Тема 13. ІДЕНТИФІКАЦІЯ ТА АУТЕНТИФІКАЦІЯ ОБ'ЄКТА

1. Ідентифікація, аутентифікація та авторизація об'єкта.

З кожним об'єктом, який приймає участь у функціонуванні комп'ютерної системи (КС) обов'язково пов'язуються певні дані, які його якимось чином позначають та однозначно характеризують (ідентифікують). Ці дані, які можуть мати вигляд числа, рядка тексту або алгоритму, називаються ідентифікаційним даними об'єкту. Якщо ідентифікаційні дані зареєстровані в КС, то відповідний об'єкт вважається законним (легальним). Об'єкти відносяться до незаконних (нелегальних), якщо їх ідентифікаційні дані в КС не зареєстровані.

Коли деякий об'єкт робить спробу увійти в КС, щоб прийняти участь у її функціонуванні, система захисту КС виконує три захисні операції:

1) ідентифікація об'єкта,

2) аутентифікація об'єкта,

3) авторизація об'єкта.

Ідентифікація об'єкта. Ця операція виконується системою захисту КС в першу чергу. Перш ніж отримати доступ до КС, об'єкт повинен назвати (ідентифікувати) себе. Для цього у загальному випадку КС запитує у об'єкта його ім'я та його ідентифікаційний номер (ідентифікатор). Ім'я об'єкта використовується в КС з метою ведення діалогу з об'єктом (імена різних об'єктів можуть співпадати). Ідентифікатор об'єкта є унікальним і використовується як позначення цього об'єкта. Комп'ютерна система перевіряє, чи є указаний ідентифікатор зареєстрованим. Якщо це так, то ідентифікація вважається успішною, і КС ставить у відповідність даному об'єкту всі його ідентифікаційні дані у повному обсязі. Після цього КС переходить до виконання наступних захисних операцій, пов'язаних з цим об'єктом. Якщо ж об'єкт виявляється нелегальним, то в залежності від політики захисту в КС даному об'єкту може бути відмовлено у доступі або запропоновано перейти до процедури реєстрації.

Аутентифікація об'єкта. Ця операція виконується системою захисту КС з метою встановлення, чи є даний об'єкт дійсно тим, за кого він себе видає.

Перевірити істинність об’єкта найпростішим способом КС може шляхом запиту в нього паролю. Проте використання паролю не є безпечним для самого обєкту. У звичайній ситуації, коли є впевненість, що КС є саме тією, за кого себе видає, об’єкт просто повідомляє ій пароль. Після цього КС, порівнявши отримане значення з точним, переконується в правах об’єкту. Але в ситуації, коли є невпевненість в повноваженнях КС, такі дії об’єкту недопустимі, оскільки КС, якщо вона насправді є зловмисником, може узнати цей пароль.

Крім знання об’єктом паролю, підтвердженням його істинності можуть бути інші ідентифікаційні дані:

- елементи апаратного забезпечення об’єкту (ключі, магнітні картки, мікросхеми тощо);
- характерні риси особистості об’єкту (відбитки пальців, тембр голосу, особливості поведінки та стиль роботи, освітній рівень, вихованість, звички тощо).

Авторизація об’єкта. Ця операція виконується системою захисту КС з метою встановлення допустимих дій об’єкту в КС, а також призначення доступних йому ресурсів КС. Саме тому цю операцію називають також наданням повноважень об’єкту.

Всі ці три розглянуті операції складають в цілому процедуру, так званої, ініціалізації і відносяться до якогось єдиного об’єкта КС, тобто мають односторонній характер. Але в багатьох випадках виявляється потрібним взаємне, двостороннє встановлення істинності об’єктів, що зв’язуються між собою каналом передачі даних. [8]

2. Взаємна перевірка істинності сторін інформаційного обміну

Взаємна перевірка істинності (аутентифікація) сторін інформаційного обміну здійснюється, як правило на початку сеансу зв’язку. Мета цієї процедури – забезпечити достатній рівень впевненості абонентів по таких чотирьох складових:

- отримувач має бути впевненим в істинності відправника даних;
- отримувач має бути впевненим в істинності переданих йому даних;

- відправник має бути впевненим, що дані отримувачеві доставлені;
- відправник має бути впевненим в істинності доставлених даних.

Для взаємної перевірки істинності найбільш надійною вважається, так звана, процедура **“рукостискання”**. *Основний зміст цієї процедури полягає в тому, що абоненти, у розпорядженні яких має знаходитися один і той же секретний ключ, виконують взаємну перевірку правильності цього ключа. Інакше кажучи, сторони визначають одна одну істинними після того, як кожна доведе правильність свого ключа. Відмітимо, що звичайною зустрічною передачею секретного ключа в істинності сторін переконатись не можливо.*

Розглянемо процедуру рукостискання двох абонентів А і Б, які володіють одним і тим же секретним ключем $К_{АБ}$ деякої симетричної криптосистеми.

Процедуру рукостискання може ініціювати будь-який із абонентів. Припустимо, що її ініціює абонент А. Для цього він відправляє абоненту Б свій ідентифікатор $ІД_А$ звичайним незахищеним каналом зв’язку. Абонент Б, отримавши ідентифікатор $ІД_А$, знаходить у власній базі даних відповідний секретний ключ $К_{АБ}$. Обидва абоненти, знаючи ідентифікатор протилежної сторони, налаштовують свої криптосистеми на ключ $К_{АБ}$, після чого вони готові приступити до процедури рукостискання.

Зауважимо, що в процедурі рукостискання обидва абоненти мають використовувати одну і ту ж відкриту односторонню функцію h. (*Що таке одностороння функція?) (Основна властивість цієї функції полягає в тому, що вона дозволяє отримати таке перетворення h(x) аргумента x, знаючи яке, відновити значення аргумента не можливо).*

Нехай першим починає цю процедуру абонент А.

1). Абонент А генерує випадкову послідовність S, шифрує її і відправляє абонентові В у вигляді криптограми *E(S).*

2). Абонент Б дешифрує криптограму *E(S)* і розшифровує послідовність S, використовуючи одну і ту ж односторонню функцію h. Внаслідок цього абоненти А і Б отримують перетворення $h_А(S)$ і $h_Б(S)$ відповідно.

4). Абонент Б шифрує перетворення $h_Б(S)$ і відправляє цю криптограму абонентові А.

5). Абонент А дешифрує криптограму і порівнює отримане перетворення $h_Б(S)$ зі своїм перетворенням $h_A(S)$. Якщо ці перетворення співпадають, то абонент А переконується в тому, що абонент Б користується тим же самим секретним ключем $K_{АБ}$, тобто абонента Б можна вважати істинним.

Якщо в істинності абонента А бажає переконатися абонент Б, то він повинен повторити цю ж саму процедуру зі свого боку.

Отже,

перевагою процедури рукостискання є те, що для підтвердження істинності жоден з абонентів не повинен передавати ніяких секретних даних;

недоліком процедури рукостискання є те, що далеко не завжди абоненти, які бажають виконати взаємну перевірку істинності, мають у своєму розпорядженні спільний секретний ключ. [8]

3. Протоколи аутентифікації з нульовою передачею знань

В загальному випадку **протокол передачі даних** – це обумовлені наперед правила передачі даних між двома пристроями, чи абонентами.

Такі протоколи називають також протоколами доведення без розголошення, коли один абонент (абонент А) доводить другому (абонент Б), що він знає певні секретні дані, не розголошуючи самі дані.

Основна ідея таких протоколів полягає в тому, що наявність секретних даних у абонента А перевіряється абонентом Б без отримання самих цих даних або їх частини. Найчастіше в таких протоколах абонент Б ставить перед абонентом А ряд запитань, відповіді на які мають бути бінарного характеру (так-ні). Із збільшенням кількості правильних відповідей t у абонента Б зростає впевненість в істинності абонента А за формулою ймовірності $p=1-0.5^t$.

(*На протоколах аутентифікації з нульовою передачею знань базується використання інтелектуальних карток з мікропроцесором (старт-карток) в різноманітних комерційних, цивільних та військових застосуваннях (картки для банкоматів, картки-перепустки). При цьому головна задача полягає в тому, щоб при пред'явленні картки оперативно виявити підробку і відмовити власнику такої картки у подальшому обслуговуванні.*

Основна ідея безпечного використання інтелектуальних карток полягає в тому, що сама картка є власником деякого секретного ключа, який вважається невід'ємною ознакою її істинності. В процесі аутентифікації картка має довести своє знання цього секретного ключа, не розголошуючи його. Успішне доведення знання секретного ключа є доказом істинності картки. Т.ч., по перше, нерозголошення картками своїх секретних ключів не дає можливості зловмисникам виготовляти подібні картки, а по-друге, не приводить до негативних наслідків при користуванні підробними банкоматами.)

Перед тим як перейти до розгляду протоколу потрібні деякі поняття.

Отже, нехай маємо деяке натуральне число $m>2$, натуральне число $a<m$ називається ***квадратичним лишком за модулем m***, якщо воно взаємно просте з модулем, тобто $НСД(a, m)=1$, і крім того, існує таке ціле число x, що $x^2=a \pmod m$. Тут число x є ***квадратичним коренем за модулем m***. Якщо ж такого цілого числа x не існує, то *a* називають квадратичним не лишком за модулем *m*. *(Детальніше про властивості квадратичних лишків можна прочитати в літературі 8, Моргун)*

Протокол аутентифікації з нульовою передачею знань запропонували у 1986 році У.Фейге, А.Фіат і А.Шамир. Розглянемо його у спрощеному вигляді.

Попередню підготовку до видачі інтелектуальних карток, які будуть використовуватись у певній прикладній галузі, здійснює Центр видачі інтелектуальних карток. В першу чергу Центр вибирає значення модуля *N*, який являє собою добуток двох секретних великих простих чисел. Сам модуль *N* є відкритим і стосується всіх карток, які будуть використовуватися у цій прикладній галузі.

Інтелектуальна картка готується за заявкою користувача, який бажає таку картку отримати. Для цього користувач надає Центру певні ідентифікаційні дані: ім'я та адресу власника картки, термін дії картки, номер банківського рахунку тощо.

З урахуванням ідентифікаційних даних Центр вибирає деяке число *S*, яке, крім того, має задовольняти умовам $1<S<N$ *і НСД(S,N)=1*. Значення *S* є секретним ключем картки.

Далі Центр обчислює число *V* за формулою $V=S^2 mod\ N$. Отже, число *V* є квадратичним залишком за модулем *N*, а число *S* є квадратичним коренем із числа *V* за модулем *N*. Знайдене число *V* є відкритим ключем картки.

Розглянемо приклад. Нехай для деякої прикладної галузі Центром вибрано модуль N=35, який є добутком двох "великих" простих чисел 5 і 7.

Припустимо також, що для деякого користувача з урахуванням його ідентифікаційних даних Центр вибрав число S=19 секретним ключем картки.

Внаслідок обчислення $V=S^2 mod\ N=19^2 mod\ 35=11$ *отримано відкритий ключ картки V=11.*

Отже N та V – відкриті параметри, а S – секретний.

Як ви думаєте, чому вибрані задачі саме обчислення квадратичного залишку та квадратичного кореня? Тому, що повертаючись до понять квадратичного залишку, обчислення квадрата деякого числа x за модулем m є односторонньою функцією. Обернені задачі – задача розпізнавання, чи справді a (V) є квадратичним залишком за модулем m, а також рівноцінна задача добування квадратичного кореня із a (V) за модулем m (тобто добування S) вважаються практично нерозв'язуваними.

Надалі у протоколах аутентифікації безпосередньо беруть участь дві сторони:

- сторона А, яка являє собою картку, видану користувачеві Центром видачі інтелектуальних карток, і яка має доводити стороні Б свою істинність;
- сторона Б, яка перевіряє, надані стороною А, і приймає остаточне рішення стосовно її обслуговування.

Протокол аутентифікації має наступний вигляд:

1). Сторона А вибирає випадкове число *r*, яке має задовольняти умові $1<r<N$. Після цього сторона А підносить обране число до квадрату за модулем *N*, тобто обчислює $x=r^2 mod\ N$. Отримане значення *x* сторона А відправляє стороні Б.

Наприклад, сторона А вибирає випадкове число $r=17$. Далі вона отримує результат піднесення до квадрату $x=r^2 mod\ N=17^2 mod\ 35=9$ і відправляє число $x=9$ стороні Б.

2). Сторона Б відправляє стороні А випадковий біт b (0 або 1).

3). Сторона А обчислює значення $y=(r\cdot S^b) mod\ N$ і відправляє отримане значення стороні Б.

Тут можливі два випадки.

Якщо $b=0$, то сторона А відправляє стороні Б значення раніше вибраного випадкового числа $y=r$, тобто $y=17$.

Якщо $b=1$, то сторона А відправляє стороні Б значення $y=(r\cdot S^b) mod\ N$, тобто $y=(17\cdot 19) mod\ 35=323\ mod\ 35=8$, яке залежить від секретного ключа S.

4). Сторона Б перевіряє конгруенцію $V^b\cdot x=y^2 (mod\ N)$.

Тут можливі два випадки.

Якщо $b=0$, то сторона Б, перевіряючи конгруенцію $x=y^2 (mod\ N)$, фактично перевіряє правильність обох направлених їй чисел x та y (оскільки, $x=r^2 mod\ N$ і $y=r$).

Для нашого прикладу маємо $9=17^2 (mod\ 35)=289 (mod\ 35)$, що є вірно.

Якщо $b=1$, то сторона Б, перевіряючи конгруенцію $V\cdot x=y^2 (mod\ N)$, фактично перевіряє знання стороною А секретного ключа S.

Для нашого прикладу маємо $11\cdot 9=8^2 (mod\ 35)$, що є вірно. Дійсно, $11\cdot 9 mod\ 35=99 mod\ 35=29$ і $8^2 mod\ 35=29$.

Вказані 4 кроки утворюють цикл протоколу. Якщо результат перевірки позитивний, то цикл повторюють з іншими випадковими значеннями r та b. Якщо ж результат перевірки виявився негативним через незнання стороною А секретного ключа і невдале його вгадування, то сторона Б припиняє протокол і відмовляє стороні А в обслуговуванні.

Вважається, що, з достатньою для практики надійністю, описаний протокол слід повторити $t=[\log_2 N]$ разів, щоб бути впевненим в істинності сторони А. Якщо результат перевірки у кожному з усіх циклів був успішним, то стороні А вдається переконати сторону Б у своєму знанні секретного ключа з ймовірністю 1. Якщо ж сторона А не знає секретного ключа, то які б

винахідливі числа x та y вона не відправляла, але сторона Б викриває її неістинність з ймовірністю p=0.5 в кожному із циклів і з ймовірністю $p=1-0.5^t$ *в останньому із t циклів.*

Для того, щоб протокол працював успішно, істинна сторона А ні в якому разі не повинна повторно використовувати значення випадкового числа r, інакше зловмисна сторона Б зможе легко обчислити значення секретного ключа S. [8]

Існує ще один протокол, який відноситься до протоколів з нульовою передачею знань і був запропонований Л.Гіллоу та Ж. Куіскуотером, носить назву протокол аутентифікації Гіллоу-Куіскуотера.

(Детально даний протокол дослідити самостійно в літературі [8])