МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ІМЕНИ СЕМЕНА КУЗНЕЦЯ

Лабораторна робота №1

“Тема №1”

з дисципліни «Математичні основи криптології»

Виконав:

Студент групи 6.04.125.010.21.2

факультету Інформаційних технологій

спеціальності 125

П.І.П. Бойко В.В.

Перевірив:

Чугай А.М.

Харків – 2022

Питання:

1. Визначте три цілі безпеки.
2. Вкажіть різницю між пасивними та активними атаками на секретну інформацію. Назвіть деякі пасивні атаки. Назвіть деякі активні атаки.
3. Перерахуйте та визначте п'ять служб безпеки, розглянутих у цьому розділі.
4. Визначте вісім механізмів безпеки, розглянутих у цьому розділі.
5. Вкажіть різницю між шифруванням і стеганографією.

Відповіді:

1. Три цілі безпеки:
   1. Конфіденційність
   2. Цілісність
   3. Доступність
2. Різниця між пасивними та активними атаками на секретну інформацію
   1. Пасивна атака – це дії, головна мета яких – отримати інформацію та система продовжує нормально працювати, а Активна – це дії з втручанням у систему, вони можуть нашкодити цілісності або готовності системи
   2. Пасивні атаки
      1. Спостереження за трафіком та його аналіз
      2. втручання
   3. Активні атаки
      1. Модифікація
      2. Імітація джерела
      3. Повторна передача інформації
      4. Відмова від повідомлення
      5. Відмова в обслуговуванні
3. П’ять служб безпеки:
   1. Конфіденційність даних
   2. Цілісність
   3. Перевірка повноважень
   4. Управління доступом
   5. Виключення відмови від постачання
4. Вісім механізмів безпеки:
   1. Шифрування
   2. Цілісність даних
   3. Цифровий підпис
   4. Встановлення повноважень змін
   5. Заповнення трафіка
   6. Управління маршрутизацією
   7. Довіреність
   8. Управління доступом
5. Різниця між шифруванням та стенографією
   1. Шифрування – зміна даних для того, щоб зловмисник в разі отримання повідомлення не зміг його отримати
   2. Стенографія – приховує повідомлення чимось

Вправи:

1. Яка служба безпеки гарантується при використанні кожного з наступних методів пересилання поштою в поштовому відділенні?
   * Звичайна пошта

ніяка служба безпеки не гарантує нічого

* + Звичайна пошта з підтвердженням доставки

готовність інформації – ми отримали повідомлення про надходження пошти, якщо це не фіктивне повідомлення ми знаємо що лист надійшов до адреси

* + Звичайна пошта з доставкою та підписом одержувача

готовність інформації та конфіденційність, бо лише конкретна людина може отримати якийсь лист

* + Рекомендований лист

ніяка служба не гарантує нічого

* + Пошта з оголошеною цінністю

цілісність інформації, якщо до нас надходить щось не те, або іншою вартістю – це означає, що були зміни протягом доставки

* + Зареєстрована кореспонденція

цілісність, конфіденційність та готовність інформації

1. Визначити тип атаки на секретну інформацію у кожному з наступних випадків:
   * Студент проникає до офісу професора, щоб отримати копію тесту, який буде проведено наступного дня.

отримання копії = аналіз трафіку, пасивна атака втручання та аналізу трафіка

* + Студент дає чек на отримання грошей на10 $купити вже стару книгу. Потім він дізнається, що чек був сплачений на100 $. –

активна імітація джерела або повторна передача інформації, якщо було 10 платежів по 10$ або активна модифікація, якщо 1 платіж на 100$

* + Студент передає сотні запитів на день, використовуючи фальшиву зворотну адресу телефону іншого студента.

Активна повторна передача інформації

1. Які механізми безпеки реалізовані в кожному з наступних випадків?
   * Університет вимагає ідентифікатор студента та пароль, щоб дозволити студенту отримати доступ до шкільного сервера.

цифровий підпис

* + Університетський сервер роз'єднує студента, якщо він отримав доступ до системи більш ніж дві години тому.

управління маршрутизацією

* + Професор відмовляється передати студентам їх оцінки електронною поштою, якщо вони не відповідають студентській ідентифікації, заздалегідь призначеній професором.

довіреність та управління доступом

* + Банк вимагає підпису клієнта вилучення клієнтом грошей.

цифровий підпис, встановлення повноважень зміни, довіреність, управління доступом

1. Яка методика (криптографія чи стеганографія) використовується у кожному з таких випадків для захисту конфіденційності?
   * Студент пише відповіді на квитки на маленькому аркуші паперу, папір згортається і вставляється в кулькову ручку, а ручка передається іншому студенту.

Стенографія

* + Щоб надіслати повідомлення, шпигун замінює кожен символ у повідомленні символом, який був узгоджений заздалегідь як заміна іншого символу

Криптографія

* + Компанія використовує спеціальні чорнила на своїх чеках, щоб запобігти підробкам.

Не криптографія не стенографія, це підтвердження цілісності даних бо дані можуть бути написані лише одним типом чорнил

* + Аспірантка використовує водяні знаки, щоб захистити свою роботу, вивішену на її сайті.

Стенографія

1. Який механізм безпеки реалізується, коли людина підписує форму при заповненні заяви на кредитну картку?

Шифрування симетричними ключами – підпис в документі та паспорті – однакові

Коментар – дуже сподобались завдання на знаходження типу атаки \ механізм безпеки \ яка методика використовується