Московский физико-технический институт(Государственный Университет)
Кафедра Радиотехники
http://www.re.mipt.ru/infsec

Эссе по курсу «Зашита информации».

Безопасность «Skype».

Чурсов А.Г.
315г.

Москва, 2007г.

Введение:

В последнее время одной из наиболее быстро развивающихся отраслей связи является IP-телефония. Skype - это запатентованная система VoIP, которая была разработана Skype Technologies. Skype работает на большинстве платформ: Windows, Mac OS X, Linux и Pocket PC. Skype – это простая компьютерная программа, которая позволяет делать массу вещей: звонить другим абонентам Skype во всем мире, звонить из Skype на стационарные и мобильные телефоны, отправлять SMS-сообщения на мобильные телефоны и даже устраивать видеоконференции.

Skype основан на технологии соединения равноправных узлов ЛВС (одноранговых узлов) методом peer-to-peer. Вместо того чтобы передавать потоки данных между абонентами через центральный сервер, они передаются напрямую через Интернет от одного компьютера к другому (peer-to-peer) либо через специальные узлы. Эти узлы, осуществляющие координацию, адресацию и маршрутизацию потоков, а также трансляцию запросов пользователей к серверу аутентификации, называются *«супер-узлами»*, при этом каждый пользователь может по своему желанию выполнять функции супер-узла, отметив в своём клиенте соответствующую опцию. Skype-клиент строит сеть из связей с другими Skype-клиентами, которая может быть затем использована для того, чтобы находить других пользователей и посылать им сообщения. А главной особенностью является то, что Skype-клиенты без труда работают за брандмауэрами (сетевыми экранами/файрволами) и системами трансляции сетевых адресов (NAT).

Система Skype получает доход за счет того, что берет оплату с пользователей за использование терминальных шлюзов, которые соединяют сеть программы Skype с телефонными сетями общего пользования.

Начало использования Skype:

В последнее время страсти все больше и больше разгораются по поводу защищенности Skype и его пользователей от различного рода диверсий. О каких диверсиях может идти речь? Для начала вкратце рассмотрим, какие именно услуги предлагает эта программа, чтобы выяснить, что от нее ожидают пользователи и что - теоретически - может произойти, если эти ожидания не оправдаются.

В упрощенном (бесплатном, а потому, очевидно, наиболее популярном) варианте использования Skype пользователь A, желающий пообщаться с пользователем B при помощи этого сервиса, закачивает и устанавливает на своем компьютере программу-клиент и заводит идентифицирующий его аккаунт - Skype-имя (логин) и пароль. Пользователь B проделывает аналогичную разовую процедуру. Затем один из них должен найти другого по его Skype-имени и вызвать того на контакт. Подобная процедура типична и для обычных текстовых мессенджеров вроде ICQ (кстати, Skype можно использовать и в таком качестве).

Что ожидает пользователь A от такого сервиса - помимо того, разумеется, что этот сервис будет как можно более дешевым, а программа не примется каждые две минуты "падать" или, что хуже, втайне собирать личную информацию с его компьютера и отсылать ее "в Центр"? Во-первых, A ожидает, что если он захочет общаться с B, то программа свяжет его именно с B, а не с неким C, выдающим себя за него. Во-вторых, A надеется, что никакому D не удастся подслушать их беседу. В-третьих, поскольку мы имеем дело с компьютерами и использованием Интернета, он еще очень хочет, чтобы зловредный E не попытался подцепиться к каналам, которые использует Skype для обмена данными беседы A и B, чтобы, перефразируем классиков, "пускать ему оттуда нехороших вирусов". И, наконец, было бы очень неплохо, чтобы его пароль, а также записи его бесед с B, если таковые ведутся, не достались ни C, ни D, ни даже E - где бы эти данные ни хранились.

Криптография в Skype:

Анализ безопасности Skype осложнен в основном по причине того, что протокол Skype является запатентованным и закрытым, единственный источник информации — это заявления самой компании о надежности программы, и та информация, которая может быть получена при техническом анализе данного программного обеспечения.

В Skype широко и в целом с умом используется криптография, при этом шифрование производится только по стандартам (стандарт симметричного шифрования AES, система публичных ключей RSA, схема восстановления сообщений с цифровой подписью ISO 9796-2, алгоритм криптографического хеширования SHA-1 и потоковый шифр RC4).

Главным секретом Skype является так называемый закрытый ключ центрального сервера, S_S. Соответствующий открытый ключ, V_S, и идентификатор этой ключевой пары хранятся в каждой клиентской программе.

На самом деле существует две пары ключей центрального сервера. Одна с длиной 1536 бит, а другая с длиной 2048 бит. Выбор, какую из пар использовать, делается сервером. Он зависит от того, приобрел ли пользователь право на использование дополнительных сервисов Skype, например SkypeOut(возможность звонить на номера сети общего пользования в программе Skype) или SkypeIn(подписчику этой услуги предоставляется в аренду телефонный номер, на который абоненту Skype могут звонить люди с любого телефона). Если да, то используется длинный ключ. Если пользователь этого не делал, то используется короткий ключ.

Использование Skype начинается с регистрации нового пользователя. Пользователь выбирает желаемые username, назовем его A, и password, назовем его P_A. Skype-клиент генерирует ключевую пару RSA(S_A и V_A) длиной 1024 бита. Закрытое значение ключа, S_A, и хеш-функция пароля, $H(P_A)$, хранятся в наиболее безопасном месте на компьютере пользователя (клиент Skype для Windows делает это при помощи Windows CryptProtectData API). Далее клиентская программа устанавливает сеанс с центральным сервером, пакеты шифруются по алгоритму AES с 256-битным ключом. Ключ этот генерируется клиентской программой с помощью платформо-зависимого генератора случайных чисел и передается на сервер в зашифрованном при помощи открытого ключа сервера виде. В ходе защищенной сессии клиентская программа передает серверу A, $H(P_A)$ and V_A. Центральный сервер проверяет означенное Skype-имя на уникальность и корректность и в случае успеха сохраняет данные о клиенте(A, $H(H(P_A))$) в своей базе. Сервер формирует и назначает персональный идентификационный сертификат для A, IC_A, который содержит RSA подпись центрального сервера, связывающую A и V_A, и идентификатор ключа S_S. IC_A пересылается пользователю A.

Идентификационный сертификат - очень интересная штука. Он представляет собой электронное удостоверение, которое может быть использовано для установления личности абонента Skype, независимо от его местонахождения. Дело в том, что процесс общения между пользователями Skype происходит при помощи технологии, основанной на соединении одноранговых узлов (peer-to-peer communications). Если говорить упрощенно, между клиентами формируется прямое соединение, и, сколько бы пользователей Skype ни общалось между собой по сети, их общение не оказывает никакой нагрузки на центральный сервер. Наличие же у пользователей заверенных сервером идентификационных сертификатов позволяет каждому из них убедиться в аутентичности собеседника, даже не обращаясь к серверу. Идентификационный сертификат действителен в течение ограниченного периода времени. Для усиления безопасности он периодически обновляется.

Теперь предположим, абонент A хочет поговорить с абонентом B, и между ними раньше не было соединения. A пытается создать прямое соединение с B. Если ему это удается, то начинается передача информации. Но не всегда удается установить соединение напрямую с нужным абонентом. Это может произойти, если Skype клиент принимающего находиться за фаерволом или NAT. Тогда вызывающий абонент передает сообщение планируемому адресату через суперузлы. Далее устанавливается новое соединение с 256-битным ключом SK_{AB}. Формируется он следующим образом: пользователь A генерирует 128 бит ключа и шифрует их с помощью открытого ключа пользователя B, затем передает шифрованное послание B. Пользователь B аналогично генерирует 128 бит ключа, шифрует их с помощью открытого ключа A и передает ему. Из двух половин по 128 бит складывается 256-битный ключ для шифрования во время сессии между A и B. Когда сессия между A и B будет завершена, ключ уничтожается. Таким образом, для каждой новой сессии используется новый ключ SK_{AB}.

Виды атак на Skype протокол передачи данных:

1. ***Man-in-the-Middle (MITM) Attacks***
   Цель этой атаки для взломщика – пародировать вызываемого и вызывающего абонентов друг для друга. Тогда информация будет проходить от вызывающего через нарушителя к вызываемому абоненту и наоборот. Целью атаки является получение доступа ко всей информации, передаваемой в процессе общения абонентов. Взломщик должен суметь убедить вызывающего в том, что он вызываемый, и наоборот. Это можно сделать при помощи сертификатов, подтверждающих личности,(истинных или фальшивых). При успешном для взломщика исходе, он может стать помехой или даже полностью блокировать передачу данных между абонентами.

2. ***Replay Attack***
   Атака повторного воспроизведения стремится убедить узел вступить в сессию с нападавшим, воспроизводя данные, захваченные нападавшим во время предыдущей сессии между целью и другим узлом. Возможные цели атаки включают дублирование ключевого потока, используемого ранее. Нападавший мог наблюдать многочисленные установления связи, вовлекающие целевой узел. Это дало бы доступ к многократным вызовам и ответам. Нападавший мог бы тогда послать вызов цели, выдавая себя за предыдущий узел. Цель ответила бы собственным вызовом. Если бы целевой вызов был идентичен тому, который нападавший наблюдал ранее для вызываемого, то нападавший мог бы тогда ответить на вызов правильно и перейти к следующим аспектам обменного протокола.

3. ***Password Guessing Attack***
   Пользователям предоставляется выбор хранить или нет их пароль Skype на компьютере, который они используют. Большинство пользователей соглашается на эту опцию. В Windows пароль передается операционной системе для защиты с использованием Windows CryptProtectData API. Пользователь, который позднее залогинится на систему, сможет использовать Skype без каких-либо удостоверений личности. Остальные пользователи, которые выбрали не сохранять их пароль, должны логиниться через клиент-сервер протокол каждый раз перед использованием Skype. Для защиты против угадывания пароля, центральный сервер Skype вызывает таймаут после серии некорректных вводов пароля.

4. ***Side-Channel Attacks***
   Известно, что во время выполнения криптографических операций может иногда утекать информация об открытом тексте или ключе из-за потребления разделяемых ресурсов, таких как памяти или времени CPU. Так, например, если злонамеренная программа запущена на той же самой платформе что и клиент Skype, то злонамеренная программа могла бы проследить биты частного ключа пользователя. Это, в конечном счете, позволило бы владельцу злонамеренной программы замаскироваться как пользователь. Но это считается незначительной проблемой, потому что злонамеренная программа, выполняющаяся на той же самой платформе, что и клиент Skype могла бы сделать намного большее повреждение.

Заключение:

Возникает закономерный вопрос — удовлетворяет ли Skype, реализующий пиринговые технологии, требованиям безопасности, предъявляемым к приложениям? По этому вопросу мнения экспертов разделились. Одни из них считают, что Skype пока не в состоянии обеспечить должный уровень защиты информации, другие — что решить эту проблему возможно уже сейчас.

Так, например, при невнимательной настройке любой компьютер с установленной копией программы может стать узлом для передачи не только своего, но и стороннего IP-трафика. Это и увеличит нагрузку на данный узел, и потребует дополнительной оплаты трафика. И то, и другое малоприятно.

Чтобы не заразить свой ПК «троянским конем» или вирусом при использовании Skype, при обмене файлами через Skype вам следует предпринимать меры предосторожности, когда вы принимаете файлы от другой стороны. Действовать нужно так же, как при работе с любой программой электронной почты, программой для передачи файлов или как при загрузке файлов из Интернета. Настоятельно рекомендуется использовать обновленные антивирусные программы для проверки всех входящих файлов, даже если вы хорошо знаете их отправителей.

Skype не содержит в себе рекламы или шпионящее программное обеспечение. Однако в Интернете можно найти установщики Skype, содержащие в себе стороннее программное обеспечение, которое может включать в себя рекламу и прораммы-шпионы. Поэтому настоятельно рекомендуется получать последнюю версию Skype, скачивая со Skype веб-сайта www.skype.com/download.

В целом, Skype можно назвать одной из самых удачных программ на рынке IP-телефонии. Хотя, становится понятна озабоченность авторов Skype о безопасности переговоров – ведь большая часть трафика проходит через третьих лиц. Однако они утверждают, что разработанный протокол защищен от перечисленных выше методов атак.

Ссылки:

1. http://www.skypeclub.ru/skype_security.htm
2. http://www.skype.com/intl/ru/security/
3. http://www.connect.ru/article.asp?id=4997
4. http://telecom.compulenta.ru/internet/phone/skype/