Доклад

Инфраструктура открытых ключей

Артамонов Т. Е.

11 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Артамонов Тимофей Евгеньевич
- студент группы НКНбд-01-21
- Российский университет дружбы народов
- https://github.com/teartamonov

Введение

Цель работы

Дать определение инфраструктуры открытых ключей и разобраться в ее работе.

Задачи

- Дать определение инфраструктуры открытых ключей(PKI).
- Разобраться в работе PKI.
- Рассмотреть основные виды архитектуры PKI.
- Проанализировать безопасность каждого вида.

Общие сведения об инфраструктуре открытых ключей

Определение инфраструктуры открытых ключей

Инфраструктура открытых ключей (Public Key Infrastructure или PKI) - набор средств, включая программное и аппаратное обеспечение, позволяющих взаимодействовать с цифровыми сертификатами, в том числе, саздавать, управлять, распространять, использовать и отзывать. В основе PKI лежит *криптографическая система с открытым ключом*.

Определение шифрования с помощью открытых ключей и принцип работы

Криптографическая система с открытым ключом - система шифрования или электронной подписи, в которой шифрование и дешифрование данных проводится с помощью пары ключей - открытого и закрытого. Открытый ключ - публичная часть ключа, которую владелец ключа отправляет тому, кто будет отправлять ему какие-либо данные. Этот ключ передается по открытому, незащищенному каналу. С помощью полученного открытого ключа отправитель шифрует данные и отправляет их владельцу ключа. Теперь владелец ключа дешифрует эти данные с помощью закрытой части ключа, которую он хранит на своем устройстве и никому не показывает.

Пример на схеме

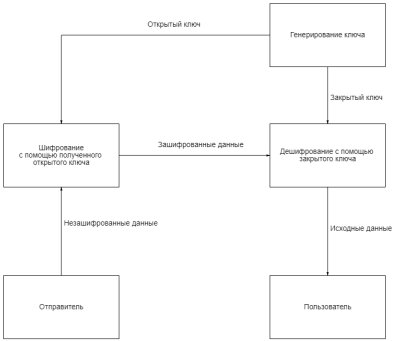

Figure 1: Простейший пример передачи данных с помощью криптографической системы

Почему нужна PKI?

По предыдущему примеру может показаться, что это это идеальный безопасный вариант передачи данных, ведь расшифровать сообщение может только владелец ключа. На самом деле этот пример уязвим, например, к такому виду атаки как “человек посередине”. Так как открытый ключ передается по открытому каналу, его может перехватить злоумышленник, создать свой ключ, и отправить свой публичный ключ отправителю. Таким образом, злоумышленник сможет читать все данные, которые будут идти от отправителя к пользователю и даже заменять их. При этом никто из участников не поймет, что их данные проходят через еще кого-то, потому что “человек посередине” сначала дешифрует сообщение своим ключом, а потом шифрует сообщение ключом пользователя. В такой ситуации нужен кто-то, кто будет проверять, действительно ли ключ принадлежит пользователю, который его отправил. Здесь и приходит на помощь *удостоверяющий центр*.

Более подробно о PKI

В основе PKI лежат следующие принципы:

- Закрытый ключ известен только его владельцу
- Удостоверяющий центр (УЦ или CA — certificate authority) создает цифровой сертификат, ставя на него свою электронную подпись - сертификат открытого ключа, удостоверяя, что закрытый ключ известен только его владельцу, а открытый свободно передается
- Никто никому не доверяет
- Все доверяют удостоверяющему центру
- УЦ проверяет принадлежит ли открытый ключ определенному человеку, который владеет закрытым ключом.

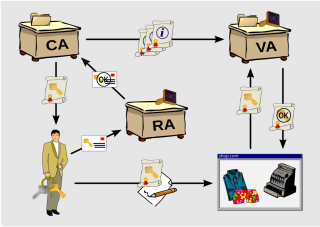

Figure 2: Пример проверки ключа при наличии Удостоверяющего, Регистрационного и Валидирующего центров

Виды архитектур

В основном выделяют 5 видов архитектур PKI, это:

- простая PKI
- иерархическая PKI
- сетевая PKI
- кросс-сертифицированные корпоративные PKI
- архитектура мостового УЦ

Виды архитектур

Простая PKI

Это самая простая система, где есть только один УЦ. Если вспомнить прошлый пример, то там мы решили проблему с доверенным лицом с помощью удостоверяющего центра. Тогда следующий логичный шаг со стороны злоумышленника выдать себя за УЦ вместо того, чтобы выдавать свой ключ за ключ пользователя. В этом случае УЦ необходимо перевыпустить все сертификаты, чтобы вернуться к работе.

Иерархическая PKI

В этой архитектуре из УЦ выстраивается иерархия, каждый УЦ подчиняется вышестоящему УЦ вплоть до главного. Пользователи разпределены по всем УЦ. В этом случае, если злоумышленник выдал себя за какой-то УЦ, то система продолжит работать, пока этот УЦ восстанавливает работоспособность.

Сетевая PKI

В этом случае так же несколько УЦ, но отношения между ними не иерархические а равноправные. В этой системе УЦ доверяют только рядом стоящим УЦ, а пользователь только тому УЦ, который выпустил ему сертификат. С такой архитектурой, независимо от того, какой УЦ был скомпрометирован, система продолжит работать: УЦ, которые выпустили сертификаты для скомпрометированного УЦ аннулируют их, как бы удаляя этот УЦ из сети. Такая система очень легко масштабируется но в ней наиболее сложное построение цепочки сертификации.

Применения

- *Электронная подпись (ЭП)* - Сторона А для документа вычисляет хеш-функцию, затем полученное значение шифруется с помощью закрытого ключа, получая ЭП. Сторона Б получает документ, ЭП и сертификат (ссылку на сертификат) стороны А, верифицирует сертификат открытого ключа стороны А в УЦ, проверяет полученную ЭП при помощи открытого ключа, вычисляет хеш-функцию документа и проверяет с расшифрованым значением. Если сертификат стороны А действителен, принимается, что документ был подписан стороной А.
- *Шифрование сообщений* - Сторона Б зашифровывает документ открытым ключом стороны А. Чтобы убедиться, что открытый ключ принадлежит стороне А, сторона Б запрашивает сертификат открытого ключа у удостоверяющего центра. Если это так, то только сторона А может расшифровать сообщение.
- *Авторизация* - Сертификаты могут использоваться для подтверждения личности пользователя и задания полномочий, которыми он наделён. Например дать право просматривать информацию или разрешение вносить изменения в материал.

Выводы

Выводы

В результате работы рассмотрели такую систему как инфраструктура открытых ключей и разобрались в ее работе, рассмотрели ее различные архитектуры и сравнили их по безопасности..

Список литературы

1. Public key infrastructure, Wikimedia Foundation, Inc., [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Public_key_infrastructure
2. Что такое PKI? Главное об инфраструктуре открытых ключей, Habr 2024, [Электронный ресурс]. URL: https://habr.com/ru/articles/655135/
3. Public Key Infrastructure, GeeksforGeeks 2024, [Электронный ресурс]. URL: https://www.geeksforgeeks.org/public-key-infrastructure/