ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ И ПРОВЕРКИ ПОДЛИННОСТИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

ДЕНИС МАКСИМОВ, *max@yandex.ru*

В статье рассмотрены современные способы защиты конфиденциальной информации и аутентификации пользователей в глобальных и корпоративных сетях, в т.ч. шифрование с открытым ключом с применением цифровых сертификатов и технология предоставления доступа на базе протокола RSA SecurID. Обсуждаются инфраструктура, особенности реализации и уязвимые стороны этих технологий.

Проблема защиты данных, идентификации, а также проверки подлинности и ограничения доступа к конфиденциальной информации в компьютерных системах решается на основе различных технологий, связанных с тем или иным способом шифрования. Использование для защиты информации симметричного алгоритма шифрования (например, стандарта шифрования данных DES) предполагает обмен секретными ключами шифрования между пользователями, что делает ее эффективной только в небольших сетях. При масштабировании сети безопасный обмен секретными ключами шифрования становится неэффективным и слишком затратным. Другим недостатком стандартного шифрования данных является необходимость обмена секретным ключом. Пользователи вынуждены передавать свои секретные ключи другим пользователям.

Для проверки подлинности и защиты информации в крупных сетях была изобретена система шифрования с открытым ключом — RSA, которую в 1977 г. предложили профессоры Массачусетского технологического института Рональд Ривест (Ronald Rivest), Ади Шамир (Adi Shamir) и Лен Адлеман (Len Adleman).

Вместо использования одного и того же ключа для шифрования и дешифрования данных, в системе RSA используется пара ключей — для шифрования и дешифрования. Каждый из ключей выполняет одностороннее преобразование данных. Причем функция одного ключа обратна функции другого: действие одного ключа может отменить только другой ключ, входящий с ним в пару.

Владелец обеспечивает общедоступный доступ к открытому ключу RSA, в то время как закрытый ключ не разглашается. Для отправки личного сообщения автор шифрует его с помощью открытого ключа получателя. Зашифрованное таким образом сообщение может быть расшифровано только с помощью закрытого ключа получателя.

Сообщение пользователя может быть зашифровано с помощью закрытого ключа, т.е. ключи RSA работают в обоих направлениях. Это составляет основу цифровой подписи, поскольку если сообщение можно расшифровать с помощью открытого ключа, значит, создатель этого сообщения зашифровал его с помощью своего закрытого ключа. Так как использовать закрытый ключ может только его владелец, зашифрованное сообщение становится аналогом электронной подписи.

ШИФРОВАНИЕ С ОТКРЫТЫМ КЛЮЧОМ И ЦИФРОВЫЕ СЕРТИФИКАТЫ

Хотя сочетание закрытого и открытого ключей шифрования решает проблему защиты данных при обмене сообщениями между пользователями, они не полностью отвечают требованиям на удостоверение подлинности информации. Например, как получатель определяет, действительно ли открытый ключ принадлежит отправителю? Когда заканчивается срок действия открытого ключа? Как аннулировать ключ в случае нарушения нормального функционирования системы? В этом случае помогает цифровой сертификат.

Подобно разрешению на вождение автомобиля, где указывается тип транспортного средства, которым водитель имеет право управлять, выдавший документы орган и т.д., цифровой сертификат содержит данные о владельце (наподобие адреса электронной почты), сроке действия сертификата, наименовании выдавшего сертификат органа, серийном номере, информации, связанной с выдачей и использованием сертификата, цифровой подписи лица, выдавшего сертификат и, возможно, другую информацию. Кроме того, сертификат содержит открытый ключ и, наконец, контрольную сумму, которая подтверждает, что сертификат является подлинным.

Центры сертификации (Certification Authority, CA) — это организации, которые выпускают сертификаты и хранят открытые ключи.

Центр сертификации поддерживает список всех подписанных сертификатов, а также список аннулированных сертификатов. Сертификат незащищен до тех пор, пока он не будет подписан, поскольку только подписанный сертификат не может быть изменен. Рассмотрим, как работают общие протоколы при обмене данными между защищенным сервером и клиентом, который, как правило, является веб-обозревателем на пользовательском компьютере.

Пользователь генерирует пару ключей (открытый и закрытый) и направляет открытый ключ в центр сертификации. Центр сертификации проверяет аутентичность отправителя и выполняет необходимые шаги, чтобы убедиться, что запрос принят от отправителя. Различные центры сертификации могут использовать различную политику по установлению безопасности. После этого веб-обозреватель (на стороне клиента) и сервер устанавливают связь в защищенном режиме по протоколу безопасных соединений (Secure Sockets Layer, SSL), который является де-факто стандартным способом защищенной связи через интернет. Технология SSL основана на использовании SSL-сертификатов, которые удостоверяют подлинность веб-сайта для пользователя обозревателя, и обеспечивает шифрованную связь, используя асимметричное шифрование. На рисунках 1 и 2 показано перемещение сертифи-

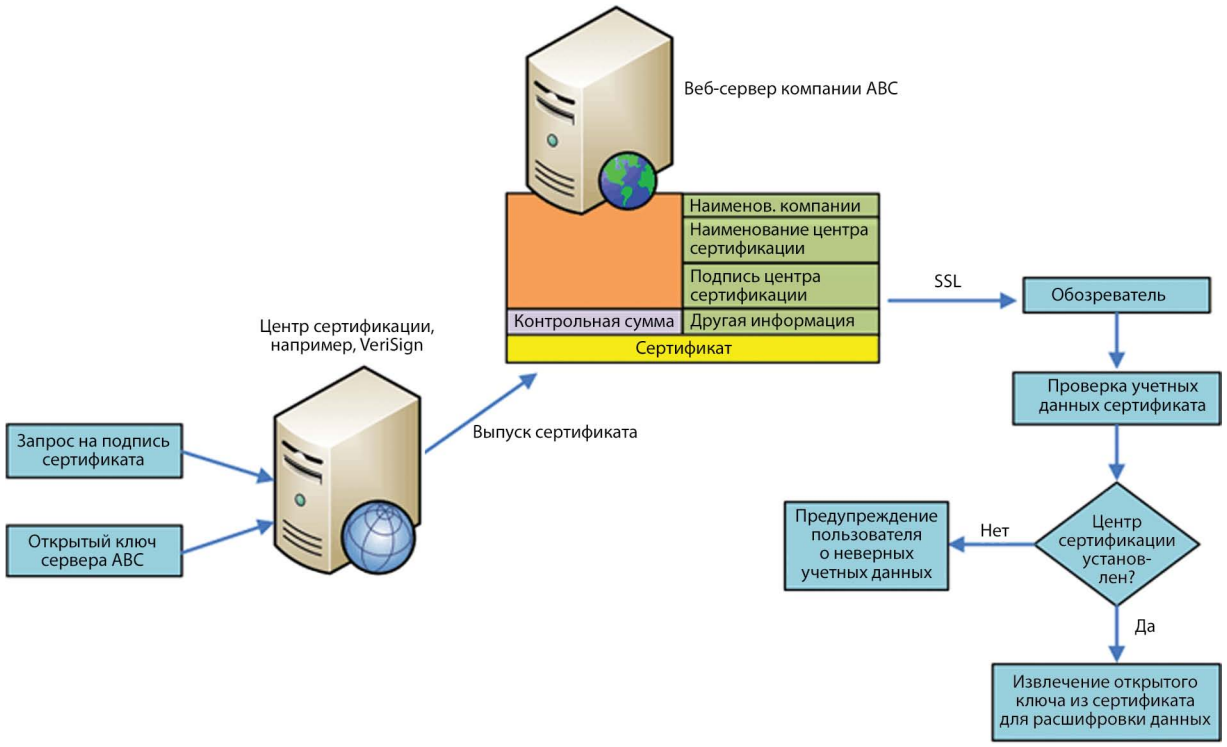


Рис. 1. **Перемещение сертификата на защищенном веб-сайте**

ката, а также этапы установления SSL-соединения.

Если пользователь хочет послать конфиденциальную информацию на веб-сервер, обозреватель обращается к цифровому сертификату сервера и получает открытый ключ для шифрования данных. Поскольку только веб-сервер имеет доступ к частному ключу, лишь он может расшифровать информацию.

Ниже приведены этапы SSL-соединения.

1. Клиент подсоединяется к веб-сайту с SSL-защитой (URL начинается с https).

2. Веб-сайт пересылает копию своего SSL-сертификата в обозреватель вместе с шифрованным подтверждением того, что он обладает соответствующим частным ключом.

3. Обозреватель клиента проверяет подпись, чтобы определить подлинность сертификата. После проверки того, что сертификат подписан одним из главных Центров сертификации (Trusted Root Certification Authorities), например VeriSign или Entrust, и определения его срока действия запускается защищенное соединение.

4. При успешном соединении (т.е. если сертификат действителен) обозреватель клиента генерирует одноразовый сеансовый ключ (симметричный ключ) и выполняет шифрование с помощью закрытого ключа сервера (извлеченного из SSL-сертификата). Затем обозреватель клиента высылает зашифрованный сеансовый ключ на сервер, так чтобы они оба имели копии ключей.

5. Сервер расшифровывает сообщение с помощью частного ключа и извлекает сеансовый ключ. Этим завершается SSL-синхронизация и разрешается защищенное соединение. Обозреватель клиента и сервер могут связываться между собой, пересылая зашифрованные сеансовым ключом данные.

Если веб-сайт не имеет SSL-сертификата, подписанного Центром сертификации, чей ключ встроен в обозреватель, то в большинстве интернет-обозревателей будет отображаться предупреждающее диалоговое окно, в котором пользователю предлагается подтвердить подлинность сайта.

ИНФРАСТРУКТУРА ЗАЩИТЫ НА ОСНОВЕ ТЕХНОЛОГИИ RSA SECURID

RSA SecurID представляет собой двухфакторный протокол аутентификации, который позволяет клиентам виртуальных частных сетей (VPN) регистрироваться на защищенном сервере. Каждое физическое устройство RSA Secure ID имеет уникальный серийный номер, указанный на обратной стороне устройства.

В процессе производства индивидуальное устройство SecurID (или токен) получает случайный 128-битный секретный ключ (начальный вектор генерации), который поддерживается в базе данных и соответствует серийному номеру устройства.

Каждые 60 с процессор устройства RSA SecurID принимает 64-битное значение текущего времени и 128-битный ключ (начальный вектор генерации) и генерирует весьма большое число (по определенному алгоритму), которое затем преобразуется (хешируется) в 6- или 8-значное число на выходе — токен-код.

Алгоритм, который обычно используется на данном этапе, основан на стандарте симметричного шифрования AES-128. В этом состоит отличие от RSA-шифрования с открытым ключом, которое основано на асимметричных ключах — паре открытый ключ/закрытый ключ.

Сгенерированный токен-код передается на веб-сайт или VPN-клиент, который отправляет его на сервер аутентификации RSA. Как только вводится имя пользователя, сервер RSA

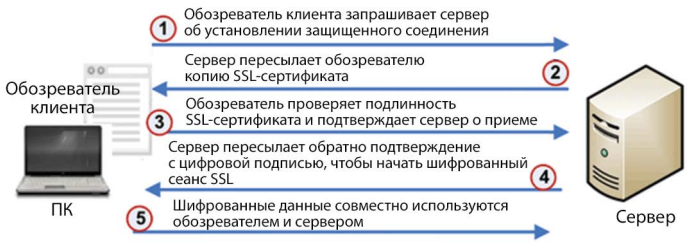


Рис. 2. **Этапы установления SSL-соединения между обозревателем и сервером**

по этому имени начинает в базе данных поиск на соответствие секретного ключа токен-коду и запускает тот же алгоритм хеширования. Таким образом, используется текущее время и ключ для генерации 8-значного выходного кода, который должен совпадать с 8-значным цифровым кодом, введенным пользователем вместе с именем пользователя. Если эти коды совпадают, пользователь получает доступ к удаленному серверу.

Если коды не совпадают, сервер добавляет к текущему времени минуту и генерирует другое 8-значное число.

При совпадении этих чисел сервер обрабатывает их как правильный токен, полагая, что нарушилась синхронизация. Синхронизация может нарушаться из-за влияния различных факторов как на стороне пользователя, так и на стороне сервера.

В случае если токен не совпадет с тремя различными секретными кодами (текущее время, 1 мин, –1 мин), сервер попытается повторить этот процесс, но в более длительном интервале времени (текущее время, 10 мин, –10 мин). Если один из кодов совпадет, сервер высылает запрос пользователю, в котором требует ввести следующее 8-значное число (следующий токен-код), который появляется на устройстве SecurID.

Если все верно, сервер позволяет пользователю зарегистрироваться, и весь процесс повторяется еще раз. Это обеспечивает защиту в случае внешней атаки на секретный код, поскольку в течение 1 мин невозможно отгадать секретный код, который представляет собой 8-значное число, т.е. 108 комбинаций цифр.

Несмотря на высокую степень защиты данной технологии, она, тем не менее, имеет ряд уязвимых сторон.

Хотя токены RSA SecurID обеспечивают защиту от атак на коды идентификации путем использования одноразовых паролей для каждого сеанса, они не гарантируют защиту от действий «человека посередине», т.е. от перехвата сообщений, которыми обмениваются корреспонденты и извлечения из них полезной информации.

Если «атакующий» организует блокировку процесса аутентификации пользователя на сервере до тех пор, пока не станет действительным следующий токен-код, он получит возможность зарегистрироваться на сервере. Сервер аутентификации SecurID постарается предотвратить выявление пароля и синхронную регистрацию пользователя и злоумышленника с помощью отклонения обоих запросов на аутентификацию, если одновременно два действующих пароля присутствуют в текущий промежуток времени.

Однако если атакующий блокирует возможность аутентификации пользователя, то сервер SecurID позволяет атакующему зарегистрироваться на сервере.

Другое слабое место в защите может быть связано с применением таких технологий как фишинг. Это одна из методик обмана и использования недостатков в защите веб-сайтов, когда по электронной почте рассылаются сообщения с предложением ввести персональные данные на мошенническом сайте, который выглядит почти идентичным законному сайту.

Если атакующий получает учетные данные, введенные пользователем в виде открытого текста, они могут быть задействованы для регистрации на сервере до момента, когда истечет срок действия токена (обычно в течение 1 мин).

В качестве альтернативного варианта используются программные токены, однако аппаратные токены более устойчивы к взлому, в то время как при программной реализации секретные ключи могут быть продублированы.

С другой стороны, аппаратные токены могут быть физически украдены (или приобретены обманным путем) у конечного пользователя. Компактный форм-фактор аппаратных токенов делает кражу намного более вероятным событием, чем сканирование компьютеров.

При такой модели атаки безопасность системы можно повысить с помощью таких механизмов шифрования/аутентификации как протокол SSL, который, как упоминалось выше, основан на использовании пары ключей — открытого и закрытого.

Отметим, что для обычной корпоративной сети RSA поддерживает только распределение секретных ключей в соответствии с серийным номером токена. Распределение секретных ключей между пользователями обычно поддерживается на уровне клиент-сервера, а не RSA. Поэтому если даже хакер получит доступ к базе данных RSA, которая хранит все токен-коды, ему понадобится список пользователей с определенным токеном.

Хакеру потребовалось бы каждую минуту заранее вычислять все варианты ключей/серийных номеров, затем перехватывать несколько раз трафик аутентификации, чтобы идентифицировать обе необходимые составляющие — пользователя и токен-кода.

Другим облегчающим задачу защиты фактором является то, что все токены SecurID сопровождаются пин-кодом и паролем. Поэтому знания только текущего токен-кода недостаточно для немедленного взлома учетной записи. Однако поскольку атакующему так или иначе следует постоянно следить за пользователем, он также может проконтролировать ввод пин-кода и пароля (которые, в отличие от токена, являются статичными величинами).

В итоге, следует отметить, что хотя RSA SecurID предоставляет высокий уровень надежности, недостаточная защита от атак «человека посередине» вызывает некоторую степень уязвимости этого метода. В такой ситуации возможным решением, направленным на повышение уровня безопасности в компьютерных системах, может, например, стать сочетание технологии RSA SecureID и шифрования с открытым ключом.

ЛИТЕРАТУРА

1. Mohit Arora. Public key cryptography and security certificates//www.eetimes.com.

2. Mohit Arora. Understanding the security framework behind RSA SecurID//www.eetimes.com.

3. Mohit Arora. Securing your apps with Public Key Cryptography & Digital Signature// www.eetimes.com.

СОБЫТИЯ РЫНКА

| TE CONNECTIVITY: РАСШИРЕНИЕ ЛИНЕЙКИ ПОСТАВОК КОМПЭЛ | В конце 2011 года компания TE Connectivity (бывшая Tyco Electronics) заключила дистрибьюторское соглашение с компанией **КОМПЭЛ**.

Продукция **TE Connectivity**, широко известная на российском рынке под брендом **Tyco Electronics**, насчитывает более полумиллиона наименований, включающих не только электрические соединители и терминалы, но также реле, изделия для ВОЛС, устройства защиты электрических и сигнальных цепей, сенсорные экраны. Изделия компании используются в производстве потребительской электроники, в электроэнергетике, в медицинской, автомобильной и аэрокосмической электронике, в телекоммуникационной индустрии.

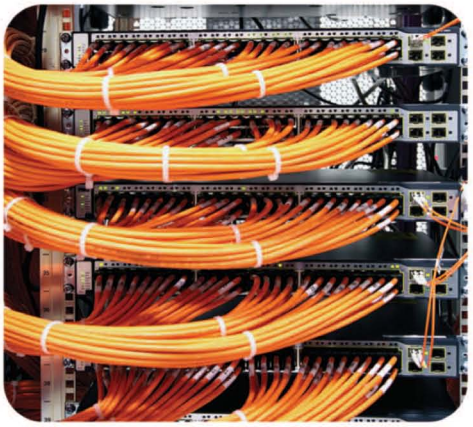
Основной объем продаж TE Connectivity в России составляют разъемы, реле, кабель и маркировочная продукция, предназначенные для применения в индустриальной, железнодорожной, автомобильной отраслях, системах автоматизации, бытовой и медицинской техники.

Первая партия продукции TE Connectivity уже поступила на московский склад компании КОМПЭЛ.

www.compel.ru

Компэл – официальный дистрибьютор TE Connectivity (Tyco Electronics)






- 500 наименований TE Connectivity (Tyco Electronics) уже на складе в Москве
- Прямой онлайн-доступ к 110 000 наименований со сроком поставки 2-4 недели
- Техническая поддержка
- Возможность индивидуальной поддержки складских запасов под проекты

TE Connectivity по итогам 2011года

- Мировой лидер в продажах разъемов
- В тройке лидеров по объему продаж реле