Міністерство освіти і науки України
Донбаська державна машинобудівна академія

КОНСПЕКТ ЛЕКЦІЙ

з дисципліни

«ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ»

(для студентів спеціальності 123"Комп'ютерна інженерія»)

Освітній рівень - бакалавр

Краматорськ 2020

ЛЕКЦІЯ 1.
ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В КОМП'ЮТЕРНИХ СИСТЕМАХ

1.1 Поняття інформаційної безпеки

Інформаці́йна безпе́ка — це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення (у цьому значенні частіше використовують термін «захист інформації»).

Інформаційна безпека держави характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) стосовно небезпечних (дестабілізаційних, деструктивних, суперечних інтересам країни тощо), інформаційним впливам, причому як до впровадження, так і до вилучення інформації.

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

1.2 Тріада CIA (конфіденційність, цілісність і доступність)

Цілями безпеки інформації є конфіденційність, цілісність і доступність. Ці три функції відомі як тріада CIA: C - конфіденційність, I - цілісність і A - доступність.

Конфіденційність

Інформація не повинна бути розкрита неавторизованих особам, неавторизованих особам або несанкціонованим процесам; це конфіденційність інформації в сфері інформаційної безпеки (а також безпеки програмного забезпечення). Крадіжка паролів або відправка конфіденційних електронних листів не тій особі - це порушення конфіденційності. Конфіденційність - це компонент конфіденційності, який захищає інформацію від неавторизованих осіб, неавторизованих об'єктів або несанкціонованих процесів.

Цілісність

Інформація або дані мають життєвий цикл. Іншими словами, інформація або дані мають час початку і час закінчення. У деяких випадках після завершення життєвого циклу інформацію (або дані) необхідно стерти (юридично). Цілісність складається з двох функцій, а саме: 1) підтримання і забезпечення точності інформації (або даних) на протязі всього життєвого циклу і 2) повнота інформації (або даних) на протязі всього життєвого циклу. Таким чином, інформація (або дані) не повинна бути зменшена або змінена несанкціонованим або невиявленим чином.

Доступність

Для того, щоб будь-яка комп'ютерна система могла служити своєї мети, інформація (або дані) повинна бути доступна, коли це необхідно. Це означає, що комп'ютерна система і її середовище передачі повинні працювати правильно. Доступність може бути знижена через оновлень системи, збоїв обладнання і відключення електроенергії. Доступність також може бути порушена атаками типу «відмова в обслуговуванні».

1.3 Закони України про захист інформації

Нижче наводиться список законодавчих актів, нормативно-правових актів (НПА) та нормативних актів щодо інформаційної безпеки (стосовно захисту інформації) в Україні, список не повний (до нього не входять НПА з обмеженим доступом та деякі НПА). Актуальні зміни на сайті Державної служби спеціального зв'язку та захисту інформації України: http://www.dstszi.gov.ua (Розділ нормативно-правова база).

Закони України:

Закон України «Про інформацію» від 02.10.1992 № 2657-XII

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР

Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII

Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

Постанови КМУ:

Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373

Постанова Кабінету міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736[1]

Нормативні документи в галузі технічного захисту інформації (НД ТЗІ)[1] та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ:

НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2

НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі

НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу

Автоматизированные системы. Требования к содержанию документов РД 50-34.698

Техническое задание на создание автоматизированной системы. ГОСТ 34.602-89

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

Галузеві стандарти:

Національний банк України

ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD)[недоступне посилання з липня 2019]

ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD)

Інформаційне законодавство України у 2011 році було оновлено з прийняттям нової редакції Закону України «Про інформацію», які були прийняті 13 січня 2011 року Верховною Радою України та набрали чинності 10 травня 2011 року. Нова редакція Закону України «Про інформацію», як базового нормативно-правового акту в інформаційній сфері, надає нове

визначення інформації – як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Цим Законом передбачений поділ за змістом інформації на такі види: інформація про фізичну особу, інформація довідково-енциклопедичного характеру, інформація про стан довкілля (екологічна інформація), інформація про товар (роботу, послугу), науково-технічна інформація, податкова інформація, правова інформація, статистична інформація, соціологічна інформація та інші види інформації.

Встановлено, що інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Відкритою вважається вся інформація, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. До інформації з обмеженим доступом не можуть бути віднесені такі відомості: про стан довкілля, якість харчових продуктів і предметів побуту, про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей, про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення, про факти порушення прав і свобод людини і громадянина, про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб та інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Крім того, в новій редакції Закону чітко прописані права журналістів та питання їх акредитації.

Згідно зі ст. 8 ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації (надалі – КСЗІ) із підтвердженою відповідністю.

1.4 SIEM (Security information and event management)

Security Information and Event Management (SIEM) являє собою систему, яка збирає інформацію для подальшого аналізу і класифікації системним адміністратором або фахівцем з ІБ.

Спочатку SIEM складалося з двох напрямків: Security Information Management, яке відповідає за інформаційну безпеку, і Security Event Management, що контролює події безпеки. У 2005 році відбувається об'єднання понять, і з'являється Security Information and Event Management.

Дані для SIEM надходять з різних джерел. До них відносяться:

журнали подій, які реєструються операційною системою або стороннім додатком

мережеве обладнання (маршрутизатори, проксі-сервери, шлюзи і т. д.)

міжмережеві екрани

сканери вразливостей - спеціальне програмне забезпечення, яке знаходить уразливості всередині інфраструктури

CRM-системи

робочі станції користувачів

антивірусне програмне забезпечення

інші ресурси, які реєструють події і здатні передавати їх через агентів або вбудованими засобами

Аудит інформаційної безпеки

Принцип роботи

SIEM використовують для моніторингу та аналізу інформації, що надходить, але сама вона не захищає інфраструктуру від зовнішніх і внутрішніх загроз. Зібрана аналітика використовується для визначення інцидентів і оптимізації захисту компанії.

Задаються критерії, за якими оцінюється стан інфраструктури. Прописується обладнання, яке буде моніториться SIEM. Якщо відбувається подія, яка виходить за рамки налаштованих шаблонів, то SIEM реагує на зміну і реєструє інцидент.

Рекомендується спочатку розгорнути систему на малій кількості пристроїв для тестування. Адміністратори перевіряють її працездатність, редагують правила, а після запускають в робочому режимі.

Додаткова можливість системи: на основі отриманих даних аналізуються дії зловмисників. Іншими словами, реєстрація інцидентів допомагає розслідувати такі події.

Вбудована функція оповіщення повідомляє адміністраторам про порушення або проблеми з email, через SMS та месенджери.

ПО являє собою гнучкий інструмент, який конфігурується по вимогам і бажанням користувача.

Складові SIEM

Програмне рішення умовно поділяють на дві складові частини. До першої відносяться агенти моніторингу. Вони встановлюються на елементи інформаційної системи, з яких знімаються показання. Другий елемент - серверна частина. Вона обробляє інформацію, що надходить від агентів,

реєструє події та інциденти на основі заданих правил. Шаблони обробки інформації та реєстрації інцидентів задаються фахівцями з ІБ під час конфігурації

SIEM-системи

Подальший аналіз зареєстрованих інцидентів лягає також на відділ ІБ. Вони за допомогою вбудованих інструментів створюють звіти, реагують на події, намагаючись не допустити повторення інцидентів надалі. Також інтегруються проміжні елементи - колектори і корелятори. Перші встановлюють як звичайні сховища. Вони фільтрують дані, відсіваючи дублі і порожні записи. Другі ж виокремлює необхідні дані серед безлічі подій. З огляду на, що інформація може надаватися в різних форматах і різного роду, SIEM-система збирає її і призводить до єдиного вигляду.

Відомі SIEM:

Splunk Enterprise Security
HPE ArcSight
McAfee NitroSecurity
Qradar
Tibco Loglogic
MaxPatrol
AlienVault Usm

1.5 Терміни та визначення

Автентифікація – процедура перевірки автентичності суб’єкта, що дозволяє переконатися в тому, що суб’єкт, який пред’явив свій ідентифікатор, насправді є саме тим суб’єктом, ідентифікатор якого він використовує.

Авторизація – процедура надання суб’єкту певних прав доступу до ресурсів системи або перевірка наявності прав при спробі виконати будь-яку дію.

Алфавіт – набір символів, який використовується для запису повідомлень.

Апаратні засоби захисту інформації – механічні, електричні, електромеханічні, електронні, електронно-механічні, оптичні, лазерні, радіолокаційні і тому подібні пристрої, що вбудовуються в інформаційні системи для вирішення завдань захисту інформації.

Атака – це дія, що робиться зловмисником, яка полягає в пошуку і використанні тієї або іншої вразливості для реалізації загрози.

Атака на шифр – спроба розкриття шифру.

Бекдор – комп’ютерна програма, яку встановлюють зловмисники на зламаному комп’ютері після отримання початкового доступу з метою повторного отримання доступу до системи.

Вірус – вид шкідливого програмного забезпечення, здатного створювати копії самого себе і вбудовуватися в код інших програм, системні області пам'яті,завантажувальні сектори, а також поширювати свої копії по різних каналах зв'язку.

Вразливість – це деяка невдала характеристика системи, яка робить можливим виникнення загрози.

Геш (цифровий відбиток, дайджест повідомлення) – результати перетворення вхідного масиву даних за допомогою геш-функції.

Геш-функція – легко обчислювана функція, яка перетворює вихідне повідомлення довільної довжини (прообраз) в повідомлення фіксованої довжини (геш-образ), для якої не існує ефективного алгоритму пошуку колізій.

Гешування – перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини.

Доступність – властивість системи, яка гарантує, що суб'єкти, які мають право доступу до інформації в потрібний момент зможуть отримати її.

Експлоїт – комп'ютерна програма, фрагмент програмного коду або послідовність команд, які використовують вразливості в програмному забезпеченні та застосовуються для здійснення атак.

Електронний цифровий підпис – реквізит електронного документу, призначений для захисту даного документу від підробки, отриманий в результаті криптографічного перетворення інформації з використанням закритого ключа ЕЦП і що дозволяє ідентифікувати власника сертифіката ключа підпису, а також встановити відсутність спотворення інформації в електронному документі.

Загроза – це потенційно можлива подія, неважливо, навмисна чи ні, яка може зробити небажаний вплив на систему, а також на інформацію, що зберігається в ній.

Захист інформації – комплекс правових, організаційних і технічних заходів і дій щодо запобігання загроз інформаційній безпеці та усунення їх наслідків в процесі збору, зберігання, обробки і передачі інформації в інформаційних системах.

Ідентифікація – процедура розпізнавання суб'єкта за його ідентифікатором.

Інформаційна безпека – стан захищеності інформації, при якому забезпечуються її конфіденційність, доступність і цілісність.

Інформація – відомості, які є об'єктом збору, зберігання, обробки, безпосереднього використання та передачі в інформаційних системах.

Ключ – змінний параметр шифру, що забезпечує вибір одного перетворення з сукупності різних для даного алгоритму і повідомлення, необхідний для шифрування і розшифровки повідомлень.

Код перевірки автентичності повідомлень (Message Authentication Code, MAC) – значення геш-функції, залежне не тільки від прообразу, а й закритого ключа.

Колізія для функції h – пара значень x та y, така, що h (x) = h (y).

Конфіденційність – властивість інформації бути відомою і доступною тільки суб'єктам системи (користувачам, програмам, процесам), які пройшли перевірку (авторизацію).

Криптоаналіз – це дослідження інформаційних систем з метою вивчення їх прихованих аспектів.

Криптографічний стійкість (крипостійкість) шифру – здатність криптографічного алгоритму протистояти можливим атакам на нього або оцінка алгоритму, здатного зламати шифр.

Криптографія – це сукупність методів перетворення інформації з метою приховання її змісту, забезпечення цілісності та справжності авторства, а також неможливості відмови від авторства.

Криптологія – наука про захист інформації, шляхом її перетворення, криптологія поєднує два напрямки – криптографію й криптоаналіз.

Криптосистеми загального використання – криптосистеми, засновані на секретності ключа і складності його підбору потенційним супротивником.

Криптосистеми обмеженого використання – криптосистеми, засновані на збереженні в секреті самого характеру алгоритмів шифрування і дешифрування.

Неспростовність – здатність засвідчувати дію, що мала місце так, щоб вона не могли бути пізніше заперечена.

Програмні засоби захисту інформації – пакети програм, окремі програми або їх частини, що використовуються для вирішення завдань захисту інформації.

Прообраз геш-функції – вхідний масив даних для перетворення геш-функцією.

Протокол – сукупність правил, що регламентують послідовність кроків, що вживаються двома або більшою кількість сторін для спільного вирішення деякої задачі, а також регламентують формати повідомлень, що пересилаються між учасниками обміну, і дії при виникненні збоїв.

Ризик – ймовірність використання вразливості системи для реалізації загрози.

Розкриття шифру – процес отримання інформації з шифрованого повідомлення без знання ключа шифру.

Розшифрування – процес відновлення вихідного повідомлення із застосуванням ключа, шифру та зашифрованого повідомлення.

Руткіт – набір програмних засобів (виконуваних файлів, скриптів, конфігураційних файлів) для: забезпечення маскування процесів, файлів, каталогів, драйверів; контролю подій, що відбуваються в системі; збору даних про систему.

Сеансовий (сесійний) ключ – ключ, який використовується абонентами в рамках одного сеансу (сесії, раунду) спілкування.

Сертифікат електронного цифрового підпису – відкритий ключ з деякою додатковою інформацією про його власника (реєстраційний номер сертифіката, ПІБ власника, термін дії тощо), підписаний ключем Центру сертифікації.

Троян – шкідлива програма, яка проникає на комп'ютер жертви під безпечним видом і наносить шкоду: передача власнику трояна приватної інформації або дає можливість дистанційно керувати зараженим комп'ютером.

Цілісність – властивість інформації, яка гарантує, що тільки певні суб'єкти можуть міняти інформацію.

Часова складність алгоритму – функція розміру вхідних і вихідних даних, що дорівнює кількості елементарних операцій, що виконуються алгоритмом для вирішення екземпляру завдання зазначеного розміру.

Шифр – сукупність методів і способів зворотного перетворення інформації з метою її захисту від несанкціонованого доступу.

Шифрування – процес застосування шифру до інформації, яку необхідно захистити, тобто перетворення вихідного повідомлення в зашифроване, за допомогою певних правил, що містяться в шифрі.

Zero-day (0-day) – це раніше невідома вразливість, яка використовується зловмисниками для виконання атак.

1.6 Зони безпеки мережі(Network Security Zones)

Зона безпеки — це частина мережі, для якої встановлено певні вимоги до безпеки. Кожна зона складається з одного інтерфейсу або групи інтерфейсів, до яких застосовується політика безпеки. Ці зони, як правило, розділені за допомогою пристрою рівня 3, такого як брандмауер.

У дуже широкому сенсі, брандмауер використовується для моніторингу трафіку, що входить і виходить від мережі. Трафік дозволяється або відхиляється на основі заздалегідь визначеного набору правил, які називаються списком керування доступом, або скорочено ACL. Хоча існує багато різних типів брандмауерів, брандмауер повинен мати наступні властивості:

- Повинен бути стійким до атак
- Повинен бути в змозі перевірити трафік між мережами
- Повинен мати можливість фільтрувати трафік

Кількість мереж, які ми можемо створити на брандмауері, залежить від кількості доступних фізичних портів. Взагалі кажучи, стандартна реалізація брандмауера передбачає розділення надійного трафіку та ненадійного трафіку. Правильна реалізація брандмауера створює дві основні зони безпеки, внутрішню та зовнішню (рис. 1.1)

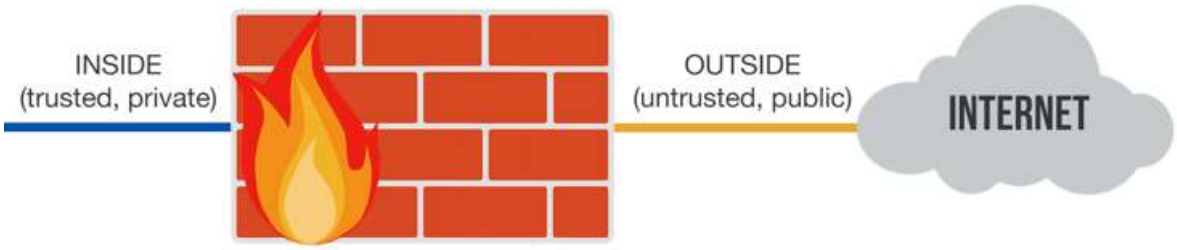


Рисунок 1.1 Внутрішня та зовнішня зони.

Внутрішню або надійну зону також називають приватною зоною. Як випливає з назви, ця зона містить активи та системи, до яких не повинен мати доступ будь-хто за межами організації. Це стосується робочих станцій користувачів, принтерів, непублічних серверів і всього іншого, що вважається внутрішнім ресурсом. Пристрої, знайдені тут, мають приватні IP-адреси, призначені в мережі.

Зовнішня або ненадійна зона також відома як громадська зона. Ця зона вважається поза контролем організації і може розглядатися як просто громадський Інтернет.

Третя базова зона безпеки називається DMZ, або демілітаризована зона. Ресурси DMZ вимагають зовнішнього доступу з зовнішньої зони. На DMZ знаходяться загальнодоступні сервери, такі як електронна пошта, веб-сервери або сервери додатків. DMZ дозволяє загальний доступ до цих ресурсів, не наражаючи приватні, внутрішні ресурси зони під загрозу(рис.1.2).

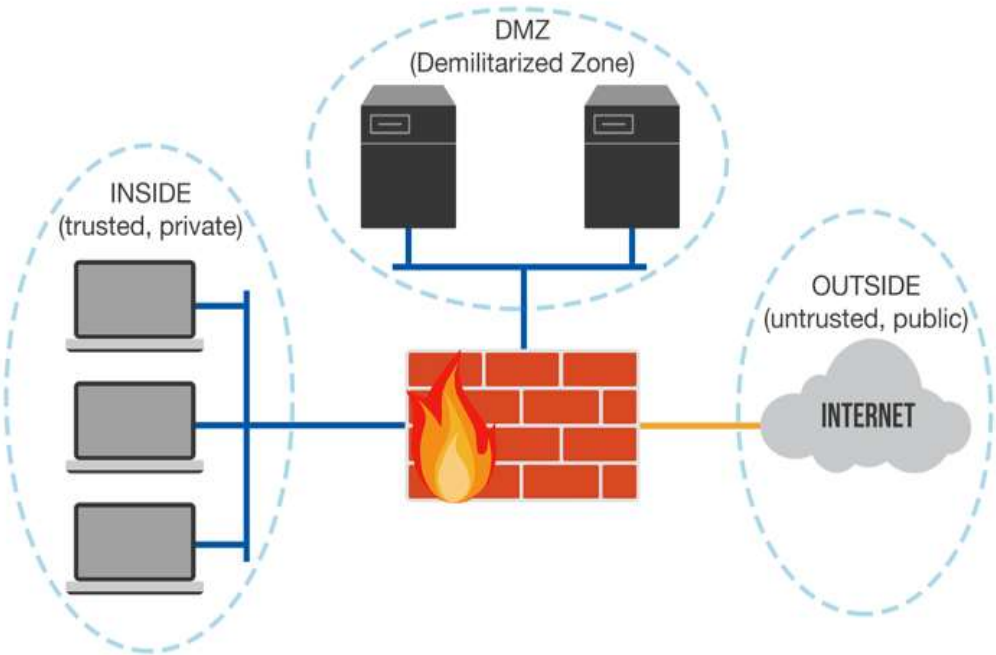


Рисунок 1.2 DMZ.

Політики фільтрування зон

У випадку мережевих зон безпеки брандмауер застосовує політику контролю доступу, визначаючи, який трафік може проходити між налаштованими зонами. При такій спільній реалізації трьох зон існує кілька рекомендованих політик фільтрації зон, які повинні бути впроваджені:

Зсередини назовні та всередині DMZ: Трафік, що походить зсередини, перевіряється, коли він рухається в напрямку або зовні, або DMZ. Наприклад, співробітник, який запитує веб-сторінку з загальнодоступного веб-сервера або має доступ до будь-якого ресурсу в DMZ. Цей тип трафіку допускається з дуже малими обмеженнями, якщо такі є.

Ззовні всередину: Трафік, що походить ззовні і рухається в бік внутрішньої сторони, повністю заблокований, якщо тільки трафік не відповідав на запит внутрішнього ресурсу. Наприклад, якщо внутрішній користувач запитує веб-сторінку із загальнодоступного веб-сервера, цей зовнішній трафік дозволено. З'єднання, які походять із публічної мережі і не являються відповіддю на запит, будуть заблоковані.

З DMZ всередину: Трафік, що походить з DMZ і рухається в бік внутрішньої сторони, також заблокований повністю, якщо тільки трафік не є відповіддю на законний запит зсередини.

Зовні DMZ: Трафік, що походить ззовні і рухається в напрямку ДМЗ, перевіряється брандмауером і вибірково дозволений або заборонений. Можуть бути передані певні типи трафіку, такі як електронна пошта, HTTP, HTTPS або DNS-трафік. Також зверніть увагу, що відповіді від ДМЗ назад назовні будуть динамічно дозволені. Іншими словами, брандмауер буде динамічно відкривати порт, щоб дозволити необхідний трафік з ДМЗ назовні в міру необхідності.

DMZ назовні: Рух, що походить з ДМЗ і подорожує назовні, вибірково дозволений на основі вимог сервісу і правил брандмауера. Наприклад, якщо в DMZ є сервер електронної пошти, який потрібно реплікувати з сервером електронної пошти в іншому місці, політика брандмауера повинна дозволити цей тип трафіку.

ЛЕКЦІЯ 2.
ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

2.1 Класифікація загроз

Розгляд можливих загроз інформаційної безпеки проводиться з метою визначення повного набору вимог до розроблюваної системи захисту. Зазвичай під загрозою (в загальному сенсі) розуміють потенційно можливу подію (вплив, процес або явище), яка може зробити небажаний вплив на систему, а також на інформацію, що зберігається в ній. Далі під загрозою безпеці інформаційної системи (ІС) будемо розуміти можливість впливу на ІС, яка прямо або непрямо може завдати їй шкоди.

В даний час відомий досить великий перелік загроз безпеки ІС, що містить сотні позицій. Перелік загроз, оцінки ймовірностей їх реалізації, а також модель порушника служать основою для аналізу ризику реалізації загроз і формулювання вимог до системи захисту ІС. Крім виявлення можливих загроз, доцільно проведення аналізу цих загроз на основі їх класифікації за рядом ознак. Кожна з ознак класифікації відбиває одну із узагальнених вимог до системи захисту. Загрози, що відповідають кожній ознаці класифікації, дозволяють деталізувати вимогу, що відображає ця ознака.

Необхідність класифікації загроз безпеки ІС обумовлена тим, що інформація, яка зберігається та оброблюється в сучасних ІС, піддана впливу надзвичайно великого числа факторів, в силу чого стає неможливим формалізувати задачу опису повної множини загроз. Тому для системи, яка захищається, зазвичай визначають не повний перелік загроз, а перелік класів загроз.

Прийнято вважати, що, незалежно від конкретних видів загроз і їх проблемно-орієнтованої класифікації, ІС задовольняє потреби експлуатуючих її осіб, якщо забезпечуються наступні важливі властивості інформації та систем її обробки: доступність, цілісність і конфіденційність інформації. Іншими словами, інформаційна безпека ІС забезпечена у разі, якщо для інформаційних ресурсів у системі підтримуються певні рівні:

- доступності (можливості за розумний час отримати необхідну інформацію);
- цілісності (неможливості несанкціонованої або випадкової модифікації інформації);
- конфіденційності (неможливості несанкціонованого отримання інформації).

Відповідно, для автоматизованих інформаційних систем загрози слід класифікувати насамперед по аспекту інформаційної безпеки (доступність, цілісність, конфіденційність), проти якого вони спрямовані в першу чергу:

- загрози порушення доступності (відмова в обслуговуванні), спрямовані на створення таких ситуацій, коли певні дії або блокують доступ до деяких ресурсів ІС, або знижують її працездатність. Наприклад, якщо один користувач системи запитує доступ до деякої служби, а інший виконує дії по блокуванню цього доступу, то перший користувач отримує відмову в обслуговуванні. Блокування доступу до ресурсу може бути постійним або тимчасовим;
- загрози порушення цілісності інформації, що зберігається в комп’ютерній системі чи переданої по каналу зв’язку, які спрямовані на її зміну або спотворення, що приводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена навмисно зловмисником, а також в результаті об’єктивних впливів з боку середовища, що оточує систему. Ця загроза особливо актуальна для систем передачі інформації – комп’ютерних мереж і систем

телекомунікацій. Навмисні порушення цілісності інформації не слід плутати з її санкціонованою зміною, яка виконується повноважними особами з обґрунтованою метою (наприклад, такою зміною є періодична корекція якої-небудь бази даних);

- загрози порушення конфіденційності, спрямовані на розголошення конфіденційної або секретної інформації. При реалізації цих загроз інформація стає відомою особам, які не повинні мати до неї доступ. У термінах комп'ютерної безпеки загроза порушення конфіденційності має місце щоразу, коли отримано несанкціонований доступ до деякої закритої інформації, що зберігається в комп'ютерній системі чи переданої від однієї системи до іншої.

Дані види загроз можна вважати первинними, або безпосередніми, оскільки їх реалізація веде до безпосередньої дії на захищену інформацію.

Класифікація можливих загроз безпеки ІС може бути проведена також по ряду інших ознак.

- За природою виникнення розрізняють:
  - Природні загрози, викликані впливами на ІС об'єктивних фізичних процесів або стихійних природних явищ;
  - Штучні загрози безпеки ІС, викликані діяльністю людини.
- За ступенем навмисності прояву розрізняють:
  - Загрози, викликані помилками або халатністю персоналу, наприклад некомпетентного використання засобів захисту; введення помилкових даних, тощо;
  - Загрози навмисної дії, наприклад дії зловмисників.
- По безпосередньому джерелу загроз. Джерелами загроз можуть бути:
  - Природне середовище, наприклад стихійні лиха, магнітні бурі, тощо;
  - Людина, наприклад вербування шляхом підкупу персоналу, розголошення конфіденційних даних, тощо;
  - Санкціоновані програмно-апаратні засоби, наприклад видалення даних, відмова в роботі операційної системи;
  - Несанкціоновані програмно-апаратні засоби, наприклад зараження комп'ютера вірусами з деструктивними функціями.
- За положенням джерела загроз. Джерело загроз може бути розташоване:
  - поза контрольованою зоною ІС, наприклад перехоплення даних, переданих по каналах зв'язку, перехоплення електромагнітних, акустичних та інших випромінювань пристроїв;
  - в межах контрольованої зони ІС, наприклад застосування підслуховуючих пристроїв, розкрадання роздруківок, записів, носіїв інформації тощо; безпосередньо в ІС, наприклад некоректне використання ресурсів ІС.
- За ступенем залежності від активності ІС. Загрози проявляються:

- незалежно від активності ІС, наприклад зламування шифрів криптозахисту інформації;
- тільки в процесі обробки даних, наприклад загрози виконання і розповсюдження програмних вірусів.

- За ступенем впливу на ІС розрізняють:
  - пасивні загрози, які при реалізації нічого не змінюють у структурі та змісті ІС, наприклад загроза копіювання секретних даних;
  - активні загрози, які при впливі вносять зміни в структуру та зміст ІС, наприклад впровадження троянських коней і вірусів.
- По етапах доступу користувачів або програм до ресурсів ІС розрізняють:
  - загрози, які проявляються на етапі доступу до ресурсів ІС, наприклад загрози несанкціонованого доступу в ІС;
  - загрози, які проявляються після дозволу доступу до ресурсів ІС, наприклад загрози несанкціонованого або некоректного використання ресурсів ІС.
- За способом доступу до ресурсів ІС розрізняють:
  - загрози з використанням стандартного шляху доступу до ресурсів ІС, наприклад незаконне отримання паролів і інших реквізитів розмежування доступу з подальшим маскуванням під зареєстрованого користувача;
  - загрози з використанням прихованого нестандартного шляху доступу до ресурсів ІС, наприклад несанкціонований доступ до ресурсів ІС шляхом використання не документованих можливостей ОС.
- За поточним місцем розташування інформації, що зберігається і оброблюваної в ІС, розрізняють:
  - загрози доступу до інформації на зовнішніх запам’ятовуючих пристроях, наприклад несанкціоноване копіювання секретної інформації з жорсткого диску;
  - загрози доступу до інформації в оперативній пам’яті, наприклад читання залишкової інформації з оперативної пам’яті; доступ до системної області оперативної пам’яті з боку прикладних програм; загрози доступу до інформації, що циркулює в лініях зв’язку, наприклад незаконне підключення до ліній зв’язку з подальшим введенням помилкових повідомлень або модифікацією переданих повідомлень; незаконне підключення до ліній зв’язку з метою прямої підміни легального користувача з подальшим введенням дезінформації та нав’язуванням помилкових повідомлень;
  - загрози доступу до інформації, яка відображається на терміналі або що друкується на принтері, наприклад запис відображуваної інформації на приховану відеокамеру.

Як вже зазначалося, небезпечний вплив на ІС поділяють на випадковий і навмисний. Аналіз досвіду проектування, виготовлення і експлуатації ІС

показує, що інформація піддається різним випадковим впливам на всіх етапах циклу життя і функціонування ІС.

- Причинами випадкових впливів при експлуатації ІС можуть бути:
- аварійні ситуації через стихійні лиха та відключення електроживлення;
- відмови і збої апаратури;
- помилки в програмному забезпеченні;
- помилки в роботі обслуговуючого персоналу і користувачів;
- перешкоди в лініях зв'язку через вплив зовнішнього середовища.

Помилки в програмному забезпеченні (ПЗ) є поширеним видом комп'ютерних порушень. Програмне забезпечення серверів, робочих станцій, маршрутизаторів написане людьми, тому воно практично завжди містить помилки. Чим вища складність подібного програмного забезпечення, тим більша вірогідність виявлення в ньому помилок і вразливостей. Більшість з них не представляють ніякої небезпеки, деякі ж можуть призвести до серйозних наслідків, таких як отримання зловмисником контролю над сервером, непрацездатність сервера, несанкціоноване використання ресурсів (використання комп'ютера як плацдарму для атаки та інше). Зазвичай подібні помилки усуваються за допомогою пакетів оновлень, які регулярно випускаються виробником ПЗ. Своєчасна установка таких пакетів є необхідною умовою безпеки інформації.

Навмисні загрози пов'язані з цілеспрямованими діями порушника. В якості порушника можуть виступати службовець, відвідувач, конкурент, найманець тощо. Дії порушника можуть бути обумовлені різними мотивами: невдоволенням службовця своєю кар'єрою, суто матеріальним інтересом (хабар), цікавістю, конкурентною боротьбою, прагненням самоствердитися будь-якою ціною тощо.

Виходячи з можливості виникнення найбільш небезпечної ситуації, обумовленої діями порушника, можна скласти гіпотетичну модель потенційного порушника:

- кваліфікація порушника може бути на рівні розробника даної системи;
- порушником може бути як стороння особа, так і законний користувач системи;
- порушнику відома інформація про принципи роботи системи;
- порушник вибере найбільш слабку ланку в захисті.

До таких порушників належать, зокрема, інсайдери. Інсайдер – це людина, допущена до роботи з інформацією, яка призначена для строго обмеженого кола осіб. Використовуючи своє становище, інсайдери крадуть інформацію. Вони можуть передавати її по електронній пошті, копіювати на різні USB-пристрої і КПК, записувати в ноутбуки, роздруковувати і виносити на папері, викладати на всілякі файлообмінні ресурси.

Найбільш поширеним і різноманітним видом комп'ютерних порушень є несанкціонований доступ (НСД). Суть НСД полягає в отриманні користувачем

(порушником) доступу до об’єкта в порушення правил розмежування доступу, встановлених відповідно до прийнятої в організації політики безпеки. НСД використовує будь-яку помилку в системі захисту і можливий при нераціональному виборі засобів захисту, їх некоректного встановлення та налаштування. НСД може бути здійснений як штатними засобами ІС, так і спеціально створеними апаратними і програмними засобами.

Перелічимо основні канали несанкціонованого доступу, через які порушник може отримати доступ до компонентів ІС і здійснити розкрадання, модифікацію та / або руйнування інформації:

- штатні канали доступу до інформації (термінали користувачів, оператора, адміністратора системи; засоби відображення і документування інформації; канали зв’язку) при їх використанні порушниками, а також законними користувачами поза межами їх повноважень;
- технологічні пульти управління;
- лінії зв’язку між апаратними засобами ІС;
- побічні електромагнітні випромінювання від апаратури, ліній зв’язку, мереж електроживлення і заземлення та ін.

З усього розмаїття способів і прийомів несанкціонованого доступу варто зупинитись на наступних поширених і пов’язаних між собою порушеннях:

- перехоплення паролів;
- маскарад;
- незаконне використання привілеїв;
- шкідливі програми.

Перехоплення паролів здійснюється спеціально розробленими програмами. При спробі законного користувача увійти в систему, програма-перехоплювач імітує на екрані дисплея введення імені та паролю користувача, які відразу пересилаються власнику програми-перехоплювача, після чого на екран виводиться повідомлення про помилку і управління повертається операційній системі. Користувач припускає, що допустив помилку при введенні пароля. Він повторює введення і отримує доступ в систему. Власник програми- перехоплювача, що отримав ім’я і пароль законного користувача, може тепер використовувати їх у своїх цілях. Існують і інші способи перехоплення паролів.

Маскарад – це виконання будь-яких дій одним користувачем від імені іншого користувача, що володіє відповідними повноваженнями. Метою маскараду є приписування будь-яких дій іншому користувачеві або при-присвоєнні повноважень і привілеїв іншого користувача. Прикладами реалізації маскараду є:

- вхід в систему під ім’ям і паролем іншого користувача (цьому маскараду передує перехоплення пароля);
- передача повідомлень у мережі від імені іншого користувача.

Маскарад особливо небезпечний в банківських системах електронних платежів, де неправильна ідентифікація клієнта через маскарад зловмисника може призвести до великих збитків законного клієнта банку.

Незаконне використання привілеїв. Більшість систем захисту встановлюють певні набори привілеїв для виконання заданих функцій. Кожен користувач отримує свій набір привілеїв: звичайні користувачі – мінімальний, адміністратори – максимальний. Несанкціоноване захоплення привілеїв, наприклад, за допомогою маскараду, призводить до можливості виконання порушником певних дій в обхід системи захисту. Слід зазначити, що незаконне захоплення привілеїв можливе або при наявності помилок у системі захисту, або через недбалість адміністратора при управлінні системою і призначення привілеїв.

Шкідливі програми. До таких програм відносяться комп'ютерні віруси, мережні черв'яки, програма «троянський кінь». Особливо вразливі до цих програм робочі станції кінцевих користувачів. Дамо коротку характеристику цих поширених загроз безпеки ІС.

Комп'ютерний вірус являє собою своєрідне явище, що виникло в процесі розвитку комп'ютерної та інформаційної техніки. Суть цього явища полягає в тому, що програми-віруси мають ряд особливостей, властивих живим організмам, вони народжуються, розмножуються і помирають. Термін «вірус» у застосуванні до комп'ютерів запропонував Фред Коен з університету Південної Каліфорнії. Історично перше визначення вірусу було дано Ф. Коеном: «Комп'ютерний вірус – це програма, яка може заражати інші програми, модифікуючи їх допомогою включення в них своєї, можливо, зміненої копії, причому остання зберігає здатність до подальшого розмноження». Комп'ютерні віруси завдають шкоди системі за рахунок швидкого розмноження і руйнування середовища проживання.

Мережний черв'як є різновидом програми-вірусу, який поширюється глобальною мережею.

«Троянський кінь» являє собою програму, яка поряд з діями, описаними в її документації, виконує деякі інші дії, що ведуть до порушення безпеки системи і деструктивних результатів. Аналогія такої програми з давньогрецьким троянським конем цілком виправдана, тому що в обох випадках оболонка, яка не викликає підозру, таїть серйозну загрозу. Радикальний спосіб захисту від цієї загрози полягає у створенні замкнутого середовища виконання програм, яке повинне захищатися від несанкціонованого доступу.

Слід зазначити, що троянські коні, комп'ютерні віруси і мережні черв'яки відносяться до вельми небезпечних загроз ІС. Особливістю сучасних шкідливих програм є їхня орієнтація на конкретне прикладне ПЗ, що стало стандартом де- факто для більшості користувачів, в першу чергу це Microsoft Internet Explorer і Microsoft Outlook. Масове створення вірусів під продукти Microsoft пояснюється не тільки низьким рівнем безпеки і надійності програм, важливу роль грає глобальне поширення цих продуктів. Автори шкідливого програмного забезпечення все активніше починають досліджувати «дірки» в

популярних СУБД, в пов'язаних з ними ПЗ і корпоративних бізнес-застосуваннях, побудованих на базі цих систем.

Шкідливі програми постійно еволюціонують, основною тенденцією їх розвитку є поліморфізм. Сьогодні вже досить складно провести межу між вірусом, черв'яком і троянською програмою – вони використовують практично одні й ті ж механізми, невелика різниця полягає лише в ступені цього використання. Структура шкідливого програмного забезпечення стала сьогодні настільки уніфікованою, що, наприклад, відрізнити поштовий вірус від черв'яка з деструктивними функціями практично неможливо. Навіть у троянських програмах з'явилася функція реплікації (як один із засобів протидії антивірусним засобам), так що при бажанні їх цілком можна назвати вірусами (з механізмом поширення у вигляді маскування під прикладні програми).

Для захисту від шкідливих програм необхідно застосування низки заходів:

- виключення несанкціонованого доступу до виконуваних файлів;
- тестування придбаних програмних засобів;
- контроль цілісності виконуваних файлів і системних областей;
- створення замкнутого середовища виконання програм.

Боротьба з вірусами, черв'яками і троянськими кіньми ведеться за допомогою ефективного антивірусного програмного забезпечення, що працює на рівні користувача і на рівні мережі. У міру появи нових вірусів, черв'яків і троянських коней потрібно оновлювати бази даних антивірусних засобів і застосувань.

Як уже зазначалося, загрози порушення доступності, цілісності і конфіденційності інформації є первинними або безпосередніми, оскільки реалізація цих загроз веде до безпосередньої дії на інформацію, яка захищається.

Для сучасних інформаційних технологій підсистеми захисту є невід'ємною частиною ІС обробки інформації. Атакуюча сторона повинна здолати цю підсистему захисту, щоб порушити, наприклад, конфіденційність ІС. Однак потрібно усвідомлювати, що не існує абсолютно стійкою системи захисту, питання лише в часі і засобах, потрібних на її подолання.

Подолання захисту також являє собою загрозу, тому для захищених систем можна розглядати четвертий вид загрози – загрозу розкриття параметрів ІС, що включає в себе підсистему захисту. На практиці будь-який проведений захід випереджається етапом розвідки, в ході якого визначаються основні параметри системи, її характеристики тощо. Результатом цього етапу є уточнення поставленого завдання, а також вибір найбільш оптимального технічного засобу.

Загрозу розкриття параметрів ІС можна вважати опосередкованою. Наслідки її реалізації не заподіюють якого-небудь збитку оброблюваній інформації, але дають можливість реалізувати первинні або безпосередні загрози, перераховані вище.

2.2 Типи атак на інформаційні системи

Стрімке зростання популярності Інтернет-технологій супроводжується зростанням серйозних загроз розголошення персональних даних, критично важливих корпоративних ресурсів, державних таємниць тощо. Кожен день зловмисники піддають загрозам мережні інформаційні ресурси, намагаючись отримати до них доступ за допомогою спеціальних атак. Ці атаки стають все більш витонченими по впливу і нескладними у виконанні. Цьому сприяють два основні чинники.

По-перше, це повсюдне проникнення мережі Інтернет. Сьогодні до цієї мережі підключені мільйони комп'ютерів. Багато мільйонів комп'ютерів будуть підключені до мережі Інтернет в найближчому майбутньому, тому ймовірність доступу зловмисників до вразливих комп'ютерів і комп'ютерних мереж постійно зростає. Крім того, широке поширення мережі Інтернет дозволяє зловмисникам обмінюватися інформацією в глобальному масштабі.

По-друге, це загальне поширення простих у використанні операційних систем і середовищ розробки. Цей фактор різко знижує вимоги до рівня знань зловмисника. Раніше від зловмисника були потрібні хороші знання і навички програмування, щоб створювати і поширювати шкідливі програми. Тепер для того, щоб отримати доступ до чужого комп'ютера, потрібно просто знати IP-адресу потрібного сайту, а для проведення атаки досить клацнути мишею.

Проблеми забезпечення інформаційної безпеки в корпоративних комп'ютерних мережах обумовлені загрозами безпеці для локальних робочих станцій, локальних мереж і атаками на корпоративні мережі, що мають вихід в загальнодоступні мережі передачі даних.

Мережні атаки настільки ж різноманітні, як і системи, проти яких вони спрямовані. Деякі атаки відрізняються великою складністю. Інші – здатний здійснити звичайний оператор, навіть не припускаючи, які наслідки може мати його діяльність.

Порушник, здійснюючи атаку, зазвичай ставить перед собою наступні цілі:

- порушення конфіденційності переданої інформації;
- порушення цілісності та достовірності інформації, що передається;
- порушення працездатності системи в цілому або окремих її частин.

З точки зору безпеки розподілені системи характеризуються насамперед наявністю віддалених атак, оскільки компоненти розподілених систем зазвичай використовують відкриті канали передачі даних і порушник може не тільки проводити пасивне прослуховування переданої інформації, але і модифікувати переданий трафік (активний вплив). І якщо активний вплив на трафік може бути зафіксований, то пасивний вплив практично не піддається виявленню. Але оскільки в ході функціонування розподілених систем обмін службовою інформацією між компонентами системи здійснюється теж по відкритих каналах передачі даних, то службова інформація стає таким же об'єктом атаки, як і дані користувача.

Атаки доступу

Атака доступу – це спроба отримання зловмисником інформації, на ознайомлення з якою у нього немає дозволу. Атака доступу спрямована на порушення конфіденційності інформації.

Підслуховування (Sniffing). Здебільшого дані передаються по комп'ютерним мережам в незахищеному форматі (відкритим текстом), що дозволяє зловмисникові, що отримав доступ до ліній передачі даних в мережі, підслуховувати або зчитувати трафік. Для підслуховування у комп'ютерних мережах використовують сніфер. Сніфер пакетів являє собою прикладну програму, яка перехоплює всі мережні пакети, що передаються через певний сегмент.

В даний час сніфери працюють в мережах на цілком законній підставі. Вони використовуються для діагностики несправностей і аналізу трафіку. Однак через те, що деякі мережні застосування передають дані в текстовому форматі (Telnet, FTP, SMTP, POP3 і т.д.), за допомогою сніферу можна дізнатися корисну, а іноді і конфіденційну інформацію (наприклад, імена користувачів і паролі). Запобігти загрозі снiфінгу пакетів можна за допомогою наступних заходів і засобів: застосування для автентифікації одноразових паролів; установка апаратних або програмних засобів, які розпізнають сніфери; застосування криптографічного захисту каналів зв'язку.

Перехоплення (Hijacking). На відміну від підслуховування, перехоплення – це активна атака. Зловмисник перехоплює інформацію в процесі її передачі до місця призначення. Перехоплення імен і паролів створює велику небезпеку, оскільки користувачі часто застосовують одні й ті ж логін та пароль для безлічі застосувань і систем. Багато користувачів взагалі мають один пароль для доступу до всіх ресурсів і застосувань. Якщо застосування працює в режимі клієнт/сервер, а автентифікаційні дані передаються по мережі у відкритому текстовому форматі, цю інформацію з великою ймовірністю можна використовувати для доступу до інших корпоративних або зовнішніх ресурсів.

В найгіршому випадку зловмисник отримує доступ до ресурсу користувача на системному рівні і з його допомогою створює атрибути нового користувача, які можна в будь-який момент застосувати для доступу в мережу і до її ресурсів.

Перехоплення сеансу (Session Hijacking). По закінченні початкової процедури автентифікації з'єднання, встановлене законним користувачем, наприклад, з поштовим сервером, перемикається зловмисником на новий вузол, а вихідному серверу надається команда розірвати з'єднання. В результаті «співрозмовник» законного користувача виявляється непомітно підміненим.

Після отримання доступу до мережі у атакуючого зловмисника з'являються великі можливості:

він може посилати некоректні дані застосуванням і мережним службам, що призводить до їх аварійного завершення або неправильного функціонування;

він може також наповнити комп'ютер або всю мережу трафіком, поки не відбудеться зупинка системи у зв'язку з перевантаженням;

нарешті, атакуючий може блокувати трафік, що призведе до втрати доступу авторизованих користувачів до мережних ресурсів.

Атаки модифікації

Атака модифікації – це спроба неправомірної зміни інформації. Така атака можлива скрізь, де існує або передається інформація; вона спрямована на порушення цілісності інформації.

Зміна даних. Зловмисник, отримавши можливість прочитати чужі дані, зможе зробити і наступний крок – змінити їх. Дані в пакеті можуть бути змінені, навіть якщо зловмисник нічого не знає ні про відправника, ні про одержувача.

Додавання даних. Інший тип атаки – додавання нових даних, наприклад, в інформацію про історію минулих періодів. Зломщик виконує операцію в банківській системі, внаслідок чого кошти з рахунку клієнта переміщуються на його власний рахунок.

Видалення даних. Атака видалення означає переміщення існуючих даних, наприклад анулювання запису про операції з балансового звіту банку, в результаті чого зняті з рахунку грошові кошти залишаються на ньому.

Атаки типу «відмова в обслуговуванні»

Атака «відмова в обслуговуванні» (Denial-of-Service, DoS) відрізняється від атак інших типів. Вона не націлена на отримання доступу до мережі або витягу з цієї мережі будь-якої інформації. DoS-атака робить мережу організації недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або програми. По суті, ця атака позбавляє звичайних користувачів доступу до ресурсів або комп'ютерів мережі організації.

Більшість DoS-атак спирається на загальні слабкості системної архітектури. У разі використання деяких серверних застосувань (таких, як веб- або FTP- сервер) DoS-атаки можуть полягати в тому, щоб зайняти всі з'єднання, доступні для цих застосувань, і тримати їх в зайнятому стані, не допускаючи обслуговування звичайних користувачів. В ході DoS-атак можуть використовуватися звичайні Інтернет-протоколи, такі як TCP і ICMP (Internet Control Message Protocol).

DoS-атакам важко запобігти, оскільки для цього потрібна координація дій з провайдером. Якщо трафік, призначений для переповнення мережі, не зупинити у провайдера, то на вході в мережу це зробити вже не можливо, тому що вся смуга пропускання буде зайнята.

Якщо атака цього типу проводиться одночасно через безліч пристроїв, то говорять про розподілену атаку «відмова в обслуговуванні» (DDoS, Distributed DoS).

Простота реалізації DoS-атак і величезна шкода, заподіяна ними організаціям і користувачам, притягують до цих атак пильну увагу адміністраторів мережної безпеки.

Відмова в доступі до інформації. В результаті DoS-атаки, спрямованої проти інформації, остання стає непридатною для використання. Інформація знищується, спотворюється або переноситься в недоступне місце.

Відмова в доступі до застосувань. Інший тип DoS-атак спрямований на застосування, що обробляють або відображають інформацію, або на комп'ютерну систему, в якій ці застосування виконуються. У разі успіху подібної атаки рішення задач, які виконуються за допомогою такого застосування, стає неможливим.

Відмова в доступі до системи. Загальний тип DoS-атак ставить своєю метою виведення з ладу комп'ютерної системи, в результаті чого сама система, встановлені на ній застосування і вся збережена інформація стають недоступними.

Відмова в доступі до засобів зв'язку. Метою атаки є комунікаційне середовище. Цілісність комп'ютерної системи і інформації не порушується, однак відсутність засобів зв'язку позбавляє користувачів доступу до цих ресурсів.

Комбіновані атаки

Комбінована атака полягає в застосуванні зловмисником декількох взаємно пов'язаних дій для досягнення своєї мети.

Підміна довіреного суб'єкту. Більша частина мереж і операційних систем використовують IP-адресу комп'ютера для того, щоб визначати, чи той це адресат, який потрібен. У деяких випадках можливе некоректне присвоєння IP- адреси (підміна IP-адреси відправника іншою адресою) – такий спосіб атаки називають фальсифікацією адреси або IP-спуфінгом (IP-spoofing).

IP-спуфінг має місце, коли зловмисник, що знаходиться всередині корпоративної мережі або за її межами, видає себе за законного користувача. Зловмисник може скористатися його IP-адресою, що знаходиться в межах діапазону санкціонованих IP-адрес, або авторизованою зовнішньою адресою, якій дозволяється доступ до певних ресурсів мережі. Зловмисник може також використовувати спеціальні програми, які формують IP-пакети таким чином, щоб вони виглядали як вихідні з дозволених внутрішніх адрес корпоративної мережі.

Атаки IP-спуфінга часто є відправною точкою для інших атак. Класичним прикладом є атака типу «відмова в обслуговуванні» (DoS), яка починається з чужої адреси, що приховує справжню особу зловмисника. Зазвичай IP-спуфінг обмежується вставкою неправдивої інформації або шкідливих команд у звичайний потік даних, що передаються між клієнтським і серверним застосуваннями або по каналу зв'язку між одноранговими пристроями.

Загрозу спуфінга можна послабити (але не усунути) за допомогою наступних заходів: правильне налаштування управління доступом із зовнішньої мережі; припинення спроб спуфінга чужих мереж користувачами мережі.

Потрібно мати на увазі наступне: IP-спуфінг може бути здійснений за умови, що автентифікація користувачів проходить на базі IP-адрес, тому введення додаткових методів автентифікації користувачів (на основі одноразових паролів або інших методів криптографії) дозволяє запобігти атаки IP-спуфінга.

Посередництво. Атака типу «посередництво» передбачає активне підслуховування, перехоплення даних, які передаються, невидимим проміжним вузлом і управління ними. Коли комп'ютери взаємодіють на мережному рівні, вони не завжди можуть визначити, з ким саме вони обмінюються даними.

Посередництво в обміні незашифрованими ключами (атака Man-in-the- Middle – «людина-в-середині»). Для проведення атаки «людина-в-середині» зловмиснику потрібен доступ до пакетів, що передаються по мережі. Такий доступ до всіх пакетів, що передаються від провайдера ISP в будь-яку іншу мережу, може, наприклад, отримати співробітник цього провайдера. Для атак цього типу часто використовуються сніфери пакетів, транспортні протоколи та протоколи маршрутизації.

У більш загальному випадку атаки «людина-в-середині» проводяться з метою крадіжки інформації, перехоплення поточної сесії і отримання доступу до приватних мережних ресурсів, для аналізу трафіку і отримання інформації про мережі та її користувачів, для проведення атак типу DoS, спотворення переданих даних і введення несанкціонованої інформації в мережні сесії.

Ефективно боротися з атаками типу «людина-в-середині» можна тільки за допомогою криптографії. Для протидії атакам цього типу використовується інфраструктура відкритих ключів PKI (Public Key Infrastructure).

Атака експлоїта. Експлоїт (exploit – експлуатувати) – це комп'ютерна програма, фрагмент програмного коду або послідовність команд, що використовують вразливості в програмному забезпеченні та застосовуються для проведення атаки на комп'ютерну систему. Метою атаки може бути як захоплення контролю над системою, так і порушення її функціонування (DoS-атака).

Залежно від методу отримання доступу до вразливого програмного забезпечення, експлоїти поділяються на віддалені і локальні:

- віддалений експлоїт працює через мережу і використовує вразливість в захисті без якого-небудь попереднього доступу до вразливої системи;
- локальний експлоїт запускається безпосередньо у вразливій системі, вимагаючи попереднього доступу до неї. Зазвичай використовується для отримання зловмисником прав суперкористувача.

Атака експлоїта може бути спрямована на різні компоненти комп'ютерної системи – серверні застосування, клієнтські програми або модулі операційної системи.

Парольні атаки. Метою цих атак є заволодіння паролем і логіном законного користувача. Зловмисники можуть проводити парольні атаки, використовуючи такі методи, як:

- підміна IP-адреси (IP-спуфінг);
- підслуховування (сніфінг);
- простий перебір.

Вгадування ключа. Криптографічний ключ являє собою код або число, необхідне для розшифрування захищеної інформації. Хоча дізнатися ключ доступу важко і такі спроби вимагають великих витрат ресурсів, тим не менш, це можливо. Зокрема, для визначення значення ключа може бути використана спеціальна програма, яка реалізує метод повного перебору. Ключ, до якого отримує доступ атакуючий, називається скомпрометованим. Атакуючий використовує скомпрометований ключ для отримання доступу до захищених даними без відома відправника і одержувача. Ключ дає можливість розшифровувати і редагувати дані.

Атаки на рівні застосувань. Ці атаки можуть проводитися декількома способами. Найпоширеніший з них полягає у використанні відомих вразливостей серверного програмного забезпечення (FTP, HTTP, веб-сервера).

Головна проблема з атаками на рівні застосувань полягає в тому, що зловмисники часто користуються портами, яким дозволено прохід через мережні екрани.

Відомості про атаки на рівні застосувань широко публікуються, щоб дати можливість адміністраторам вирішити проблему за допомогою корекційних модулів (патчів). На жаль, багато зловмисників також мають доступ до цих відомостей, що дозволяє їм вчитися.

Неможливо повністю виключити атаки на рівні застосувань. Зловмисники постійно відкривають і публікують на своїх сайтах в мережі Інтернет нові вразливі місця прикладних програм.

Тут важливо здійснювати хороше системне адміністрування. Щоб зменшити вразливість від атак цього типу, можна зробити наступні заходи:

- аналізувати лог-файли операційних систем і мережні лог-файли за допомогою спеціальних аналітичних програм;
- відстежувати дані CERT про слабкі місця прикладних програм;
- користуватися самими свіжими версіями операційних систем і застосувань і останніми корекційними модулями (патчами);
- використовувати системи виявлення вторгнень IDS (Intrusion Detection Systems).

Аналіз мережного трафіку. Метою атак подібного типу є прослуховування каналів зв'язку і аналіз даних, які передаються, та службової інформації з метою вивчення топології мережі та архітектури побудови системи, отримання критичної інформації користувачів (наприклад, паролів користувачів або номерів кредитних карт, що передаються у відкритому вигляді). Атакам цього типу схильні такі протоколи, як FTP і Telnet, особливістю яких є те, що ім'я та пароль користувача передаються в рамках цих протоколів у відкритому вигляді.

Мережна розвідка.

Мережна розвідка – це збір інформації про мережу за допомогою загальнодоступних даних і застосувань. При підготовці атаки проти якої-небудь мережі зловмисник, як правило, намагається отримати про неї якомога більше інформації.

Мережна розвідка проводиться у формі запитів DNS, ICMP-тестування (Ping Sweep) і сканування портів. Запити DNS допомагають зрозуміти, хто володіє тим чи іншим доменом і які адреси цьому домену належать. ICMP-тестування адрес, розкритих за допомогою DNS, дозволяє побачити, які вузли реально працюють в цій мережі. Отримавши список вузлів, зловмисники використовують засоби сканування портів, щоб скласти повний список сервісів, які підтримуються цими вузлами. В результаті отримується інформація, яку можна використовувати для злому.

Зловживання довірою. Даний тип дій не є атакою в повному сенсі цього слова. Він являє собою зловмисне використання відносин довіри, що існують в мережі. Типовим прикладом такого зловживання є ситуація в периферійній частині корпоративної мережі. У цьому сегменті зазвичай розташовуються сервери DNS, SMTP і HTTP. Оскільки всі вони належать до одного і того ж сегменту, злом одного з них призводить до злому і всіх інших, так як ці сервери довіряють іншим системам своєї мережі.

Ризик зловживання довірою можна знизити за рахунок більш жорсткого контролю рівнів довіри в межах своєї мережі. Системи, розташовані з зовнішнього боку мережного екрану, ніколи не повинні користуватися абсолютною довірою з боку систем, захищених мережним екраном.

Відносини довіри повинні обмежуватися певними протоколами і по можливості автентифікуватися не тільки по IP-адресами, але і за іншими параметрами.

Соціальна інженерія

Соціальна інженерія – це мистецтво маніпулювання людьми через виконання дій, або розголошення конфіденційної інформації іншим способом, ніж як через засоби технічного руйнування баз даних.

Вказане явище є значно розвиненим як в Україні, так і в інший країнах. Я переконаний, що кожному із нас хоча б одного разу приходив «лист щастя», в якому повідомлялося, що саме ти став щасливчиком та виграв автомобіль. Саме за допомогою таких простих дій, які впливають на психологічні характеристики людської особистості шахраї намагаються заволодіти нашими персональними даними (іншою конфіденційною інформацію) із явно більш негативною метою, ніж заповнити анкету для отримання бонусної карти в популярному магазині.

Соціальна інженерія базується на досить простих психологічних особливостях людини, таки як: принцип зворотності («ти мені – я тобі»), принцип соціальної перевірки (ви оцінюєте свою поведінку в контексті поведінки більшості), повага до авторитетів (ви будете більше довіряти лікарю та поліцейському, аніж пересічній людині). Всі ці принципи застосовуються і при здійсненні «офлайнового» шахрайства, однак мають свою специфіку під час вчинення у мережі Інтернет.

Найбільш популярною схемою впливу на особу, яка використовується в соціальній інженерії є схема Шейнова, яка полягає у таких кроках: формування цілі впливу на об'єкт (1), пошук інформації про об'єкт (2), виявлення найбільш зручних цілей впливу (3), створення найбільш сприятливих умов для впливу на об'єкт (4), примус до потрібної дії (5), результат (6).

Найбільш поширеними типами атак соціальної інженерії є фішінг і фармінг.

Фішинг (Phishing). Фішинг є відносно новим видом Інтернет-шахрайства, мета якого – отримати ідентифікаційні дані користувачів. Сюди відносяться крадіжки паролів, номерів кредитних карт, банківських рахунків, PIN-кодів та іншої конфіденційної інформації, що дає доступ до грошей користувача. Фішинг не використовує технічні недоліки програмного забезпечення, а легковірність користувачів мережі Інтернет. Сам термін phishing, співзвучний з fishing (риболовля), розшифровується як password harvesting fishing – виуджування пароля. Дійсно, фішинг дуже схожий на рибну ловлю. Зловмисник закидає в Інтернет приманку і «виловлює» всіх «рибок» – користувачів мережі Інтернет, які клюнуть на цю приманку.

Зловмисник створює практично точну копію сайту обраного банку (електронної платіжної системи, аукціону тощо). Потім за допомогою спам-технології по електронній пошті розсилається лист, складений таким чином, щоб бути максимально схожим на даний лист від обраного банку. При складанні листа використовуються логотипи банку, імена і прізвища реальних керівників банку. В такому листі, як правило, повідомляється про те, що із-за зміни програмного забезпечення в системі інтернет-банкінгу користувачеві необхідно підтвердити або змінити свої облікові дані. В якості причини для зміни даних можуть бути названі вихід з ладу ПЗ банку або ж напад зловмисників. Наявність правдоподібної легенди, що спонукає користувача до необхідних дій – неодмінна складова успіху шахраїв-фішерів. У всіх випадках мета таких листів одна – змусити користувача клацнути по наведеним посиланням, а потім ввести свої конфіденційні дані (пароль, номер рахунку, PIN-код) на фальшивому сайті банку (електронної платіжної системи, аукціону). Зайшовши на фальшивий сайт, користувач вводить у відповідні рядки свої конфіденційні дані, а далі аферисти отримують доступ в кращому випадку до його поштової скриньки, а в гіршому – до електронного рахунку.

Успіху фішинг-афер сприяє низький рівень обізнаності користувачів про правила роботи компаній, від імені яких діють злочинці. Зокрема, близько 5% користувачів не знають простого факту: банки не розсилають листів з проханням підтвердити в онлайн номер своєї кредитної картки, її PIN-код. Основним захистом від фішингу поки залишаються спам-фільтри. На жаль, програмний інструментарій для захисту від фішингу володіє обмеженою ефективністю, оскільки зловмисники експлуатують в першу чергу не вразливості в ПЗ, а людську психологію.

З'явилося поєднане з фішингом поняття – фармінг.

Фармінг (Pharming). Це ще один вид шахрайства, що ставить за мету отримати персональні дані користувачів, але не через пошту, а прямо через офіційні веб-сайти. Фармери замінюють на серверах DNS цифрові адреси легітимних веб-сайтів на підроблені, в результаті чого користувачі перенаправляються на сайти шахраїв. Цей вид шахрайства ще небезпечніше, оскільки помітити підробку практично неможливо.

Для захисту від фішингу та фармінгу розробляються технічні засоби безпеки, насамперед плагіни для популярних браузерів. Суть захисту полягає в блокуванні сайтів, що потрапили в чорні списки шахрайських ресурсів. Наступним кроком можуть стати системи генерації одноразових паролів для інтернет-доступу до банківських рахунків та записів в платіжних системах, повсюдне поширення додаткових рівнів захисту за рахунок комбінації введення пароля з використанням апаратного USB-ключа.

Застосування ботнетів. Ботнет (зомбі-мережа) – це мережа комп'ютерів, заражених шкідливою програмою, яка дозволяє кіберзлочинцям віддалено керувати зараженими машинами (кожною окремо, частиною комп'ютерів, що входять в мережу, або всією мережею цілком) без відома користувача. Такі програми називаються ботами.

Ботнети володіють потужними обчислювальними ресурсами, є загрозливою кіберзброєю і хорошим способом заробляння грошей для зловмисників. При цьому зараженими машинами, що входять в мережу, господар ботнету може керувати звідки завгодно: з іншого міста, країни чи навіть з іншого континенту, а організація мережі Інтернет дозволяє робити це анонімно.

Управління комп'ютером, який заражений ботом, може бути прямим і опосередкованим.

У разі прямого управління зловмисник може встановити зв'язок з інфікованим комп'ютером і керувати ним, використовуючи вбудовані в тіло програми-бота команди.

У випадку опосередкованого управління бот сам з'єднується з центром управління або іншими машинами в мережі, посилає запит і виконує отриману команду.

У будь-якому випадку господар зараженої машини, як правило, навіть не підозрює про те, що вона використовується зловмисниками. Саме тому заражені шкідливою програмою-ботом комп'ютери, що знаходяться під таємним наглядом кіберзлочинців, називають ще зомбі-комп'ютерами, а мережа, до якої вони входять – зомбі-мережею. Найчастіше зомбі-машинами стають персональні комп'ютери домашніх користувачів.

Ботнети можуть використовуватися зловмисниками для вирішення кримінальних завдань різного масштабу: від розсилки спаму до атак на державні мережі.

Анонімний доступ в мережу. Зловмисники можуть звертатися до серверів в мережі Інтернет, використовуючи зомбі-машини, і від імені заражених машин здійснювати кіберзлочини, наприклад зламувати веб-сайти або переводити вкрадені грошові кошти.

Продаж і оренда ботнетів. Один з варіантів незаконного заробітку за допомогою ботнетів ґрунтується на здачі ботнету в оренду або продаж готової мережі. Створення ботнетів для продажу є окремим напрямком кіберзлочинного бізнесу.

Крадіжка конфіденційних даних. Цей вид кримінальної діяльності постійно приваблює кіберзлочинців, а з допомогою ботнетів «улов» у вигляді різних паролів для доступу до електронної пошти, FTP-ресурсів, веб-сервісів) та інших конфіденційних даних користувачів збільшується в тисячі разів! Бот, яким заражені комп'ютери в зомбі-мережі, може завантажити іншу шкідливу програму, наприклад троянця, що краде паролі. У такому разі інфікованими троянською програмою виявляться всі комп'ютери, що входять в цю зомбі-мережу, і зловмисники зможуть отримати паролі зі всіх заражених машин. Вкрадені паролі перепродаються або використовуються, зокрема, для масового зараження веб-сторінок (наприклад, паролі для всіх знайдених FTP-акаунтів) з метою подальшого поширення шкідливої програми-бота і розширення зомбі- мережі.

Перераховані атаки на IP-мережі можливі в силу ряду причин:

- використання загальнодоступних каналів передачі даних. Найважливіші дані передаються по мережі у незашифрованому вигляді;
- вразливості в процедурах ідентифікації, реалізованих в стеку TCP/IP. Ідентифікуюча інформація на рівні IP передається у відкритому вигляді;
- відсутність в базовій версії стека протоколів TCP/IP механізмів, що забезпечують конфіденційність і цілісність переданих повідомлень;
- автентифікація відправника здійснюється за його IP-адресою. Процедура автентифікації виконується тільки на стадії встановлення з'єднання, а в подальшому достовірність прийнятих пакетів не перевіряється;
- відсутність можливості контролю за маршрутом проходження повідомлень у мережі Інтернет, що робить віддалені мережні атаки практично безкарними.

ЛЕКЦІЯ 3.
КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ.

3.1 Криптографія і її основні поняття

В перекладі з грецької мови слово криптографія означає тайнопис. Основне призначення криптографії – утаємничити необхідну інформацію.

Криптографія надає засоби для захисту інформації і тому є складовою діяльності з забезпечення безпеки інформації.

Існують різні засоби втаємничення інформації:

• Приховування каналу передачі повідомлення.

• Маскування змісту повідомлення з використанням стеганографічних методів.

• Ускладнення можливості перехоплення самого повідомлення противником.

• Інші.

На відміну від перерахованих методів криптографія не «приховує» повідомлення, а перетворює їх у форму, недоступну для розуміння противником. Таке перетворення забезпечується використанням криптографічних систем.

Криптографічна система – це набір апаратних і програмних засобів, інструкцій і правил, за допомогою яких, використовуючи криптографічні перетворення, можна зашифрувати повідомлення і розшифрувати криптограми різними способами, один з яких вибирається за допомогою секретного ключа.

Шифрування– процес перетворення вихідного тексту (P) в зашифрований текст (C) за допомогою шифруючої функції (E) з секретним ключем шифрування (Ke) у відповідності з обраним алгоритмом шифрування: C=EKe(P).

Розшифрування – обернений шифруванню процес перетворення зашифрованого тексту (C) в вихідний текст (P) за допомогою функції розшифрування (D) з секретним ключем розшифрування (Kd) у відповідності з обраним алгоритмом шифрування: P=DKd(C).

Криптографічний ключ – це параметр, використовуваний в криптографічному алгоритмі для вибору конкретного криптографічного перетворення.

Криптографічна стійкість – в широкому сенсі: здатність криптосистеми або криптоалгоритму протистояти атакам з використанням методів криптоаналізу; у вузькому сенсі: чисельна характеристика складності взлому криптографічного алгоритму з врахуванням тих науково-технічних способів і засобів, які може використовувати криптоаналітик.

Сімейство обернених перетворень защифрування і розшифрування називають шифром.

Алгоритми шифрування і розшифрування можуть відрізнятись, відповідно можуть розрізнятись і ключі шифрування і розшифрування.

Приклади алгоритмів шифрування:

Підстановочний шифр він же моноалфавітний шифр (греч. μονος — один) — алгоритм шифрування, який полягає у заміні знаків відкритого тексту іншими знаками, які є ключем.

Наприклад, зашифруємо ключем «а-x, б-y, в-z, г-n … і т. д.» слово «гав», отримаємо шифртекст «nxz».

г -> n

а -> x

в -> z

Шифр підстановки з ключем 3 використовував ще Юлій Цезар; тому його також називають шифром Цезаря. У 1 в. н.е. Юлій Цезар під час війни з

галлами, листуючись зі своїми друзями в Римі, заміняв у повідомленні першу літеру латинського алфавіту (A) на четверту (D), другу (B) - на п'яту (E), нарешті, останню - на третю

Підстановочний шифр відноситься до класу моноалфавітних шифрів, в яких кожній букві кодованого тексту ставиться у відповідність однозначно якась шифрована буква

Перестановочний шифр — алгоритм шифрування, який полягає у перестановці знаків відкритого тексту згідно з певним правилом, яке є ключем.

Наприклад, текст «знак», зашифрований ключем «3421», буде виглядати так: «казн».

з н а к
3 4 2 1
\ \ / /
/ / \ \
1 2 3 4
к а з н

Суть поліалфавітного шифру полягає в циклічному застосуванні декількох моноалфавітних шифрів до певного числа букв шифруємого тексту. Наприклад, нехай у нас є деяке повідомлення x 1, x 2, x 3,... .. x n,... ... x 2n,... .., яке треба зашифрувати. При використанні поліалфавітного шифру є кілька моноалфавітних шифрів (наприклад, n штук). І в нашому випадку до першої букви застосовується перший моноалфавітний шифр, до другої букві - другий, до третьої - третій ... .. до n-ої букві - n-й, а до n +1 знову перший, ну і так далі. Таким чином, виходить досить-таки складна послідовність, яку вже не так просто розкрити, як один моноалфавітний шифр. Найважливішим ефектом, що досягається при використанні поліалфавітного шифру, є маскування частот появи тих чи інших літер у тексті, на підставі якої зазвичай дуже легко розкриваються моноалфавитні шифри.

Одним із поліалфавітних шифрів є шифр Віженера.

Шифр Віженера (фр. Chiffre de Vigenère) - метод поліалфавітного шифрування буквеного тексту з використанням ключового слова.

Цей метод є простою формою поліалфавітної заміни. Шифр Віженер винаходився багаторазово. Вперше цей метод описав Джован Баттіста Беллазо (італ. Giovan Battista Bellaso) у книзі La cifra del. Sig. Giovan Battista Bellaso в 1553 році, проте в XIX столітті отримав ім'я Блеза Віженера, французького дипломата. Метод простий для розуміння і реалізації, він є недоступним для простих методів криптоаналізу.

Для зашифровування може використовуватися таблиця алфавітів, звана tabula recta або квадрат (таблиця) Віженера. Якщо за основу взяти латинськой алфавіт, то таблиця Віженер складатиметься з рядків по 26 символів, причому кожна наступний рядок зсувається на 1 позицію. Таким чином, в таблицю виходить 26 різних шифрів Цезаря. На різних етапах кодування шифр Віженера використовує різні алфавіти з цієї таблиці. На кожному етапі шифрування використовуються різні алфавіти, обрані в залежності від символу ключового слова.

3.2 Симетричні криптосистеми

Симетричні криптосистеми – спосіб шифрування, в якому для шифрування і дешифрування застосовується один і той же криптографічний ключ. Ключ алгоритму повинен зберігатися в секреті обома сторонами. До винаходу схеми асиметричного шифрування єдиним існуючим способом було симетричне шифрування.

Алгоритми шифрування і дешифрування даних широко застосовуються в комп'ютерній техніці в системах приховування конфіденційної і комерційної інформації від не коректного використання сторонніми особами. Головним принципом у них є умова, що особа яка приймає повідомлення, заздалегідь знає алгоритм шифрування, а також ключ до повідомлення, без якого інформація є всього лише набір символів, що не мають сенсу.

Симетричні криптоалгоритми виконують перетворення невеликого (1 біт або 32-128 біт) блоку даних в залежності від ключа таким чином, що прочитати оригінал повідомлення можна тільки знаючи цей секретний ключ.

3.3 Класифікація симетричних криптоалгоритмів

Криптографічних алгоритмів існує безліч. В загальному вони призначені для захисту інформації. Симетричні криптоалгоритми відносяться до криптоалгоритмів з ключем.

Вони поділяються на:

Потокові шифри – побітна обробка інформації. Шифрування і дешифрування в таких схемах може обриватися в довільний момент часу, як тільки з'ясовується, що потік що передається перервався, і також відновлюється при виявленні факту продовження передачі.

Скремблер – це набір біт, які міняються на кожному кроці по визначеному алгоритму. Після виконання кожного наступного кроку на його виході появляється шифруючий біт (0 або 1), який накладається на поточний біт інформаційного потоку операцією XOR.

Блочні шифри – перетворення блоку вхідної інформації фіксованої довжини. і отримують результуючий блок того ж обсягу. Схема застосовується при пакетній передачі інформації та кодування файлів.

Шифр TEA - один із самих простих в реалізації, але стійких криптоалгоритмів;

Мережа Фейштеля – метод оборотних перетворень тексту, при якому значення, обчислені від однієї з частин тексту, накладається на інші частини. Часто структура мережі виконується таким чином, що для шифрування і дешифрування використовується один і той же алгоритм - різниця полягає лише в порядку використання матеріалу ключа.

Стандарт AES – стандарт блочних шифрів США з 2000 року.

3.4 Блокові алгоритми і режими шифрування

Для побудови стійкого шифру, зручного для практичного використання, можна запропонувати такі підходи:

1. Блоковість. Вибираємо довжину ключа меншою за довжину повідомлення, розбиваємо повідомлення на окремі блоки і шифруємо кожний з них (крім, можливо, останнього) шляхом сумування з ключем по модулю два.

2. Режими шифрування. Для збільшення стійкості блокового шифрування можна забезпечити використання при шифруванні кожного наступного блоку результатів шифрування попереднього блоку (наприклад, в якості нового ключа шифрування для блоку). Тоді зловмисник не зможе розшифрувати блок криптотексту, доки не розшифрує всі попередні блоки.

3. Багатораундовість. Додатково збільшити стійкість блокового шифрування можна з рахунок багаторазового виконання шифрування кожного блоку за умови, що функція шифрування є нелінійним перетворенням.

В блокових алгоритмах вхідна послідовність розбивається на блоки – ділянки певної довжини (найчастіше, по 64 біти). Якщо довжина відкритого тексту виявляється некратною довжині блоку, застосовується операція доповнення (padding) останнього блоку до необхідної довжини, яка полягає у дописуванні необхідної кількості нулів або випадкового набору символів (Рис.3.1).

Рис.3.1. Представлення даних в блоковому алгоритмі

Криптографічне перетворення в блокових алгоритмах шифрування здійснюється над кожним блоком окремо (Рис.3.2). Його сутність полягає у застосуванні до блока багаторазово математичного перетворення. Внаслідок цього результуюче перетворення виявляється криптографічно більш сильним, ніж перетворення над окремо взятим блоком. Метою таких перетворень є створення залежності кожного біту блоку шифротексту від кожного біту ключа і кожного біту відкритого тексту:

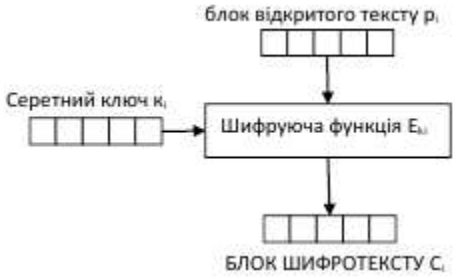


Рисунок 3.2. Схема шифрування блоку даних в блоковому алгоритмі

Зашифрований блок може використовуватися для шифрування наступного, в результаті чого кожний блок отримає контекст, що властивий всьому повідомленню (Рис.3.3). Такі механізми шифрування використовуються для уникнення від деяких атак, заснованих на стиранні або вставки блоків, і визначаються відповідним режимом шифрування.

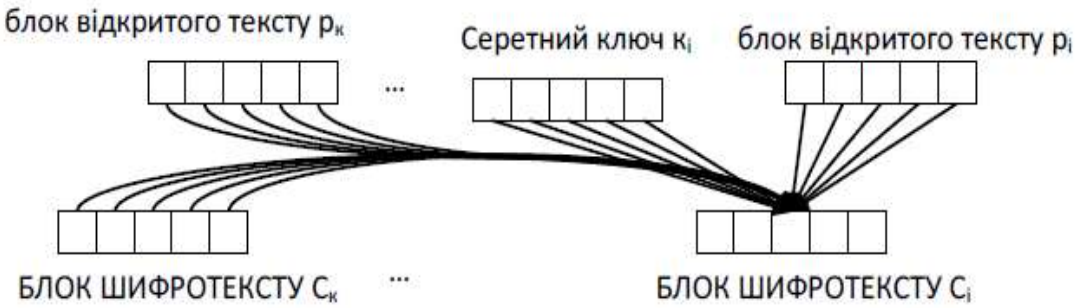


Рисунок4.3. Механізм режимів шифрування

Режим шифрування – метод застосування блокового шифру, в якому для забезпечення вищого рівня криптостійкісті шифрування блоків вхідного повідомлення здійснюється з використання блоків криптотексту.

Розрізняють п’ять основних режимів шифрування:

1. ECB (Electronic Codebook Mode) – режим електронної кодової книги.
2. CBC (Cipher Block Chaining Mode) – режим зціплення блоків по криптотексу.
3. CFB (Cipher Feedback Mode) – режим з оберненим зв’язком по криптотексу.
4. OFB (Output-Feedback Mode) – режим з оберненим зв’язком по виходу.
5. CTR (Coutner) – режим з лічильником.

Блокові алгоритми шифрування сьогодні є основним засобом криптографічного захисту інформації. Основні переваги блокових алгоритмів шифрування:

- Висока швидкість шифрування/розшифрування.
- Висока гарантована стійкість, яка до того ж може бути доведена математично.
- Можливість ефективної програмної реалізації.

Розглянемо деякі з блокових режимів шифрування.

3.2.1 Режим електронної кодової книги (ECB)

В цьому режимі блоки відкритого тексту шифрують ся незалежно від інших за допомогою одного й того ж ключа.

Шифрування описується рівнянням: $C_i=E_{ki}(p_i)$ для $i=1\div N$, де C_i та p_i – блоки відповідно зашифрованого і відкритого тексту, E_{ki} – функція шифрування.

Рисунок 3.3. Схема шифрування в режимі ECB

Розшифрування здійснюється за допомогою функції розшифрування $p_i=D_{ki}(C_i)$:

Рисунок 3.4. Схема розшифрування в режимі ECB

Такий режим є криптографічно слабким. Основні недоліки:

Режим не є критичним по відношенню до вставки і втрати блоків в процесі передачі.

- Однакові блоки будуть перетворюватись в такі ж самі, що може дати ключ для аналізу вмісту повідомлення.
- Перевагою режиму є те, що шифрування (розшифрування) блоків може виконуватись паралельно.

3.2.2 Режим зціплення блоків по криптотексу (CBC)

В цьому режимі шифрування кожний блок відкритого тексту, крім першого, складається по модулю 2 (операція XOR) з попереднім зашифрованим блоком. Шифрування першого блоку здійснюється за допомогою початкового вектора ініціалізації (синхропосилки), яка передається по відкритому каналу передачі даних.

Шифрування описується рівнянням: $C_i= E_{ki}(p_i \text{ XOR } C_{i-1})$ для $i=2\div N$, C_0 – синхропосилка (Рис.3.5).

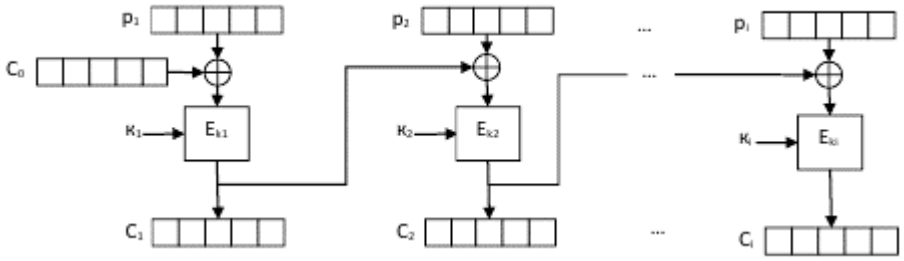


Рисунок 3.5. Схема шифрування в режимі CBC

Розшифрування описується рівнянням: $p_i = C_{i-1} \text{XOR } D_{ki}(C_i)$ для $i=2 \div N$, C_0 – синхропосилка (Рис.3.6).

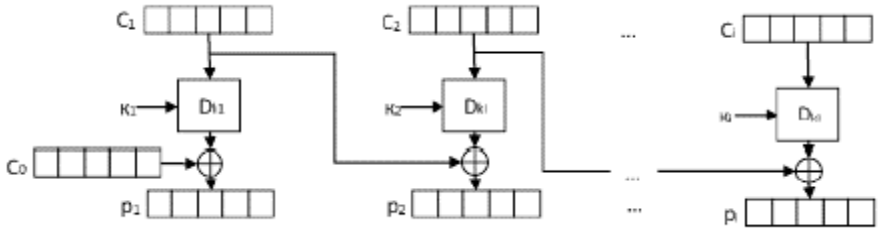


Рисунок 3.6. Схема розшифрування в режимі CBC

Важливо відмітити, що останній блок шифротексту залежить від ключів, синхропосилки і всіх бітів відкритого тексту. Тому його можна розглядати в якості ідентифікатора повідомлення. Цей ідентифікатор широко використовується для автентифікації повідомлення та відправника і називається кодом автентифікації повідомлення або MAC (Message Authentication Code).

Коди автентифікації повідомлень не забезпечують секретність, але гарантують автентифікацію і цілісність. Вони дають впевненість, що повідомлення прийшло саме від тієї людини, який позначений як автор, і що повідомлення по дорозі не змінилося. Хто завгодно може прочитати повідомлення. Але той, хто знає ключ MAC, може впевнитися, що воно не було змінено.

Для використання MAC Аліса спочатку домовляється з Бобом про ключ. Потім, коли вона хоче послати Бобу повідомлення, вона обчислює MAC повідомлення і додає його до повідомлення. Коли Боб отримує повідомлення,він обчислює його MAC і порівнює його з тим значенням MAC, яке прислала Аліса. Якщо вони збігаються, то він може бути впевнений у двох речах: повідомлення дійсно прийшло від Аліси і це повідомлення незмінене. Банки використовують таку просту систему автентифікації вже кілька десятиліть.

MAC постійно використовуються в Інтернет, наприклад, у протоколі IPsec, щоб гарантувати, що IP-пакети не були змінені в проміжку між відправленням і прибуттям на місце призначення. Їх використовують у всіх

можливих протоколах міжбанківських переказів для встановлення автентичності повідомлень.

Переваги режиму CBC:

- Режим CBC є критичним по відношенню до вставки і втрати блоків в процесі передачі.
- Забезпечується автентифікація повідомлення та відправника на основі MAC.

Недоліком режиму є те, що шифрування (розшифрування) не піддається розпаралеленню.

3.5 Мережі Фейстеля

Мережею Фейстеля називається метод оборотних перетворень тексту, при якому значення, обчислене від однієї з частин тексту, накладається на інші частини.

Часто структура мережі виконується таким чином, що для шифрування і розшифрування використовується один і той самий алгоритм - відмінність полягає тільки в порядку використання матеріалу ключа.

В схемі Фейстеля кожний блок розбивається на ліву (l0) і праву (r0) частини, над якими здійснюються S раундів шифрування. Після завершення S раундів шифрування ліва (Ls) і права (Rs) частини міняються місцями:

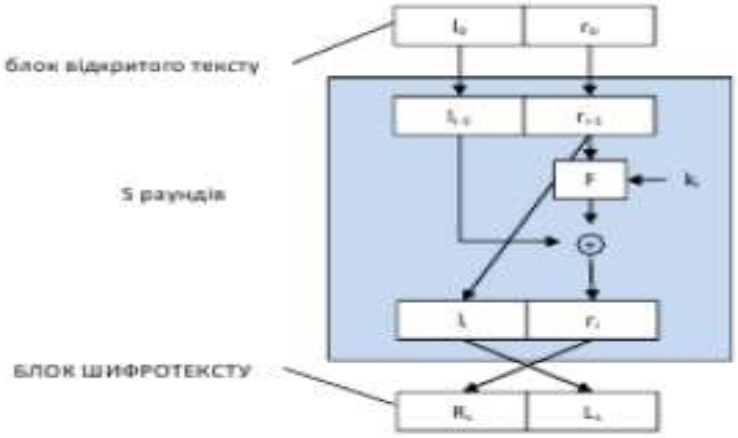


Рисунок 3.7 Схема мережі Фейстеля

Кожний раунд шифрування здійснюється за правилом:

$$l_i = r_i\text{-}1,\ r_i = l_{i-1} + F(k_i, r_{i-1}).$$

Процес розшифрування шифру Фейстеля принципово не відрізняється від процесу шифрування. Застосовується той самий алгоритм, але на вхід подається шифрований текст, а підключі використовуються в зворотній послідовності: для першого раунду береться підключ S—го раунду

шифрування, для другого – (S-1) -ий, і так далі до тих пір, поки не буде введений ключ для останнього раунду. Ця властивість даної схеми шифрування вилась дуже зручною, тому що для розшифрування не потрібно вводити інший алгоритм, відмінний від алгоритму шифрування.

Мережа Фейстеля надійно зарекомендувала себе як крипостійка схема проведення криптоперетворень, і її можна знайти практично в будь-якому сучасному блоковому шифрі.

Цікава особливість шифру Фейстеля полягає в тому, що функція раунду є оберненою незалежно від властивості функції F.

Для створення криптостійкого шрифту залишилося визначити:

- Спосіб генерування підключів ki.
- Кількість раундів S.
- Визначити функцію F.

Відповіді на ці питання були дані в ході роботи над шифром DES.

3.6 Криптосистема DES

3.6.1 Загальна характеристика

Алгоритм DES (Data Encryption Standard) був розроблений у 1977 році і рекомендований Національним бюро стандартів США в якості основного засобу криптографічного захисту інформації як в державних, так і в комерційних структурах. Він став першим доступним всім бажаючим офіційним алгоритмом і першим світовим стандартом, що проіснував більше 20 років. Тому його слід відмітити як найважливішу віху на шляху криптографії від чисто військового використання до широкомасштабного застосування.

DES – алгоритм блокового шифрування з довжиною блоку 64 біти і симетричним ключем довжиною 56 біт. На практиці ключ має довжину 64 біти,з яких кожний восьмий використовується для контролю парності байту.

Головні риси шифру DES визначаються тим, що він ґрунтується на схемі Фейстеля з такими параметрами:

довжина блоку – 64 біти,
кількість раундів – 16,
розмір ключа – 56 бітів,
розмір кожного з підключів k_1, k_2, …, k_{16} – 48 бітів.

3.6.2 Алгоритм шифрування

Структура алгоритму DES показана на рис.3.8.

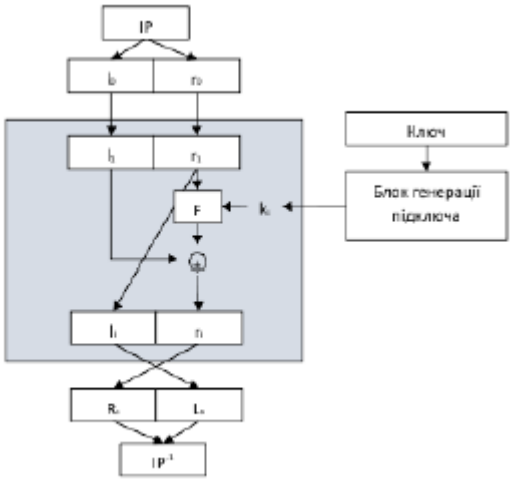


Рисунок 3.8. Структура алгоритму DES

Алгоритм DES описується за допомогою трьох етапів:

1. До вхідного блоку довжиною 64 біти застосовується фіксована початкова перестановка IP, яка описується виразом $(l_0,r_0) \leftarrow$ IP (Вхідний блок).

Тут l_0 та r_0 називаються лівою і правою половинами блоку, кожна з яких має довжину 32 біти.

Перестановка IP застосовується для того, щоб здійснити початкове розсіювання статистичної структури повідомлення. Вона є фіксованою і відкритою (Рис.3.9).

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	36	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Рисунок 3.9 Матриця початкової перестановки IP

2. Виконуються 16 раундів з таких операцій:

- Права половина блоку перетворюється функцією F з використанням поточної ключової послідовності довжиною 48 біт, яка знімається з виходу блоку вироблення ключової послідовності.
- Результат перетворення правої половини складається по модулю 2 з лівою частиною, а сума записується у вихідний регістр, при цьому вихідна права половина за допомогою операції зсуву записується на місце вихідної лівої половини.

Їх можна описати рівняннями:

$$l_i = r_i\,,\ r_i = l_i\ F(r_{i-1},k_i)\ ,$$

де k_i – ключ раунду, який складається з 48-бітового підрядка 56-бітного вихідного ключа, F – функція шифрування, яка представляє собою перестановочний шифр. Ці операції перестановки забезпечують значний рівень «дифузії повідомлення».

3. До результату 16-го раунду (L16, R16) застосовується завершуюча перестановка, яка є оберненою до початкової перестановки(Рис.3.10)

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

Рисунок 3.10. Матриця завершуючої перестановки IP

3.6.3 Структура функції F

Структура функції F зображена на рис.3.11.

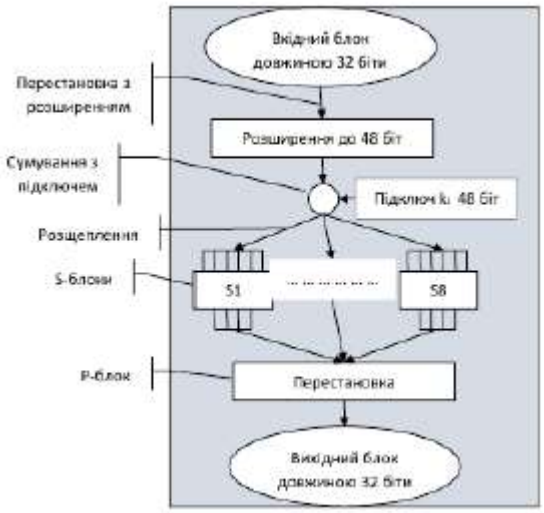


Рисунок 3.11 Структура функції F

В кожному раунді перетворення F складається з п’яти кроків:

1. Перестановка з розширенням. Права половина з 32 бітів розширюється до 48 бітів і перемішується. Ця операція передбачає дописування у вихідну послідовність окремих бітів у відповідності з підстановкою розширення (рис.3.12).

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Рисунок 3.12 Матриця підстановки розширення

Підстановка розширення забезпечує, що один вхідний біт впливає на дві заміни через S-блоки, що створює «лавиноподібний» ефект – мала відмінність між двома наборами вхідних даних перетворюється у велику на виході.

2. Сумування з підключем. До отриманого після перестановки з розширенням рядка з 48 бітів і підключа довжиною також 48 бітів застосовується операція виключаю чого АБО, тобто кожна пара відповідних бітів складається по модулю 2.

48-бітний підключ отримується з 56-бітного ключа у такий спосіб. Біти ключа записуються у два 28-бітні циклічних регістрів зсуву, які переміщують вміст в кожному такті на кількість бітів, що залежить від номера раунду (рис.3.13).

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Рисунок 3.13 Значення циклічного зсуву в 16-ти раундах шифрування.

Результуюча послідовність отримується шляхом вибірки 48 бітів з вмісту регістрів (рис.3.14).

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Рисунок 3.14 Матриця вибірки з вмісту регістрів

3. Розщеплення. Результат сумування з підключем розщеплюється на 6 частин по 8 бітів в кожному, кожна з яких передається в один з восьми S-блоків. 4) S-блок . Перетворює набір з 6 бітів в набір з 4 бітів.

S-блоки є нелінійними компонентами алгоритму DES, які і забезпечують криптостійкість шрифту. Кожний S-блок представляє собою пошукову таблицю з чотирьох рядків і шістнадцяти стовпців (Таблиця 5.1). Шість бітів, що входять до блоку, визначають який рядок і стовпець необхідно використовувати для заміни. Перший і шостий біт

задають номер рядка, а інші – номер стовпця. Вихід S-блоку – бітове представлення числа відповідної комірки таблиці.

Таблиця 5.1. Підстановки в S-блоках

S1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S4															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S5															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	6	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S7															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	12
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

4) P-блок. Вихід S-блоків з восьми 4-бітових елементів надходить до P-блоку, в якому відбувається перестановка (рис.3.15).

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	16
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Рисунок 3.15 Матриця Р-перестановки

Розшифровування в алгоритмі DES відбувається аналогічно шифруванню з тією різницею, що вибірка ключової послідовності в раундах розшифровування буде оберненою, тобто k_{16}, k_{15} … k_1.

3.7 Асиметричні криптосистеми

3.7.1 Концепція криптосистем з відкритим ключем.

Ефективними системами криптографічного захисту даних є асиметричні криптосистеми, які також називають криптосистемами з відкритим ключем. В таких системах для зашифровування даних використовується один ключ, а для розшифровування – інший ключ (звідси і назва – асиметричні). Перший ключ є відкритим і може бути опублікованим для використання усіма користувачами системи, які шифрують дані. Розшифровування даних за допомогою відкритого ключа неможливе. Для розшифровування даних отримувач зашифрованої інформації використовує другий ключ, який є секретним. Зрозуміло, що ключ розшифровування не може бути визначеним з ключа зашифровування.

Узагальнена схема асиметричної криптосистеми з відкритим ключем наведена на рис. 3.15. В цій криптосистемі застосовують два різних ключі: K_B – відкритий ключ відправника A; k_B – секретний ключ отримувача B. Генератор ключів доцільно розміщувати на стороні отримувача B (щоб не пересилати секретний ключ k_B по незахищеному каналу). Значення ключів K_B та k_B залежать від початкового стану генератора ключів. Розкриття секретного ключа k_B за відомим відкритим ключем K_B повинно бути задачею, яку неможливо розв’язати розрахунковими методами.

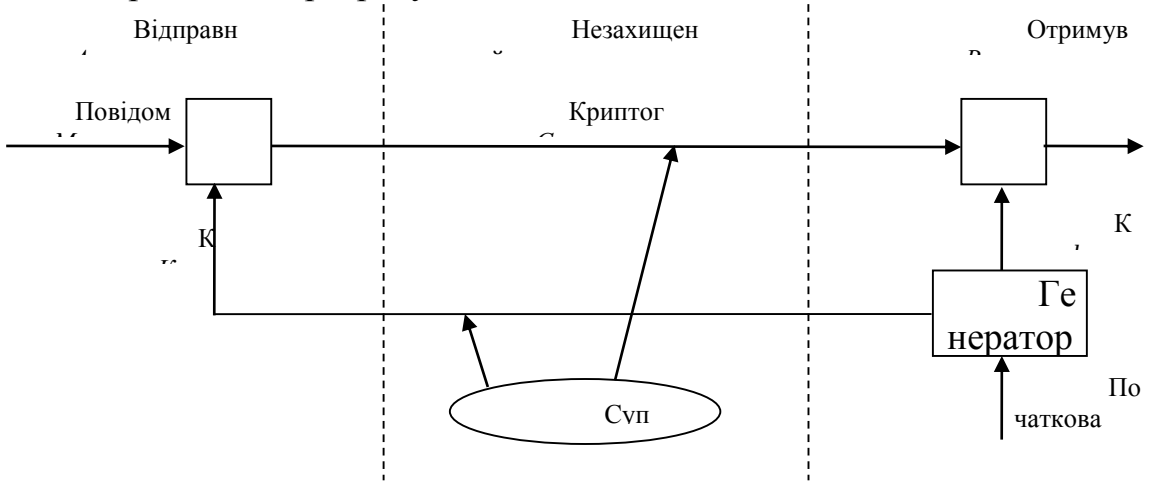


Рис. 3.15. Узагальнена схема асиметричної криптосистеми з відкритим ключем

Наведемо характерні особливості асиметричних криптосистем:

1. Відкритий ключ K_B та криптограма C можуть бути відправлені по незахищеним каналам (супротивнику відомі K_B та C).
2. Алгоритми шифрування та розшифровування
$$E_B: M \to C,$$
$$D_B: C \to M$$
є відкритими.

Захист інформації в асиметричній криптосистемі базується на секретності ключа k_B. У. Діффі та М. Хелман сформулювали вимоги, виконання яких забезпечує безпеку асиметричної криптосистеми:

1. Генерація пари ключів (K_B, k_B) отримувачем B на основі початкової умови повинна бути простою.
2. Відправник A, знаючи відкритий ключ K_B та повідомлення M, може легко генерувати криптограму
$$C = E_{K_B}(M) = E_B(M).$$
3. Отримувач B, використовуючи секретний ключ k_B та криптограму C, може легко відновити вихідне повідомлення
$$M = D_{K_B}(C) = D_B(C) = D_B[E_B(M)].$$
4. Супротивник, знаючи відкртий ключ K_B, при спробі вирахувати секретний ключ k_B наштовхується на нездоланну обчислювальну проблему.
5. Супротивник, знаючи пару (K_B, C), при спробі розшифрувати вихідне повідомлення M наштовхується на незоланну обчислювальну проблему.

3.7.2 Однонаправлені функції.

Концепція асиметричних криптографічних систем з відкритим ключем базується на застосуванні однонаправлених функцій. Неформально однонаправлену функцію можна визначити наступним чином. Нехай X та Y – довільні множини. Функція
$$f: X \to Y$$
є однонаправленою, якщо для всіх $x \in X$ можна легко обчислити функцію
$$y = f(x), \text{ де } y \in Y.$$
І в той же час для більшості $y \in Y$ досить складно отримати значення $x \in X$, таке, що $f(x)=y$ (при цьому вважають, що існує по крайній мірі одне таке значення x). Основним критерієм віднесення функції f до класу однонаправлених функцій є відсутність ефективних алгоритмів оберенного перетворення $Y \to X$.

В якості першого прикладу однонаправленої функції розглянемо цілочисельне множення. Пряма задача – розрахунок добутку двох дуже великих чисел P та Q
$$N = P*Q,$$
є відносно нескладною задачею для ЕОМ.

Обернена задача – факторизація великого цілого числа (знаходження дільників P та Q великого цілого числа $N=P*Q$), є задачею, яку практично

неможливо розв'язати засобами сучасних ЕОМ при достатньо великих значеннях N. За сучасними оцінками теорії чисел при цілому $N \approx 2^{664}$ та $P \approx Q$ для факторизації числа N знадобиться біля 10^{23} операцій.

Іншим характерним прикладом однонаправленої функції є модульна експонента з фіксованими основою та модулем. Нехай A та N – цілі числа, такі, що $1 \le A \le N$. Визначимо множину Z_N:

$$Z_N = \{0,1,2,...,N-1\}.$$

Тоді модульна експонента з основою A по модулю N являє собою функцію

$$f_{A,N}: Z_N \to Z_N,$$

$$f_{A,N}(x) = A^x \pmod N,$$

де X – ціле число, $1 \le x \le N-1$.

Існують ефективні алгоритми, які дозволяють досить швидко розрахувати значення функції $f_{A,N}(x)$. Якщо $y = A^x$, то природно записати $x = \log_A(y)$. Тому задачу знаходження функції оберненої до функції $f_{A,N}(x)$ називають задачею знаходження дискретного алгоритму чи задачею дискретного логарифмування. Задача дискретного логарифмування формулюється наступним чином. Для відомих цілих A, N, y знайти ціле число x, таке, що

$$A^x \bmod N = y.$$

Алгоритм розрахунку дискретного логарифму за прийнятний час поки не знайдений. Тому модульна експонента вважається однонаправленою функцією.

За сучасними оцінками теорії чисел при цілих числах $A \approx 2^{664}$ та $N \approx 2^{664}$ розв'язання задачі дискретного логарифмування (знаходження показника степеня x для відомого y) потребує біля 10^{26} операцій – задача має в 1000 раз більшу обчислювальну складність, ніж задача розкладання на множники. При збільшенні довжини чисел різниця в оцінках складності задач зростає. Слід зазначити, що поки не вдалося довести, що не існує ефективного алгоритму обчислення дискретного логарифму за прийнятний час. У зв'язку з цим, модульна експонента віднесена до однонаправлених функцій умовно, що, проте, не заважає з успіхом застосовувати її на практиці.

Другим важливим класом функцій, що використовуються при побудові криптосистем з відкритим ключем, є так звані однонаправлені функції з „таємним ходом". Існує неформальне визначення такої функції: функція

$$f: X \to Y$$

відноситься до класу одннаправлених функцій з „таємним ходом" в тому випадку, якщо вона є однонаправленою і, крім того, можливе ефективне обчислення оберненої функції, якщо відомий „таємний хід" (секретне число, рядок тексту чи інша інформація, що асоціюється з цією функцією). Прикладом такої функції є функція, що використовується в криптосистемі RSA.

3.7.3 Криптосистема шифрування даних RSA.

Алгоритм RSA було запропоновано в 1978 році трьома авторами: Р. Райвестом (Rivest), А. Шаміром (Shamir) та А. Алдеманом (Aldeman). Алгоритм названо за першими буквами прізвищ його авторів. Алгоритм RSA став першим повноцінним алгоритмом з відкритим ключем, який може працювати як у режимі шифрування даних, так і в режимі електронного цифрового підпису.

Надійність алгоритму базується на складності факторизації великих чисел та складності обчислення дискретних алгоритмів. В криптосистемі RSA відкритий ключ K_B, секретний ключ k_B, повідомлення M та криптограма C належать множині цілих чисел

$$Z_N=\{0,1,2,...,N\text{-}1\},$$

де N – модуль:

$$N=P*Q$$

Тут P і Q – випадкові великі прості числа. Для забезпечення максимальної безпеки P і Q вибирають однакової довжини і зберігають в секреті. Множина Z_N з операціями додавання та множення по модулю N утворює арифметику по модулю N.

Відкритий ключ K_B вибирають відкритим чином так, щоб виконувалися умови:

$$1<K_B\varphi(N),\ НСД(K_B,\varphi(N))=1,$$
$$\varphi(N)=(P\text{-}1)(Q\text{-}1)$$

де $\varphi(N)$ – функція Ейлера.

Функція Ейлера вказує кількість додатніх цілих чисел в інтервалі від 1 до N, які є взаємно простими з N . Друга із вказаних вище умов означає, що відкритий ключ K_B та функція Ейлера $\varphi(N)$ повинні бути взаємно простими (їх найбільший спільний дільник (НСД) повинен бути рівним 1). Далі, використовуючи розширений алгоритм Евкліда, розраховують секретний ключ k_B, який задовольняє наступній умові:

$$k_B*K_B\equiv1(\mathrm{mod}\varphi(N)),$$

або

$$k_B=K_B^{-1}(\mathrm{mod}(P\text{-}1)(Q\text{-}1)).$$

Цей ключ легко розрахувати, оскільки отримувач знає пару простих чисел (P,Q) і може легко розрахувати $\varphi(N)$. Нагадаємо, що k_B та N повинні бути взаємно простими.

Відкритий ключ K_B використовують для шифрування даних, а секретний ключ k_B – для розшифровування. Перетворення шифрування визначає криптограму C через пару (відкритий ключ K_B, повідомлення M) відповідно до формули:

$$C = E_{K_B}(M) = E_B(M) = M^{K_B} (\mathrm{mod}\, N).$$

Знаходження функції, оберненої до $C = M^{K_B} (\mathrm{mod}\, N)$ (визначення значення M за відомими значеннями C, K_B та N), є практично нездійсненною задачею при $N \approx 2^{512}$.

Проте обернену задачу – розшифровування криптограми C, – можна розв'язати, використовуючи пару – секретний ключ k_B та криптограма C за формулою:

$$M = D_{K_B}(C) = D_B(C) = C^{k_B} (\mathrm{mod}\, N).$$

Таким чином, якщо криптограму

$$C = M^{K_B} (\mathrm{mod}\, N)$$

піднести до степеня k_B, то в результаті відновлюється вихідний відкритий текст M, оскільки

$$\left(M^{K_B}\right)^{k_B} = M^{K_B k_B} = M^{n\varphi(N)+1} \equiv M (\mathrm{mod}\, N)$$

Таким чином, отримувач, який створює криптосистему, захищає два параметри: 1) секретний ключ k_B та 2) пару чисел (P,Q), добуток яких дає значення N. З іншої сторони, отримувач відкриває значення модуля N та відкритий ключ K_B.

Противнику відомі тільки значення K_B та N. Якщо б він зміг розкласти число N на множники P та Q, він зміг би обчислити значення функції Ейлера

$$\varphi(N)=(P-1)(Q-1)$$

та визначити значення секретного ключа k_B. Проте, як уже зазначалося, факторизація дуже великого N за допомогою обчислень є нездійсненною на даний час задачею (за умови, що довжина вибраних P та Q складає достатню кількість десяткових знаків).

Приклад

1. Оберемо два простих числа: p = 17, q = 19;
2. Обчислимо n = 17 * 19 = 323, fi = (p - 1) * (q - 1) = 16 * 18 = 288;
3. Оберемо e = 7 (НСД(e, fi) = 1) та розв'яжемо рівняння 7 * d ≡ 1 (mod 288), звідки d = 247.

Побудовано RSA систему: p = 17, q = 19, n = 323, e = 7, d = 247.

Відкритий ключ: n = 323, e = 7, секретний ключ: d = 247.

1. m = 4. Кодування: 47 mod 323 = 234. Декодування: 234247 mod 323 = 4.
2. m = 123. Кодування: 1237 mod 323 = 251. Декодування: 251247 mod 323 = 123.

3.7.4 Протокол Діффі — Геллмана

Протокол Діффі-Геллмана (англ. Diffie–Hellman key exchange (D–H)) — це метод обміну криптографічними ключами. Один з перших практичних прикладів узгодження ключа, що дозволяє двом учасникам, що не мають жодних попередніх даних один про одного, отримати спільний секретний ключ із використанням незахищеного каналу зв'язку. Цей ключ можна

використати для шифрування наступних сеансів зв'язку, що використовують шифр з симетричним ключем.

Схему вперше оприлюднили Вітфілд Діффі і Мартін Геллман у 1976, хоча пізніше стверджувалось, що її кількома роками раніше винайшов Малколм Вільямсон у GCHQ, британській розвідувальній агенції. 2002 року Геллман запропонував називати алгоритм Обмін ключами Діффі-Геллмана-Меркле у визнання внеску Ральфа Меркле в винайденні криптосистем із відкритим ключем.

Хоча протокол Діффі-Геллмана є анонімним (без автентифікації) протоколом встановлення ключа, він забезпечує базу для різноманітних протоколів з автентифікацією, і використовується для забезпечення цілковитої прямої секретності в недовговічних режимах Transport Layer Security (відомих як EDH або DHE залежно від комплектації шифру).

Опис алгоритму

Узгодження спільного таємного ключа відбувається таким чином.

Нехай G — скінченна циклічна група потужністю |G| породжена g.

Аліса і Боб таємно обирають два випадкових цілих числа s_A та s_B, в інтервалі [0, |G| − 1]. Потім вони таємно обчислюють числа $a_A = g^{s}{}_A$ та $a_B = g^{s}{}_B$ відповідно, та обмінюються ними через незахищений канал передачі даних. Нарешті, Аліса та Боб обчислюють $a_{BA} = a_B{}^{s}{}_A = g^{s}{}_B{}^{s}{}_A$ та $a_{AB} = a_A{}^{s}{}_B = g^{s}{}_A{}^{s}{}_B$ відповідно. Слід зазначити, що $a_{AB} = a_{BA}$, і тому це число може служити спільним таємним ключем K Аліси та Боба.

Точніше, тепер Аліса та Боб можуть скористатись відображенням елементів множини G у простір іншої криптосистеми. Наприклад, вони можуть використати блок даних необхідного розміру (зокрема, молодші біти) значення a_{AB} як ключ звичайної блочної криптосистеми.

Були запропновані варіанти протоколу Діффі-Геллмана для різних множин. Зокрема: мультиплікативні групи над великими скінченними полями (поля простих чисел або розширення), мультиплікативна група залишків за модулем складеного числа, еліптичні криві над скінченними полями, якобіан гіпереліптичних кривих над скінченним полем, та факторгрупи уявних квадратичних полів.

Однак, базовий варіант протоколу узгодження ключа анонімний, тут відсутня можливість автентифікації абонентів. Таким чином, протокол вразливий для атаки «людина посередині». Припустімо, що зловмисник C здатен здійснювати підміну повідомлень, якими обмінюються Аліса та Боб. Тоді він може згенерувати числа $s^{*}{}_A$ та $s^{*}{}_B$, і відповідно, отримати два узгоджених ключа: $g^{s}{}_A{}^{s^{*}}{}_B$ та $g^{s^{*}}{}_A{}^{s}{}_B$. В результаті зловмисник отримує можливість повністю контролювати обмін повідомленнями між Алісою та Бобом. При цьому вони не здатні виявити підміну та вважатимуть, що зв'язуються один з одним.

Для розв'язання цієї проблеми були запропоновані підсилені варіанти протоколу. Зокрема:

Попереднє поширення сертифікатів (англ. static DH),

Протоколи MTI (за прізвищами авторів англ. Matsumoto, Takashima, Imai),

Відкритий розподіл ключів із використанням автопідписаних ключів,

Протокол KEA (англ. Key Exchange Algorithm),

Протокол «уніфікована модель» (англ. unified model),

Протокол MQV (автори: англ. Law, Menezes, Qu, Solinas, Vanstone).

З автентифікацією абонентів:

Протокол STS (англ. station-to-station),

Протокол DHKE.

Приклад

Єва — криптоаналітик, прослуховувач. Вона читає листування Боба і Аліси, але не може змінити вмісту повідомлень.

s = секретний ключ. s = 2

g = відкрите просте число. g = 5

p = відкрите просте число. p = 23

a = секретний ключ Аліси. a = 6

A = відкритий ключ Аліси. $A = g^a \bmod p = 8$

b = секретний ключ Боба. b = 15

B = відкритий ключ Боба. $B = g^b \bmod p = 19$

Аліса	
знає	не знає
p = 23	b = ?
g = 5	
a = 6	
$A = 5^6 \bmod 23 = 8$	
$B = 5^b \bmod 23 = 19$	
$s = 19^6 \bmod 23 = 2$	
$s = 8^b \bmod 23 = 2$	
$s = 19^6 \bmod 23 = 8^b \bmod 23$	
s = 2	

Боб	
знає	не знає
p = 23	a = ?
g = 5	
b = 15	
$B = 5^{15} \bmod 23 = 19$	
$A = 5^a \bmod 23 = 8$	
$s = 8^{15} \bmod 23 = 2$	
$s = 19^a \bmod 23 = 2$	
$s = 8^{15} \bmod 23 = 19^a \bmod 23$	
s = 2	

Єва	
знає	не знає
p = 23	a = ?
g = 5	b = ?
	s = ?
$A = 5^a \bmod 23 = 8$	
$B = 5^b \bmod 23 = 19$	
$s = 19^a \bmod 23$	
$s = 8^b \bmod 23$	
$s = 19^a \bmod 23 = 8^b \bmod 23$	

3.8 Аутентифікація. Електронний цифровий підпис

Ідентифікація - це призначення об'єкту системи унікальної умовної позначки, яка дозволяє однозначно визначити цей об'єкт. Під аутентифікацією розуміється перевірка справжності об'єкту, що пред'явив даний ідентифікатор. Аутентифікація заснована на інформації, яка може бути відома тільки істинному користувачеві системи.

Нехай в комунікаційної мережі, забезпеченою системою шифрування RSA, абонент А бажає поширити відкрите повідомлення m і підтвердити своє авторство. Всім користувачам мережі доступний відкритий ключ абонента А - пара чисел (n, e). Крім того, А тримає в секреті свій закритий ключ d - едине

число, разом з e та n = pq задовольняє порівнянні ed≡1 (mod (p-1) (q-1)). Для здійснення свого завдання А представляє m в числовому вигляді, нехай виявиться m <n, і обчислює s = (md) mod n - це його цифровий підпис. Потім він розсилає по мережі пару чисел (m, s). Абонент В, прочитавши m і бажаючи переконатися в тому, що надіслав повідомлення насправді той, за кого він себе видає, витягує з RSA-довідника мережі належить А відкритий ключ (n, e) і знаходить з його допомогою число (se) mod n. Якщо отримане число збігається з m, перевіряючий переконується в тому, що цілісність вихідного повідомлення не порушена, тобто в процесі передачі воно не було змінено, і що надіслав це повідомлення знає закритий ключ, пов'язаний з відкритим ключем абонента А, тобто це і є А.

Наприклад, якщо кріптографіческімі параметрами абонента А в системі є p = 3, q = 11, n = 33, e = 7, d = 3 і розсилається повідомлення це m = 2, то підписом А буде s = (md) mod 33 = (23) mod 33 = 8. Абоненти мережі отримають пару чисел (2, 8). Бажаючи перевірити авторство А і справжність повідомлення 2, В обчислює: (se) mod n =

= (87) mod 33 = ((23) 7) mod 33 = (221) mod 33 = ((25) 4 · 2) mod 33 = ((32) 4 · 2) mod 33 = ((- 1) 4 · 2) mod 33 = 2

і приходить за результатами проведених одночасно аутентифікації і перевірки цілісності до позитивного висновку.

Якою була б підпис абонента А під повідомленням m = 2, якщо б він вибрав e = 3 і тоді отримав би d = 7?

Використана в описаній процедурі аутентифікації ідея цифрового підпису придбала фундаментальне значення для сучасного електронного документообігу. Оскільки реалізація цієї ідеї неможлива без засобів сучасної обчислювальної техніки, прийнято говорити про електронний цифровий підпис (ЕЦП).

Діловий обмін інформацією між користувачами інформаційної мережі передбачає, зокрема, передачу даних, спрямованих на здійснення тих чи інших дій. При цьому має бути забезпечений захист від різних зловмисних вчинків, таких як відмова відправника від переданого повідомлення, приписування їм авторства іншій особі, зміна тексту одержувачем або будь-ким іншим і т.п. Протягом століть надійною перешкодою на шляху подібних небажаних можливостей була власноручний підпис відправника на переданій документі. Залучення мережі Інтернет для фінансової і торговельної діяльності спонукало зацікавлені структури до пошуку настільки ж надійного електронного засобу забезпечення безпеки відповідного документообігу. В результаті з'явилася наступна загальна схема електронного цифрового підпису, заснована на практиці асиметричної криптографії. Користувач А має в своєму розпорядженні два ключа: закритий, який він тримає в секреті, і відкритий, який може бути доступний будь-якому іншому користувачеві. За допомогою свого закритого ключа А виготовляє з оригінального тексту деяке інше повідомлення - це його ЕЦП. Потім А передає вихідний текст разом зі своїм ЕЦП абоненту В, забезпечуючи його при необхідності своїм відкритим ключем (або В сам може знайти цей ключ в довіднику мережі). Далі В

здійснює другий етап процедури ЕЦП: він перевіряє підпис абонента А за допомогою його відкритого ключа. При цьому відбувається і перевірка цілісності отриманого повідомлення. який може бути доступний будь-якому іншому користувачеві. За допомогою свого закритого ключа А виготовляє з оригінального тексту деяке інше повідомлення - це його ЕЦП. Потім А передає вихідний текст разом зі своїм ЕЦП абоненту В, забезпечуючи його при необхідності своїм відкритим ключем (або В сам може знайти цей ключ в довіднику мережі). Далі В здійснює другий етап процедури ЕЦП: він перевіряє підпис абонента А за допомогою його відкритого ключа. При цьому відбувається і перевірка цілісності отриманого повідомлення. який може бути доступний будь-якому іншому користувачеві. За допомогою свого закритого ключа А виготовляє з оригінального тексту деяке інше повідомлення - це його ЕЦП. Потім А передає вихідний текст разом зі своїм ЕЦП абоненту В, забезпечуючи його при необхідності своїм відкритим ключем (або В сам може знайти цей ключ в довіднику мережі). Далі В здійснює другий етап процедури ЕЦП: він перевіряє підпис абонента А за допомогою його відкритого ключа. При цьому відбувається і перевірка цілісності отриманого повідомлення. він перевіряє підпис абонента А за допомогою його відкритого ключа. При цьому відбувається і перевірка цілісності отриманого повідомлення. він перевіряє підпис абонента А за допомогою його відкритого ключа. При цьому відбувається і перевірка цілісності отриманого повідомлення.

Суттєвим моментом є те, що підпис залежить від тексту переданого повідомлення: найменша зміна в ньому обов'язково тягне за собою зміну підпису, зокрема підпис, яка супроводжує один документ, неможливо перенести на інший. Якщо підпис успішно пройшла перевірку, який підписав не може відмовитися від неї, оскільки відкритий ключ, який використовується при перевірці, однозначно визначається зберігаються у нього закритим ключем.

ЕЦП визнається аналогом власноручного підпису в багатьох країнах світу. У числі перших, хто взяв відповідний закон, були США, де з літа 2000 року документи з ЕЦП отримали таку ж юридичну силу, як і підписані від руки. Через рік, у липні 2001 року, директиву, юридично визнає ЕЦП в державах-членах європейського Союзу, прийняла Європейська комісія.

3.9 Хеш-функция.

Повільність алгоритмів асиметричного шифрування сильно затягує процеси виготовлення і перевірки ЕЦП в разі підписуються текстів великої довжини. Тому необхідним елементом всіх практичних процедур ЕЦП є використання так званих функцій хешування, або хеш-функцій.

Хеш-функція призначається для компактного представлення довгих послідовностей (слів). Вона перетворює повідомлення довільної довжини над даними алфавітом в блок фіксованої довжини над тим же алфавітом, тобто виробляє згортку всіх повідомлень (слів) в повідомлення (слова) однієї і тієї ж заданої довжини. Функція хешування, розроблена в 1992 році Ривестом MD-5

дає 128-бітове хеш-значення (зване дайджестом повідомлення, Message Digest).

Неважко придумати приклади хеш-функцій: нехай, скажімо, згорткою повідомлення є його початковий п’ відрізок або просто перша буква. Однак криптографічний хеш-функція h повинна для будь-якого слова p не тільки досить просто обчислювати його згортку h (p), а й володіти такими захисними властивостями:

1) (протидія визначенням прообразу) якщо відомо, що q є згорткою деякого слова, то практично неможливо знайти слово p, для якого h (p) = q;

2) (протидія виявленню другого прообразу) для даного слова p неможливо знайти інше слово p 'з такою ж згорткою: h (p') = h (p);

3) (протидія колізії) неможливо знайти два різних слова p і p' з однаковою згорткою: h (p) = h (p').

В алгоритмах ЕЦП перед виготовленням підписи вихідне повідомлення m замінюється його згорткою h (m), де h - обрана для даної процедури ЕЦП хеш-функція. Хеш-функція SHA (Secure Hash Algorithm), що застосовується в американському стандарті ЕЦП 1994 року, видає 160-бітові значення і має велику схожість з MD-5, яка не була стандартизована через виявлену слабкості у протидії колізії. Порівняльна швидкість хешування (Кбайт / с): MD-5 - 174, SHA - 75.

Крім виконання завдання компактного представлення інформації, криптографічні хеш-функції, володіючи вищевказаними властивостями протидії, можуть служити і для аутентифікації повідомлень. Код перевірки справжності повідомлення, або MAC (Message Authentication Code) - це залежить від секретного ключа криптографічний хеш-функція. Якщо абоненти мережі A і B використовують загальний секретний ключ k, то A, посилаючи для B повідомлення m, прикріплює до нього MAC - хеш-значення h (k || m) (до повідомлення попереду приписується ключ, створюючи єдиний масив). Так як B знає ключ k, то, отримавши повідомлення, скажімо m ', він визначить h (k || m') і, порівнявши це значення з надісланим MAC h (k || m), побачить, змінилося чи ні вихідне повідомлення під час передачі.

Коди MAC використовуються не тільки для аутентифікації файлів, якими обмінюються користувачі, але і для перевірки збереження особистих файлів при можливому шкідливому впливі: власник складає таблицю MAC своїх файлів і при зверненні до будь-якого з них звіряє його знову обчислений MAC зі значенням, записаним в таблиці.

Хеш-алгоритми: алгоритми хешування створюють хеш повідомлення та шифрують його. Вони використовують математичну формулу для хешування, і вкрай важко втрутитися в повідомлення і все одно створити той самий хеш. В основному, хешування дозволяє одержувачу перевіряти, чи отримано повідомлення цілим, без втручання третьої сторони.

SHA (алгоритми безпечного хешування): існує кілька алгоритмів безпечного хешування, і вони в першу чергу відрізняються довжиною хешування. Це SHA-1, SHA-256, SHA-384 та SHA-512. У SHA-1 бітова

довжина становить 160 біт, у SHA-256 це 256 бітів, для SHA-384, 384 біт і в SHA-512 вона становить 512 біт.

MD2, MD4, MD5 (серії алгоритмів побудови дайджесту-повідомлення): це інший тип хеш-алгоритмів. Ці алгоритми були розроблені Рівестом. Усі три алгоритми приймають повідомлення довільної довжини та видають 128-бітний дайджест повідомлення. MD2 призначений для 8-бітових машин, а MD4, MD5 - для 32-бітних машин. Ці алгоритми в основному використовуються для програм цифрового підпису.

3.10 Інфраструктура відкритих ключів (PKI)

Інфраструктура відкритих ключів використовує принципи криптографічної системи захисту інформації з відкритим ключем.

Інфраструктура управління відкритими ключами складається з:

Центру сертифікації (засвідчувального центру);

Кінцевих користувачів;

Опціональних компонентів (центру реєстрації та мережевого довідника).

Центр сертифікації створює електронний документ – сертифікат відкритого ключа користувача, таким чином засвідчуючи факт того, що закритий ключ відомий лише власнику цього сертифіката, відкритий ключ (public key) вільно передається в сертифікаті. Засвідчувальний центр підтверджує або спростовує належність відкритого ключа заданій особі, яка володіє відповідним закритим ключем. Сертифікат містить відкритий ключ користувача і ідентифікуючу цього користувача інформацію (а також іншу службову інформацію). Сертифікат засвідчується ЕЦП засвідчувального центру.

Основні завдання системи PKI:

Забезпечення конфіденційності інформації;

Забезпечення цілісності інформації;

Забезпечення автентифікації користувачів і ресурсів;

Забезпечення можливості підтвердження здійснених користувачами дій з інформацією;

У криптографії X.509 є стандартом для інфраструктури відкритого ключа (PKI) та інфраструктури управління привілеями (PMI). X.509 серед іншого визначає стандартні формати сертифікатів відкритих ключів, списки відкликання сертифікатів, сертифікати атрибутів та алгоритм перевірки шляху сертифікації.

В інфраструктурі відкритих ключів:

1. Для кодування / декодування повідомлення потрібен ключ, і безпека повідомлення залежить від безпеки ключа.

2. Текст шифру є закодованим повідомленням та

3. Сертифікат - це документ із цифровим підписом довіреного органу.

Інфраструктура відкритих ключів складається з двох важливих сертифікатів:

1. Кореневі сертифікати - ідентифікує Центр сертифікації, CA та

2. Сертифікати посвідчення особи, які ідентифікують такі пристрої, як сервери та інші пристрої, які хочуть брати участь у PKI.

Налаштування PKI на маршрутизаторі шлюзу

Команда crypto map <назва карти> надається на рівні інтерфейсу. Правильна послідовність команд:

```
Router1(config)# interface GigabitEthernet 1/0
Router1(config-if)# crypto map MyCmap -1
Router1(config-if)# exit
```

Список відкликаних сертифікатів (CRL): Це список сертифікатів із їх серійними номерами, які були скасовані ЦС з якихось причин. Зазвичай причини полягають у закінченні терміну дії сертифіката (термін дії сертифіката минув) або в тому, що приватний ключ був порушений, видано новий сертифікат тощо. До CRL можна отримати доступ за допомогою декількох протоколів, включаючи LDAP та HTTP. CRL також можна отримати через SCEP. Простий протокол реєстрації сертифікатів (SCEP) - це протокол, який використовується для реєстрації та інших операцій з інфраструктурою відкритих ключів (PKI)

Протокол статусу онлайн-сертифіката (OSCP): тут клієнт надсилає запит на пошук статусу сертифіката та отримує відповідь, не знаючи повного списку скасованих сертифікатів

Стандарти криптографії з відкритим ключем (коротше, іменовані як PKCS) - це специфікації, вироблені лабораторіями RSA у співпраці з розробниками безпечних систем у всьому світі. Вклади з серії PKCS стали частиною багатьох формальних та фактичних стандартів, включаючи документи ANSI X9, PKIX, SET, S / MIME та SSL.

PKCS # 1: Забезпечує стандарти для реалізації схем криптографічного шифрування із відкритим ключем на основі алгоритму RSA та схем цифрового підпису з додатком.

PKCS # 3: Описує метод реалізації угоди про ключ Діффі-Хеллмана, за допомогою якої дві сторони можуть домовитись про секретний ключ, який відомий тільки їм (і, зокрема, не відомий підслуховувачу, який слухає діалог, за яким сторони погодили ключ). Потім цей секретний ключ можна використовувати, наприклад, для шифрування подальших комунікацій між сторонами.

PKCS # 7: Описує криптографічний синтаксис повідомлень (CMS): CMS визначає синтаксис, який використовується для цифрового підпису, перетравлення, автентифікації або шифрування довільного вмісту повідомлення.

PKCS # 10: Стандарт синтаксису запиту на сертифікацію

PKCS # 12: Стандарт синтаксису обміну персональною інформацією. PKCS # 12 v1.0 описує синтаксис передачі для особистої інформації про особу, включаючи приватні ключі, сертифікати, різні секрети та розширення.

Простий протокол реєстрації сертифікатів (SCEP): SCEP - це протокол, який використовується для реєстрації та інших операцій з інфраструктурою відкритих ключів (PKI). SCEP не є відкритим стандартом, і лише пристрої Cisco та деякі інші підтримують його.

Ви можете легко налаштувати SCEP за допомогою ASDM. Реєстрація та використання SCEP, як правило, слід за цим робочим процесом:

1. Отримайте копію сертифіката Центру сертифікації (CA) та підтвердьте його.

2. Створіть CSR та надішліть його надійно в ЦС.

3. Опитуйте сервер SCEP, щоб перевірити, чи був підписаний сертифікат.

4. Повторно зареєструйтесь, якщо це необхідно, щоб отримати новий сертифікат до закінчення терміну дії поточного сертифіката.

5. За потреби отримайте CRL.

Нижче наведено важливі компоненти інфраструктури відкритих ключів (PKI):

Цифрові сертифікати	Цифрові "посвідчення особи", видані довіреними третіми сторонами (які називаються Центром сертифікації або CA), які ідентифікують користувачів та машини. Їх можна надійно зберігати в цифрових гаманцях або в каталогах
Відкриті та закриті ключі	Формує базис PKI для безпечного зв'язку на основі секретного закритого ключа та математично пов'язаного відкритого ключа
Secure sockets layer (SSL)	Криптографічний протокол.
Центр сертифікації (CA)	Діє як довірений, незалежний провайдер цифрових сертифікатів

Інфраструктура відкритих ключів

Користувачеві потрібно зробити телефонний дзвінок до ЦС, щоб підтвердити відкритий ключ кореневого сертифіката.

1. show crypto isakmp sa detail- Перегляньте детальну інформацію про тунель IKE Phase 1, що використовується

2. show crypto isakmp sa detail - Перегляньте детальну інформацію для існуючих тунелів IKE Phase 2. Існує одна вхідна асоціація безпеки (SA) та одна вихідна. Вони обидва мають різні номери SA, які використовуються для відстеження цих сеансів.

3. show crypto engine connections active - команда надає статистику, щоб перевірити, чи працює шифрування та дешифрування.

4. show crypto map - надає деталі крипто-карти та де вона застосовується, показуючи зміст наборів перетворень IKE Phase 2, поточний пристрій та іншу інформацію.

ЛЕКЦІЯ 4.
БЕЗПЕЧНЕ УПРАВЛІННЯ. ЗАХИСТ ПЛОЩИНИ УПРАВЛІННЯ (MPP).

4.1. Забезпечення управління трафіком

Коли ви маєте справу з захистом великої комп'ютерної мережі, перше запитання, яке ви задаєте: З чого я почну? Тож спочатку нам потрібно класифікувати, описати та виявити існуючі вразливості. Площина управління містить, як ми будемо підключатись до пристроїв, якими ми будемо керувати, і з якими привілеями, а також хто може отримати доступ до системи та що він може зробити. План управління також включає в себе те, як підтримувати повідомлення про події, що надсилаються на комутатори / маршрутизатори або з них. Одне з найкращих рішень для управління нашими пристроями - це використання кабелю для перекидання, але у випадку величезної топології це не є великою проблемою. Найкраще рішення - налаштувати віддалені пристрої та зафіксувати певну IP-адресу для управління, захистити доступ за допомогою паролів та забезпечити шифрування трафіку.

4.1.1 Найкращі практики управління площиною

+ Повторне блокування пароля для входу: нам потрібно встановити фіксовану кількість помилкових спроб входу, і після них обліковий запис буде автоматично заблоковано.

+ Зашифровані протоколи управління: У кожному завданні управління повинно використовуватися шифрування, таке як SSH, HTTPS, OOB, і забезпечувати наявність абсолютно окремої мережі для управління та кінцевих пристроїв.

+ Ведення журналу та моніторинг: Журналювання не повинно включати лише конфігурацію користувачів, а також системні події, генеровані пристроями. Ми повинні згадати в нашій площині рівень журналу, що нам потрібна та класифікується найважливіша інформація, і яку інформацію не слід реєструвати. Ми також повинні виділити достатню кількість місця для збереження журналів; ми можемо використовувати сервер журналів, який збирає весь файл журналу в мережі, і переконатися, що всі журнали, надіслані в мережі, зашифровані; ми можемо використовувати інший сервер для збереження увійдіть у хмару, наприклад, щоб гарантувати, що ніхто не зможе змінити або змінити ці файли.

+ Захищені системні файли: Ми повинні переконатися, що ніхто не може видалити конфігурацію або образ IOS наших мережевих пристроїв. Якщо конфігурація або образ IOS не знайдені, пристрій не працюватиме. "Cisco

пропонує еластичну функцію конфігурації. Ця функція постійно підтримує захищену робочу копію образу IOS маршрутизатора та файлів конфігурації запуску. Після ввімкнення адміністратор не може віддалено вимкнути функції (лише якщо він підключений безпосередньо). Захищені файли називаються захищеним завантажувальним набором .

4.1.2 Параметри зберігання імен користувачів, паролів та правил доступу

Існує багато варіантів зберігання такої інформації, як служба AAA, де ми можемо знайти сервер ACS, сервер Radius та сервер Tacacs +, всі вони мають однаковий тип функцій, і вони дозволяють зберігати імена користувачів, паролі та правила. Ми можемо використовувати цю послугу для авторизації користувачів, підключених до нашої мережі за допомогою VPN, ми аутентифікуємо цих користувачів, а потім уповноважуємо їх отримувати доступ до таких пристроїв та надавати їм необхідні привілеї. Крім того, ми можемо використовувати цю послугу для автентифікації користувачів, що мають доступ до маршрутизаторів, та надання їм належних привілеїв для управління (наприклад, оболонка EXEC для адміністраторів).

4.1.3 Обмеження адміністратора шляхом призначення рівня доступу.

Призначивши рівень доступу, ми можемо обмежити привілеї користувачів, ми можемо асимілювати такі привілеї для користувача та скасувати деякі команди.

4.1.4 Використання файлів реєстрації

Файли журналів важливі для розслідування атак та проблем конфігурації, і Cisco IOS надає іншу можливість збереження цих файлів:

+ Консоль: може надсилати файли журналів на підключений пристрій через певний порт.

+ vty лінії: Надіслати файл журналу на віддалений термінал за допомогою SSH, наприклад, повинен запустити команду terminal monitor, щоб дозволити користувачам, підключеним до цієї лінії vty, бачити журнал повідомлення.

+ Буфер: Обидва наведені вище рішення не зберігають файл журналу, однак ми можемо зберігати ці файли журналів в пам'яті пристрою, де ми поміщаємо його в буфер.

+ Сервер SNMP: Маршрутизатори / комутатори / сервери в мережі надсилають файли журналів на сервер SNMP.

+ Сервери Syslog: Повідомлення журналу можна надсилати безпосередньо на різні сервери Syslog.

Рівні важливості Syslog наведені в таблиці 4.1:

Таблиця 4.1 – Рівні важливості Syslog.

Severity Level	Level Name	Description
0	Emergencies	System unusable
1	Alerts	Immediate action needed
2	Critical	Critical conditions
3	Errors	Error conditions
4	Warnings	Warning conditions
5	Notifications	Normal but significant conditions
6	Informational	Informational messages only
7	Debugging	Debugging messages

4.2 Впровадження заходів безпеки для захисту площини управління

4.2.1 Впровадження надійних паролів

- Призначення пароля для користувача:

R#username Peerlyst secret P4ssw0rd (цей пароль хешується за допомогою MD5, а потім зберігається)

- Для консольної лінії:

```
R(config)#line consol 0
R(config-line)#password P4ssw0rd$
R(config-line)#login
R(config-line)#exit
```

- Для лінії vty (telnet або ssh):

```
R(config)#line vty 0 9
R(config-line)#password P4ssw0rd$
R(config-line)#login
R(config-line)#exit
```

- Для лінії aux:

```
R(config)#line aux 0
R(config-line)#no exec
```

R(config-line)#password P4ssw0rd$
R(config-line)#login
R(config-line)#exit

- Зашифруйте відкриті паролі :

R(config)#service password-encryption

- Показати конфігурацію:

R(config)#do show run | begin line

4.2.2 Аутентифікація користувача за допомогою AAA

Розглянемо питання про те, як увімкнути службу AAA зі списками методів, які обмежать привілеї користувачів:

- Увімкнути функцію aaa:

R(config)# aaa new-model

- Встановити Tacacs сервер і ключ:

R(config)#tacacs-server host 1.1.1.1
R(config)#tacacs-server key P4ssw0rd$

- Спершу автентифікуйте користувача з локальної бази даних, а потім за допомогою заданого зашифрованого паролю:

R(config)#aaa authentication login default local enable

- Аутентифікуйте список користувачів MYLIST спочатку з сервера Tacacs, другий з локальної бази даних і, нарешті, за допомогою заданого зашифрованого паролю:

R(config)#aaa authentication login MYLIST group tacacs local enable

- Список методів авторизації для привілейованого режиму виконання :

R(config)#aaa authorization commands 15 TAC15 group tacacs+ local

- На сервер логування будуть записуватися команди, введені користувачем, рівень привілеїв команд 15:

R(config)#aaa accounting commands 15 TAC-acc start-stop group tacacs+

- Створіть локального користувача для маршрутизатора:

R(config)#username admin privilege 15 secret ziJ@D7dk(éAJ8

- Застосувати метод авторизації та лініях vty:

R(config)#line vty 0 4
R(config-line)#login authentication MYLIST
R(config-line)#authorization commands TAC15
R(config-line)#accounting commands 15 TAC-acc

- Дозволити логування в буфер та команда очистки:

R(config)#logging buffered 7
R(config)#end
R#clear log

- Увімкніть режим налагодження для усунення проблем AAA для маршрутизаторів Cisco:

R#debug aaa authentication
R#debug aaa authorization
R#debug aaa accounting
- Щоб визначити підключеного користувача наберіть:

R> who

4.2.3 Рівень привілеїв RBAC

Ми можемо реалізувати RBAC в службі AAA, де правила налаштовані на сервері ACS і обмежити те, що можуть робити користувачі. Розглянемо, як створювати та призначати команди для заданого рівня привілеїв:

- Призначте команду для налаштування терміналу на рівень 8 привілеїв та встановіть для нього пароль:

R(config)#privilege exec level 8 configure terminal
R(config)#enable secret level 8 0 Nfez8@ajef
R(config)#end

-Доступ для привілеїв 8-го рівня:

R>enable 8

- Призначити користувачеві привілей 8:

R(config)#username Hamza privilege 8 secret Password213

4.2.4 Впровадження Parser Views

У цій частині ми побачимо, як створювати і працювати з parser views:

- Встановіть пароль і активуйте AAA:

R(config)#enable secret Passwd0!
R(config)#aaa new-model
R(config)#end

- Створення View:

R#enable view (after this command you will be asked to enter your secret password “Passwd0!”)
R(config)#parser view VIEW-1
R(config-view)#secret VIEWdad@ (set password required to enter the view)
R(config-view)#commands exec include ping
R(config-view)#command exec include all show
R(config-view)#commands exec include configure
R(config-view)#commands configure include access-lists
R(config-view)#exit
R(config)#exit

- Перевірка View:

R>enable view VIEW-1

- Подивитися, яке view використовується:

R(config)#username hamza view VIEW-1 secret Passw0rd$

- Створення користувача, якому буде зіставлений заданий view:
R (конфігурація) #username hamza view VIEW-1 secret Passw0rd $

4.2.5 SSH та HTTPS

Коли ми будемо віддалено підключатись до пристрою, щоб використовувати зашифроване з'єднання, таке як HTTPS або SSH, щоб увімкнути SSH у маршрутизаторі, нам потрібно виконати наступні дії:
- Визначити ім’я хосту:

Router(config)#hostname R

- Визначити доменне ім’я:

R(config)#ip domain-name medium.com

- Створити новий крипто-ключ (нам потрібно зробити ці два кроки перед створенням ключа):

R(config)#crypto key generate rsa

- Створити користувача:

R(config)#username Hamza secret hamza123

- Налаштуйте рядок vty:

R(config)#line vty 0 9
R(config-line)#login local

- Тепер ми можемо підключитися через SSH:

R#ssh -l Hamza 1.1.1.1
R>show ssh

Якщо ми хочемо використовувати HTTPS, нам просто потрібно виконати наступні налаштування:

- Активувати SSL:

R(config)#ip http secure-server

- Встановіть спосіб автентифікації користувача:

R(config)#ip http authentication local

4.2.6 Впровадження функцій реєстрації

Активувати Syslog настільки просто, що нам просто потрібно виконати такі команди:

- Спочатку нам потрібно вимкнути інтерфейс, потім активний журнал і ми знову активувати інтерфейс:

R(config)#int fa0/0
R(config-if)#shutdown
R(config-if)#exit

R(config)#service timestamps log datetime
R(config)#int fa0/0
R(config-if)#no shutdown

4.2.7 Особливості SNMP

Простий протокол керування мережею SNMP є найбільш часто використовуваним для протоколів управління мережею.

Розглянемо компоненти SNMP:

+ Менеджер SNMP: називається сервер управління мережею NMS.

+ Агент SNMP: Запускається на керованому пристрої.

+ Інформаційна база управління: MIB містить інформацію про керовані пристрої.

Менеджер SNMP може надсилати інформацію та отримувати запити; Існує три типи повідомлень SNMP:

+ GET: Використовується для отримання інформації з керованих пристроїв.

+ SET: Використовується для встановлення значення змінної або запуску дії на керованому пристрої.

+ TRAP: Використовується керованим пристроєм для сповіщення менеджера SNMP про подію.

Існує ризик, якщо зловмисник отримає доступ до MIB або він надішле багато повідомлень SET багатьом пристроям у мережі, деякі пристрої мають два паролі за замовчуванням: "загальнодоступний" лише для читання та "приватний" для читання-запису. SNMPv1 та 2 намагалися виправити ці уразливості, але виправлення все ще є слабким, сьогодні SNMPv3 використовує концепцію рівня безпеки та модель безпеки:

+ Модель безпеки: Становить аутентифікацію користувача та групи.

+ Рівень безпеки: Визначає алгоритм, що використовується для пакетів SNMP:

+ noAuthNoPriv: немає автентифікації, не шифрується для конфіденційності.

+ AuthNoPriv: Аутентифікація за допомогою HMAC, MD5 або SHA.

+ AuthPriv: Шифрування за допомогою CBC або DES.

Конфігурування SNMPv3:

- Налаштуйте «загальний рядок» community string лише для читання зі списком доступу 99, щоб обмежити доступ:

R(config)#access-list 99 permit 192.168.1.1 /24
R(config)#snmp-server group medium-group v3 noauth (activate v3)
R(config)#smtp-server user medium-user medium-group v3
R(config)#snmp-server community mediumRO 99
R(config)#snmp-server trap-source Fa0/0 (set interface)
R(config)#smtp-server host 192.168.1.2 version 3 noauth medium-user

4.2.8 Налаштування NTP

Оскільки ми активуємо Syslog, нам потрібно встановити час, щоб знати, коли кожна подія реєструється. Щоб перевірити з'єднання NTP через CLI, виконаємо такі команди:

R#show ntp status
R#show ntp association

4.2.9 Протокол для безпечного копіювання

Функція SCP забезпечує автентифікацію, коли ми намагаємось скопіювати конфігурацію пристрою або файл образу пристрою. Для реалізації SCP потрібна активна служба AAA. Розглянемо команду enable:

R(config)#ip scp server enable

4.2.10 Захист образу Cisco IOS та конфігураційних файлів

У разі видалення як файлової системи flash, так і NVRAM, Cisco надає функцію, за допомогою якої пристрій може відновити образ IOS та файли конфігурації з безпечного місця, яке віддалений користувач не може видалити. Для цього використовуються команди:

R(config)#secure boot-image
R(config)#secure boot-config
R#show secure bootset

ЛЕКЦІЯ 5.
КОНЦЕПЦІЇ ОРГАНІЗАЦІЇ АВТЕНТИФІКАЦІЇ, АВТОРИЗАЦІЇ ТА АУДИТУ(AAA).

5.1 Визначення автеніфікації, авторизації та аудиту.

У мережевому інфраструктурному пристрої Cisco, на якому запущено IOS, за замовчуванням автентифікація здійснюється за допомогою лінійного пароля (консоль або лінія vty), а авторизація - за допомогою пароля 15 рівня. І лінійна автентифікація, і ввімкнення авторизації рівня 15 хороші, якщо у вас є лише дуже мала кількість мережевої інфраструктури.

Ваша мережа зростає, і якщо ви керуєте великим мережевим середовищем, автентифікація за допомогою локальної бази даних користувачів пристрою та авторизація з використанням дозволу рівня 15 не є масштабованим рішенням. Настав час подумати про рішення Cisco AAA.

AAA розшифровується як автентифікація, авторизація та аудит.

Аутентифікація: Аутентифікація - це процес, при якому ідентифікація пристрою або користувача перевіряється, коли вони намагаються отримати доступ до мережевого ресурсу та підтверджують, що вони є насправді ті, ким вони себе декларують. Для автентифікації зазвичай використовується комбінація ідентифікатора користувача / пароля для автентифікації користувачів. Також доступні інші типи автентифікації, такі як біометрична автентифікація або автентифікація за допомогою цифрових сертифікатів. Аутентифікація дає відповідь на запитання "Хто ти?" або "Ви та сама людина, якою представляєтеся?"

Авторизація: Авторизація - це процес після автентифікації, який використовується для визначення того, чи має користувач, який намагається отримати доступ до будь-якого пристрою, даних або виконати команду, дозвіл на доступ до цього пристрою, даних або виконання команди. Авторизація дає відповідь на питання "Чи дозволено вам виконувати це завдання?"

Аудит: Аудит можна визначити як відстеження даних, доступу, використання, подій або мережевих ресурсів. Аудит - це реєстрація, облік та моніторинг даних, доступу, використання, подій мережевих ресурсів. Аудит дає відповідь на питання "Що ви робили?", "Хто за це відповідає?"

Два широко прийняті протоколи AAA - це RADIUS і TACACS +

5.2 AAA RADIUS і TACACS +, різниця між RADIUS і TACACS +

RADIUS (Remote Authentication Dial-in User Service) - це протокол AAA, який підтримує постачальник. Вперше RADIUS був розроблений компанією Livingston Enterprises Inc у 1991 році, яка згодом об’єдналася з Alcatel Lucent. Пізніше RADIUS став стандартом Інженерної робочої групи (IETF). Деякі реалізації сервера RADIUS використовують порт UDP 1812 для автентифікації RADIUS, а порт UDP 1813 для обліку RADIUS. Деякі інші реалізації використовують порт UDP 1645 для повідомлень про автентифікацію RADIUS, а порт UDP 1646 для обліку RADIUS

TACACS + - ще один протокол AAA. TACACS + був розроблений компанією Cisco від TACACS (система контролю доступу контролера доступу до терміналів, розроблена в 1984 році для Міністерства оборони США). TACACS + використовує TCP і забезпечує окремі послуги автентифікації, авторизації та бухгалтерського обліку. Порт, що використовується TACACS +, - TCP 49.

Протокол RADIUS або TACACS + може забезпечити центральний протокол автентифікації для автентифікації користувачів, маршрутизаторів, комутаторів або серверів. Якщо ваша мережа зростає і якщо ви керуєте великим мережевим середовищем, автентифікація за допомогою локальної бази даних користувачів пристрою та авторизація за допомогою авторизації рівня 15 привілеїв не є масштабованим рішенням. Протокол AAA (Authentication Authorization Accounting), такий як RADIUS або TACACS +, може забезпечити краще централізоване рішення автентифікації у великій корпоративній мережі.

Основні відмінності між RADIUS та TACACS + можна подати в таблиці, як показано нижче.

RADIUS	TACACS +
RADIUS використовує UDP як протокол транспортного рівня	TACACS + використовує TCP як протокол транспортного рівня
RADIUS використовує UDP-порти1812 та 1813/1645 та 1646	TACACS + використовуєTCP-порт 49
RADIUS шифрує лише паролі	TACACS + шифрує весь зв'язок
RADIUS поєднує автентифікацію та авторизацію	TACACS + трактує аутентифікацію, авторизація та аудит роздільно
RADIUS - це відкритий протокол, що підтримується багатьма постачальниками	TACACS + - це власний протокол Cisco
RADIUS - це легкий протокол, який споживає менше ресурсів	TACACS + - це важкий протокол, який споживає більше ресурсів
РАДІУС обмежуєтьсяя режимом привілеїв	TACACS + підтримує 15 рівнень привілеїв
В основному використовується для доступу до мережі	В основному використовується для адміністрування пристроїв

ЛЕКЦІЯ 6
КОНЦЕПЦІЯ ПОБУДОВИ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ VPN.

6.1 Визначення VPN

VPN (англ. Virtual Private Network - віртуальна приватна мережа) - узагальнена назва технологій, що дозволяють забезпечити одне або кілька мережних з'єднань (логічну мережу) поверх іншої мережі (наприклад, Інтернет). Незважаючи на те, що комунікації здійснюються по мережах з меншим або невідомим рівнем довіри (наприклад, по публічних мережах), рівень довіри до побудованої логічної мережі не залежить від рівня довіри до базових мереж завдяки використанню засобів криптографії (шифрування, аутентифікації, інфраструктури відкритих ключів, засобів для захисту від повторів і змін переданих по логічної мережі повідомлень).

Залежно від застосовуваних протоколів і призначення, VPN може забезпечувати з'єднання трьох видів: вузол-вузол, вузол-мережа та мережа-мережа.

6.2 Переваги використання VPN з'єднання

Основною причиною впровадження технології VPN є створення безпечного підключення до іншої кінцевій точці. Створення WAN-з'єднання дуже дороге і може бути недоцільним для окремих користувачів, що створюють з'єднання клієнта з сервером. Інформація, яка циркулює між двома кінцевими точками VPN, зашифрована, і, отже, ніяке втручання не може статися, коли інформація передається по мережі загального користування.

VPN також можна використовувати, щоб приховати вашу конфіденційність, маскуючи дійсну IP-адресу комп'ютера користувача. Онлайн-геймери можуть використовувати віртуальну мережу для приховування IP-адреси своїх комп'ютерів, а власники бізнесу можуть застосовувати її можливості для зміни IP-адреси, щоб захистити свої конфіденційні дані від різноманітних конкурентів.

6.3.Недоліки використання VPN з'єднань

Оскільки весь віртуальний мережевий трафік зашифрований, навантаження, що передається по VPN, буде на 10-15% вище. Це змушує:

- Задіяні пристрої використовувати більше обчислювальної потужності для шифрування інформації.
- Відправляти більше даних по мережі, що позначиться на збільшенні часу для передачі повідомлень.

Однак з розвитком комп'ютерних та мережевих технологій додаткова потужність обробки, необхідна для шифрування / дешифрування і додаткової передачі даних, має незначний вплив на загальне використання мережі.

Ще одним мінусом є те, що не всі VPN-пристрої взаємодіють між собою добре. Мережевий інженер, що впроваджує цю технологію, повинен перевірити сумісність між двома кінцевими точками. Точно так же з'єднання з клієнтом і сервером може привести до уповільнення (або погіршення якості обслуговування), якщо VPN не налаштований правильно.

6.4 Рівні реалізації VPN

Зазвичай VPN розгортають на рівнях не вище мережевого, так як застосування криптографії на цих рівнях дозволяє використовувати в незмінному вигляді транспортні протоколи (такі як TCP, UDP).

Користувачі Microsoft Windows позначають терміном VPN одну з реалізацій віртуальної мережі - PPTP, причому використовувану часто не для створення приватних мереж.

Найчастіше для створення віртуальної мережі використовується інкапсуляція протоколу PPP в який-небудь інший протокол - IP (такий спосіб використовує реалізація PPTP - Point-to-Point Tunneling Protocol) або Ethernet (PPPoE) (хоча і вони мають відмінності).

Технологія VPN останнім часом використовується не тільки для створення власне приватних мереж, а й деякими провайдерами «останньої милі» на пострадянському просторі для надання виходу в Інтернет.

При належному рівні реалізації і використанні спеціального програмного забезпечення мережа VPN може забезпечити високий рівень шифрування переданої інформації. При правильному налаштуванні всіх компонентів технологія VPN забезпечує анонімність в Мережі.

6.5 Структура VPN

VPN складається з двох частин: «внутрішня» (підконтрольна) мережа, яких може бути декілька, і «зовнішня» мережа, через яку проходить інкапсульоване з'єднання (зазвичай використовується Інтернет).

Можливо також підключення до віртуальної мережі окремого комп'ютера.

Підключення віддаленого користувача до VPN проводиться за допомогою сервера доступу, який підключений як до внутрішньої, так і зовнішньої (загальнодоступною) мережі. При підключенні віддаленого користувача (або під час активного з'єднання з іншого захищеною мережею) сервер доступу вимагає проходження процесу ідентифікації, а потім процесу аутентифікації. Після успішного проходження обох процесів віддалений користувач (віддалена мережа) наділяється повноваженнями для роботи в мережі, тобто відбувається процес авторизації.

6.6 Класифікація VPN

Класифікувати рішення VPN можна за кількома основними параметрами:

За ступенем захищеності використовуваного середовища:

Захищені

Найбільш поширений варіант віртуальних приватних мереж. З його допомогою можливо створити надійну і захищену мережу на основі ненадійної мережі, як правило, Інтернету. Прикладом захищених VPN є: IPSec, OpenVPN і PPTP.

Довірчі

Використовуються у випадках, коли передавальну середу можна вважати надійною і необхідно вирішити лише завдання створення віртуальної підмережі в рамках більшої мережі. Проблеми безпеки стають неактуальними. Прикладами подібних рішень VPN є: Multi-protocol label switching (MPLS) і L2TP (Layer 2 Tunnelling Protocol) (точніше буде сказати, що ці протоколи перекладають завдання забезпечення безпеки на інші, наприклад L2TP, як правило, використовується в парі з IPSec).

За способом реалізації

У вигляді спеціального програмно-апаратного забезпечення

Реалізація мережі VPN здійснюється за допомогою спеціального комплексу програмно-апаратних засобів. Така реалізація забезпечує високу продуктивність і, як правило, високий ступінь захищеності.

У вигляді програмного рішення

Використовують персональний комп'ютер зі спеціальним програмним забезпеченням, що забезпечує функціональність VPN.

Інтегроване рішення

Функціональність VPN забезпечує комплекс, вирішальний також завдання фільтрації мережевого трафіку, організації мережевого екрану і забезпечення якості обслуговування.

По призначенню

Intranet VPN

Використовують для об'єднання в єдину захищену мережу декількох розподілених філій однієї організації, які обмінюються даними по відкритих каналах зв'язку.

Remote Access VPN

Використовують для створення захищеного каналу між сегментом корпоративної мережі (центральним офісом або філією) і одиночним користувачем, який, працюючи вдома, підключається до корпоративних ресурсів з домашнього комп'ютера, корпоративного ноутбука, смартфона або інтернет-кіоску.

Extranet VPN

Використовують для мереж, до яких підключаються «зовнішні» користувачі (наприклад, замовники або клієнти). Рівень довіри до них набагато нижче, ніж до співробітників компанії, тому потрібне забезпечення спеціальних «рубежів» захисту, що запобігають або обмежують доступ останніх до особливо цінної, конфіденційної інформації.

Internet VPN

Використовується для надання доступу до інтернету провайдерами, зазвичай якщо по одному фізичному каналу підключаються кілька користувачів. Протокол PPPoE став стандартом в ADSL-підключення.

L2TP був широко поширений в середині 2000-х років в будинкових мережах: в ті часи внутрішньо трафік не оплачувалася, а зовнішній коштував дорого. Це давало можливість контролювати витрати: коли VPN-з'єднання вимкнено, користувач нічого не платить. В даний час (2012) провідний інтернет дешевий або безлімітний, а на стороні користувача часто є маршрутизатор, на якому вмикати-вимикати інтернет не так зручно, як на комп'ютері. Тому L2TP-доступ відходить в минуле.

Client / Server VPN

Він забезпечує захист переданих даних між двома вузлами (Не мережами) корпоративної мережі. Особливість даного варіанту в тому, що VPN будується між вузлами, що перебувають, як правило, в одному сегменті мережі, наприклад, між робочою станцією і сервером. Така необхідність дуже часто виникає в тих випадках, коли в одній фізичній мережі необхідно створити кілька логічних мереж. Наприклад, коли треба розділити трафік між

фінансовим департаментом та відділом кадрів, які звертаються до серверів, що знаходяться в одному фізичному сегменті. Цей варіант схожий на технологію VLAN, але замість поділу трафіку використовується його шифрування.

За типом протоколу

Існують реалізації віртуальних приватних мереж під TCP / IP, IPX і AppleTalk. Але на сьогоднішній день спостерігається тенденція до загального переходу на протокол TCP / IP, і абсолютна більшість рішень VPN підтримує саме його. Адресація в ньому найчастіше вибирається відповідно до стандарту RFC5735, з діапазону Приватних мереж TCP / IP.

За рівнем мережевого протоколу

За рівнем мережевого протоколу на основі зіставлення з рівнями еталонної мережевої моделі ISO / OSI.

Таким чином, VPN - це найбільш ефективна з усіх доступних простому користувачеві технологія для анонімної роботи в інтернеті на сьогоднішній день.

Лекція 7

7.1. Визначення IPSec

Віртуальна приватна мережа (VPN) забезпечує безпечний тунель через загальнодоступну і, отже, небезпечну мережу. Як відомо, VPN найчастіше використовується, надаючи користувачам доступ до електронної пошти, документів, принтерів і системам з їх домашньої мережі. І безпеку таких даних критично важлива.

IPSEC, скорочено IP Security, являє собою набір протоколів, стандартів і алгоритмів для захисту трафіку по ненадійною мережі, такий як Інтернет. IPsec підтримується практично всіма маршрутизаторами і дозволяє убезпечити дані в мережі.

IPsec надає служби безпеки на рівні IP, дозволяючи системі вибирати необхідні протоколи безпеки, визначати алгоритми, використовувані для служб, і вводити будь-які криптографічні ключі, необхідні для надання запитаних послуг. IPsec може використовуватися для захисту одного або декількох «шляхів» між двома хостами, між двома шлюзами безпеки або між шлюзом безпеки і хостом. (Термін «шлюз безпеки» використовується у всіх документах IPsec для посилання на проміжну систему, яка реалізує протоколи IPsec. Наприклад, маршрутизатор або брандмауер, який реалізує IPsec, є шлюзом безпеки.)

Набір служб безпеки, які може надавати IPsec, включає в себе контроль доступу , цілісність без встановлення з'єднання, аутентифікацію джерела даних, відмова від повторних пакетів (форма часткової цілісності послідовності), конфіденційність (шифрування) і обмеженість конфіденційності трафіку. Оскільки ці послуги надаються на рівні IP, вони можуть використовуватися будь-яким протоколом більш високого рівня, наприклад TCP, UDP, ICMP, BGP і т. д.

Конфіденційність: запобігає крадіжці даних, використовуючи шифрування.

Цілісність: гарантує, що дані не будуть змінені або замінені, використовуючи алгоритм хешування.

Аутентифікація: підтверджує особистість відправки даних хоста, використовуючи попередньо розділені ключі або центр сертифікації (CA).

- Anti-replay: запобігає дублюванню зашифрованих пакетів, підписуючи унікальний порядковий номер. IPsec DOI також підтримує узгодження IP-стиснення [SMPT98], мотивоване частково наглядом, що, коли шифрування використовується в IPsec, воно запобігає ефективному стисненню по більш низьким рівням протоколу.

7.2 Робота протоколу IPsec.

IPsec використовує два протоколи для забезпечення безпеки трафіку - Authentication Header (AH) і Encapsulating Security Payload (ESP)

IP Authentication Header (AH) забезпечує цілісність без встановлення з'єднання, аутентифікацію джерела даних і додаткову службу захисту від повтору.

AH використовує хеш-алгоритм для обчислення значення хеша як для корисного навантаження, так і для заголовка пакета, забезпечуючи цілісність пакета. Однак це викликає дуже специфічну проблему. AH не працюватиме через NAT-пристрій. NAT змінює IP-заголовок пакета під час перекладу, але значення хеша не змінюється. Таким чином, приймаючий пристрій буде вважати, що пакет був змінений при передачі і відхилив пакет.

Протокол Encapsulating Security Payload (ESP) може забезпечувати конфіденційність (шифрування) і обмежену конфіденційність трафіку. Він також може забезпечувати підключення. Він також може забезпечити цілісність без встановлення з'єднання, аутентифікацію джерела даних і службу захисту від повтору. (Один або інший набір цих служб безпеки повинен застосовуватися щоразу, коли викликається ESP.)

ESP виконує функції конфіденційності, аутентифікації і цілісності. Таким чином, ESP виконує шифрування і за своєю суттю більш безпечний, ніж AH. ESP вводить в пакет як додатковий заголовок, так і трейлер. ESP також використовує алгоритм хешування для цілісності даних. Однак хеш не включає IP-заголовок пакета, і, таким чином, ESP буде (зазвичай) працювати через NAT-пристрій.

Обидва AH і ESP є транспортними засобами для контролю доступу на основі розподілу криптографічних ключів та управління потоками трафіку по відношенню до цих протоколів безпеки.

Ці протоколи можуть застосовуватися окремо або в поєднанні один з одним для забезпечення необхідного набору служб безпеки в IPv4 і IPv6. Кожен протокол має два режими: транспортний і режим тунелю. У транспортному режимі протоколи забезпечують захист в основному для

протоколів верхнього рівня; в тунельному режимі протоколи застосовуються до тунельованих IP-пакетів.

IPsec дозволяє користувачеві (або системного адміністратора) контролювати ступінь деталізації, в якій пропонується служба безпеки. Наприклад, можна створити один зашифрований тунель для перенесення всього трафіку між двома шлюзами безпеки або окремий зашифрований тунель, який може бути створений для кожного TCP-з'єднання між кожною парою хостів, взаємодіючих через ці шлюзи. Керівництво IPsec має включати кошти для вказівки:

- які служби безпеки використовувати і в яких комбінаціях
- гранулярность, при якій повинна застосовуватися дана захист
- алгоритми, використовувані для забезпечення криптографічної безпеки

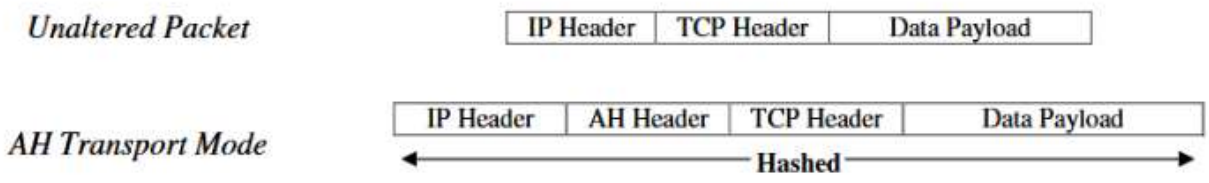
Оскільки ці служби безпеки використовують загальні секретні значення (криптографічні ключі), IPsec спирається на окремий набір механізмів для розміщення цих ключів. (Ці ключі використовуються для служб аутентифікації / цілісності і шифрування.) Цей документ вимагає підтримки як ручного, так і автоматичного розподілу ключів. Він визначає конкретний підхід на основі відкритого ключа для автоматичного управління ключами, але можуть використовуватися інші автоматизовані методи поширення ключів. Наприклад, можна використовувати системи на основі KDC, такі як Kerberos і інші системи з відкритим ключем, такі як SKIP.

Кожен протокол IPSEC (AH або ESP) може працювати в одному з двох режимів:

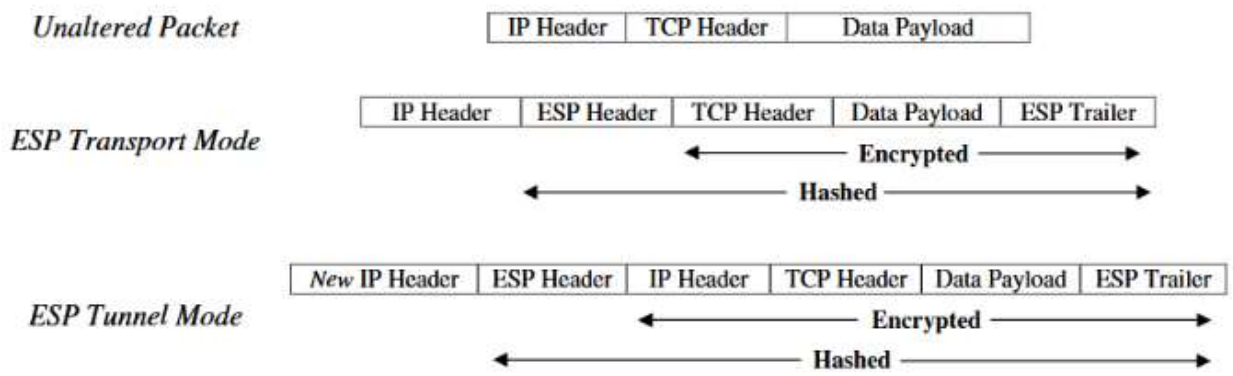
• Режим транспорту. Вихідні IP-заголовки залишаються недоторканими. Використовується при забезпеченні зв'язку з одного пристрою на інший один пристрій.

• Режим тунелю - весь вихідний пакет хешіруется і / або шифрується, включаючи як корисне навантаження, так і будь-які вихідні заголовки. Під час транзиту до пакету застосовується тимчасовий IP-заголовок.

Нижче показано, як AH змінює IP-пакет:



Нижче показано, як ESP змінює IP-пакет:



ESP в режимі тунелю зазнає труднощів NAT, подібні AH. Це може бути полегшено шляхом реалізації NAT Traversal (NAT-T).

7.3 Сфери застосування IPsec

Існує кілька способів реалізації IPsec на хості або в поєднанні з маршрутизатором або брандмауером (для створення шлюзу безпеки). Нижче наведено кілька загальних прикладів:

a. Інтеграція IPsec в власну реалізацію IP. Для цього потрібен доступ до вихідного коду IP і застосуємо як до хостів, так і до шлюзів безпеки.

b. Реалізації «Bump-in-the-stack» (BITS), де IPsec реалізується «під» існуючої реалізацією стека протоколів IP, між власним IP-адресою і драйверами локальної мережі. Доступ до вихідного коду для IP-стека не потрібно в цьому контексті, роблячи цей підхід впровадження відповідним для використання з застарілими системами. Такий підхід, коли він прийнятий, зазвичай використовується на хостах.

c. Використання зовнішнього кріптопроцессора є спільною конструктивною особливістю систем мережевої безпеки, які використовуються військовими, і деяких комерційних систем. Його іноді називають реалізацією «Bump-in-the-wire» (BITW). Такі реалізації можуть бути призначені для обслуговування хоста або шлюзу (або обох). Зазвичай пристрій BITW є IP-адресою. За підтримки одного хоста він може бути аналогічний реалізації BITS, але за підтримки маршрутизатора або брандмауера він повинен працювати як шлюз безпеки.

7.4 Конфіденційність і шифрування

Дані, надіслані в текстовому вигляді через Інтернет, можуть бути легко перехоплені і вкрадені. Через це конфіденційні дані повинні бути зашифровані при відправленні через ненадійну мережу або домен.

Клавіші генерують значення, що використовуються для шифрування і дешифрування даних. Чим довше ключ, тим він безпечніший. Довжина ключа вимірюється в бітах. Існують два типи ключів: симетричні і асиметричні.

Симетричні ключі можуть використовуватися як для шифрування, так і для дешифрування даних. Більш конкретно, той же ключ використовується як для шифрування пакету (на відправляє пристрої), так і для дешифрування цього пакета (на приймаючому пристрої). Симетричне шифрування ключів є ефективним, але не дуже добре масштабується в великих середовищах.

Для асиметричних ключів потрібен окремий ключ для шифрування (відкритий ключ) і дешифрування (закритий ключ). Відкриті ключі відкрито обмінюються між пристроями для шифрування даних під час передачі. Приватні ключі ніколи не обмінюються.

Розглянемо діаграму на рис 7.1.

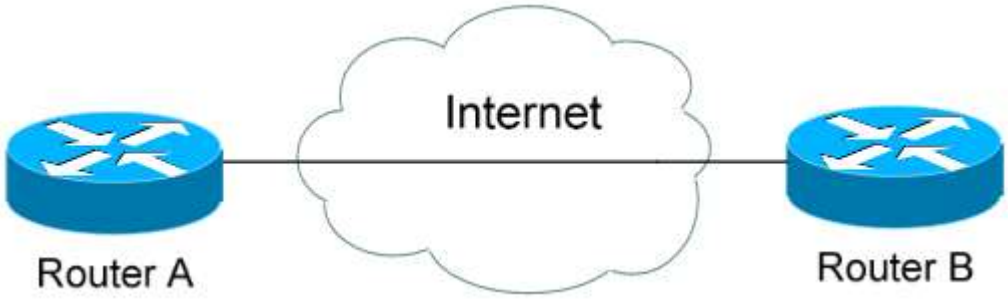


Рис. 7.1 Обмін інформацією між маршрутизаторами

Припустимо, що ми використовуємо інфраструктуру відкритого / закритого ключа:

• Обидва маршрутизатора A і Router B мають свій власний закритий ключ.

• Обидва маршрутизатора A і Router B обмінюються унікальними відкритими ключами.

• Коли Router B шифрує дані, призначені для маршрутизатора A, він використовує відкритий ключ Router A. (і навпаки)

• Маршрутизатор A розшифровує дані, використовуючи свій закритий ключ. Тільки приватні ключі можуть розшифрувати дані. Таким чином, навіть якщо дані і відкритий ключ були перехоплені, забезпечується конфіденційність.

7.6 Асоціації IKE і IPSEC

Прихильники IPSEC VPN встановлюють Security Association (SA), «з'єднання» або «політику» між двома кінцевими точками тунелю VPN. SA є одностороннім тунелем між однорангових мережами VPN.

Таким чином, для забезпечення повної зв'язку необхідно встановити два SA, по одному для кожного напрямку. Перш ніж SA може бути встановлена,

необхідно узгодити кілька параметрів між однорангових вузлами VPN, і ключі повинні бути створені і обмінюватися. Протокол обміну ключами Інтернету (IKE) управляє цим процесом переговорів, на порте 500UUDP.

Набори політик IKE створюються для узгодження декількох параметрів, в тому числі:

- Алгоритм шифрування (наприклад, DES, 3DES або AES)
- Хешірующій алгоритм (такий як MD5 або SHA-1)
- Метод аутентифікації (наприклад, загальні ключі або підпису RSA)
- Група Diffie-Hellman (DH) для створення та обміну ключами
- Термін служби SA, який вимірюється в секундах або в кілобайтах

Політики IKE часто називаються політиками інтернет-безпеки і політикою управління ключами (ISAKMP). Кілька політик IKE можуть бути створені на тимчасовій мережі VPN. Під час процесу узгодження VPN-вузли поділяють список налаштованих політик IKE. SA буде створена тільки в тому випадку, якщо між однолітками існує точна політика відповідності.

7.7 П'ять кроків IPSEC

Функцію IPSEC можна описати в п'ять етапів:

1. Будь-який трафік, який повинен бути захищений і відправлений через тунель, ідентифікується як цікавий трафік, зазвичай використовуючи список доступу.

2.IKE (обмін ключами через Інтернет) Етап 1 ініційований. Аутентифікація між перами перевіряється, ключі обмінюються, і набори політик IKE дозволені. У разі успіху створюється IKE SA.

3.IKE (обмін ключами через Інтернет) Етап 2 ініційований. IPSEC TransformSets узгоджуються, і в разі успіху створюється IPSEC SA.

4. Фактично дані передаються з використанням узгодженої політики небезпеки.

5. Сеанс зривається після закінчення терміну життя SA. SA буде створена тільки в тому випадку, якщо між однолітками існує точна політика відповідності