Безпека операційних систем і комп'ютерних мереж

Лекція 13

Особливості розподілених систем і Інтернету з міркувань безпеки

Мережні, або віддалені атаки

- Розподіл ресурсів та інформації у просторі робить можливим специфічний вид атак — так звані *мережні*, або *віддалені* атаки (англ. — *network attacks*, *remote attacks*).
  - Під віддаленою атакою розуміють атаку на розподілену обчислювальну систему, що здійснюється програмними засобами по каналах зв'язку
  - Така атака може здійснюватись як на протоколи і мережні служби, так і на операційні системи і прикладні програми вузлів мережі
- Атаки на протоколи:
  - Інформаційний обмін у мережі здійснюється за допомогою механізму повідомлень
  - Людина практично не бере участі в штатному функціонуванні мережі
    - У вузлах мережі знаходяться апаратні і програмні засоби, які діють автоматично, без втручання оператора
  - Засоби, що забезпечують інформаційний обмін, повинні відповідати на повідомлення-запити, які надходять з мережі і регламентуються протоколами взаємодії
  - Спеціальним чином створені запити можуть викликати такі відповіді автоматичних засобів, які призведуть до порушення політики безпеки
- Атаки на дані:
  - Атаки, що спрямовані на інформацію, що передається мережею

Особливості Інтернету

- Мережа Інтернет доступна
- Мережа має глобальний масштаб
- В Інтернеті присутні і активно діють численні зловмисники
  - професіонали
  - допитливі підлітки, які знайшли інструменти злому (відповідне програмне забезпечення доступне в мережі) і тепер намагаються їх випробувати
- В глобальній мережі одночасно діють представники:
  - кримінальних структур
  - різних політичних партій і течій
  - правоохоронних органів і спецслужб різних країн
- Атака на систему, що підключена до мережі, може бути мотивована матеріально чи політично
- Зловмисники, навіть якщо вдасться їх вистежити, можуть знаходитись у іншому правовому полі (в іншій державі) і бути недосяжними для покарання

Типові атаки на розподілені системи

- Джерело: **IT Baseline Protection Manual — BSI** (Federal Agency for Security in Information Technology, Germany) — October 2000
- В якості типових атак, які можуть застосовуватись для нападу на розподілені системи, і які слід моделювати під час випробувань стійкості систем до атак, названі такі:
  - вгадування паролів або атаки за словником;
  - реєстрація і маніпуляції з мережним трафіком;
  - імпорт фальшивих пакетів даних;
  - експлуатація відомих уразливостей програмного забезпечення (мови макросів, помилки в ОС, служби віддаленого доступу тощо).

Типові атаки на розподілені системи (інша точка зору)

- Джерело: ***Медведовский И. Д., Семьянов П. В., Леонов Д. Г.*** **Атака на Internet. – 2-е изд. – М.: ДМК, 1999. – 336 с.**
- Як типові віддалені атаки автори виділяють такі:
  - аналіз мережного трафіка;
  - підміна довіреного об’єкта в розподіленій системі;
  - впровадження в розподілену систему фальшивого об’єкта через нав’язування фальшивого маршруту;
  - впровадження в розподілену систему фальшивого об’єкта шляхом використання недоліків алгоритмів віддаленого пошуку;
  - відмова в обслуговуванні.

Причини уразливості розподілених систем

- Фахівці називають такі причини, через які розподілені системи можуть бути уразливими:
  - використання спільного середовища передачі (наприклад, Ethernet, радіоканал);
  - застосування нестійких алгоритмів ідентифікації віддалених активних і пасивних об’єктів;
  - використання протоколів динамічної (адаптивної) маршрутизації;
  - застосування алгоритмів віддаленого пошуку;
  - можливість анонімного захоплення активним об’єктом багатьох фізичних або логічних каналів зв’язку.
- Джерело: ***Медведовский И. Д., Семьянов П. В., Леонов Д. Г.*** **Атака на Internet. – 2-е изд. – М.: ДМК, 1999. – 336 с.**

Базові документи у сфері захисту розподілених систем

- ISO/IEC 7498-2:1989, Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture
- CCITT Recommendation X.800, Security Architecture for Open Systems Interconnection for CCITT Applications. – CCITT: Geneva – 1991
  - CCITT – The International Telegraph and Telephone Consultative Committee; тепер називають ITU-T
  - Рекомендації X.800 узгоджені зі стандартом ISO/IEC 7498-2
- IT Baseline Protection Manual. – BSI (Federal Agency for Security in Information Technology) – October 2000

Подальший розвиток міжнародних стандартів

- ISO/IEC 10745 та ITU-T X.803 “Upper Layers Security Model”
- ISO/IEC 13594 та ITU-T X.802 “Lower Layers Security Model”
- ISO/IEC 10181-1 та ITU-T X.810 “Security Frameworks for open systems, Part 1: Overview”
- ISO/IEC 10181-2 та ITU-T X.811 “Security frameworks for open systems, Part 2: Authentication framework”
- ISO/IEC 10181-3 та ITU-T X.812 “Security frameworks for open systems, Part 3: Access control framework”
- ISO/IEC 10181-4 та ITU-T X.813 “Security frameworks for open systems, Part 4: Non-repudiation framework”
- ISO/IEC 10181-5 та ITU-T X.814 “Security frameworks for open systems, Part 5: Confidentiality framework”
- ISO/IEC 10181-6 та ITU-T X.815 “Security frameworks for open systems, Part 6: Integrity framework”
- ISO/IEC 10181-7 та ITU-T X.816 “Security frameworks for open systems, Part 7: Security audit framework”

Сервіси безпеки

- Рекомендації X.800 виділяють такі функції (сервіси) безпеки:
  - автентифікація;
  - керування доступом;
  - конфіденційність даних;
  - цілісність даних;
  - невідмовлюваність, або неспростовність (non-repudiation)

Автентифікація

- Цей сервіс забезпечує автентифікацію сторін, що спілкуються (communicating peer entity), і автентифікацію джерела даних
- Автентифікація сторін
  - Застосовується в момент встановлення з'єднання, а також іноді під час передачі даних, для підтвердження автентичності сутностей з'єднання
  - Цей сервіс у момент його використання забезпечує впевненість у тому, що суб'єкт не використовує "маскарад" або несанкціоноване повторення попереднього сеансу зв'язку
  - Можуть застосовуватись різні схеми автентифікації, що забезпечують різний ступінь захисту
- Автентифікація джерела даних
  - Це підтвердження автентичності джерела блоку даних
  - Сервіс, який реалізується засобами певного рівня моделі OSI, надається для сутностей вищого рівня і підтверджує автентичність сутності також вищого рівня
  - Цей сервіс не забезпечує захист від повторення або пошкодження даних

Керування доступом

- Цей сервіс забезпечує захист від несанкціонованого використання ресурсів, доступних через взаємодію відкритих систем
- Керування доступом може застосовуватись до різних типів доступу до ресурсу
  - використання комунікаційного ресурсу,
  - зчитування,
  - записування,
  - видалення інформаційного ресурсу,
  - виконання ресурсу обробки

Конфіденційність даних

- Ці сервіси забезпечують захист даних від несанкціонованого розкриття
- Розрізняють кілька сервісів конфіденційності даних:
  - конфіденційність даних при обміні з встановленням з'єднання
    - цей сервіс захищає всю інформацію користувачів, але може (в залежності від рівня моделі OSI) не захищати інформацію запиту на встановлення з'єднання
  - конфіденційність даних при обміні без встановлення з'єднання
    - цей сервіс захищає всю інформацію користувачів;
  - конфіденційність окремих полів даних
    - цей сервіс забезпечує захист інформації в окремих обраних полях даних у сеансі з встановленням або без встановлення з'єднання;
  - конфіденційність трафіка
    - цей сервіс забезпечує захист тієї інформації, яку можна здобути під час аналізу трафіка

Цілісність даних

- Ці сервіси спрямовані на протидію активним загрозам
- Розрізняють такі сервіси цілісності даних:
  - цілісність даних при обміні з встановленням з'єднання з відновленням
    - цей сервіс забезпечує цілісність усіх даних користувача при обміні з встановленням з'єднання;
    - він може полягати у виявленні будь-якої модифікації, додавання, видалення або повторення будь-яких даних і здійснює спробу відновити дані;
  - цілісність даних при обміні з встановленням з'єднання без відновлення
    - те ж саме, що й попередній сервіс, але без спроби відновлення;
  - цілісність окремих полів даних при обміні зі встановленням з'єднання
    - цей сервіс забезпечує цілісність окремих обраних полів даних у сеансі з встановленням з'єднання, і визначає, чи були ці поля модифіковані, додані, видалені або повторені;
  - цілісність даних при обміні без встановлення з'єднання
    - цей сервіс на відміну від попередніх при реалізації на певному рівні моделі OSI забезпечує гарантії цілісності даних за запитом сутності вищого рівня;
    - сервіс забезпечує цілісність окремого блоку даних, що передається без встановлення з'єднання, і може полягати у визначенні, чи був блок даних модифікованим;
    - також додатково може забезпечуватись обмежена форма виявлення повторення;
  - цілісність окремих полів даних при обміні без встановлення з'єднання
    - цей сервіс забезпечує цілісність окремих обраних полів у окремому блоці даних, що передається без встановлення з'єднання, і полягає у визначенні, чи були обрані поля модифікованими

Невідмовлюваність (non-repudiation)

- Цей сервіс (унеможливлення відмови від вчинених дій) має дві форми, які можуть забезпечуватись кожна окремо або обидві разом:
  - Невідмовлюваність з підтвердженням справжності джерела даних
    - цей сервіс надає одержувачу даних підтвердження їхнього джерела, що захищає від будь-якої спроби відправника відмовитись від факту відправлення даних чи справжності (вірогідності) їхнього вмісту;
  - Невідмовлюваність з підтвердженням доставки
    - цей сервіс надає відправнику даних підтвердження доставки даних, що захищає від будь-якої спроби одержувача відмовитись від факту одержання цих даних або їхнього вмісту

Розподіл сервісів безпеки по рівнях моделі ISO

Сервіс	Рівень						
	1	2	3	4	5	6	7
Автентифікація сторін			+	+			+
Автентифікація джерела даних			+	+			+
Керування доступом			+	+			+
Конфіденційність даних при обміні з встановленням з’єднання	+	+	+	+		+	+
Конфіденційність даних при обміні без встановлення з’єднання		+	+	+		+	+
Конфіденційність окремих полів даних						+	+
Конфіденційність трафіка	+		+				+
Цілісність даних при обміні з встановленням з’єднання з відновленням				+			+
Цілісність даних при обміні з встановленням з’єднання без відновлення			+	+			+
Цілісність окремих полів даних при обміні з встановленням з’єднання							+
Цілісність даних при обміні без встановлення з’єднання			+	+			+
Цілісність окремих полів даних при обміні без встановлення з’єднання							+
Невідмовлюваність з підтвердженням справжності джерела даних							+

Специфічні механізми безпеки

- Для реалізації деяких сервісів безпеки на певному рівні моделі OSI можуть впроваджуватись такі механізми:
  - шифрування;
  - цифровий підпис;
  - керування доступом;
  - контроль цілісності даних;
  - автентифікаційний обмін;
  - заповнення трафіка;
  - керування маршрутом;
  - нотаризація.

Шифрування (Encipherment)

- Шифрування може захищати окремі дані або потік даних (шифрування трафіка) і може використовуватись іншими механізмами або заміняти деякі інші механізми
- Можуть застосовуватись оборотні та необоротні алгоритми шифрування, а з числа оборотних алгоритмів — симетричні й асиметричні
- Необоротні алгоритми можуть використовувати або не використовувати ключі, причому якщо ключ застосовується, він може бути і відкритим, і приватним
- Впровадження алгоритму шифрування майже завжди передбачає також впровадження механізму керування ключами (за винятком деяких необоротних алгоритмів)

Цифровий підпис

- Механізми цифрового підпису визначають дві процедури:
  - підписування блоку даних;
  - перевірку підписаного блоку даних.
- Процедура підписування блоку даних
  - використовує приватну (унікальну і конфіденційну) інформацію того, хто підписує
  - використовує або шифрування блоку даних, або обчислення криптографічної контрольної суми з використанням приватної інформації користувача, що здійснює підпис
- Процедура перевірки підписаного блоку даних
  - використовує процедури і інформацію, які є загальнодоступними, але з яких неможливо знайти приватну інформацію про того, хто підписує
  - фактично, дозволяє перевірити, чи справді цифровий підпис було зроблено з використанням приватної інформації того, хто підписав блок даних

Керування доступом (1/3)

- Ці механізми можуть використовувати для визначення і встановлення прав доступу сутності
  - ідентифікацію сутності
  - або деяку інформацію про сутність (як належність до деякої відомої чисельності сутностей)
  - або посвідчення, пред'явлене сутністю
- Якщо сутність намагається здійснити неавторизований (несанкціонований) доступ (використати неавторизований ресурс, або використати недозволений метод доступу до авторизованого ресурсу), функція керування доступом перешкодить здійсненню такого доступу і, можливо, згенерує повідомлення про інцидент (для ініціювання протидії або з метою аудиту)

Керування доступом (2/3)

- Механізми керування доступом можуть використовувати один чи кілька із зазначених далі видів та джерел інформації:
  - бази даних керування доступом, в яких зберігаються права доступу сутностей
    - ці бази можуть підтримуватись централізовано або на кінцевих системах
    - права доступу можуть зберігатись у вигляді списків керування доступом або матриці ієрархічної чи розподіленої структури
      - використання бази даних керування доступом передбачає, що сутності перед цим були автентифіковані
  - інформація автентифікації, володіння якою і надання якої є доказом авторизації
    - наприклад, паролі
  - посвідчення, володіння якими і пред'явлення яких є доказом дозволу доступу до сутності або ресурсу, які вказані у посвідченні
  - мітки безпеки, асоційовані з сутностями (суб'єктами та об'єктами доступу), які можуть використовуватись для надання або заборони доступу, як правило, на основі політики безпеки;
  - час спроби доступу
  - маршрут спроби доступу
  - тривалість спроби доступу

Керування доступом (3/3)

- Механізми керування доступом можуть бути задіяні на будь-якій із сторін, що здійснюють зв’язок, або в проміжній точці
  - Механізми, що задіяні у точці, яка ініціює доступ, і у проміжних точках, повинні перевіряти, чи відправник авторизований для зв’язку з одержувачем та/або для використання комунікаційних ресурсів
  - У разі зв’язку без встановлення з’єднання вимоги механізму, що реалізований у кінцевій точці, повинні бути апріорі відомими у точці, що ініціює доступ

Контроль цілісності даних

- Існують два аспекти цілісності:
  - цілісність окремого блоку даних або поля інформації
  - цілісність потоку блоків даних або полів інформації
- Для забезпечення цих двох видів сервісу цілісності у загальному випадку бувають задіяні різні механізми
  - контроль цілісності потоку без контролю окремих блоків даних (полів) не є практичним
- Процедура контролю цілісності окремого блоку даних (поля) включає в себе два процеси
  - Один на стороні, що передає, другий — на тій, що приймає
  - На стороні, що передає, до блоку даних додається інформація, яка є функцією від цього блоку даних (циклічна або криптографічна контрольна сума, яка може також бути зашифрованою)
  - На стороні, що приймає, генерується аналогічна контрольна сума, що потім порівнюється з одержаною
  - Цей механізм сам не захищає від повторення блоків даних
- Перевірка цілісності потоку блоків даних (тобто захист від втрати, перевпорядкування, дублювання, вставлення та модифікації даних) вимагає додаткового впровадження порядкових номерів, часових штампів або криптографічного зв’язування (коли результат шифрування чергового блоку залежить від попереднього).
  - При зв’язку без встановлення з’єднання використання часових штампів може забезпечити обмежений захист від дублювання блоків даних

Автентифікаційний обмін

- Механізми автентифікаційного обміну впроваджуються на певний рівень моделі OSI для підтвердження автентичності сторони (сутності)
  - Якщо механізм не підтверджує автентичність сутності, здійснюється
    - заборона з'єднання
    - або закриття вже встановленого з'єднання
    - а також, можливо, генерується повідомлення про інцидент (для ініціювання протидії або з метою аудиту).
- Для здійснення автентифікаційного обміну можуть застосовуватись деякі з таких методів:
  - використання автентифікаційної інформації (такої як паролі), яку надає відправник і перевіряє одержувач;
  - криптографічні методи;
  - демонстрація характеристик або можливостей сутності.
- При використанні криптографічних методів вони можуть поєднуватись з протоколами "рукостискання" для протидії повторенню даних.
- Методи автентифікаційного обміну в залежності від обставин можуть використовуватись разом з:
  - часовими штампами і синхронізацією годинників;
  - двох- і трьохстадійними процедурами "рукостискання" (для односторонньої і двохсторонньої автентифікації, відповідно);
  - сервісами невідмовлюваності, що досягаються механізмами цифрового підпису та/або нотаризації.

Заповнення трафіка

- Механізми заповнення трафіка застосовуються для забезпечення різних рівнів захисту від аналізу трафіка
- Ці механізми ефективні лише у поєднанні із засобами забезпечення конфіденційності

Керування маршрутом

- Маршрути можуть обиратись динамічно або статично таким чином, щоб використовувати лише фізично безпечні підмережі, вузли комутації та канали
- Кінцеві системи у разі виявлення неодноразових атак на деякому маршруті можуть звертатись до провайдера мережних послуг для встановлення з’єднання за іншим маршрутом
- Передача даних, що мають мітки безпеки, через певні підмережі, вузли комутації та канали може бути заборонена політикою безпеки
- Ініціатор з’єднання, або відправник даних, що передаються без встановлення з’єднання, може вказати обмеження на маршрут, щоби уникати певних підмереж, вузлів комутації та каналів

Нотаризація

- Механізм нотаризації забезпечує завірення таких характеристик даних, що передаються між двома (або більше) сутностями, як
  - цілісність,
  - джерело,
  - час,
  - призначення.
- Завірення забезпечується третьою стороною, якій довіряють сутності, що взаємодіють, і яка має достатню інформацію, щоб її завіренням можна було довіряти
- Кожна сутність, що взаємодіє із застосуванням механізму нотаризації, використовує цифровий підпис, шифрування і контроль цілісності

Універсальні механізми безпеки

- Раніше були названі механізми безпеки, специфічні для певних сервісів чи рівнів моделі OSI
- Крім цього, рекомендації X.800 визначають універсальні, або, як вони були названі, *всеохоплюючі* (*pervasive*) механізми безпеки
- До них віднесені:
  - довірена функціональність;
  - мітки безпеки;
  - детектування подій;
  - аудит безпеки;
  - відновлення безпеки.

Довірена функціональність

- Будь-яка функціональність, що безпосередньо забезпечує механізми безпеки або надає доступ до таких механізмів, повинна бути довіреною
- Процедури, які застосовуються для підтвердження, що апаратні та/або програмні компоненти дійсно заслуговують довіри, знаходяться поза межами Рекомендацій X.800

Мітки безпеки

- Ресурси, що включають дані, можуть мати асоційовані з ними мітки безпеки
- Найтиповіше використання міток безпеки — визначення через них рівня чутливості (наприклад, конфіденційності даних)

Детектування подій

- Детектування подій, що пов’язані з безпекою, включає детектування явних порушень безпеки
  - може також включати детектування “нормальних” подій, таких як
    - успішні входи в систему
    - доступи до об’єктів
- Детектування різних подій, що пов’язані з безпекою, може спричиняти одну або кілька із зазначених дій:
  - локальне інформування про подію;
  - віддалене інформування про подію;
  - реєстрація події у журналі;
  - дія по відновленню.

Аудит безпеки

- Аудит безпеки — це незалежний огляд і аналіз системних записів і дій з метою перевірки
  - адекватності керування системою,
  - відповідності до встановленої політики і процедур,
  - оцінки завданих пошкоджень,
  - а також для рекомендацій стосовно змін у керуванні, політиці і процедурах.
- Аудит безпеки вимагає запису інформації, що має відношення до безпеки, у протокол аудиту
  - Реєстрація і запис інформації відноситься до механізмів безпеки
  - Аналіз і генерація звітів відноситься до функцій керування безпекою

Відновлення безпеки

- Відновлення безпеки обробляє запити від таких механізмів як обробка подій і виконує дії по відновленню як результат застосування набору правил
- Дії по відновленню можуть бути трьох типів:
  - миттєві
    - наприклад, миттєве відключення чи розрив з'єднання
  - тимчасові
    - наприклад, тимчасове блокування деякої сутності
  - тривалі
    - наприклад, занесення сутності у "чорний список" або зміна ключової інформації

Взаємозв’язок сервісів і механізмів безпеки (1/2)

Сервіс	**Механізм**							
	Шифрування	Цифровий підпис	Керування доступом	Цілісність даних	Автентифікаційний обмін	Заповнення трафіка	Керування маршрутом	Нотаризація
Автентифікація сторін	+	+			+			
Автентифікація джерела даних	+	+						
Керування доступом			+					
Конфіденційність даних при обміні з встановленням з’єднання	+						+	
Конфіденційність даних при обміні без встановлення з’єднання	+						+	
Конфіденційність окремих полів даних	+							
Конфіденційність трафіка	+					+	+	
Цілісність даних при обміні з встановленням з’єднання з відновленням	+			+				

Взаємозв’язок сервісів і механізмів безпеки (2/2)

Сервіс	**Механізм**							
	Шифрування	Цифровий підпис	Керування доступом	Цілісність даних	Автентифікаційний обмін	Заповнення трафіка	Керування маршрутом	Нотаризація
Цілісність даних при обміні з встановленням з’єднання без відновлення	+			+				
Цілісність окремих полів даних при обміні з встановленням з’єднання	+			+				
Цілісність даних при обміні без встановлення з’єднання	+	+		+				
Цілісність окремих полів даних при обміні без встановлення з’єднання	+	+		+				
Невідмовлюваність з підтвердженням справжності джерела даних		+		+				+
Невідмовлюваність з підтвердженням доставки		+		+				+

Керування безпекою (1/4)

- У загальному випадку в розподіленій системі можуть бути впроваджені різні політики безпеки
- Ті сутності, для яких встановлена єдина політика безпеки і які знаходяться під єдиним адміністративним керуванням, можуть поєднуватись у так званий “домен безпеки” (Security Domain)
- Адміністрування безпеки взаємодії відкритих систем включає в себе поширення інформації, яка необхідна для роботи сервісів та механізмів безпеки, а також збирання та аналіз інформації про їх функціонування
  - Прикладами можуть бути
    - розповсюдження криптографічних ключів,
    - установка параметрів захисту,
    - реєстрація звичайних та надзвичайних подій безпеки,
    - активація та деактивація сервісів тощо.

Керування безпекою (2/4)

- Концептуальною основою адміністрування безпеки є інформаційна база керування безпекою (Security Management Information Base, SMIB)
  - Ця база не обов'язково існує у вигляді єдиного або розподіленого сховища, але кожна з кінцевих систем повинна мати інформацію, що необхідна для реалізації обраної політики безпеки
- SMIB може реалізовуватись у вигляді:
  - таблиці даних;
  - файла;
  - даних або правил, що впроваджені у програмне забезпечення.
- Керування безпекою може вимагати обміну даними, що стосуються безпеки, між різними системами
  - Усі протоколи керування, а особливо протоколи керування безпекою, а також комунікаційні канали, якими здійснюється обмін, є потенційно уразливими
  - Це вимагає особливої уваги до захисту протоколів керування

Керування безпекою (3/4)

- Визначені три категорії дій у керуванні безпекою взаємодії відкритих систем:
  - адміністрування системи у цілому;
  - адміністрування сервісів безпеки;
  - адміністрування механізмів безпеки.
- Адміністрування сервісів безпеки включає такі типові дії:
  - визначення об’єктів, що підлягають захисту конкретним сервісом;
  - визначення і підтримка правил підбирання механізмів безпеки (при наявності альтернатив) для забезпечення потрібного сервісу безпеки;
  - взаємодія з іншими адміністраторами стосовно механізмів безпеки, які вимагають узгоджених дій;
  - взаємодія з іншими функціями адміністрування сервісів безпеки та функціями адміністрування механізмів безпеки.

Керування безпекою (4/4)

- Дії з адміністрування механізмів безпеки визначаються переліком задіяних механізмів
- Типовий, але не вичерпний, список такий:
  - керування ключами;
  - керування шифруванням;
  - керування механізмом цифрового підпису;
  - керування параметрами доступу;
  - керування цілісністю даних;
  - керування автентифікацією;
  - керування заповненням трафіка;
  - керування маршрутизацією;
  - керування нотаризацією.