Доклад

Инфраструктура открытых ключей

Городянский Фёдор Николаевич

Содержание

1 Цель работы 5

2 Теоретическое введение 6

3 Как именно это работает? 7

4 Цифровая идентификация 8

5 Для чего используется PKI? 9

6 Является ли PKI панацеей? 11

7 Выводы 12

Список иллюстраций

Список таблиц

1 Цель работы

Узнать, что такое Инфраструктура открытых ключей.

2 Теоретическое введение

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**, также известный как «Internet PKI», был определен RFC 5280 и дополнен CA/Browser Forum. 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.

Внутри PKI имеется открытый криптографический ключ, который используется не для шифрования ваших данных, а, скорее, для аутентификации общающихся сторон. Это как вышибала возле элитного клуба: ты не попадешь туда, если тебя нет в списке. Однако без этого «вышибалы» концепция безопасного онлайн-общения будет невозможна.

3 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. Кстати, этот принцип является воплощением ассиметричной криптографии.

Так шифруются данные в инфраструктуре открытых ключей. Но давайте не будем забывать, что проверка личности не менее важна при работе с PKI, и именно здесь в игру вступают сертификаты.

4 Цифровая идентификация

Сертификаты PKI чаще всего рассматриваются как цифровые паспорта, содержащие множество присвоенных данных. Одна из наиболее важных частей информации в таком сертификате связана с открытым ключом: сертификат – это механизм, с помощью которого этот ключ передается. Точно так же, как, например, когда вы предоставляете кому-то своё удостоверение личности.

Но на самом деле это удостоверение недействительно, если оно не выдано каким-то легитимным органом. В нашем случае такой орган — это центр сертификации (ЦС). Здесь есть подтверждение надежного источника, что субъект является тем, за кого себя выдает.

Имея это в виду, становится очень легко понять, из чего состоит PKI:

• **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).

5 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.

Использование PKI растет в геометрической прогрессии, в наши дни даже микроволновая печь может подключиться к Instagram. Этот развивающийся мир устройств Интернета вещей ставит перед нами новые задачи, и даже устройства, которые, казалось бы, существуют в закрытых средах, теперь требуют безопасности. Взять даже тот самый «злой кондиционер», о котором мы говорили во введении. Многие из наиболее убедительных примеров использования PKI сегодня сосредоточены вокруг Интернета вещей. Производители автомобилей и производители медицинских изделий — вот ещё два ярких примера отраслей, которые в настоящее время внедряют PKI для устройств Интернета вещей. Электронная система медицинского освидетельствования Эдисона также является прекрасным примером, но мы прибережем его для будущего более глубокого

рассмотрения.

6 Является ли PKI панацеей?

Как и в любой технологии, правильное исполнение иногда важнее «умного» дизайна. В недавнем исследовании Института Понемона были опрошены почти 603 специалиста в области ИТ и безопасности в 14 отраслях промышленности, чтобы понять текущее состояние PKI и практики управления цифровыми сертификатами. 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 организаций обслуживание PKI становится скорее бременем, чем панацеей от всех бед.

7 Выводы

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.