8. Kuznetsov A. A. Formation of pseudo-random sequences of maximum period of transformation of elliptic curves / A. A. Kuznetsov, D. L Prokopovych-Tkachenko, A. A. Smirnov // International Journal of Computational Engineering Research (UCER).Vol. 3, Issue 5, Version 3. - India. Delhi. - 2013. - P. 26-33.
25. Пат. UA 78038, МПК (2013.01) G09C 1/00. Спосіб формування Послідовностей псевдовипадкових чисел / Л. С. Сорока, О. О. Кузнецов, Д І. Прокопович-Ткаченко та ін. - J6 и2012 08718; заявл. 16.07. 2012; опубл. 11.03.2013, Бюл. No 5. - 3 с.
26. Пат. UA 80375, МПК (2013.01) G09C 1/00 Пристрій формування послідовностей псевдовипадковнх чисел / Д С . Сорока, О. О. Кузнецов, Д І. Прокопович-Ткаченко та ін. — Jit U201213846; заявл. 16.07. 2012; опубл. 27.05.2013,Бюл.No 10.-3 с.
27. Сорока Л. С. Дослідження генераторів псевдовипадковнх послідовностей на еліптичних кривих / ДС.Сорока, О.О.Кузнецов, Д LПрокопович-Ткаченко // Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку : збірник тез доповідей науково-практичної конференції академії внутрішніх військ МВС України, Харків, 21-22 березня 2012 р. - Х .: Академія внутрішніх військ МВС України. - 2012. - С 47-49.

28. Кузнецов О. О. Формування псевдовипадковнх послідовностей максимального періоду із перетворенням на еліптичних кривих / О. О. Кузнецов, Д І. Прокопович-Ткаченко // Праці IV міжнародної науково-практичної конференції «Обробка сигналів і негаусовських процесів», присвяченої пам'яті професора Ю. П. Кунченка: тези доповідей / М-во освіти і науки України, Черкас, держ технол. ун-т. - Черкаси : ЧДТУ, 2013. - С. 63-65.
29. Кузнецов А. А. Обеспеченис безопасностн информационних технологий и систем в таможенном деле / А. А. Кузнецов, Д И. Прокопович-Ткаченко // Таможенному делу - идеи молодих: сборник материалов международной научно- практической конференции. - М .: Изд-во Российской таможенной академии, 2013. - С. 124-125.
30. Прокопович-Ткаченко Д І. Удосконалення методу авторизації та автенгнфікації безпроводового доступу з мстою захисту економічної інформації / Д LПрокопович-Ткаченко // Математическое моделированне процсссов в зкономике в управлений инновационньїми процессами (ММП-2013): тезиси докладов международной научно-практической конференции, Апуигта, 9-15 сентября 2013 г. - Харьков : ХНУРЗ, 2013. - С. 178.