ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Класифікація програмних засобів захисту

КРИПТОЛОГІЯ

Криптологія – це наука, що складається із двох частин (наук): криптографії і криптоаналізу.

Криптографія – це наука про способи перетворення (шифрування) інформації з метою її захисту від незаконних користувачів.

Криптоаналіз – це наука (і практика її застосування) про методи і способи розкриття шифрів.

Тобто криптографія – це захист, а саме розробка шифрів, а криптоаналіз – це напад, а саме атака на шифри.

Зашифрування – це процес перетворення інформації, при якому її зміст стає незрозумілим для суб'єктів, що не мають відповідних повноважень.

Результатом зашифрування інформації називають *шифротекстом* або *криптограмою*.

Розшифрування – це процес відновлення інформації із шифротексту.

Алгоритми, використовувані при зашифруванні і розшифруванні інформації, звичайно не є конфіденційними, а конфіденційність шифротексту забезпечується використанням при зашифруванні додаткового параметра, називаного *ключем* шифрування.

Знання ключа шифрування дозволяє виконати правильне розшифрування шифротексту.

Розкриття шифру – це процес одержання інформації із шифротексту без знання застосованого ключа.

Атака на шифр – це спроба розкриття цього шифру.

Стійкістю шифру – це здатність шифру протистояти будь-яким атакам на нього.

Всі методи шифрування інформації розділяються на:

- методи симетричного шифрування;
- методи асиметричного шифрування.

Метод симетричного шифрування передбачає використання одного і того ж ключа, що зберігається у секреті, для за шифрування і для розшифрування даних.

Основним недоліком симетричного шифрування є те, що секретний ключ повинен бути відомий і відправнику, і одержувачу. З одного боку, це створює нову проблему розповсюдження ключів. З іншого боку, одержувач на підставі наявності зашифрованого і розшифрованого повідомлень не може довести, що він одержав це повідомлення від конкретного відправника, оскільки таке ж повідомлення він міг згенерувати самостійно.

Симетричні алгоритми шифрування можна розділити на:

- потокові;
- блочні.

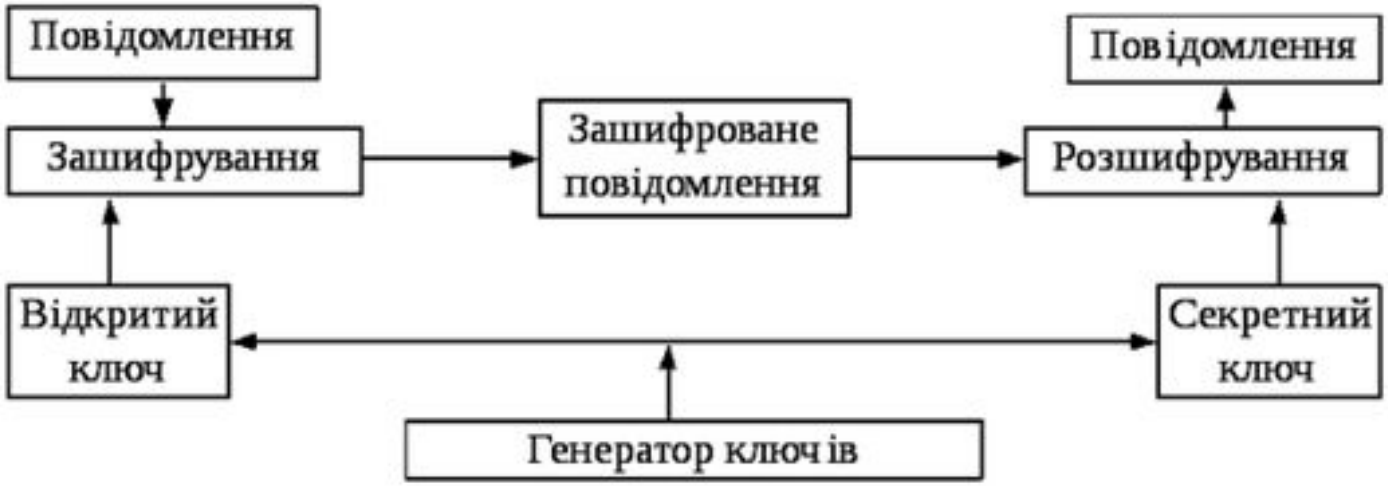
Потокові алгоритми шифрування послідовно обробляють текст повідомлення.

Блочні алгоритми працюють з блоками фіксованого розміру.

Схема використання методу симетричного шифрування

Метод асиметричного шифрування передбачає використання двох ключів. Один з них, несекретний (він може публікуватися разом з іншими відкритими відомостями про користувача), застосовується для зашифрування, інший (секретний, відомий тільки одержувачу) – для розшифрування.

Схему використання методу асиметричного шифрування



Найвідомішими асиметричними криптографічними системами є системи RSA (Rivest, Shamir, Adleman), Діффі-Хелмана, Эль-Гамаля і криптосистема на основі еліптичних кривих.

Основними застосуваннями асиметричних криптосистем є:

- передача секретного ключа симетричного шифрування відкритою мережею (відправник зашифровує цей ключ за допомогою відкритого ключа одержувача, який тільки і зможе розшифрувати отримане повідомлення за допомогою свого секретного ключа);
- системи електронного цифрового підпису для захисту електронних документів (власник документа засвідчує його дійсність за допомогою свого секретного ключа, після чого будь-який власник відповідного відкритого ключа зможе перевірити автентичність даного документа).

Методи асиметричного шифрування також дозволили вирішити важливе завдання спільного формування секретних ключів (це принципово, якщо сторони не довіряють один одному), що обслуговують сеанс взаємодії при початковій відсутності загальних секретів.

Однак сучасні асиметричні криптосистеми не можуть повністю замінити симетричні криптосистеми з таких причин:

- велика тривалість процедур зашифрування і розшифрування (приблизно в 1000 разів більше ніж при симетричному шифруванні);
- необхідність використання істотно більш довгого ключа шифрування для забезпечення тої ж криптостійкості шифру (наприклад, симетричному ключу довжиною 56 бітів відповідає асиметричний ключ довжиною 384 біти, а симетричному ключу довжиною 112 бітів – асиметричний ключ довжиною 1792 біти).

ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ СИСТЕМ

Однією з найбільш серйозних загроз для інформації, що зберігається і оброблюється за допомогою комп'ютерних систем, є несанкціонований доступ до неї. І відповідно, одним із головних завдань систем захисту інформації - є завдання ідентифікації та автентифікації. Тому розглянемо ці задачі докладніше і проаналізуємо способи їх вирішення.

Ідентифікація – процедура присвоєння ідентифікатора об'єкту комп'ютерної системи або встановлення відповідності між об'єктом і його ідентифікатором; впізнання.

Автентифікація – процедура перевірки відповідності пред'явленого ідентифікатора об'єкта комп'ютерної системи на предмет приналежності його цьому об'єкту; встановлення або підтвердження автентичності.

Тобто термін "ідентифікація" може використовуватися в трьох випадках, коли:

- Об'єкту присвоюється ідентифікатор.
- Перевіряється, чи є в системі об'єкт із пред'явленим ідентифікатором (іменем).
- Виконується впізнання перевіряємого об'єкту. Тобто в даному випадку ідентифікація включає в себе крім перевірки наявності в системі об'єкту із пред'явленим ідентифікатором, перевірку приналежності пред'явленого ідентифікатора об'єкту, який його надав (автентифікація).

Автентифікація – це більш конкретне поняття, ніж ідентифікація. Вона може реалізовуватися як окрема функція, а може бути частиною ідентифікації, але її наявність – це обов'язковий атрибут в системах захисту серйозних організацій. Тому далі, більш детально зупинимося саме на розгляді процесу автентифікації.

Автентифікація, як правило, виконується у двух випадках:

- При вході в комп'ютерну систему або для отримання доступу до будь-яких інших комп'ютерних ресурсів (файлів, папок, принтерів і т.д.).
- Періодично під час роботи в системі. Ця процедура ще іншими словами називається моніторингом.

Звісно, перший випадок застосування частіше зустрічається. Якщо до автентифікації не вводився ідентифікатор, то в цьому випадку автентифікація необхідна для визначення, чи має даний користувач право доступу до запитаних їм ресурсів, і якщо так то якими саме правами він володіє. Якщо ж спочатку вводиться ідентифікатор, тоді після цього перевіряється, чи насправді в системі є користувач з таким ідентифікатором і визначається, якими саме правами він володіє, і тільки потім виконується автентифікація, при якій перевіряється, чи насправді пред'явлений ідентифікатор належить тій людині, яка його представила.

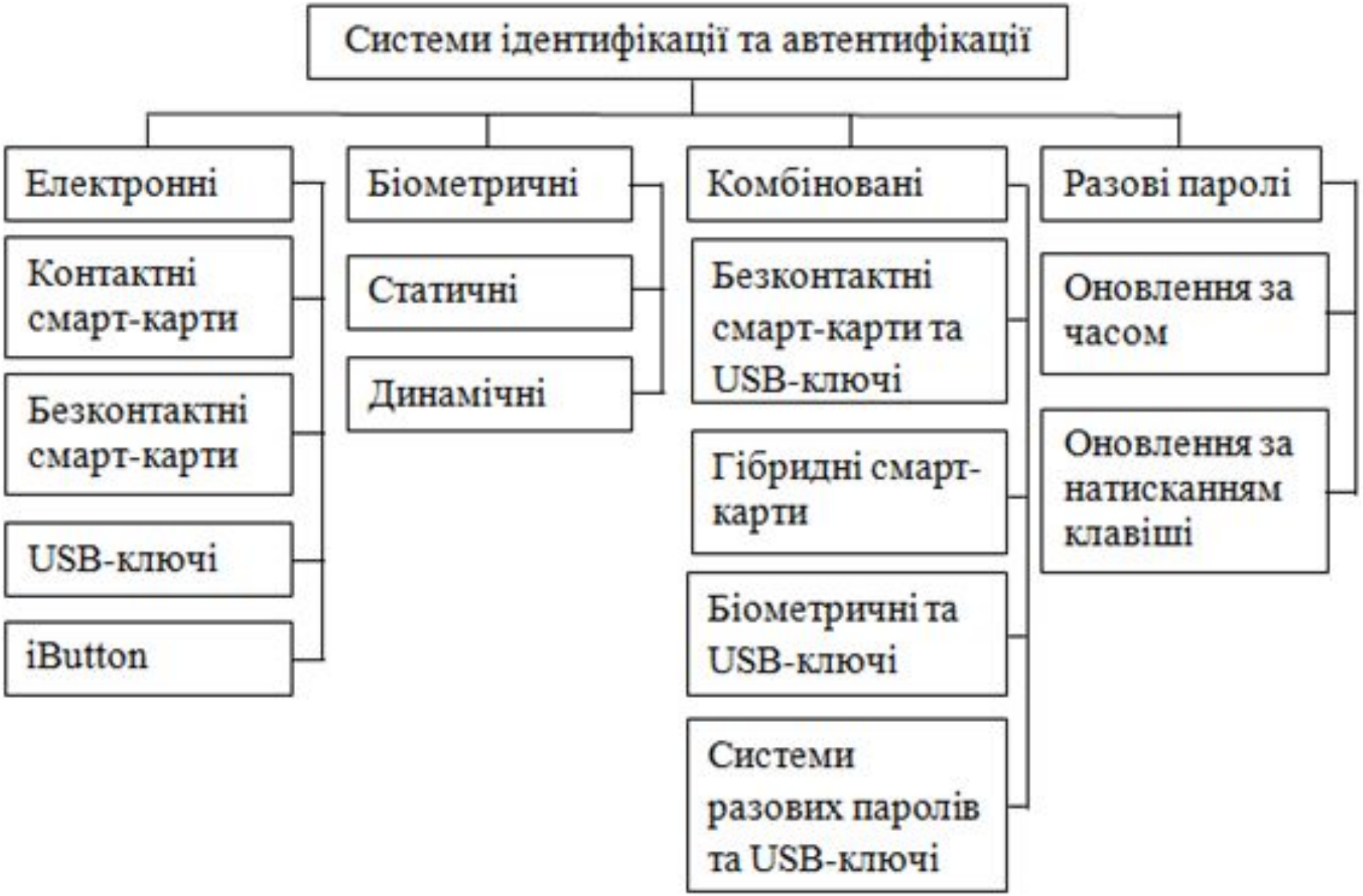
Зазвичай при вході в систему, або при спробі доступу до інших ресурсів, спочатку виконується ідентифікація (перевіряється, чи є об'єкт із заданим ідентифікатором в системі), а потім автентифікація користувача. У процесі ідентифікації встановлюється взаємно однозначна відповідність між безліччю сутностей системи і безліччю ідентифікаторів. Ідентифікація дозволяє розрізняти суті системи при контролі доступу, аудиті і т.д. Потім виконується автентифікація, яка представляє собою перевірку справжності ідентифікаторів.

У процесі ідентифікації і автентифікації користувач або програма (претендент) запитує доступ у системи (верифікатора). Спочатку здійснюється ідентифікація. Верифікатор вимагає від претендента пред'явити деякий ідентифікатор і перевіряє приналежність пред'явленого ідентифікатора безлічі зареєстрованих в системі. У випадку коректності ідентифікатора верифікатор виконує процедуру автентифікації (наприклад, запитує пароль), щоб впевнитися, що претендент є саме тим, за кого себе видає. Допуск претендента в систему дозволяється тільки у випадку вдалого завершення процедури автентифікації. В більшості систем встановлюється ще деяке порогове значення для числа спроб пред'явлення некоректного ідентифікатора і пароля, при перевищенні якого всі подальші спроби доступу даного претендента до системи блокуються .

Моніторинг виконується періодично під час роботи в системі. Зазвичай непомітно для об'єкта, що спостерігається, хоча інколи користувача відкрито просять пройти автентифікацію. Моніторинг виконується з різною метою, наприклад:

- Для захисту від порушника, який скористався залишеним легальним користувачем доступом до захищаємої системи. Наприклад, якщо зареєстрований користувач в процесі роботи залишив без нагляду включений комп'ютер, не заблокував його.
- Для захисту від неуважних працівників в особливо відповідальних організаціях, в яких невелика помилка може привести до серйозних наслідків. Якщо працівник постійно неуважно працює, то, як правило, в таких організаціях, за допомогою моніторингу визначається, при прийомі на роботу або в перший час роботи і такого працівника або не приймають на таку роботу, або переводять на менш відповідальні завдання. Якщо уважний працівник раптово почав робити багато помилок в роботі або виконувати якісь невластиві йому дії, значить, він захворів або у нього які-небудь інші проблеми. Ці зміни за допомогою моніторингу повинні бути відразу виявлені і такий працівник повинен бути тимчасово відсторонений від відповідальних робіт.

Класифікація систем ідентифікації та автентифікації



В різних випадках переважніше виявляються різні типи автентифікації. Згідно нормативним документам в області захисту інформації існує три типи автентифікації, які використовують для розпізнання, відповідно:

- Щось, відоме користувачеві.
- Щось, чим володіє користувач.
- Щось притаманне користувачеві.

До автентифікації, яка використовує "щось, відоме користувачеві" відноситься розпізнання за паролем, за персональним ідентифікаційним номером, за якою-небудь іншою інформацією, яку знає тільки конкретний користувач (або група користувачів). Також може використовуватися інформація, що підтверджує, що саме із вказаного місця в даний момент часу відбувається звернення до ресурсу, а не відбувається фальсифікація по лініях зв'язку або з інших комп'ютерів. Таким доказом може бути інформація, яку можна побачити тільки в даному місці в даний момент часу. Такий тип автентифікації простий в реалізації, але не дуже надійний, так користувачеві необхідно пам'ятати багато секретної інформації (наприклад, пароль), не завжди осмисленої, а порушник може підібрати її без спеціального обладнання, питання тільки в часі і можливостях.

Автентифікація, яка використовує "щось, чим володіє користувач" має на увазі розпізнавання за допомогою смарт-карти, магнітної карти, генератору запитів-відповідей, електронного ключа або фізично прошитого криптографічного ключа. До переваг такої автентифікації можна віднести складність і високу вартість підробки інформації, використовуваної для розпізнавання. Але є і недоліки. По-перше, в деяких випадках необхідне спеціальне обладнання не тільки для користувачів, але і для перевіряючого боку (в комп'ютері). А, по-друге, таку інформацію (у вигляді карти, брелка і т.д.) можна втратити або її можуть вкрасти. І за той час поки користувач повідомить про це адміністратора і він прийме відповідні заходи порушник може скористатися вкраденою інформацією, а легальний користувач в цей час не буде мати доступ до відповідних ресурсів.

До автентифікації, яка використовує "щось, властиве користувачеві" відноситься розпізнавання за біометричними показниками людини. Наприклад, по відбитку пальця, райдужній оболонці ока, голосу, рукописному підпису, клавіатурному почерку і т.д. Деякі системи біометричної автентифікації досить дорогі (особливо використовуване обладнання), але в останній час ціни на такі пристрої дуже знижуються. Крім того, при поганому налаштуванні біометричних систем або неправильному їх підборі, ефективність від їх застосування може бути недостатньою. Однак при такій автентифікації інформація, яка використовується для розпізнавання завжди з собою, її не можна забути, втратити, вкрасти (не рахуючи фізичних травм). І при правильному виборі біометричної системи і її налаштуванні, ефективність від її застосування значно вище від інших типів автентифікації.

Таким чином, можна сказати, що в основі методів автентифікації можуть лежати, наступні принципи:

- Знання претендентом деякої секретної інформації (наприклад, пароля).
- Пред'явлення претендентом деяких незмінних характеристик (наприклад, відбитків пальців).
- Надання претендентом доказів того, що він знаходиться в деякому певному місці (можливо, в якийсь певний час).
- Встановлення справжності претендента деякою третьою стороною, якій довіряє верифікатор (цей принцип не відноситься до трьох описаних раніше типів автентифікації, але іноді застосовується).

Часто для надійності використовуються різні комбінації цих принципів. Хоча, потрібно відмітити, що не кожен з цих принципів автентифікації (і, відповідно, методів) можна використовувати завжди. Так, наприклад, якщо автентифікується не людина, а процес (програма, яка запитує або передає будь-яку інформацію), то автентифікація за допомогою відбитка пальця (або іншої характеристики) не може бути застосована.

За призначенням автентифікацію можна поділити на два основних типи:

- Автентифікація суб'єкта. Вона вирішує задачу встановлення справжності ідентифікатора, висунутого суб'єктом взаємодії (наприклад, користувач, прикладних процесів і т.п.) і зазвичай використовується при доступі до ресурсів.
- Автентифікація об'єкта. Вона встановлює справжность ідентифікатора деякого об'єкта. В якості доказів справжності зазвичай використовується підтвердження того, що джерелом даного об'єкта є власник вказаного ідентифікатора (наприклад, відправник електронної пошти, власник банківського рахунку і т.п.).

Автентифікація суб'єкта

Автентифікація суб'єкта полягає в обміні автентифікаційною інформацією, яка повинна переконати верифікатора в тому, що претендентом пред'явлений справжній ідентифікатор. Для захисту цієї автентифікаційної інформації зазвичай використовують криптографічні алгоритми. Автентифікація суб'єкта поділяється на:

- Одностороннюю.
- Взаємну.

Коли виконується одностороння автентифікація, автентифікується тільки один суб'єкт. У разі взаємної автентифікації, два взаємодіючих суб'єкта автентифікують один одного. Звичайно, взаємну автентифікацію можна виконати, об'єднавши два сеанси односторонньої автентифікації. Але при цьому можуть виникнути вразливості. У цьому випадку можливі атаки за допомогою перехоплення і повтору, навіть якщо при односторонній автентифікації цих проблем не було. Крім того, якщо використовувати взаємну автентифікацію, а не два сеанси (об'єднані) односторонньої автентифікації, то число повідомлень в протоколах такої автентифікації можна зробити значно менше подвоєного числа повідомлень відповідної односторонньої автентифікації. Одним з найбільш популярних засобів автентифікації суб'єкта є механізми на основі паролів, тому розглянемо їх докладніше.

Паролі

Суть парольних схем полягає в наступному: претендент пред'являє свій пароль, а потім верифікатор порівнює цей введений пароль з наявними у себе в базі безліччю паролів. Парольний захист є прикладом автентифікації, яка для перевірки справжності претендента використовує "щось, відоме користувачеві". У такого засобу автентифікації є досить серйозні недоліки:

- Можливість несанкціонованого доступу до паролів, які зберігаються в пам'яті комп'ютера .
- Велика ймовірність вгадування пароля.
- Можливість перехоплення пароля при введенні або при передачі.

З огляду на те, що зараз більшість комп'ютерних систем використовують розподілену обробку інформації, можна сказати, що третій недолік парольної автентифікації стає досить актуальним, тому розглянемо засоби його усунення (або зменшення).

Для того щоб захистити пароль при передачі краще, щоб претендент на доступ до захищаємого об'єкту передавав не саме пароль, а його образ, який він повинен вирахувати за допомогою будь-якої обчислюваної в одну сторону функції h, наприклад, хеш-функції. Тобто претендент після того, як пройшов ідентифікацію, пред'являє пароль p ', обчислює значення q' = h (p ') і посилає q' верифікатору. А верифікатор для кожного ідентифікатора зберігає величину q = h (p).

Коли верифікатор отримує q, він порівнює q і q '. Якщо вони рівні, то верифікатор робить висновок, що був введений правильний пароль і надає їм доступ до захищаємого об'єкту. Такий спосіб захисту переданого пароля досить ефективний, тому що навіть якщо зловмисник визначить q, відстеживши сеанс успішної автентифікації, йому досить важко буде визначити p. Однак такий захист ефективний тільки, якщо порушник може передавати свою інформацію тільки з терміналу претендента.

Якщо розглядати випадок, коли порушник може передавати свою інформацію, підключаючись безпосередньо до лінії зв'язку, то для того щоб захистити від компрометації верифікатора обчислення q '= h (p') повинен виконувати сам верифікатор.

Можливий ще третій варіант дій порушника - порушник записує інформацію, яка передається легальним користувачем (претендентом) по лінії зв'язку, а потім виконує її. В цьому випадку розглянуті засоби захисту пароля не допомагають. Для захисту в даному випадку пароль треба захищати від повтору. Для цього можна використовувати функцію h, яка буде залежати від часу, дати, порядкового номера чого-небудь (яка постійно змінюється), або інших неповторюваних даних.

Також для посилення парольного захисту використовують і інші способи.

Симетричні методи автентифікації суб'єкта

Для автентифікації суб'єкта можуть використовуватися симетричні методи, тобто методи із застосуванням симетричних алгоритмів шифрування. Суть цих методів полягає в наступному. Для шифровки претендент і розшифровки верифікатор використовують загальний секретний ключ К. Спочатку претендент на цьому таємному ключі зашифровує своє повідомлення, при цьому він вводить у відкритий або зашифрований текст якесь конкретне контрольне значення (КЗ). При отриманні повідомлення верифікатор намагається його розшифрувати і перевіряє правильність контрольного значення. Якщо ці дві процедури проходять успішно, то верифікатор робить висновок, що претендент дійсно той за кого себе видає.

При використанні симетричних методів досить популярний протокол "запит - відповідь". У цьому випадку спочатку верифікатор посилає претенденту випадковий запит x, після чого претендент зашифровує отриманий запит і посилає верифікатору відповідь y = Ek (x), верифікатор, отримавши відповідь, перевіряє відповідність запиту і відповіді, тобто перевіряє чи істинна рівність x = Ek-1 (y).

Розглянутий варіант досить легко застосовується в разі, якщо в системі працює мало користувачів. Якщо ж це розрахована на багато користувачів система, то виникає проблема з практичним застосуванням симетричних криптографічних методів, так як для реалізації цих методів кожен верифікатор (кожен хост, сервер і т.д.) повинен зберігати секретний ключ K_i і інформацію про кожного користувача, який може скористатися ключем K_i. Для вирішення цієї проблеми додають, при автентифікації, в сеанс зв'язку довірену третю сторону (сервер автентифікації). Із цим сервером автентифікації поділяють секретний ключ кожен користувач і кожен верифікатор.

Існують різні способи взаємодії з таким сервером:

♦ Перший спосіб заключається в наступному. Претендент на своєму секретному ключі зашифровує повідомлення і відправляє зашифрований текст верифікатору. Коли верифікатор його отримує, він не може відразу здійснити автентифікацію, тому що не знає ключа користувача. Тому він спочатку звертається до серверу автентифікації для отримання у нього необхідного ключа. Для захисту передаваємих по лінії зв'язку даних верифікатор і сервер автентифікації використовують один загальний секретний ключ. Після того як пройшов обмін із сервером автентифікації, тобто верифікатор отримав необхідний для розшифровки секретний ключ, верифікатор виконує автентифікацію претендента.

♦ Другий спосіб відрізняється тим, що претенденту спочатку необхідно отримати дозвіл на доступ, яке він потім повинен передати верифікатору. Для отримання цього доступу він спочатку звертається до серверу автентифікації. В данному випадку для захисту передаваємих по лінії зв'язку даних один загальний секретний ключ використовують претендент і сервер автентифікації. Претендент отримує дозвіл на доступ до верифікатора лише в тому випадку, якщо він знає секретний ключ. Приколадом такого способу використання симетричної автентифікації є система Kerberos.

Схема симетричної автентифікації із використанням довереної третьої сторони може забезпечити і взаємну автентифікацію.

Несиметричні методи автентифікації суб’єкта

Іншим різновидом методів автентифікації суб'єкта є несиметричні методи автентифікації суб'єкта. Вони використовують несиметричні криптографічні алгоритми (з відкритим ключем). Суть цих методів полягає в наступному. Спочатку верифікатор формує якесь повідомлення і відправляє його претенденту для того, щоб він його підписав. Отримавши повідомлення, претендент підписує його, використовуючи для цього свій секретний ключ, і відправляє це підписане повідомлення назад верифікатору. Отримавши його, верифікатор перевіряє підпис за допомогою відомого йому відкритого ключа справжнього користувача. Якщо цей підпис справжній, то верифікатор робить висновок, претендент дійсно той за кого себе видає. Для того, щоб порушник не міг організувати повтор перехопленого повідомлення, в даному методі, також можна додавати в передане повідомлення будь-яку є повторювану величину (дату, час, номер і т.д.)

Використовувати довірену третю сторону в несиметричних методах немає сенсу, так як характеристики таких систем автентифікації в достатній мірі захищають від розкриття ключа претендента за відомим ключем верифікатора. Але для перевірки підпису верифікаторам зазвичай необхідні сертифіковані відкриті ключі. А сертифікати на ці відкриті ключі, як правило, видають спеціальні сервери, які не є безпосереднім учасником сеансу автентифікації.

Одним з найбільш типових прикладів автентифікації суб'єкта з відкритим ключем є схеми, які представлені в стандарті CCITT Recommendation X.509.

Доказ з нульовим розголошенням знань

Ще одним різновидом способів автентифікації суб'єкта є автентифікація, яка використовує докази з нульовим розголошенням знань (zero-knowledge proofs). Суть і, в той же час, перевага такої автентифікації в тому, що наявність інформації у претендента перевіряється без розкриття цієї самої інформації (або її частини) верифікатору або третій стороні.

В таких схемах автентифікації зазвичай верифікатор задає претенденту кілька питань. За допомогою наявної у нього секретної інформації претендент обчислює відповідь на кожне з отриманих питань і відправляє їх (відповіді) назад верифікатору. Проаналізувавши отримані відповіді, верифікатор з досить високим ступенем впевненості робить висновок, що претендент дійсно знає необхідну секретну інформацію (але, при цьому, навіть частина цієї інформації у відповідях фактично не розкривається). Залежно від конкретної схеми автентифікації може використовуватися різна кількість запитань, і, відповідно, відповідей, крім того, можуть бути різні за складністю обчислення, які повинні виконуватися обома сторонами.

На практиці це досить популярний метод автентифікації суб'єкта.

Автентифікація на основі доказу з нульовим розголошенням знань є одним з найбільш ефективних криптографічних методів, тобто більш сильними з точки зору криптографії. Але є і недоліки. Вони полягають в тому, що в багатьох таких схемах автентифікації пересилається велика кількість інформації і, крім того, необхідні більш складні протоколи. Наприклад, для проведення простої однобічної автентифікації іноді потрібно кілька обмінів.

Автентифікація користувачів

Як вже було сказано раніше, парольні методи не ідеальні, у них є недоліки. Розглянуті методи, які засновані на симетричних і несиметричних алгоритмах і на доказах з нульовим розголошенням знань не можуть бути заміною парольного захисту і, як правило, не використовуються безпосередньо для автентифікації користувачів. Основною причиною цього є той факт, що довгі випадкові вектори секретного ключа досить важко запам'ятати. Рішенням цієї проблеми може бути використання пристрою взаємної довіри. У цьому випадку ці типи методів можна комбінувати.

Автентифікація на базі такого підходу полягає в наступному. Спочатку пристрій взаємної довіри автентифікує користувача, який пред'являє пароль, а після цього кінцевий верифікатор з допомогою криптографічних методів автентифікує цей пристрій. Як приклад такого підходу можна назвати ключі генерації паролів і смарт-карти.

У разі ключів генерації зв'язок користувача, який пов'язаний з паролем, і криптографічної системи виконується за рахунок встановлення взаємно однозначної відповідності між парою "користувач - пароль" і секретним ключем криптографічного системи. Для захисту пароля часто використовується хеш-функція. Але, крім цього, результуюче значення визначається спеціальним чином і використовується в якості ключа криптографічного системи. Завдяки цьому значенню криптосистема автентифікації може однаково обслуговувати і користувача, і автоматизовану систему з вбудованим ключем. Цей факт значно підвищує популярність таких систем захисту.

У разі смарт-карти можна сказати, що процесор цієї карти виконує роль претендента. Він взаємодіє з верифікатором або на близькому термінальному пристрої, або у віддаленій, доступній з мережі системі. Коли схеми автентифікації на основі смарт-карт тільки починали розвиватися, в них використовувалися хеш-функції і прості криптосистеми з відкритим ключем. Останнім часом частіше використовують схеми автентифікації на базі доказу з нульовим розголошенням знань.

Автентифікація об’єкта

Автентифікація об'єкта відрізняється від автентифікації об'єкта. При виконанні автентифікації об'єкта (або іншими словами - автентифікації джерела даних) перевіряється істинність ідентифікатора, який передається разом з деякими даними. На відміну від автентифікації суб'єкта, коли претендент повинен бути активним учасником процесу автентифікації, в разі автентифікації об'єкта такої необхідності немає. При автентифікації об'єкта одним із головних завдань є контроль цілісності даних. Тому що коли верифікатор отримує повідомлення, він повинен бути впевнений в тому, що надіслана йому від претендента інформація, не була змінена.

Для виконання автентифікації об'єкта зазвичай використовують криптографічні способи, такі як є шифрування симетричним алгоритмом, імітовставка і цифровий підпис.

При шифруванні за допомогою симетричних алгоритмів до початку сеансу обміну і претенденту, і верифікатору відомий метод обчислення деякого контрольного значення (КЗ) вихідного повідомлення і необхідний секретний ключ. Для того щоб при передачі даних їх захистити, претендент додає до них КЗ, після чого, зашифровує результат. При отриманні зашифрованого повідомлення верифікатор їх розшифровує і виділяє з нього КЗ. Якщо верифікатор визначає коректність контрольного значення, то він робить висновок, що повідомлення дійсно прийшло від справжнього власника ідентифікатора.

Якщо при автентифікації об'єкта використовується імітовставка, то вона, як правило, грає роль контрольного значення, яке приєднується до відкритих (як у випадку шифрування) або до зашифрованих даних.

Симетричні алгоритми і імітовставки можна застосовувати тільки тоді, коли претендент і верифікатор довіряють один одному. Це пояснюється тим, що при використанні цих алгоритмів і претендент, і верифікатор можуть обдурити один одного, тобто якщо верифікатор заявляє третій стороні, що він отримав повідомлення від претендента, а претендент заперечує факт відправки даного повідомлення, то з цього випливає, що один з них обманює. Але хто саме обманює визначити формальними методами не можна. Тому коли необхідно довести справжність ідентифікатора третім особам (в тому випадку, коли верифікатор не може змінити текст отриманого повідомлення), зазвичай використовують цифровий підпис.

Аутентифікація, яка використовує "щось, чим володіє користувач"

Інший тип автентифікація - це автентифікація, яка для розпізнавання використовує "щось, чим володіє користувач". Можна сказати, що така автентифікація використовує майнові характеристики. Право доступу до об'єкта визначається наявністю певного предмета. В різний час для цієї мети використовувалися різні предмети. Система "механічний замок - ключ" вже давно не відповідіє сучасним вимогам безпеки. Вона легко вразлива, в ній неможлива ідентифікація суб'єкта доступу - маючи ключ (або його копію), отримати доступ може хто завгодно і в будь-який час. Зараз використовують електронні ключі і карти (смарт, проксіміті-, контактні, безконтактні), різні DallasLock і Touch Меморі.

Існує п'ять основних видів карт:

- Карти зі штрихкодом на основі технології BAR-коду. Ця технологія відома в більшій мірі в торгівлі. Такі карти дешеві та прості у виготовленні. Вони друкуються на принтері або виконуються від руки. Інформація з них зчитується за допомогою сканера штрих-коду. Однак для таких карт притаманний серйозний недолік - їх досить легко підробити, так як зняти копію з них можна за допомогою практично будь-якої копіювальної техніки. Крім того, її можна вкрасти.
- Магнітні картки, в яких інформація записується на магнітну стрічку, вміщену на пластиковий або паперовий носій. Для зчитування інформації з картки її необхідно плавно протягнути через щілину відповідного пристрою, що зчитує. При цьому необхідно дотримуватися певної швидкості протягування, так як і карта, і голівка, що зчитує піддаються сильному механічному зносу, щілина зчитувача засмічується. Це є одним з недоліків цього виду карт. Крім того, таким картам також властивий недолік, який був у попереднього виду карт - їх також легко підробити, навіть без використання спеціалізованого обладнання. І її також можна вкрасти.

♦ Карти Віганда. Вони засновані на фізичному ефекті Виганда, який полягає в тому, що при наявності магнітного поля короткі провідники певного складу викликають в приймальнику індукційний струм. Карта стандартного розміру виконана з пластика з запресованими в нього провідниками. Зчитування інформації з карти відбувається при вставлянні її в щілину зчитувального пристрою. У цих карт також є недоліки. Карта досить тендітна, тому її необхідно оберігати від ударів. Таку карту підробити практично неможливо, проте доступ до неї не захищений, а значить, той хто викрав карту може нею скористатися.

♦ Проксимити карти. Такі карти містять мікросхему і антену, що дозволяє використовувати їх на відстані від зчитувача, уникаючи механічного контакту і підвищуючи пропускну здатність системи. Харчування карти здійснюється або від вбудованої батареї (тоді дальність зчитування може досягати 5 м), або за рахунок енергії яку випромінює зчитувач (при цьому дальність не перевищує 70 см). До недоліків можна віднести наступне: карти досить дорогі, доступ до них не захищений, при використанні відповідного обладнання можлива підробка.

♦ "Чіпові" карти. Вони поділяються на:

- Карти з пам'яттю (memory card).
- Java-карти (із вбудованим java-движком).
- смарт-карти з кристалом, які реалізують обчислення (мікропроцесорні або процесингові).
- За способом доступу такі карти можуть бути:
- Контактні – взаємодія зі зчитувачем відбувається на основі фізичного зіткнення металевих контактів смарт-карти з контактами рідера.
- Безконтактні – зчитування і запис здійснюються за допомогою радіосигналу, переданого і прийнятого індуктором смарт-карти.

І у тих, і у інших свої переваги та недоліки. Системи на основі безконтактних смарт-картах при всіх своїх плюсах (відсутність механічного зносу, висока пропускна здатність і т. Д.) Менш захищені, так як зловмиснику може бути доступний протокол обміну між картою і зчитувачем і, тоді він може перехопити дані, що передаються (нехай і в зашифрованому вигляді). Мінусом для використання контактних смарт-карт є знос контактів рідера і контактних майданчиків карти. Але контактні картки істотно дешевше безконтактних.

Іншим видом пристроїв автентифікації, що використовують "щось, чим володіє користувач" є електронні ключі. Вони являють собою інтегральну схему в металевому корпусі з контактами. Доступність контактів контролера полегшує зловмиснику вплив на систему доступу. При наявності спеціалізованого обладнання і підготовки можливе виготовлення підробки. Великого поширення набули останнім часом і так звані USB ключі - компактні носії інформації з USB-портом. Вони можуть використовуватися як для захисту програмного забезпечення, так і для ідентифікації. Наприклад, ключ eToken, він аналогічний смарт-карті з захищеною пам'яттю і процесором. Це смарт-карта і маленький зчитувач в одному пристрої.

Зараз багато систем захисту для ідентифікації користувача використовують електронні ключі-таблетки. Можна також використовувати більш широкопрофільні рішення - наприклад, зберігання авторизаційних даних на смарт-карті або USB-ключі. За допомогою такого пристрою можна вводити дані в вікно запиту пароля, вставивши карту в рідер. Вбудований генератор паролів створить пароль будь-якої довжини і складності. У різних системах одночасно можна зберегти на карті різну кількість авторизаційних даних. Кількість облікових записів, як правило, обмежується тільки розміром карти.

Деякі ключі eToken дають можливість обійтися без придумування паролів. Деякі такі ключі призначені для зберігання згенерованих паролів. Деякі дозволяють перейти до використання цифрових сертифікатів і зберігати їх і закриті ключі шифрування в eToken.

Розглянувши такі пристрої автентифікації можна сказати, що, звичайно, замість безлічі складних паролів для доступу до мережі і різних додатків легше просто підключити свій персональний електронний ключ eToken до USB порту і ввести PIN-код.

Автентифікацію, яка використовує “щось притаманне користувачеві”, тобто біометричну автентифікацію розглянемо на наступній лекції.