Безпека операційних систем і комп'ютерних мереж

Лекція 3

Розроблення захищених ОС

Поняття захищеної операційної системи

- Будемо вважати захищеною таку ОС, яка передбачає захист від основних загроз:
  - Сканування файлової системи
  - Викрадення ключової інформації
  - Підбирання паролів
  - Збирання сміття
  - Перевищення повноважень
  - Програмних закладок
  - Жадібних програм

Підходи до побудови захищених операційних систем

- Розроблення захищених систем “з нуля”
- Побудова так званих “довірених” (trusted) версій шляхом модернізації існуючих систем

Розроблення захищених систем “з нуля”

- При розробці захищених систем “з нуля” на етапі проектування закладаються усі функціональні можливості та архітектурні рішення, що розраховані на сертифікацію за встановленим класом вимог
- Головною рисою цього підходу є розробка методів гарантованої реалізації встановлених вимог
- Застосовується класична схема проектування захищених систем:
  - визначення вимог безпеки;
  - розробка моделі безпеки;
  - визначення об’єктів взаємодії;
  - визначення правил керування доступом;
  - вибір механізмів керування доступом;
  - вибір методів ідентифікації й автентифікації сторін, що взаємодіють;
  - визначення множини подій, що підлягають аудиту;
  - реалізація системи.

Побудова “довірених” версій шляхом модернізації існуючих систем

- При побудові “довірених” версій шляхом модернізації існуючих систем, як правило:
  - додають функції шифрування і цифрового підпису,
  - підсилюють керування доступом шляхом впровадження мандатного керування,
  - розподіляють обов’язки адміністратора системи між різними обліковими записами або “ролями”,
  - впроваджують додаткові засоби ідентифікації й автентифікації, аудиту та моніторингу.

Порівняння підходів до побудови захищених операційних систем

- Прикладів розроблення захищених систем “з нуля” небагато через складність і значну вартість проведення таких робіт
  - Лише таким чином вдавалося створити системи, які в подальшому були сертифіковані на відповідність найвищим класам вимог: Trusted Xenix, Trusted Mach, Harris CX/SX, XTS 300 STOP
- Перевагою побудови “довірених” версій шляхом модернізації існуючих систем є економічна ефективність
  - Вона зумовлена меншим обсягом робіт з розробки та реалізації системи, а також можливістю збереження сумісності з існуючими рішеннями
  - Модернізовані системи наслідують імідж систем-прототипів, а це підвищує довіру до них за рахунок відомості фірм-розробників, дозволяє використати наявний досвід експлуатації й супроводження
  - Удосконалення існуючих систем може привести лише до обмежених результатів у досягненні безпеки інформації
  - Типовими прикладами такого підходу є ОС Trusted Solaris, СКБД Trusted Oracle
- Обидва підходи не суперечать один одному, а є рівноправними складовими технології побудови захищених ІКС

Принципи створення захищених систем

- Принцип інтегрованості
- Принцип інваріантності
- Принцип уніфікації
- Принцип адекватності
- Принцип коректності

Принцип інтегрованості

- Засоби захисту повинні бути вбудовані в систему таким чином, щоби усі без виключення механізми взаємодії знаходились під їх контролем
  - Найпростішим методом, що реалізує цей принцип при створенні ОС, є максимальне обмеження числа механізмів взаємодії та інтеграція засобів захисту безпосередньо в ці механізми

Принцип інваріантності

- Засоби захисту не повинні залежати від особливостей реалізації утиліт і прикладних програм, і не повинні враховувати логіку їх функціонування
- Засоби захисту повинні бути універсальними для усіх типів взаємодій
  - Для ОС інваріантність засобів захисту може бути досягнута шляхом застосування строго регламентованої парадигми функціонування програм, що обмежує способи взаємодій

Принцип уніфікації

- Засоби захисту мають бути універсальними, що дозволяє використовувати їх без змін як для реалізації різних моделей безпеки, так і для керування доступом до об’єктів різної природи
  - Повинна існувати однозначна відповідність між взаємодіями суб’єктів і об’єктів, що контролюються, та операціями доступу, керування якими описується моделями безпеки
  - При розробленні ОС слідування цьому принципу приводить до необхідності створення універсального інтерфейсу доступу, що об’єднує всі способи взаємодій між суб’єктами й об’єктами, всі функції якого однозначним чином відображаються на множину операцій, що описуються моделлю безпеки

Принцип адекватності

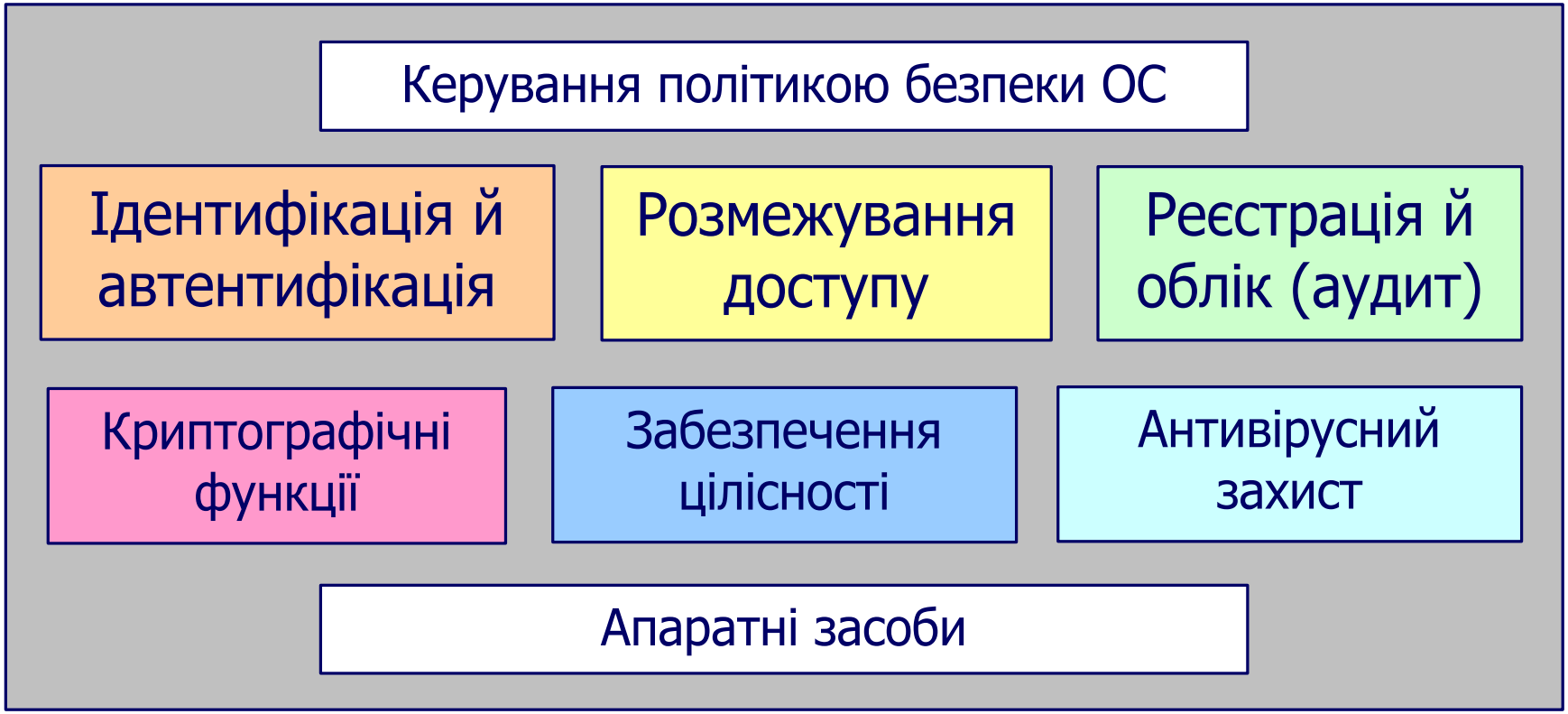
- Для забезпечення реальної здатності протидіяти атакам необхідно виключити усі чинники, які спричиняють виникнення вразливостей
  - Усі механізми реалізації атак базуються на використанні наявних вразливостей
  - Головною причиною появи вразливостей є непослідовність в реалізації контролю доступу
    - Існуючі системи містять привілейовані засоби та служби, які передають користувачам частину своїх повноважень, минаючи засоби контролю
      - Типовий приклад – механізм SUID/SGID в системі UNIX
  - Переважну більшість причин появи вразливостей можна усунути, реалізувавши в системі керування доступом на основі універсального інтерфейсу та єдиного механізму взаємодії без будь-яких виключень
  - Також необхідною є мінімізація обсягу довіреного коду самих засобів захисту з метою зменшення ймовірності появи в них помилок.

Принцип коректності

- Засоби захисту повинні реалізовувати керування доступом відповідно до формальних моделей
  - Наявність несуперечливої моделі безпеки:
    - дозволяє формально обґрунтувати безпеку системи,
    - надає об’єктивний критерій коректності її роботи,
    - може бути основою для побудови вичерпних тестів, що перевіряють правильність роботи засобів захисту в усіх режимах і обставинах.

Типова архітектура комплексу засобів захисту операційних систем

Основні підсистеми КЗЗ ОС



Основні підсистеми КЗЗ ОС

1. Розмежування доступу
   - Кожному користувачеві надається доступ лише до тих захищених об’єктів, доступ до яких дозволений йому політикою безпеки
   - Ця підсистема безпосередньо реалізовує політику безпеки
2. Ідентифікація й автентифікація
   - Жодний користувач не може розпочати роботу в середовищі захищеної ОС, не надавши системі свого ідентифікатора і не підтвердивши справжність наданого ідентифікатора за допомогою додаткової інформації, що автентифікує цього користувача
3. Аудит
   - В захищеній ОС здійснюється реєстрація всіх подій, що є потенційно небезпечними
   - Підсистема аудиту здійснює захист журналів, в яких відбувається реєстрація, від НСД
   - Також ця підсистема може надавати засоби для аналізу журналів і відстеження джерел тих чи інших подій

Основні підсистеми КЗЗ ОС

4. Керування політикою безпеки
   - Захищена ОС повинна надавати інтерфейси, які дозволяють адміністраторам ефективно вирішувати завдання з підтримання адекватної політики безпеки
   - Обов'язково надаються інтерфейси для настроювання підсистем розмежування доступу, ідентифікації й автентифікації, аудиту
5. Криптографічні функції
   - Криптографічні функції застосовуються для захисту конфіденційності і цілісності інформації, для автентифікації і забезпечення неможливості відмовлення від авторства
   - Криптографічні функції можуть використовуватись в якості самостійних засобів захисту, або в якості допоміжних механізмів в інших засобах
6. Забезпечення цілісності
   - Будь-яка сучасна ОС надає додаткові засоби для захисту цілісності даних не лише від НСД, але й від випадкових помилок, а також від аварій і збоїв системи
     - В першу чергу це стосується даних у файлових системах
   - Такі засоби реалізують можливості відкату, а також автоматизацію процесу створення резервних копій і відновлення з них

Основні підсистеми КЗЗ ОС

7. Антивірусний захист
   - Як правило, під підсистемою антивірусного захисту розуміють сукупність програм, які надають можливість виявляти і знешкоджувати відомі шкідливі програми, які відносяться як до вірусів (у широкому розумінні – включаючи троянських коней, мережевих хробаків, шпигунські програми), так і до засобів здійснення атак
   - Без антивірусного захисту в наш час неможливо підтримувати ОС у безпечному стані, особливо якщо вона встановлена на комп'ютері, що підключений до мережі
   - Як правило, антивірусні засоби не входять до складу ОС, а постачаються окремо
8. Апаратні засоби
   - КЗЗ ОС спирається на функції захисту, реалізовані в апаратних засобах – процесорі і системній платі

Особливості архітектури КЗЗ ОС

- КЗЗ ОС практично завжди є сукупністю значної кількості програмних модулів
  - частина модулів КЗЗ виконується у режимі ядра, а частина – у режимі користувача, тобто як прикладні програми
- В деяких ОС, де використовується більша кількість рівнів привілеїв процесів (кілець захисту), будується ієрархія засобів захисту
- В сучасних ОС КЗЗ чітко виділяється в архітектурі системи
  - наприклад, Windows
- Зустрічаються такі ОС, в яких підсистеми і окремі компоненти КЗЗ розпорошені по всій системі
  - наприклад, традиційні системи Unix і Linux
- Як правило, підсистема захисту дозволяє додавати додаткові модулі, які реалізують підсилені функції захисту, для чого передбачаються відповідні інтерфейси

Адміністративні заходи захисту

- *Постійний контроль коректності функціонування ОС*, зокрема, її підсистеми захисту
  - реєстрація подій у системі (*event logging*);
  - контроль цілісності файлів, зокрема, файлів, що містять програмний код компонентів ОС;
  - виконання тестів на коректність функціонування компонентів ОС.
- *Організація й підтримання адекватної політики безпеки*
  - Політика безпеки в ОС фактично визначає:
    - які користувачі мають доступ до яких компонентів ОС;
    - які користувачі мають доступ до яких об’єктів, що знаходяться під керуванням ОС (наприклад, файлів на диску, зовнішніх носіїв, пристроїв введення-виведення тощо);
    - яким чином користувачі ОС ідентифікують себе і які вимоги висунуті стосовно їхніх атрибутів доступу;
    - які події повинні реєструватись у системних журналах.
  - Політика безпеки повинна постійно коригуватись з урахуванням змін у конфігурації ОС, номенклатурі і настроюваннях встановлених прикладних програм, спроб порушників подолати захист ОС, поточних загроз (наприклад, епідемій небезпечних вірусів).
- *Навчання користувачів*
- *Створення резервних копій*
- *Постійний контроль змін в конфігураційних даних і політиці безпеки ОС*

Адекватна політика безпеки

- Адекватна політика безпеки в ОС – це така політика безпеки, яка забезпечує захист від визначеної множини загроз з достатньою надійністю
- Вибір і підтримання адекватної політики безпеки – одна з найважливіших задач адміністратора ОС
- Не слід вважати адекватною політику безпеки, яка забезпечує максимальний можливий захист
  - Як правило, підвищення захищеності пов'язано з обмеженням функціональності і утрудненням роботи користувачів
    - Чим жорсткіша політика, що регламентує правила автентифікації, тим менше ймовірність, що неуповноважений користувач отримає доступ до системи. Але тим більше зусиль необхідно затратити і уповноваженому користувачу, щоби підтвердити свої повноваження.
    - Система розмежування доступу обмежує можливості користувачів по створенню файлів у певних каталогах. Але переважна більшість сучасних програм під час своєї роботи створює тимчасові файли. Часто одночасно створюється кілька різних файлів у різних каталогах. Якщо програма намагається створити тимчасовий файл у каталозі, в якому поточному користувачеві створювати файли заборонено, то така операція буде неуспішною.
    - Чим складніші функції виконує система захисту, чим ретельніші перевірки вона здійснює, тим більшу частину ресурсів займає система захисту. Дія системи захисту може помітно уповільнити роботу ОС, а особливо суттєво уповільнити виконання деяких функцій, швидкість виконання яких складає уявлення користувачів щодо швидкодії системи.
    - Система захисту вимагає від адміністраторів системи додаткових знань, умінь і значних витрат часу на підтримання адекватної політики безпеки. Чим більше функцій захисту, тим більше часу повинні додатково витрачати адміністратори. Крім того, помилки адміністрування стають ймовірнішими і більш критичними.
- Єдиної адекватної політики безпеки на всі можливі випадки не існує й існувати не може
  - Адекватна політика безпеки визначається задачами тієї інформаційної системи, яка побудована з застосуванням конкретної ОС, а також діючими загрозами безпеці інформації у конкретній ІКС
    - Наприклад, одна й та сама серверна ОС може забезпечувати функціонування і Web-сервера, і сервера баз даних, і сервера електронного документообігу, а одна й та сама клієнтська ОС – і домашнього комп'ютера, і робочої станції у корпоративному середовищі.
  - Також адекватна політика безпеки може залежати від версії застосованої ОС, її конфігурації, встановленого прикладного ПЗ.

Основні етапи визначення і підтримання адекватної політики безпеки (1/2)

1. Аналіз загроз
   - Вивчають можливі загрози безпеці конкретного екземпляру ОС
   - Будують модель загроз
   - Оцінюють ризики
   - Визначають пріоритети у захисті від конкретних загроз
2. Формування вимог до політики безпеки
   - Визначають засоби і методи, які будуть застосовані для захисту від кожної окремої загрози
     - Як правило, неминучим є компроміс між вадами захисту від певних загроз і утрудненням роботи користувачів у системі
   - Результатом робіт є формування набору вимог до реалізації політики безпеки у вигляді переліку методів і засобів захисту, які повинні бути реалізованими
3. Формальне визначення політики безпеки
   - Здійснюють чітке визначення засобів, які будуть реалізовувати ті вимоги, що були сформульовані на попередньому етапі
     - Зокрема, з'ясовується, чи можна домогтися виконання зазначених вимог лише штатними засобами ОС, або необхідно встановлювати додатково спеціальне ПЗ
   - Формулюють вимоги до конфігурації ОС і усіх додаткових програм, що реалізують функції захисту, якщо такі встановлені
   - Результатом робіт є детальний перелік конфігураційних настроювань ОС і додаткових програм
     - Повинні бути передбачені різні нештатні ситуації і відповідні настроювання ОС для таких ситуацій.

Основні етапи визначення і підтримання адекватної політики безпеки (2/2)

4. Втілення політики безпеки
   - Виконують настроювання ОС і додаткових програм, які реалізують функції захисту, у точній відповідності до формалізованої політики безпеки
5. Підтримання і корекція політики безпеки
   - Ретельний контроль дотримання політики безпеки, що була розроблена на третьому етапі
     - Контроль обов'язково включає перевірки налаштовувань засобів захисту у складі ОС і може виконуватись за допомогою спеціального ПЗ
   - Відстеження повідомлень про
     - появу нових загроз (наприклад, розповсюдження в Інтернеті небезпечних вірусів)
     - виявлення раніше невідомих уразливостей
     - розроблення виправлень для ОС і прикладного ПЗ
   - У деяких випадках може знадобитись корекція політики безпеки
     - Виявлення уразливостей, для усунення яких немає необхідних виправлень
     - Будь-які зміни в самій системі
       - Наприклад, встановлення нового програмного продукту може вимагати корекції політики безпеки, по-перше, для забезпечення нормального функціонування цього програмного продукту (розширення повноважень), а по-друге, для виключення шляхів несанкціонованого доступу, які можуть в результаті з'явитись (додаткові обмеження).