Архитектура вычислительных систем

Лекция 8. Безопасность

Artem Beresnev

t.me/ITSMDao

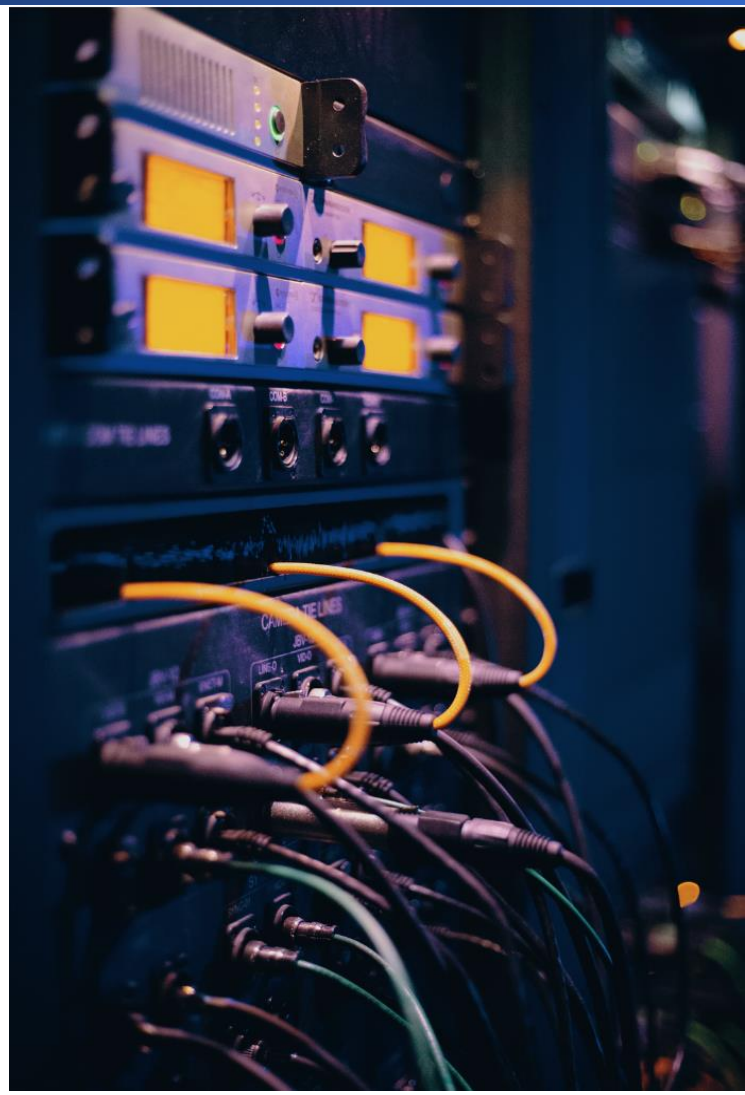
t.me/ITSMDaoChat

План

- Немного о безопасности
- Основные понятия шифрования
- SSH
- сегодня без котиков

Что такое Информационная безопасность?

Только познакомимся



Понятие безопасности

Информационная безопасность— это процесс обеспечения конфиденциальности, целостности и доступности информации.

- Конфиденциальность: Обеспечение доступа к информации только авторизованным пользователям.
- Целостность: Обеспечение достоверности и полноты информации и методов ее обработки.
- Доступность: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Обеспечение безопасности

Идеологии безопасности

- ## Безопасность через неясность

  Попытка обороняющейся стороны обезопасить систему, максимально усложнив ее, запутав внутренние взаимосвязи и исходный код, чтобы потенциальному взломщику было труднее в ней разобраться и попытаться найти слабые места в защите. Отказ от публикации исходного кода криптосистем считается одним из примеров подобной практики, однако история учит тому, что реально этот подход дает лишь временную отсрочку перед окончательным взломом.

- ## Безопасность через открытость

  Открытость — это состояние вычислительной системы (или нескольких систем), которое не является уязвимостью, но:

  - позволяет атакующему производить сбор защищенной информации;
  - позволяет атакующему скрывать свою деятельность;
  - содержит возможности, которые работают корректно, но могут быть легко использованы в неблаговидных целях;
  - является первичной точкой входа в систему, которую атакующий может использовать для получения доступа или информации.

Основные понятия

Идентификация - установление личности субъекта (лат. identifico - отождествлять)

Аутентификация - подтверждение подлинности субъекта (англ. authentication)

Авторизация - проверка прав доступа субъекта к ресурсам (англ. authorization)

Идентификация

Идентификация — процесс распознавания субъекта в компьютерной системе или на веб-ресурсе при помощи анализа его идентификатора (имени и/или пароля либо любой другой информации о пользователе, которая воспринимается системой или ресурсом).

SID

SID (Security ID) – уникальный в приделах жизни системы идентификатор субъекта безопасности.

Относительно него даются разрешения.

Имена субъектов – атрибуты или поля структуры идентифицирующейся SID.

Аутентификация

Аутентификация (англ. *authentication*, от греч. — реальный, истинный) — процесс проверки принадлежности субъекту прав доступа к информационным ресурсам системы или веб-сайта в соответствии с предъявленным им идентификатором; подтверждение (установление) подлинности субъекта.

Аутентификация

Процедура аутентификации включает в себя определенный набор элементов:

- **субъект**, который проходит аутентификацию (авторизированный пользователь);
- **характеристика субъекта** (идентификатор, который он предъявляет для проверки подлинности);
- **владелец системы аутентификации** (хозяин информационного ресурса или веб-сайта);
- **механизм аутентификации** (ПО, которое проверяет подлинность предъявленного идентификатора);
  - **механизм авторизации** (предоставление или лишение субъекта прав доступа после успешной или безуспешной аутентификации).

Аутентификация

Методы аутентификации делятся на четыре основные группы в зависимости от используемых в процессе проверки подлинности средств. Так, различают методы, основанные на:

- Знаниях, которыми владеет субъект (парольные методы).
- Предметах, которые принадлежат субъекту (комбинированные).
- Свойствах данных субъекта (биометрические).
- Информации, которая имеет непосредственное отношение к субъекту.

Методы Аутентификации

Парольные методы

Наиболее распространенные методы аутентификации, основанные на секретных характеристиках субъектов — паролях. В процессе проверки подлинности система сравнивает указный пользователем пароль с эталонным паролем, который хранится в ее БД в зашифрованном виде. Для аутентификации посредством данного метода могут использоваться постоянные (многоразовые, неизменные для каждой сессии) или динамические (одноразовые, постоянно меняющиеся для каждой сессии) пароли.

Комбинированные методы

Сущность данного метода заключается в использовании для подтверждения подлинности субъекта помимо пароля дополнительных предметов (мобильных телефонов, смарт-карт, токенов) или атрибутов (криптографических сертификатов). Авторизация при помощи предметов и атрибутов субъекта происходит только при наличии специального устройства, которое может считывать информацию с перечисленных идентификаторов.

Биометрические методы

Для аутентификации посредством биометрического метода субъекты должны пройти сканирование и анализ одного или нескольких физиологических (отпечатки пальцев, радужная оболочка глаза, сетчатка глаза, кисть руки, черты лица) или поведенческих характеристик (подпись, тембр голоса, клавиатурный почерк). Данный метод, как правило, используется только на особо важных объектах и системах, так как требует наличия специальной дорогостоящей техники и оборудования.

Методы, основанные на информации о субъекте

Данная группа методов относится к новейшим механизмам аутентификации: в основе лежит использование спутниковой системы навигации GPS. Основным идентификатором подлинности субъекта является его местонахождение.

Комбинированные методы

Биометрическая аутентификация

Особое мнение (2002)

Классификация и виды аутентификации

В основе классификации механизмов аутентификации лежит ряд определенных критериев. Так, по степени доверия и направленности процесса различают следующие виды:

- **Односторонняя** проверка подлинности (субъект доказывает владельцу системы свои права доступа к информационным ресурсам или интернет-сайту).
- **Двусторонняя** аутентификация (обоюдная проверка и установление подлинности как субъекта, так и владельца системы).

Авторизация

Авторизация — процесс проверки прав пользователя на осуществление определенных действий в системе.

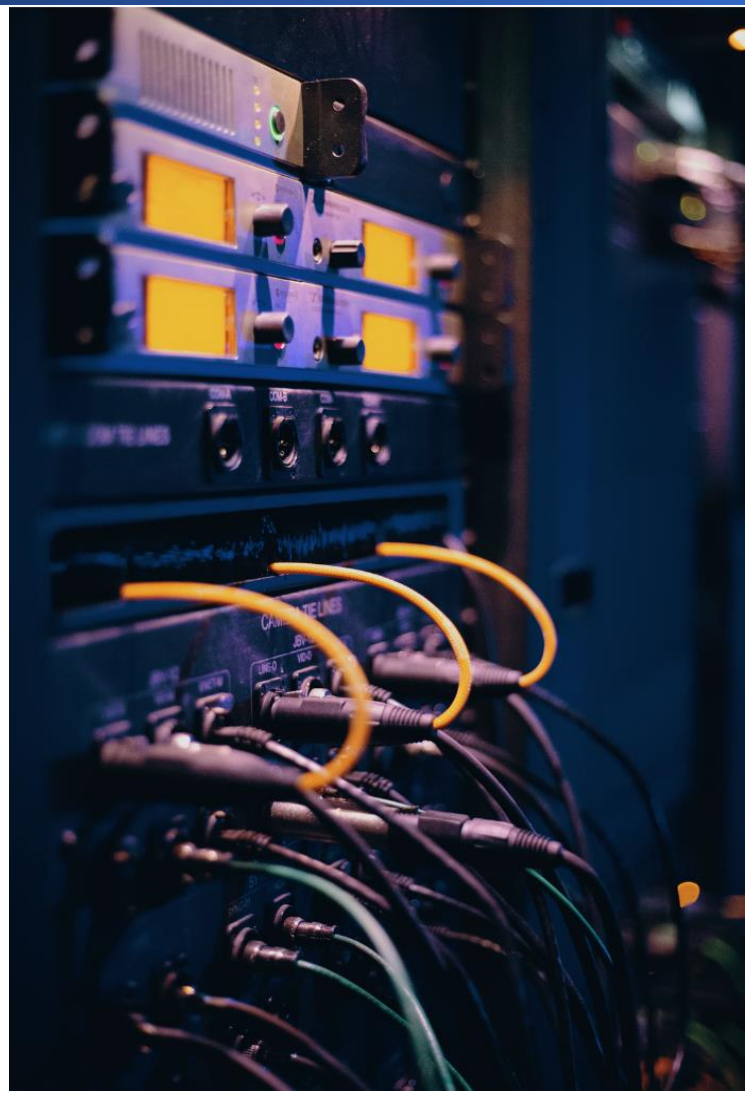
Авторизация проходит в два последовательных этапа:

- **определение возможности доступа** пользователя в компьютерную систему посредством идентификации и аутентификации;
- **одобрение или отклонение запроса** на доступ.

Главным образом авторизация необходима для сохранения конфиденциальности и целостности информации в системе.

Основные сведения о шифровании

Только познакомимся



Классификация алгоритмов шифрования

- **Симметричные** (с секретным, единым ключом, одноключевые, single-key).
  - Потоковые (шифрование потока данных):
    - с одноразовым или бесконечным ключом (infinite-key cipher);
    - с конечным ключом (система Вернама - Vernam);
    - на основе генератора псевдослучайных чисел (ПСЧ).
  - Блочные (шифрование данных поблочно):
    - Шифры перестановки (permutation, P-блоки);
    - Шифры замены (подстановки, substitution, S-блоки):
      - моноалфавитные (код Цезаря);
      - полиалфавитные (шифр Вижденера, цилиндр Джефферсона, диск Уэтстоуна, Enigma);
    - Составные (таблица 1):
      - Lucipher (фирма IBM, США);
      - DES (Data Encryption Standard, США);
      - FEAL-1 (Fast Enciphering Algoritm, Япония);
      - IDEA/IPES (International Data Encryption Algorithm/
      - **AES**
      - B-Crypt (фирма British Telecom, Великобритания);
      - ГОСТ 28147-89 (СССР); * Skipjack (США).

- **Асимметричные** (с открытым ключом, public-key):
  - Диффи-Хеллман DH (Diffie, Hellman);
  - Райвест-Шамир-Адлеман RSA (Rivest, Shamir, Adleman);
  - Эль-Гамаль ElGamal.
  - ГОСТ Р 34.11-2012

Симметричные алгоритмы шифрования

$$T \rightarrow F(T;k) \rightarrow S \rightarrow \tilde{F}(S;k) \rightarrow T$$

Основная проблема – передача ключа k

https://www.kinopoisk.ru/film/2771/

Асимметричные алгоритмы шифрования 1/3

$1)\ n1 \rightarrow G() \rightarrow ok1, pk1$

$2)\ n1 \rightarrow delete$

$1)\ n2 \rightarrow G() \rightarrow ok2, pk2$

$2)\ n2 \rightarrow delete$

Генерация симметричных ключей

Асимметричные алгоритмы шифрования 2/3

$ok1, pk1$

$ok1$

$ok2$

$ok2\ pk2$

Обмен открытыми ключами

Асимметричные алгоритмы шифрования 2/3

$ok1, pk1$ $ok2$

$ok2$ $pk2$ $ok1$

$$T \rightarrow F(T; ok2) \rightarrow S \rightarrow \tilde{F}(S; pk2) \rightarrow T$$

шифрообмен

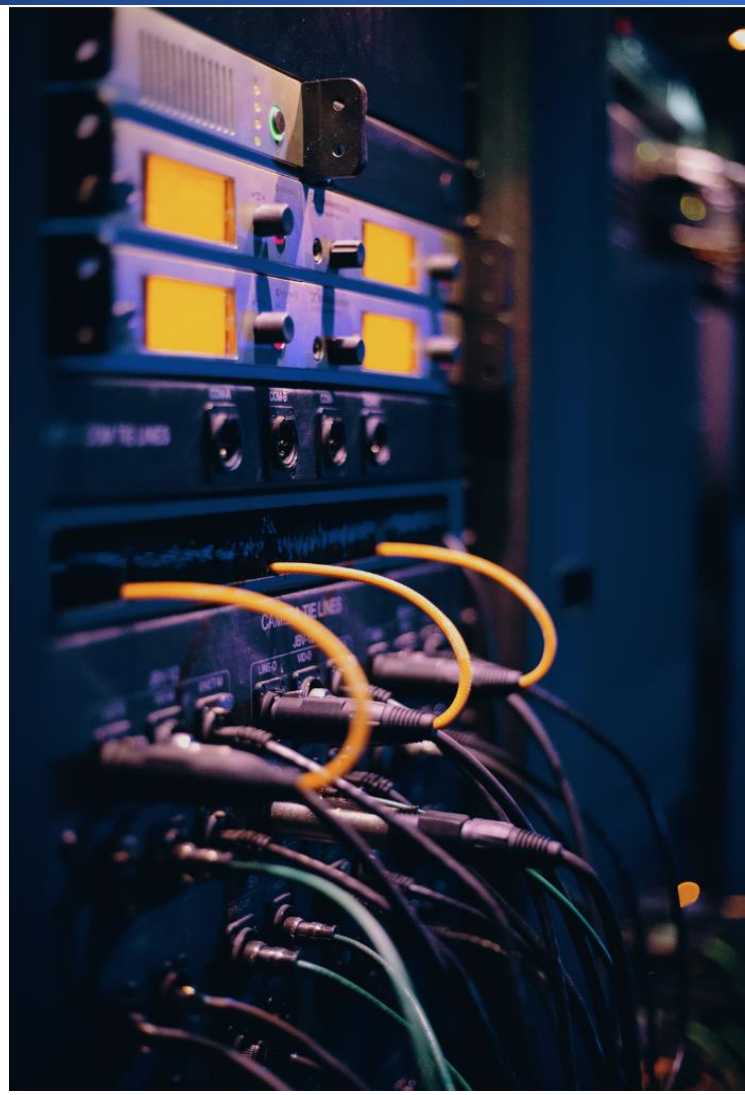
Сравнение симметричных и асимметричных алгоритмов шифрования

Симметричный алгоритм	Ассиметричный алгоритм
✓ Криптостойкость при равной длине ключа	
✓ Скорость	
✓ Рост объема шифротекста	
✓ Вычислительные затраты	
Проблема передачи ключа	✓

Внимание!
Рассматривается сферический конь в вакууме

SSH

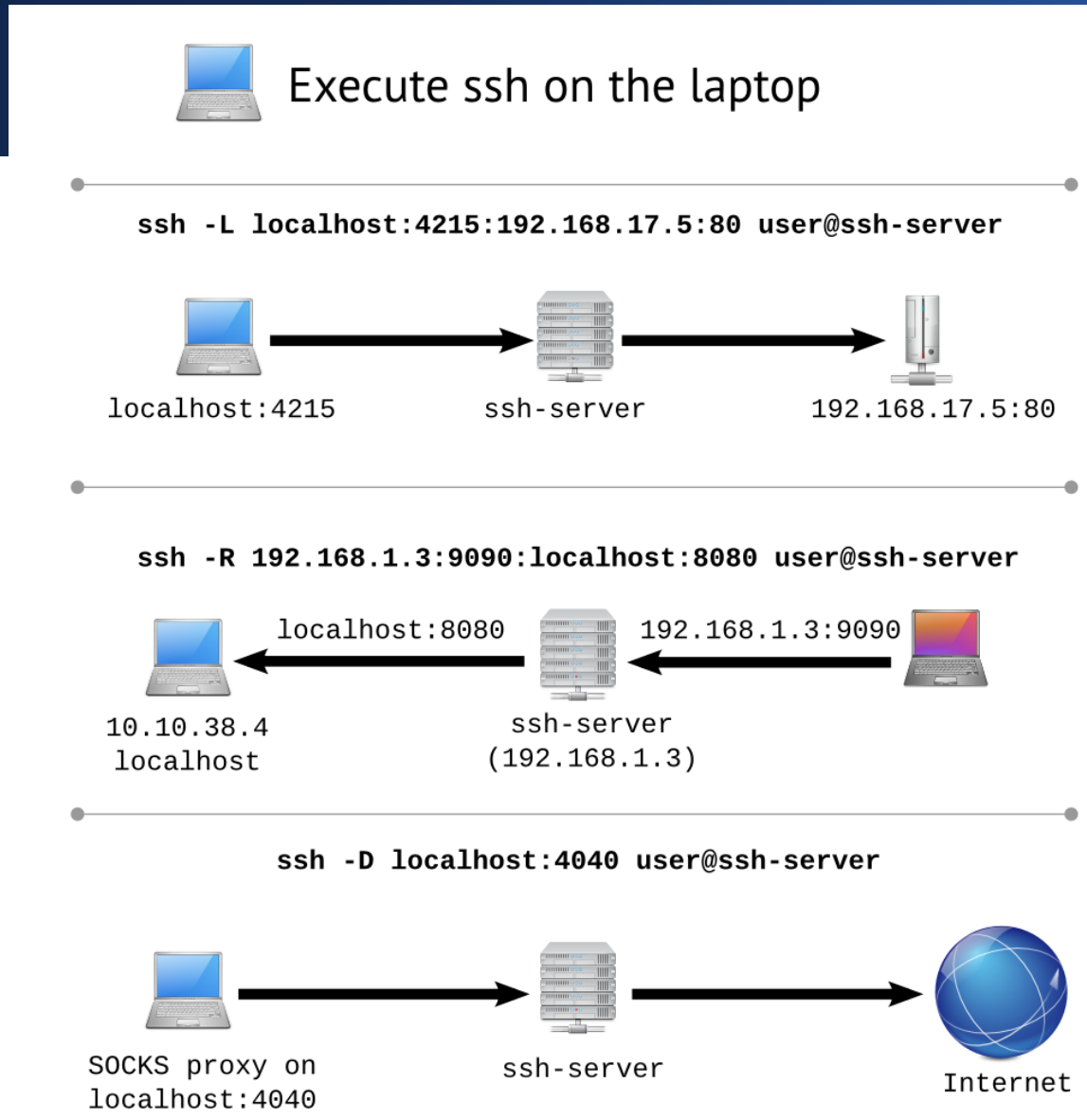
Что это и какие основные приемы работы существуют?



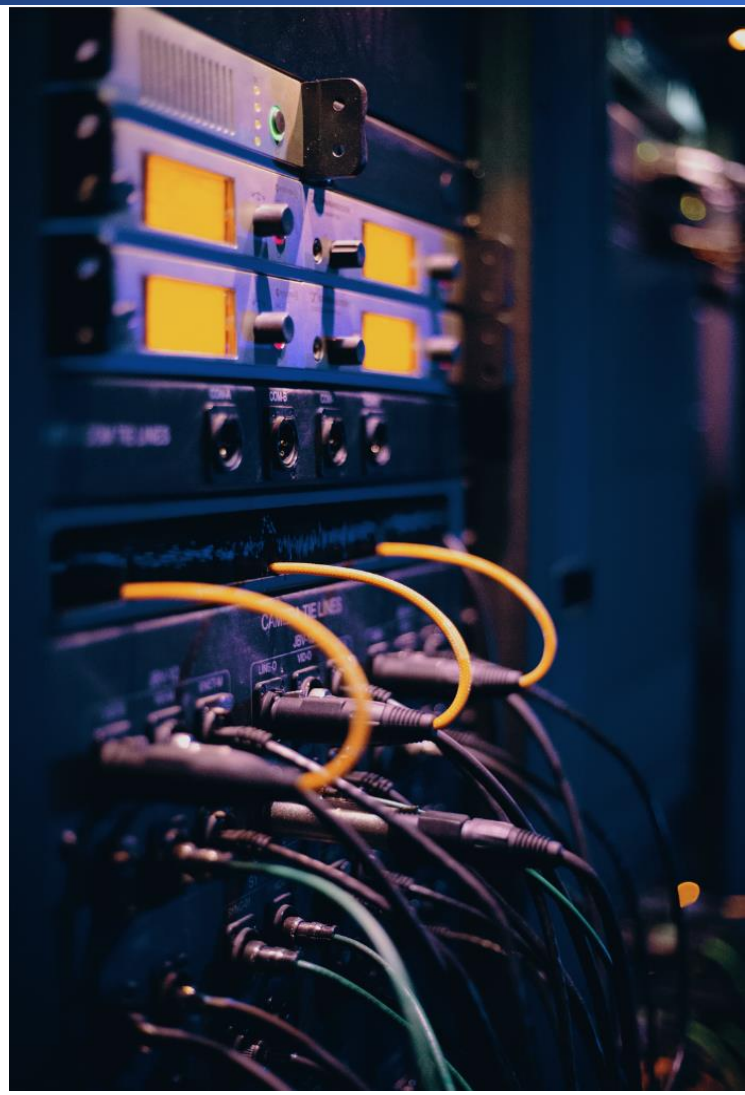
SSH

- SSH (англ. Secure Shell — «безопасная оболочка»)
- Использует гибридную криптосистему для генерации сеансного ключа для шифрования всего трафика
- Аутентификация может быть по паролю, по паре открытый и закрытый ключ, может быть многофакторной
- Используется для:
  - Удаленного управления
  - Туннелирования
  - Проскирования
  - Передачи файлов

Туннелирование



Итоги



Выводы

- Обсудили общие моменты, связанные с безопасностью
- Узнали какие алгоритмы шифрования бывают и что такое гибридная криптосистема
- Узнали как использовать SSH и как используются разные алгоритмы шифрования