Основные понятия информационной безопасности

Д. С. Кулябов, А. В. Королькова

Содержание

Цели информационной безопасности

Основные цели информационной безопасности

- Конфиденциальность
- Целостность
- Работоспособность

Конфиденциальность

- Самый общий аспект информационной безопасности.
- Необходимо защитить нашу конфиденциальную информацию.
- В военных организациях важно сохранение секретности важной информации.
- В промышленности важно сохранение информации от конкурентов.
- Необходимо сохраняться секретность учётных записей клиентов.
- Необходима при хранении информации.
- Необходима при передаче информации.

Целостность

- Информация изменяется постоянно.
- Изменения должны быть сделаны только разрешёнными объектами и с помощью разрешённых механизмов.
- Нарушение целостности — не обязательно результат злонамеренного действия.

Работоспособность

- Информация должна быть доступна разрешённым объектам.
- Информация бесполезна, если она не доступна.

Виды атак на информацию

Вмешательство

- Неправомочный доступ или перехват данных.
- Для предотвращения вмешательства данные должны быть представлены так, что перехвативший не сможет понять их.
- Использование шифрования для предотвращения вмешательства.

Наблюдение за трафиком и его анализ

- Анализируя сетевой трафик, можно получить дополнительную информацию.
- Часть информации открыта.
- Статистические данные, связанные с перехватываемой информацией.

Модификация

- После прерывания или доступа к информации атакующий изменяет информацию.

Имитация источника (spoofing)

- Имитация кого-то, кто имеет право на производимые действия.
- Имитация приёмника.

Повторная передача информации (атака воспроизведения)

- Атакующий получает копию сообщения и передает эту копию с целью дезорганизации процесса или попытки повторить его.

Отказ от сообщения

- Передатчик сообщения может отрицать факт передачи.
- Приёмник сообщения может отрицать, что он получил сообщение.

Отказ в обслуживании (Denial of Service — DoS)

- Атака на сервер.
  - Перегрузка сервера фиктивными запросами.
  - Прерывание запросов клиента. Клиент увеличивает количество запросов.
- Атака на клиент.
  - Удаление ответа сервера. Клиент считает, что сервер не отвечает.
  - Прерывание запросов клиента. Клиент считает, что сервер не отвечает.

Типы атак

Пассивные атаки

- Цель атакующего состоит в том, чтобы только получить информацию.

Активные атаки

- Изменяют данные или повреждают систему.

Классификация атак

Атака	Тип атаки	Угроза
Вмешательство	Пассивная	Конфиденциальности
Анализ трафика	Пассивная	Конфиденциальности
Модификация	Активная	Целостности
Имитация источника	Активная	Целостности
Повторная передача информации	Активная	Целостности
Отказ от сообщения	Активная	Целостности
Отказ в обслуживании	Активная	Работоспособности

Услуги информационной безопасности

Услуги информационной безопасности ITU-T

ITU-T (X.800) определил пять услуг, связанных с целями информационной безопасности.

- Конфиденциальность данных
- Целостность данных
- Установление подлинности (аутентификация)
- Исключение отказа от сообщений
- Управление доступом

Конфиденциальность данных

- Защита данные от попытки их раскрытия.
- Охватывает:
  - конфиденциальность целого сообщения;
  - конфиденциальность части сообщения;
  - защищает от наблюдения за трафиком и анализа трафика.

Целостность данных

- Защита данных от
  - модификации,
  - вставки,
  - удаления,
  - повторной передачи.
- Может защищать целое сообщение или часть сообщения.

Установление подлинности (аутентификация)

- Установление подлинности (аутентификацию) оператора на другом конце линии.
- Установление подлинности передатчика или приёмника в течение установления соединения (установление подлинности объектов равного уровня).
- Установление подлинности источника данных (установление подлинности происхождения данных).

Исключение отказа от сообщений

- Защищает от отказа от сообщения передатчиком или приёмником данных.
- Приёмник может доказать происхождение сообщения, используя идентификатор передатчика.
- Передатчик для доказательства использует подтверждение доставки.

Управление доступом

- Защита против неправомочного доступа к данным.
- Доступ включает в себя:
  - чтение,
  - запись,
  - изменение данных,
  - запуск на выполнение,
  - и др.

Механизмы информационной безопасности

Механизмы безопасности

- Шифрование
- Целостность данных
- Цифровая подпись
- Обмен сообщениями для опознавания
- Заполнение трафика
- Управление маршрутизацией
- Доверенность
- Управление доступом

Шифрование

- Гарантирует конфиденциальность.
- Два метода: криптография и стеганография.

Целостность данных

- Добавка в конце данных короткий контрольный признак (check value).
- Контрольный признак создаётся отдельно от данных.
- Приёмник получает данные и контрольный признак:
  - создаёт новый контрольный признак;
  - сравнивает только что созданный контрольный признак с полученным;
  - если эти два контрольных признака совпадают, целостность данных была сохранена.

Цифровая подпись

- Отправитель может подписать данные.
- Приёмник может проверить подпись.

Обмен сообщениями для опознавания

- Два объекта обмениваются некоторыми сообщениями, чтобы доказать, что эти объекты известны друг другу.

Заполнение трафика

- Возможность вставлять в трафик данных некоторые фиктивные данные, чтобы сорвать попытки злоумышленников использовать его для анализа.

Управление маршрутизацией

- Выбор и непрерывное изменение различных доступных маршрутов между отправителем и приёмником для того, чтобы препятствовать противнику в перехвате информации на определённом маршруте.

Доверенность

- Выбор третьей стороны с целью доверить ей контроль обменом между двумя объектами.

- Доказывает, что пользователь имеет право доступа к данным:
  - пароль,
  - PIN-код,
  - и др.

Соотношение между услугами и механизмами

Услуга безопасности	Механизм обеспечения безопасности
Конфиденциальность данных	Шифрование и управление маршрутизацией
Целостность данных	Шифрование, цифровая подпись, контрольные признаки целостности данных
Проверка полномочий	Шифрование, цифровая подпись, установление правомочности изменений
Исключение отказа от сообщений	Цифровая подпись, целостность данных и доверенность
Управление доступом	Механизм управления доступом

Методы информационной безопасности

Два метода шифрования для реализации механизма безопасности:

- Криптография
- Стеганография

Значение термина

- Криптография (от греч. κρυπτός «скрытый» + γράφω «пишу»).

Механизмы криптографии

- Совокупность трёх механизмов:
  - шифрование симметричными ключами,
  - шифрование асимметричными ключами,
  - хеширование.

Шифрование симметричными ключами

- Шифрование с секретным ключом (криптография с секретным ключом).
- Применяется единственный ключ засекречивания и для шифрования, и для расшифровки.

Шифрование асимметричными ключами

- Шифрование асимметричными ключами (шифрование с открытыми ключами, криптография с открытыми ключами).
- Два ключа вместо одного:
  - открытый ключ (public key),
  - индивидуальный или секретный (private key).

Хеширование

- Из сообщения переменной длины может быть создан дайджест фиксированной длины (обычно намного меньшего размера, чем исходное сообщение).

Значение термина

- Стеганография (от греч. στεγανός «скрытый» + γράφω «пишу»; букв. «тайнопись»).

Криптография vs. стеганография

- Криптография защищает содержание сообщения.
- Стеганография защищает сам факт наличия каких-либо скрытых посланий.

Резюме

Резюме I

- Для информационной безопасности были определены три главные цели:
  - конфиденциальность,
  - целостность,
  - работоспособность.

Резюме II

- Конфиденциальности информации угрожают два типа атак:
  - вмешательство,
  - анализ трафика.
- Целостности информации угрожают четыре типа атак:
  - модификация,
  - имитация источника,
  - повторная передача информации,
  - отказ от сообщения.
- Работоспособности информации угрожает атака:
  - прекращение обслуживания запроса.

Резюме III

- ITU-T определил несколько услуг информационной безопасности:
  - конфиденциальность данных,
  - целостность данных,
  - установление подлинности,
  - исключение отказа от сообщений,
  - управление доступом.

Резюме iv

- ITU-T рекомендует механизмы обеспечения безопасности:
  - шифрование,
  - целостность данных,
  - цифровая подпись,
  - установление правомочности изменений,
  - заполнение трафика,
  - управление маршрутизацией,
  - доверенность,
  - управление доступом.

Резюме v

- Два метода защиты информации:
  - криптография,
  - стеганография.

Контрольные вопросы

Контрольные вопросы

1. Определите три цели безопасности.
2. Укажите различие между пассивными и активными атаками на секретную информацию.
3. Назовите некоторые пассивные атаки.
4. Назовите некоторые активные атаки.
5. Перечислите и определите пять служб безопасности.
6. Перечислите и определите восемь механизмов безопасности.
7. Укажите различие между шифрованием и стеганографией.