А.М. Шуваева, А.В. Яковлев

МОДЕЛИРОВАНИЕ ПРОТОКОЛА SSL НА ОСНОВЕ СЕТИ ПЕТРИ

(Тамбовский государственный технический университет)

Введение. Существует множество технологий для реализации устойчивой аутентификации. На текущий момент наиболее распространены два протокола обеспечения безопасности на транспортном уровне: протокол SSL (Secure Sockets Layer) и протокол TLS (Transport Layer Security).

Особенности протокола SSL. Протокол обеспечивает конфиденциальность обмена данными между клиентом и сервером, использующими TCP/IP, причём для шифрования используется асимметричный алгоритм с открытым ключом. SSL предоставляет канал, имеющий три основных свойства [1]: аутентификация; надёжность; частность канала.

Сначала SSL делит данные на блоки 214 байтов или меньше. Каждый фрагмент данных сжат методом, согласованным по договору между клиентом и сервером. Чтобы сохранять целостность данных, SSL использует ключевую хэш-функцию для создания кода проверки подлинности (MAC). Чтобы обеспечить конфиденциальность, первоначальные данные и код проверки подлинности зашифрованы с использованием криптографии с симметричными ключами. К зашифрованной полезной нагрузке добавляется заголовок [1].

Для обмена подлинными и конфиденциальными сообщениями клиенту и серверу нужны шесть криптографических объектов секретности. Для их создания между двумя сторонами должен быть установлен один предварительный главный секретный код [1,2]. Для двух объектов, чтобы начать обмен данными, установление сеанса необходимо, но не достаточно, они должны создать между собой соединение. Объекты обмениваются двумя случайными числами и создают, используя главный секретный код, ключи и параметры, необходимые для того, чтобы обмениваться сообщениями, включая установление подлинности и секретность.

Сеанс может состоять из многих соединений. Соединение между двумя сторонами может быть закончено и восстановлено в пределах одного и того же сеанса. Сеанс может быть приостановлен и продолжен снова.

SSL использует два признака, чтобы отличить криптографическую секретность: «писать» (ключ для подписи/зашифрования исходящего сообщения) и «читать» (ключ для подтверждения/расшифрования прибывающего сообщения).

SSL содержит четыре протокола на двух уровнях [1]: протокол передачи записей; протокол установления соединения; протокол изменения параметров шифрования; аварийный протокол.

Процедура установления связи происходит в четыре фазы [1], изображенных на рис. 1.

В фазе I клиент и сервер объявляют характеристики безопасности, устанавливается ID сеанса, согласуется конкретный метод сжатия. Далее, выбирают два случайных числа, чтобы создать главный секретный код. В этой фазе сто-

роны обмениваются двумя сообщениями: «ClientHello» и «ServerHello». В фазе II сервер, если необходимо, подтверждает свою подлинность. Фаза III предназначена для подтверждения подлинности клиента. От клиента серверу можно передать до трех сообщений. В фазе IV клиент и сервер передают сообщения, чтобы изменить спецификацию шифра и закончить процедуру установления связи, происходит обмен четырьмя сообщениями [2].

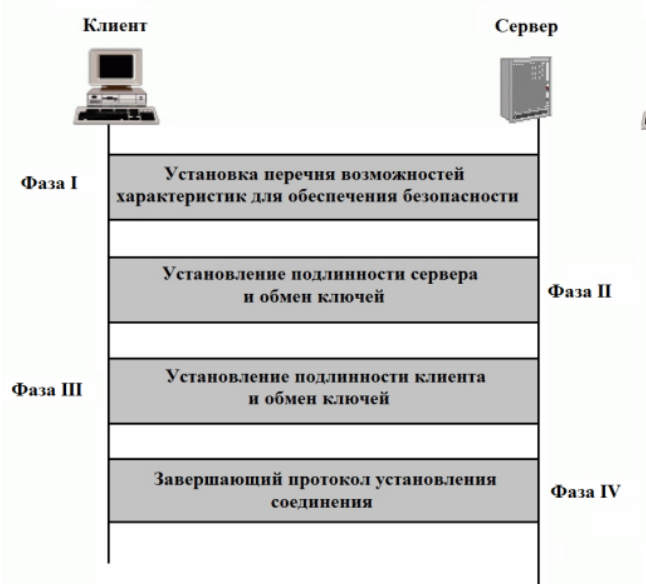

Рис. 1. Протокол установления соединения

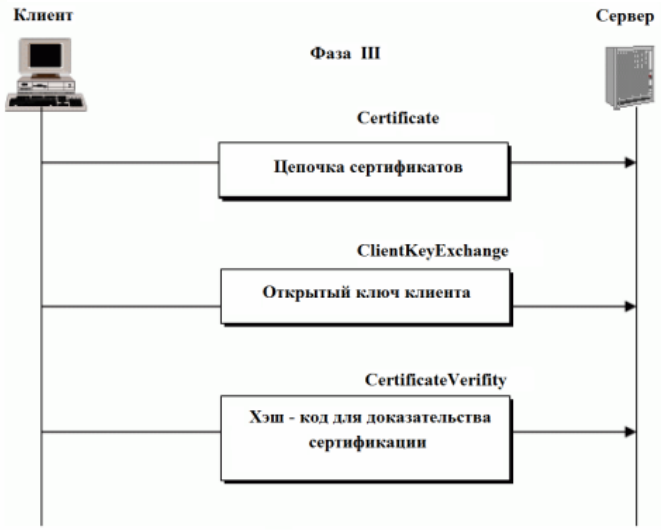

Рис. 2. Протокол установления соединения (фаза III)

Рассмотрим подробнее фазу III (рис. 2) [1].

Сертификат. Чтобы сертифицировать себя на сервере, клиент передает сообщение «Certificate», включающее цепочку сертификатов. Такое сообщение передают, только если сервер запросил сертификат в фазе II.

ClientKeyExchange. После передачи сообщения «Certificate» клиент передает сообщение «ClientKeyExchange», которое включает в себя вклад в предварительный главный секретный код.

Верификация сертификата. Если клиент передал сертификат, объявляющий о наличии открытого ключа в сертификате, он должен доказать, что знает и соответствующий секретный ключ. Доказательство владения секретным ключом он представляет, создавая сообщение и подписывая его секретным ключом [2].

Преимуществом SSL является то, что он независим от прикладного протокола. Протоколы приложения, такие как HTTP, FTP, TELNET и другие могут работать поверх протокола SSL совершенно прозрачно.

Основными целями протокола являются: криптографическая безопасность; совместимость; расширяемость; эффективность. SSL поддерживает три типа аутентификации: аутентификация обеих сторон, аутентификация сервера с неаутентифицированным клиентом и полная анонимность [2].

Атака типа «злоумышленник посередине» предполагает участие трех сторон: сервера, клиента и злоумышленника, находящегося между ними. В данной

ситуации злоумышленник может перехватывать все сообщения, следующие в обоих направлениях, и подменять их. Злоумышленник представляется сервером для клиента и клиентом для сервера. Но такая атака невозможна при использовании протокола SSL, так как для проверки подлинности источника используются сертификаты, заверенные центром сертификации.

Протокол SSL состоит из двух основных частей: протокола рукопожатия, отвечающего за процедуру аутентификации и выработки ключей защищенного обмена, и протокола передачи данных.

Наиболее сложная часть протокола SSL – протокол рукопожатия, состоящая из последовательного обмена сообщениями между инициатором протокола или клиентом и сервером. Подробно последовательность шагов протокола SSL изложена в источнике [1].

Динамическая модель протокола SSL на основе сети Петри [3]. Обозначения элементов этой сети следующие:

1) конечное множество позиций:

$P = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}, p_{15}, p_{16}, p_{17}, p_{18}, p_{19}, p_{20}, p_{21}, p_{22}, p_{x1}, p_{x2}\}$.

2) конечное множество переходов:

$T = \{t_1,t_2,t_3,t_4,t_5,t_6,t_7,t_8,t_9,t_{10},t_{11},t_{12},t_{13},t_{14},t_{15},t_{16}\}$.

3) множество входных позиций перехода:

$I(t_1)=\{p_1\}$, $I(t_2)=\{p_1, p_{11}\}$, $I(t_3)=\{p_3, p_{12}\}$, $I(t_4)=\{p_4\}$, $I(t_5)=\{p_5, p_{10}\}$, $I(t_6)=\{p_6\}$, $(t_7)=\{p_7\}$, $I(t_8)=\{p_8, p_{13}\}$, $I(t_9)=\{p_9, p_{x1}\}$, $I(t_{10})=\{p_{14}\}$, $I(t_{11})=\{p_9, p_{x2}\}$, $I(t_{12})=\{p_{16}\}$, $I(t_{13})=\{p_{15}\}$, $I(t_{14})=\{p_{16}, p_{19}\}$, $I(t_{15})=\{p_{17}, p_{20}\}$, $I(t_{16})=\{p_{18}\}$.

4) множество выходных позиций перехода:

$O(t_1)=\{p_2, p_{10}\}$, $O(t_2)=\{p_3\}$, $O(t_3)=\{p_4\}$, $O(t_4)=\{p_9, p_{13}\}$, $O(t_5)=\{p_6\}$, $O(t_6)=\{p_7, p_{11}\}$, $O(t_7)=\{p_8, p_{12}\}$, $O(t_8)=\{p_{16}\}$, $O(t_9)=\{p_9\}$, $O(t_{10})=\{p_{16}\}$, $O(t_{11})=\{p_{14}, p_{15}\}$, $O(t_{12})=\{p_5\}$, $O(t_{13})=\{p_{17}, p_{19}\}$, $O(t_{14})=\{p_{18}\}$, $O(t_{15})=\{p_{21}\}$, $O(t_{16})=\{p_{20}, p_{22}\}$.

5) начальная маркировка:

$\mu_0=\{1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1\}$.

Динамическая модель, выполнена с помощью программного продукта Pipe 3.0 и изображена на рис. 3.

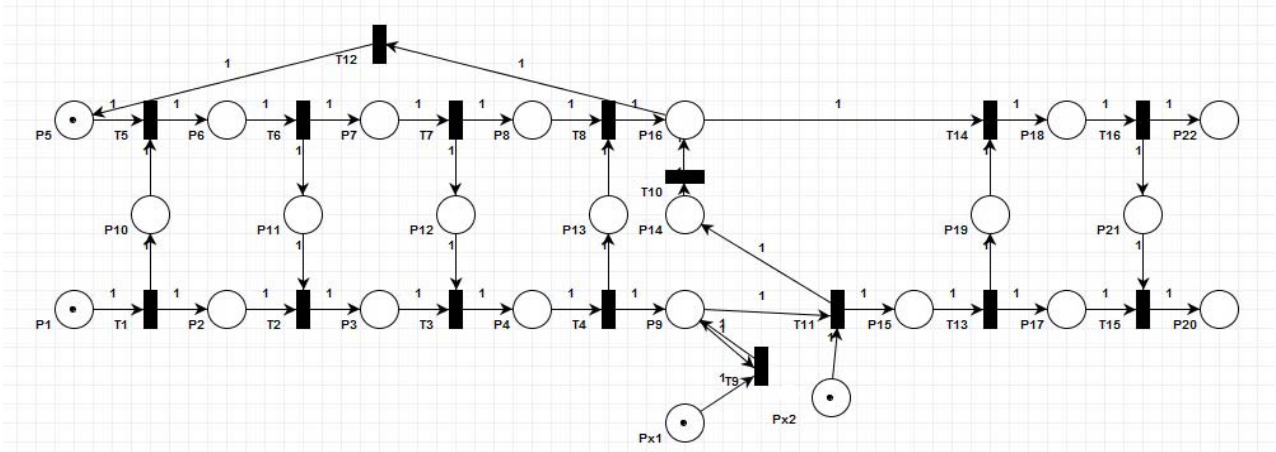

Рис. 3. Сеть Петри, моделирующая алгоритм работы протокола SSL.

Таблица 1 – Содержание компонентов модели протокола SSL

Обозн. Элемента	Описание	Маркировка	Обозн. элемента	Описание
p_1, p_5	Начальное состояние	$\mu\{p_1\}=1$, $\mu\{p_5\}=1$	t_1	Отправить сообщение «ClientHello»
P_2	Отправлен запрос на установление соединения		t_2	Получить сообщение «ServerHello»
p_3, p_7	Соединение установлено		t_3	Получить сертификат сервера
p_4	Сертификат сервера получен		t_4	Отправить сертификат клиента
p_8	Сертификат сервера отправлен		t_5	Получить сообщение «ClientHello»
p_9	Подсистема идентификации клиента		t_6	Отправить сообщение «ServerHello»
p_{10}	Сообщение «ClientHello»		t_7	Отправить сертификат сервера
p_{11}	Сообщение «ServerHello»		t_8	Получить сертификат клиента
p_{12}, p_{13}	Сообщение «Сертификат сервера (клиента)»		t_9	Проверка идентификатора
p_{14}	Отправлено сообщение об ошибке		t_{10}	Отправить сообщение об ошибке
p_{15}	Позитивный отклик		t_{11}	Проверка аутентичности параметра
p_{16}	Продолжение/прерывание сеанса		t_{12}	Вернуться в начальное состояние
p_{17}, p_{18}	Отправлено/получено сообщение «Finished» (от клиента)		t_{13}	Отправить сообщение «Finished» (от клиента)
p_{19}, p_{20}, p_{21}	Получено сообщение «Finished» (от сервера)		t_{14}	Получить сообщение «Finished» (от клиента)
p_{22}	Отправлено сообщение «Finished» (от сервера)		t_{15}	Получить сообщение «Finished» (от сервера)
p_{x1}	Ввод идентификатора	$\mu\{p_{x1}\}=1$	t_{16}	Отправить сообщение «Finished» (от сервера)
p_{x2}	Генерация и ввод значения	$\mu\{p_{x2}\}=k$		

Заключение. Таким образом, была построена модель, реализующая алгоритм работы криптографического протокола SSL на основе сетей Петри, а также проведен анализ по таким параметрам, как ограниченность, безопасность, активность, обратимость и достижимость тупиковой разметки. Из проанализированных поведенческих свойств модели можно сделать вывод, что каждое свойство для реальных протоколов важно и должно соблюдаться: ограниченность – это следствие безопасности, достижимость тупиковой разметки – это конечность функционирования модели, активность – работоспособность и необходимость данного перехода.

Литература

1. Семенов Ю.А. Протокол SSL. Безопасный уровень соединителей – [Электронный ресурс]. – Режим доступа: http://book.itep.ru/6/ssl_65.htm [Дата обращения 10.02.2014].
2. SSL - Аутентификация и обмен ключами – [Электронный ресурс]. – Режим доступа: http://chinapads.ru/c/s/ssl_-_autentifikatsiya_i_obmen_klyuchami [Дата обращения 10.02.2014]
3. Питерсон Дж. Теория сетей Петри и моделирование систем./ Дж. Питерсон - М.: Мир, 1984 - 264 с.