Современные методы криптографии в контексте безопасности UNIX

Презентация

Филипьева Ксения Дмитриевна

08 апреля 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Филипьева Ксения Дмитриевна
- НБИбд-02-23
- студент
- Российский университет дружбы народов
- 1132230795@rudn.ru

Вводная часть

Актуальность

Актуальность темы “Современные методы криптографии в контексте безопасности UNIX” обусловлена следующими факторами:

1. Растущая важность защиты цифровой информации в современном мире.
2. Широкое распространение и использование операционных систем семейства UNIX в различных сферах.

Актуальность

3. Необходимость эффективного применения современных методов криптографии с учетом специфики UNIX-систем.
4. Потребность специалистов в области информационной безопасности, системных администраторов и разработчиков в получении знаний и рекомендаций по внедрению передовых криптографических решений для защиты данных и коммуникаций в UNIX-средах.

Объект и предмет исследования

Объектом исследования данной презентации являются современные методы криптографии, применяемые для обеспечения безопасности операционных систем семейства UNIX.

Цель

Изучение современных методов криптографии и их применения в обеспечении безопасности операционных систем семейства UNIX.

Задачи

1. Перечислить современные алгоритмы симметричного шифрования, применяемые в UNIX-системах.
2. Назвать примеры алгоритмов асимметричного шифрования и их краткую характеристику.
3. Указать современные хеш-функции и их основное назначение в UNIX-системах.

Задачи

4. Кратко описать общие принципы управления криптографическими ключами.
5. Перечислить криптографические протоколы, используемые для обеспечения безопасности сетевых коммуникаций в UNIX.
6. Отметить важность комплексного подхода к безопасности UNIX, включающего криптографию.

Основная часть

Симметричное шифрование

Симметричное шифрование — это метод, при котором для шифрования и дешифрования данных используется один и тот же ключ.

1. Advanced Encryption Standard

Стандарт шифрования, принятый правительством США

2. ChaCha20

Алгоритм, разработанный Дэниелом Бернштейном

Асимметричное шифрование

Асимметричное шифрование, также известное как криптография с открытым ключом, использует пару ключей - открытый и закрытый. Открытый ключ может быть известен всем и используется для шифрования данных, а закрытый ключ держится в секрете и используется для дешифрования.

1. Rivest-Shamir-Adleman

Основан на сложности факторизации больших чисел

2. Elliptic Curve Cryptography

Криптография на эллиптических кривых

Хеш-функции

Хеш-функции — это криптографические функции, которые преобразуют входные данные произвольной длины в выходные данные фиксированной длины (хеш). Хорошие криптографические хеш-функции обладают свойствами необратимости и устойчивости к коллизиям.

1. Secure Hash Algorithm 2

Семейство хеш-функций, включающее SHA-256 и SHA-512

2. SHA-3

Основан на алгоритме Keccak и обеспечивает высокий уровень безопасности

Управление ключами

Управление криптографическими ключами включает в себя генерацию, хранение, распространение и уничтожение ключей. Для безопасного управления ключами используются следующие методы:

1. Генерация случайных ключей: для создания криптографических ключей используются надежные генераторы случайных чисел, такие как /dev/urandom в Linux.
2. Хранение ключей: ключи должны храниться в защищенном месте, например, на смарт-картах или в аппаратных модулях безопасности (HSM).

Управление ключами

3. Распространение ключей: для безопасной передачи ключей используются протоколы, такие как Diffie-Hellman или RSA.
4. Уничтожение ключей: когда ключи больше не нужны, они должны быть надежно удалены, чтобы предотвратить их восстановление.

Протоколы безопасности

Современные UNIX-системы используют различные криптографические протоколы для обеспечения безопасности сетевых коммуникаций:

1. SSL/TLS (Secure Sockets Layer/Transport Layer Security) - протоколы, обеспечивающие конфиденциальность и целостность данных в интернете. Они широко используются для защиты веб-трафика (HTTPS), электронной почты (SMTPS, IMAPS) и других приложений.
2. IPsec (Internet Protocol Security) - набор протоколов для защиты сетевых коммуникаций на уровне I P. IPsec обеспечивает конфиденциальность, целостность и аутентификацию данных.
3. SSH (Secure Shell) - протокол для безопасного удаленного доступа к UNIX-системам. SSH использует симметричное и асимметричное шифрование для защиты данных.

Результаты

Вывод

Современные методы криптографии играют ключевую роль в обеспечении безопасности UNIX-систем. Симметричное и асимметричное шифрование, хеш-функции, управление ключами и криптографические протоколы - все эти инструменты работают вместе, чтобы защитить данные от несанкционированного доступа, изменения и раскрытия.

Источники и литература

https://www.kaspersky.ru/resource-center/definitions/what-is-cryptography

https://practicum.yandex.ru/blog/chto-takoe-kriptografiya/

Спасибо за внимание