Доклад

Инфраструктура открытых ключей

Городянский Ф.Н.

29 апреля 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Городянский Фёдор Николаевич
- студент фФМиЕН
- Российский университет дружбы народов
- 1132226456@pfur.ru
- https://Fedass.github.io/ru/

Элементы презентации

Актуальность

Инфраструктура открытых ключей (ИОК, англ. PKI — Public Key nfrastructure)— это термин, подразумевающий набор мер и политик, позволяющих развертывать и управлять одной из наиболее распространенных форм онлайн-шифрования — шифрованием с открытым ключом. Помимо того, что PKI является хранителем ключей для вашего браузера, он также обеспечивает защиту различных инфраструктур, включая внутреннюю коммуникацию внутри организаций, Интернета вещей (IoT), одноранговых соединений (P2P) и так далее. Существует два основных типа PKI:

• **Веб-PKI** - По умолчанию он работает с браузерами и со всем остальным, что использует TLS (вы, вероятно, используете его каждый день).

• **Внутренний (или локальный) PKI** — это PKI, который вы используете для собственных нужд, а именно для зашифрованных локальных сетей, контейнеров данных, корпоративных ИТ-приложений или корпоративных конечных точек, таких как ноутбуки и телефоны. В общем-то, его можно использовать для всего, что вы хотите идентифицировать.

Как именно это работает?

Как именно это работает?

PKI выстраивается вокруг двух основных концепций – ключи и сертификаты. Как и в случае с машиной «Энигма», где настройки используются для шифрования сообщения (или установления безопасного протокола), ключом внутри PKI является длинная строка битов, используемая для шифрования или дешифрования закодированных данных. Основное различие между машиной Enigma и PKI заключается в том, что с последней вы должны каким-то образом сообщить получателю настройки, используемые для кодирования зашифрованного сообщения.

Инфраструктура открытых ключей называется именно так, потому что каждая сторона в защищенном соединении имеет два ключа: открытый и закрытый.

Открытый ключ известен всем и используется во всей сети для кодирования данных, но доступ к данным невозможен без закрытого ключа, который используется для декодирования. Эти два ключа связаны сложными математическими функциями, которые трудно перепроектировать или взломать грубой силой.

Цифровая идентификация

PKI включает в себя:

• **Центр сертификации**, который выдает цифровые сертификаты, подписывает их своим открытым ключом и хранит в репозитории для справки;

• **Регистрирующий орган**, который проверяет личность тех, кто запрашивает цифровые сертификаты. Центр сертификации может выступать в качестве своего регистрационного органа или использовать для этого третью сторону;

• **База данных сертификатов**, в ней хранятся как сами сертификаты, так и их метаданные и, самое главное, даты истечения срока действия;

• **Политика сертификатов** — описание процедур PKI (в основном это набор инструкций, который позволяет оценить, насколько надежен PKI).

Для чего используется PKI?

Для чего используется PKI?

PKI отлично подходит для защиты веб-трафика: данные, проходящие через Интернет, могут быть легко перехвачены и прочитаны, если они не зашифрованы. Более того, может быть трудно доверять личности отправителя, если нет какой-то процедуры проверки.

Сертификаты SSL/TLS (защищающие действия в Интернете) демонстрируют наиболее распространенную реализацию PKI, но список на этом не заканчивается. PKI также может быть использован для:

• Цифровых подписей в программном обеспечении; • Ограниченного доступа к корпоративным интранетам и VPN; • Бесплатного доступа к Wi-Fi без пароля в зависимости от владельца устройства; • Процедуры шифрования электронной почты и данных.

Является ли PKI панацеей?

Является ли PKI панацеей?

В недавнем исследовании Института Понемона были опрошены почти 603 специалиста в области ИТ и безопасности в 14 отраслях промышленности, чтобы понять текущее состояние PKI. Это исследование выявило широко распространенные пробелы и проблемы, например:

• 73% специалистов по безопасности признают, что цифровые сертификаты по-прежнему вызывают незапланированные простои и сбои в работе приложений;

• 71% специалистов утверждают, что миграция в облако требует значительных изменений в их практике применения PKI;

• 76% говорят, что неспособность защитить ключи и сертификаты подрывает доверие, на которое опирается их организация в своей работе.

Однако самая большая проблема заключается в том, что большинству организаций не хватает ресурсов для поддержания PKI. Более того, только 38% респондентов утверждают, что у них есть персонал для надлежащего поддержания PKI. Таким образом, для большинства

Результаты

Подводя итог, можно сказать, что PKI — это бесшумный охранник, который обеспечивает конфиденциальность обычных потребителей онлайн-контента. Однако в руках настоящих профессионалов он становится мощным инструментом, создающим практически бесконечно масштабируемую инфраструктуру шифрования. Он живет в вашем браузере, вашем телефоне, вашей точке доступа Wi-Fi, во всем Интернете и за его пределами. Однако самое главное, что правильно настроенный PKI — это буфер между вашим бизнесом и самозваным кондиционером, который хочет заполучить ваши деньги.