Подход к противодействию кросс – протокольным атакам

М. А. Кожевников, email: kmaxss@yandex.ru[1]
А. В. Алямкин, email: Alexandralyamkin@yandex.ru[1]
Г. В. Васильев, email: gleb_mesarthim@mail.ru [1]
К. В. Торгашов, email: torgashov18@mail.ru [1]

[1] Краснодарское высшее военное училище им. С. М. Штеменко

Аннотация. *В данной работе проводится исследование влияния IPv4 на измерение количества уязвимых и эксплуатируемых сервисов при проведении кросс-платформенных атак.*

Ключевые слова: *кросс-протокольная атака, веб-сервер, TLS, стандарт X.509,ALPN.*

Введение

С помощью протокола Transport Layer Security (TLS) между двумя конечными точками связи устанавливаются конфиденциальные и аутентифицированные каналы. В типичных протоколах конечного пользователя, таких как HTTP, SMTP или IMAP, сервер TLS аутентифицируется на клиента путем предоставления сертификата X.509. В этом случае сервер идентифицируется по полю Common Name (CN) или расширению Subject Alternate Name (SAN) в сертификате, которое содержит одно или несколько имен хостов или шаблонов подстановочных знаков (например, * . bank . com).

Поскольку TLS не защищает целостность самого TCP-соединения (т.е. IP и порт источника, IP и порт назначения), злоумышленник может перенаправить трафик TLS для конечной точки и протокола службы TLS на другую, замещающую конечную точку и протокол службы TLS. Если клиент считает сертификат заменяющего сервера действительным для предполагаемого сервера, например, если сертификаты с подстановочным знаком разделяются между поддоменами, аутентификация соединения нарушается [1-4]. Это может привести к возникновению кросс-протокольной атаки на прикладном уровне, когда клиент неосознанно отправляет данные протокола для предполагаемого сервера на заменяющий сервер, который ожидает другой протокол, потенциально ставя под угрозу безопасность любого из серверов на прикладном уровне.

В целом, кросс-протокольные атаки можно рассматривать между любыми двумя протоколами, защищенными TLS. Хотя некоторые

комбинации протоколов с большей вероятностью приведут к успешным атакам, чем другие, даже совершенно разные форматы данных могут быть совместимы [5-7].

1. Методология исследования TLS

Было оценено количество HTTPS-серверов, которые уязвимы для кросс-протокольных атак с SMTP, IMAP, POP3 или FTP при сканировании адресного пространства IPv4 в масштабах всего интернета путем поиска серверов с надежными, совместимыми сертификатами. Кроме того, было проанализировано, как эти серверы реагируют на недействительные имена серверов с помощью SNI и как они реагируют, если не могут выбрать действительный протокол прикладного уровня с помощью ALPN.

Чтобы оценить, сколько серверов приложений имеют доверенные сертификаты, совместимые с HTTPSсерверами, было произведено множественное сканирование IPv4 на стандартных и известных портах приложений для SMTP (25, 587, 465, 26, 2525), IMAP (143, 993), POP3 (110, 995) и FTP (21, 990), используя ZMap и ZGrab 2.0. Были исключены все узлы, которые не смогли завершить рукопожатие TLS. Затем было определено, какие из этих серверов имеют путь доверия к общедоверенному корневому ЦС. ЦС считался общедоверенным, если ему доверяют Mozilla, Google, Microsoft, Apple, Oracle или OpenJDK. Затем были собраны все доверенные сертификаты и были извлечены их общие имена (CN) и измененные имена субъектов (SAN), чтобы найти соответствующие HTTPS-серверы.

Для записей, содержащих символ *, угадывались поддомены, заменяя * на www. Затем производились попытки подключиться к хостам на порт 443 с использованием протокола HTTPS и производился сбор представленных сертификатов.

Были произведены еще два сканирования тех серверов приложений SMTP, IMAP,POP3 и FTP, которые предлагали доверенный сертификат. В ходе первого сканирования оценивалось количество серверов приложений, которые допускают неправильные имена хостов SNI, выполнив рукопожатие TLS с именем хоста SNI example.com. Фиксировалось успешное завершение квитирования TLS, несмотря на несовпадающее имя хоста. Во время второго сканирования оценивалось количество серверов приложений, которые допускают корректные протоколы прикладного уровня, выполнив рукопожатие TLS с тем же расширением ALPN, которое было отправлено браузером Chrome. Регистрировалось успешное завершение рукопожатия TLS, несмотря на несовпадение идентификаторов протоколов.

2. Результаты сканирования Интернета

Кросс-протокольные атаки на HTTPS могут быть выполнены с использованием SMTP, IMAP, POP3 и FTP в качестве серверов приложений. С помощью этих протоколов могут быть произведены атаки на загрузку, скачивание и отражение.

Результаты сканирования можно увидеть в рис. 1. По всем протоколам 62,85% обнаруженных серверов приложений TLS были использованы как правило, доверенные сертификаты. Заметным исключением является FTP на порту 21, где количество доверенных сертификатов составило всего 44%. Возможное объяснение заключается в том, что сертификаты FTP серверов из десяти подписываются частными центрами сертификации, которым браузеры обычно не доверяют. Было обнаружено, что около 25% недоверенных сертификатов FTP были подписаны такими частными ЦС.

			Server IPs with TLS		Certificate Names (CN & SAN)	
Protocol	**Port**	**STARTTLS**	**Total**	**Valid Certificate**	**# Unique**	**# HTTPS**
SMTP	25	Yes	3,427,465	1,744,052 (50,88%)	1,048,090	782,710 (74.68%)
SMTP	587	Yes	3,495,626	2,471,893 (70,71%)	1,176,374	821,534 (69.85%)
SMTPS	465	-	3,511,544	2,450,062 (69,77%)	1,046,240	724,557 (69.27%)
SMTP	26	Yes	565,672	514,425 (90,94%)	130,624	79,234 (60.66%)
SMTP	2525	Yes	231,009	139,536 (60,40%)	50,514	31,009 (61.40%)
IMAP	143	Yes	3,707,577	2,463,293 (66,44%)	1,103,455	782,410 (70.92%)
IMAPS	993	-	3,919,999	2,597,232 (66,26%)	1,287,370	926,313 (71.97%)
POP3	110	Yes	3,551,226	2,342,545 (65,96%)	983,912	690,111 (70.15%)
POP3S	995	-	3,828,411	2,580,379 (67,40%)	1,170,197	848,744 (72.56%)
FTP	21	Yes	4,826,891	2,130,271 (44,13%)	675,432	421,923 (62.48%)
FTPS	990	-	305,646	282,382 (92,39%)	115,292	95,197 (62.73%)
Total			31,371,066	19,716,070 (62,85%)	2,088,328	1,441,628 (69.03%)

Рис. 1. Результаты сканирования всего интернета по протоколам и портам

Сначала показано количество IP-адресов, которые предоставляют данную услугу и позволяют успешно выполнить рукопожатие TLS. Затем показано количество IP-адресов, предоставляющих сертификат, который считается действительным для браузера (за исключением соответствия имени хоста). Далее показано количество уникальных имен, найденных в CN и SAN действительных сертификатов. Наконец, приводится количество HTTPS-серверов, которые были найдены среди этих имен, с *, замененным на www, как наиболее распространенное предположение для веб-серверов, использующих сертификаты с подстановочным знаком.

По всем проанализированным протоколам были собраны в общей сложности 2 088 328 различных имен хостов. Поиск HTTPS – серверов по этим именам хостов выявил в общей сложности 1 441 628 HTTPS-серверов, для которых существует по крайней мере один сервер SMTP, POP3, IMAP или FTP, использующий в целом доверенный сертификат, что составляет 69% от всех проверенных уникальных имен хостов. Из этих веб-серверов 24 202 были в списке Tranco 1 млн самых известных хостов в Интернете. Это означает, что для большинства серверов с доверенными сертификатами на SMTP, POP3, IMAP или FTP, существует HTTPS-сервер с совместимым сертификатом, уязвимый для общей атаки по перекрестному протоколу TLS, где данные приложений обрабатываются сервером-заменителем, а не предполагаемым веб – сервером.

На основе баннерного сканирования были подсчитаны все уникальные веб-серверы (среди 1,4 млн кандидатов), для которых был определён хотя бы один сервер приложений. Иногда один и тот же веб-сервер эксплуатируется несколькими серверами приложений (например, IMAP и POP3), поэтому общее число уникальных веб-серверов меньше, чем сумма по всем протоколам.

В общей сложности было обнаружено 197 уникальных имен хостов веб-серверов, которые могут быть атакованы с использованием уязвимого SMTP, IMAP, POP3 или FTP-сервера с доверенным и совместимым сертификатом.

3. Меры противодействия

Предыдущие попытки остановить кросс-протокольные атаки пытались смягчить проблему на уровне приложений, например, закрыв соединение, если вместо допустимой команды обнаружен HTTP [8-11]. С практической точки зрения неразумно ожидать, что разработчики будут знать обо всех (включая будущие) возможных межпротокольных атаках и будут защищаться от них одна за другой.

Хотя такие меры потенциально могут остановить использование путаницы отдельных протоколов, они не могут остановить атаку в целом. Всякий раз, когда клиент заканчивает рукопожатие S_{sub} к сожалению, аутентификация, как и было обещано TLS, уже нарушена. На данный момент обмен прикладными данными еще не осуществлялся, поэтому никакие контрмеры прикладного уровня не могут предотвратить общую кросс-протокольную атаку.

4. Контрмеры с помощью сертификатов

Распространенной практикой является использование разных (несовместимых) сертификатов для разных конечных точек службы.

Однако применение такой политики на практике является сложной задачей. Проверка сертификатов ограничивается именами хостов, и поэтому каждая служба должна быть размещена на уникальном поддомене. Кроме того, ни на один сертификат не следует подавать в суд более чем за одно имя хоста, что фактически запрещает использование сертификатов с подстановочными знаками. Однако очень распространенные использование подстановочных сертификатов на практике показывает, что они представляют значительную ценность для администраторов. Даже строгая эксклюзивность сертификатов не предотвращает все возможные атаки. Злоумышленник все еще может украсть файл cookie, используя службу, размещенную на сервере поддомена, или выполнить атаки с фиксацией сеанса.

Другая идея состояла бы в том, чтобы определить различные способы использования сертификатов для различных служб. В то время как стандарт X. 509 определяет расширение для использования ключей расширения, это расширение позволяет отличать сертификаты сервера TLS только от сертификатов, используемых для электронной почты подпись, IPSec или OCSP и не обеспечивает механизм аутентификации протокола приложения поверх TLS.

Можно сделать вывод, что необходимые организационные и поведенческие изменения для достижения эксклюзивности сертификата настолько велики, что их можно рассматривать только как долгосрочную контрмеру [12].

Точно так же, как расширение ALPN защищает от межпротокольных атак, расширение SNI может защитить от атак с использованием разных имен хостов, если оно реализовано строго (т. е. соединение прерывается, если не найден соответствующий хост), что разрешено стандартом. Это может защитить от кросс-протокольных атак, когда у предполагаемого сервера и сервера-заменителя разные имена хостов, а также от некоторых атак с использованием одного и того же протокола, таких как путаница с виртуальным хостом HTTPS или атаки с путаницей контекста.

К сожалению, некоторые серверы в настоящее время не полностью осведомлены об именах хостов, за которые они несут ответственность. Добавление строгой проверки SNI на эти серверы может привести к разрыву соединений, если имена хостов отсутствуют или клиенты неправильно настроены. Тем не менее, рекомендуется включить строгую проверку SNI, если это возможно, в частности, для новых конфигураций.

Заключение

Таким образом, было проведено исследование влияния IPv4 на измерение количества уязвимых и эксплуатируемых сервисов при проведении кросс-платформенных атак. Был просканирован Интернет с целью оценивания количества серверов приложений, которые допускают неправильные имена хостов SNI и количества серверов приложений, которые допускают корректные протоколы прикладного уровня, выполнив рукопожатие TLS с тем же расширением ALPN, которое было отправлено браузером Chrome. Регистрировалось успешное завершение рукопожатия TLS, несмотря на несовпадение идентификаторов протоколов. Также были определены меры противодействия кросс-платформенным атакам.

Список литературы

1. Казарин, И. С. Обзор сетевых атак на информационные системы / И. С. Казарин, Е. М. Михайлова // В сборнике: Интеллектуальный потенциал XXI века: ступени познания. Сборник материалов XXXIX Молодежной международной научно-практической конференции. Под общей редакцией С.С. Чернова. – 2017. – С. 140-148.
2. Диченко, С. А. Концептуальная модель обеспечения целостности информации в современных системах хранения данных / С. А. Диченко // Информатика: проблемы, методология, технологии. Сборник материалов XIX международной научно-методической конференции. Под ред. Д. Н. Борисова. – Воронеж, 2019. – С. 697-701.
3. Dichenko, S. Two-dimensional control and assurance of data integrity in information systems based on residue number system codes and cryptographic hash functions / S. Dichenko, O. Finko // Integrating Research Agendas and Devising Joint Challenges International Multidisciplinary Symposium ICT Research in Russian Federation and Europe. – 2018. – P. 139-146.
4. Диченко, С. А. Контроль и восстановление целостности данных в защищенных информационно-аналитических системах / С. А. Диченко, О. А. Финько // Труды Военно-космической академии имени А.Ф.Можайского. – 2021. – № 676. – С. 36-49.
5. Горбачев, И. Е. Особенности обеспечения ИБ критической инфраструктуры с учетом специфики АСУ ТП / И. Е. Горбачев, Р. В. Лукьянов, А. М. Сухов // Защита информации. Инсайд. – 2016. – № 2 (68). – С. 30-37.
6. Диченко, С. А. Контроль и восстановление целостности многомерных массивов данных посредством криптокодовых конструкций / С. А. Диченко, О. А. Финько // Программирование. – 2021. – № 6. – С. 3-15.

7. Сухов, А. М. Алгоритм применения методов и моделей противодействия компьютерным вторжениям / А. М. Сухов, С. В. Калиниченко, В. И. Якунин // Защита информации. Инсайд. – 2016. – № 6 (72). – С. 38-41.

8. Диченко, С. А. Безопасные генераторы псевдослучайных линейных последовательностей на арифметических полиномах для защищенных систем связи / С. А. Диченко, О. А. Финько // Нелинейный мир. – 2013. – Т. 11. – № 9. – С. 632-645.

9. Сачков, И. К. Автоматизация противодействия бот-атакам / И. К. Сачков, А. Н. Назаров // T-Comm: Телекоммуникации и транспорт. – 2014. – Т. 8. – № 6. – С. 5-9.

10. Диченко, С. А. Снижение вводимой избыточности при обеспечении устойчивости информационно-аналитических систем в условиях компенсации последствий деструктивных воздействий злоумышленника / С. А. Диченко, О. А. Финько // Автоматизация процессов управления. – 2020. – № 4 (62). – С. 38-48.

11. Дементьев, В. Е. Понятийный аппарат протокольной защиты информационно-телекоммуникационной сети / В. Е. Дементьев, А. В. Дементьева, Д. А. Маняшин // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей. – 2016. – С. 70-74.

12. Сухов, А. М. Методика моделирования процесса функционирования системы обнаружения вторжений в компьютерную сеть в задачах исследования эффективности / А. М. Сухов, И. Е. Горбачев, В. И. Якунин // Проблемы информационной безопасности. Компьютерные системы. – 2017. – № 2. – С. 23-30.