ИПМ им.М.В.Келдыша РАН

Абрау-2017 • Труды конференции

А.В. Никешин, В.З. Шнитман

Верификация протокола EAP и его методов в беспроводных сетях

Рекомендуемая форма библиографической ссылки

Никешин А.В., Шнитман В.З. Верификация протокола EAP и его методов в беспроводных сетях // Научный сервис в сети Интернет: труды XIX Всероссийской научной конференции (18-23 сентября 2017 г., г. Новороссийск). — М.: ИПМ им. М.В.Келдыша, 2017. — С. 369-376. — URL: http://keldysh.ru/abrau/2017/43.pdf doi:10.20948/abrau-2017-43

Размещена также презентация к докладу

Верификация протокола EAP и его методов в беспроводных сетях

А.В. Никешин, В.З. Шнитман

Институт системного программирования Российской академии наук

Аннотация. В данной работе представлен опыт верификации протокола аутентификации EAP при использовании беспроводных соединений. Беспроводная среда передачи данных является одной из областей, в которой активно используется данный протокол безопасности. А широкое распространение в последнее время мобильных устройств предъявляет дополнительные требования к системе безопасности передачи информации, и в том числе к аутентификации устройств. В работе использовался новый тестовый набор, разработанный с использованием технологии UniTESK и методов мутационного тестирования. Технология UniTESK позволяет автоматизировать процесс верификации сетевых протоколов на основе их формальных моделей, а методы мутационного тестирования позволяют протестировать устойчивость реализации протокола к искаженным сообщениям.

Ключевые слова: безопасность, аутентификация, EAP, методы EAP, протоколы, тестирование, оценка устойчивости, Интернет, стандарты, формальные методы спецификации

1. Введение

Беспроводные технологии получают все большее распространение, обеспечивая мобильность пользователей и доступность сетей и различных сервисов там, где раньше они были недоступны. Однако данные технологии создают новые проблемы безопасности. С одной стороны, передаваемая информация стала практически общедоступной, с другой – некоторые системы, считавшиеся ранее достаточно изолированными (например, системы управления самолетами), неожиданно перешли в класс публичных и оказались плохо подготовлены к таким изменениям. В таких условиях к системам контроля доступа и защиты данных предъявляются очень высокие требования.

В настоящее время различные стандарты беспроводных соединений используют в качестве протокола контроля доступа и установления ключей расширяемый протокол аутентификации (EAP), специфицированный в RFC 3748 [1]. EAP определяет общую схему аутентификации для контроля доступа к различным ресурсам. Реальные механизмы аутентификации и криптографические схемы, используемые для достижения желаемых целей безопасности, определяются в так называемых методах EAP. Выбор

конкретного метода происходит после того, как аутентифицирующая сторона (authenticator) получит дополнительную информацию от партнерского узла. Многочисленные методы EAP специфицированы в отдельных документах RFC [2].

Первоначально EAP был разработан и использовался для простой аутентификации пользователей при получении доступа в Интернет через проводную телефонную сеть общего пользования с использованием протокола точка-точка (Point to Point Protocol, PPP) [3]. Поэтому первые методы аутентификации EAP не требовали серьезных мер безопасности. В других средах передачи данных (как проводных, так и беспроводных) требования к безопасности изменились, появилась необходимость включить взаимную аутентификацию устройств, установления криптографических ключей, шифрование данных и другие методы защиты. Это привело к появлению многочисленных методов EAP, предлагающих схемы безопасности различного уровня. Стоит отметить, что EAP не предназначен для передачи больших объемов данных, но может использоваться в связке с другими стандартными протоколами, создавая для них, например, криптографические ключи.

Применительно к беспроводным сетям архитектура EAP определяет трех участников:

- Партнер (peer): Мобильное устройство (например, портативный компьютер), желающее получить доступ к сети через беспроводное соединение, чтобы использовать предоставляемый сервис или осуществлять доступ к данным в этой сети.

- Аутентификатор: Беспроводная точка доступа, с которой соединяется партнер. В общем случае аутентификатор используется как ретранслятор, передавая пакеты EAP между партнером и сервером EAP. Это избавляет от необходимости обновлять все аутентификаторы для поддержки нового метода EAP. Сервер EAP информирует аутентификатор о результате аутентификации. На основе этого результата аутентификатор либо предоставляет, либо запрещает доступ партнера к сети.

- Сервер EAP: Внутренний сервер, который выполняет аутентификацию партнера и определяет, прошла ли аутентификация успешно или нет. Сервер EAP осуществляет обмен данными с аутентификаторами, которые действуют как ретранслирующие устройства, и информирует их о результатах. Если используемый метод EAP вычисляет криптографические ключи, то некоторые из них могут передаваться сервером обратно аутентификатору.

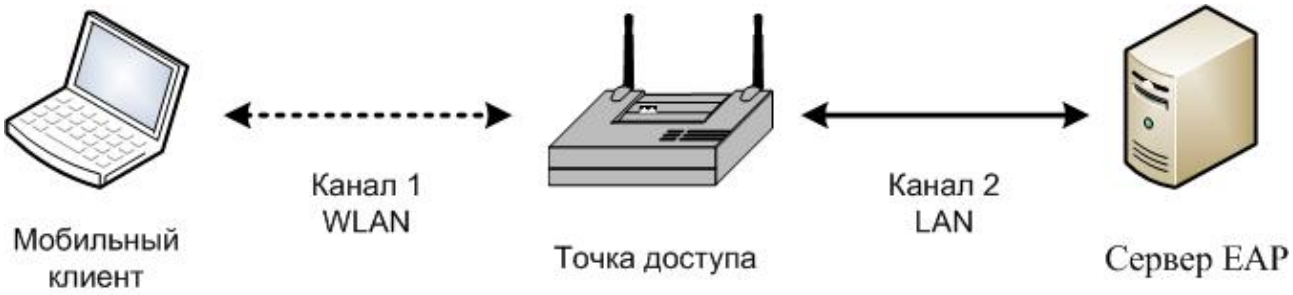

Рис. 1. Модель передачи данных EAP

Мобильный клиент (партнер) запрашивает доступ к сети, подключаясь к точке доступа (аутентификатору). Точка доступа выбирает метод аутентификации в соответствии со своей политикой безопасности и передает данные от клиента серверу EAP. Сервер EAP выполняет аутентификацию клиента и передает результаты обратно точке доступа, которая предоставляет, либо запрещает доступ клиента к сети. Фактически аутентификация EAP выполняется между партнером и сервером EAP. При этом аутентификаторам в режиме ретрансляции не требуется самостоятельно поддерживать какой-либо метод EAP. Как правило, точка доступа и сервер EAP соединены через проводную сеть. Однако в некоторых случаях (например, в сценариях роуминга), между ними могут размещаться дополнительные объекты пересылки сообщений. Документ IEEE 802.11 [4] для беспроводных сетей (WLAN) использует IEEE 802.1X [5] для инкапсуляции сообщений EAP в сообщения проводных сетей (LAN) (EAPOL).

Указанная схема аутентификации допускает некоторые вариации. В некоторых реализациях аутентификатор может выполнять одновременно роль сервера EAP, тогда протокол EAP затрагивает только две стороны. Кроме того, сервер EAP может не хранить данные для аутентификации клиентов и обращаться за ними к внешней базе данных.

В описанной схеме EAP работает поверх беспроводного канала (WLAN) и проводного канала (LAN) (см. рис. 1). По причине использования разных сред передачи данных, EAP выполняется через разные стеки сетевых протоколов. Обычно партнер и аутентификатор осуществляют обмен данными поверх протокола нижнего уровня, используемого беспроводным каналом. С другой стороны, аутентификатор и сервер EAP осуществляют обмен данными поверх более высоких уровней в стеке протоколов, таких как AAA и IP [6]. Поскольку аутентификатору в режиме ретрансляции не требуется поддерживать сами методы аутентификации, то у него нет уровня методов EAP.

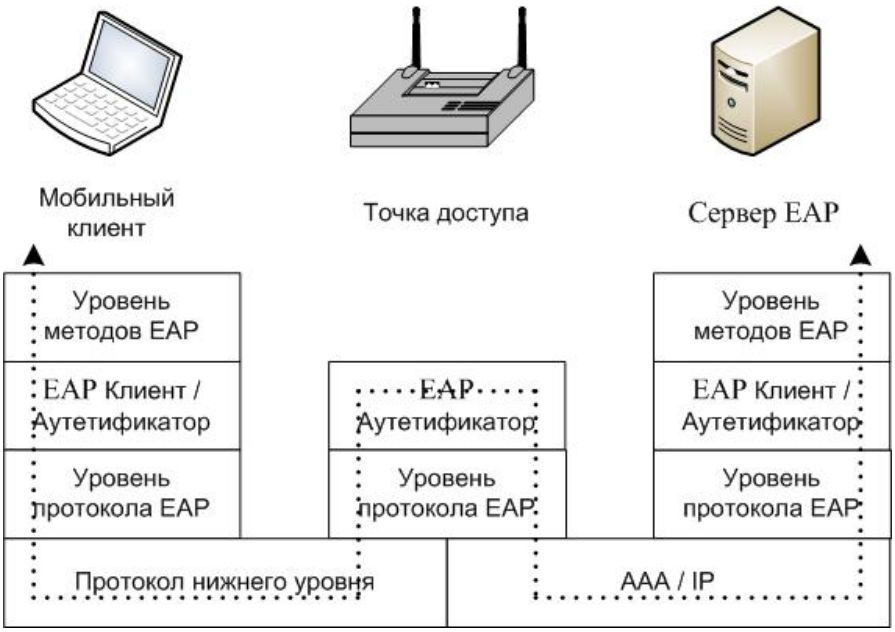

Рис. 2. Стеки протоколов EAP

Как отмечалось выше, распространение беспроводных технологий привело к появлению новых типов угроз безопасности, ориентированных на беспроводные соединения. Это вызвано тем, что в отличие от проводных систем, злоумышленнику нет необходимости физически соединяться с системой, а достаточно просто находиться в радиусе действия связи. Более доступными для компрометации являются точки доступа, поскольку часто размещаются в общедоступных местах. Злоумышленник может попытаться получить над ними управление и, как следствие, доступ к передаваемым ключам безопасности. Так же появилась возможность довольно легко создавать фальшивую точку доступа, которая позволяет злоумышленнику получать чувствительные к безопасности данные клиентов, понижать уровень стойкости согласуемых криптографических алгоритмов и др. Также, по причине доступности, все типы пассивных и активных атак, известных для проводных систем, становятся более вероятными для беспроводных соединений.

2. Методы верификации протокола EAP

В настоящее время существует большое разнообразие расширений протокола EAP, реализующих широкий набор методов аутентификации и использующих различные средства аутентификации. Тестирование реализаций данного протокола является важной задачей как для проверки совместимости различных реализаций, так и для проверки их корректности и надежности. Тестирование может проводится как на соответствие спецификации, так и на входных данных, противоречащих спецификации или не определяемых ею, что особенно актуально для протоколов безопасности.

В наших проектах по тестированию сетевых протоколов мы используем уже проверенное сочетание методов тестирования: автоматизированное

тестирование на соответствие формальным спецификациям и методы мутации данных.

В наших экспериментах используется разработанная нами на основе спецификаций RFC модель протокола EAP и некоторых его методов, описывающая сложную схему функционирования протокола.

Для тестирования реализаций на соответствие формальным спецификациям используется технология UniTESK [7], предоставляющая средства автоматизации тестирования на основе использования конечных автоматов. Состояния тестируемой системы определяют состояния автомата, а тестовые воздействия – переходы этого автомата. При выполнении перехода заданное воздействие передается на тестируемую реализацию, после чего регистрируются реакции реализации и автоматически выносится вердикт о соответствии наблюдаемого поведения спецификации. В UniTESK алгоритм обхода конечного автомата реализован как внутренний компонент и не зависит от протокола и тестируемой системы.

Для обнаружения неадекватного поведения тестируемой системы (завершение из-за фатальной ошибки, "подвисание", ошибки доступа к памяти) в ситуациях, не определенных спецификацией мы используем методы мутационного тестирования. Данный подход является развитием идеи fuzz-генератора Бартона Миллера [8, 9]. Мутации подвергаются правильные сообщения, сформированные на основе разработанной модели протокола, что позволяет изменять данные на любом этапе обмена этого протокола. При этом совместное использование корректных и измененных сообщений позволяет тестовому сценарию "преодолеть" необходимые проверки в реализации, пройти через все значимые состояния и в каждом состоянии протестировать устойчивость реализации протокола к искаженным пакетам.

3. Устройство тестового стенда

В данной работе мы используем схему организации доступа по протоколу EAP, состоящую из трех сетевых узлов: мобильного компьютера, точки доступа и сервера EAP (см. рис. 1).

На мобильном узле исполняется основной поток управления тестовой системы под управлением UniTESK, обход тестового автомата и верификация наблюдаемых реакций. Мобильный узел общается с точкой доступа по беспроводному каналу.

В качестве точки доступа используется Cisco Aironet LAP1242AG [10].

На третьем узле установлена тестируемая реализация протокола, выполняющая роль сервера EAP. Тестовые сообщения протокола, сформированные модельной реализацией, передаются через точку доступа тестируемой системе, после чего регистрируются реакции тестируемого узла.

Точка доступа соединена с сервером EAP проводным каналом. Доступ к серверу EAP осуществляется посредством протокола AAA RADIUS [11, 12].

В качестве реализации протокола EAP выбрана реализация FreeRADIUS [13]. Данная реализация позиционируется разработчиком как самый распространенный сервер RADIUS, к достоинствам которого относятся свободное распространение, открытый исходный код, развитая функциональность, в том числе поддержка многочисленных методов аутентификации EAP. Данная реализация уже использовалась нами на предыдущем этапе проекта [14] для более качественной отладки тестового набора и настройки тестового стенда. Кроме того, широкое распространение этой реализации представляет интерес для тестирования на соответствие стандарту протокола EAP (что необходимо, как минимум, для обеспечения совместимости с другими реализациями). Сервер установлен под ОС Ubuntu 16.04 [15].

В качестве второй реализации протокола EAP используется Windows Server 2012 [16].

Для текущих экспериментов был выбран метод аутентификации EAP-SIM [17], использующий параметры и алгоритмы SIM-карты для аутентификации и создания криптографических ключей. Данный метод основан на механизмах аутентификации GSM (GSM – стандарт мобильных сетей второго поколения). Алгоритмы A3/A8, используемые SIM-картой и GSM оператором, принимают 128-битное случайное число RAND и секретный ключ с SIM-карты в качестве входных данных и выдают 32-битное хэш-значение и 64-битный ключ Kc, используемые для аутентификации и шифрования данных. В отличие от самого стандарта GSM метод EAP-SIM не использует ключ Kc непосредственно для шифрования данных из-за его слабой криптографической стойкости. Вместо этого, несколько значений RAND используются для генерации нескольких ключей Kc, которые затем объединяются для создания более сильных ключей безопасности. EAP-SIM обеспечивает взаимную аутентификацию партнеров, защиту целостности сообщений, криптографическую защиту некоторых данных, а также механизм быстрой переустановки параметров безопасности. Использование метода EAP-SIM предполагает наличие на стороне клиента специализированного устройства для работы с SIM-картами. При этом процесс аутентификации проходит прозрачно для клиента, ему не требуется вводить какие-либо данные.

4. Результаты тестирования

Хотя метод EAP-SIM разрабатывался для аутентификации специализированных устройств, использующих SIM-карты, в наших экспериментах такие устройства не применяются. Вместо этого, все необходимые параметры задаются вручную при настройке сервера EAP и управляющей тестовой системы. На данный момент в рамках технологии UniTESK (с использованием инструмента JavaTesK [18])

- разработана модель метода аутентификации EAP-SIM, которая интегрирована разработанную ранее модель базового протокола EAP,

- разработана спецификация и медиаторы для метода EAP-SIM,
- разработан набор тестов, покрывающий часть требований спецификации.

На данных момент выявлено несколько отклонений реализации FreeRADIUS от требований спецификации. Разработка тестового набора продолжается.

5. Заключение

В данной работе представлен опыт верификации протокола аутентификации EAP при использовании беспроводных соединений. Беспроводная среда передачи данных является одной из областей, в которой активно используется данный протокол безопасности. А широкое распространение в последнее время мобильных устройств предъявляет дополнительные требования к системе безопасности передачи информации, и в том числе к аутентификации устройств. В работе использовался новый тестовый набор, разработанный с использованием технологии UniTESK и методов мутационного тестирования. Технология UniTESK позволяет автоматизировать процесс верификации сетевых протоколов на основе их формальных моделей, а методы мутационного тестирования позволяют протестировать устойчивость реализации протокола к искаженным сообщениям.

Этот подход доказал свою эффективность и в наших предыдущих проектах, обеспечив обнаружение различных отклонений от спецификации и других ошибок при тестировании сетевых протоколов [19, 20].

Проект выполняется при поддержке РФФИ, проект № 16-07-00603 «Верификация функций безопасности и оценка устойчивости к атакам реализаций протокола аутентификации EAP».

Литература

1. IETF RFC 3748, B. Aboba, et al. “Extensible Authentication Protocol (EAP)”, June 2004.
2. Extensible Authentication Protocol (EAP) Registry. — URL: http://www.iana.org/assignments/eap-numbers/eap-numbers.xhtml
3. IETF RFC 1661, W. Simpson “The Point-to-Point Protocol (PPP)”, July 1994.
4. IEEE Standard 802.11-2007, Institute of Electrical and Electronics Engineers, "Standard for Local and metropolitan area networks - specific requirements – part 11: Wireless LAN Medium Access Control and Physical Layer specifications", 2007.
5. IEEE Standard 801.1X-2004, Institute of Electrical and Electronics Engineers, “Standard for Local and metropolitan area networks, Port-Based Network Access Control”, 2004.
6. IETF RFC 791, “Internet Protocol”, September 1981.

7. Bourdonov I., Kossatchev A., Kuliamin V., and Petrenko A. UniTesK Test Suite Architecture. // Proceedings of FME 2002. LNCS 2391, pp. 77-88, Springer-Verlag, 2002
8. B. P. Miller, D. Koski, C. P. Lee, V. Maganty, R. Murthy, A. Natarajan, and J. Steidl. Fuzz revisited: A re-examination of the reliability of UNIX utilities and services // Office, vol. 1525, no. October 1995, pp. 1–23, 1995.
9. B. P. Miller, L. Fredriksen, and B. So. An empirical study of the reliability of UNIX utilities // Commun. ACM, vol. 33, pp. 32–44, December 1990.
10. Cisco Aironet 1240 AG Series. — URL: http://www.cisco.com/c/en/us/support/wireless/aironet-1240-ag-series/tsd-products-support-series-home.html
11. IETF RFC 2865, C. Rigney, S. Willens, A. Rubens and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", June 2000.
12. IETF RFC 3579, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", B. Aboba and P. Calhoun, September 2003.
13. FreeRADIUS. — URL: http://freeradius.org .
14. Никешин А.В., Пакулин Н.В., Шнитман В.З. Подходы к разработке тестового набора для тестирования реализаций протокола EAP и его методов // Научный сервис в сети Интернет: труды XVIII Всероссийской научной конференции (19-24 сентября 2016 г., г. Новороссийск). — М.: ИПМ им. М.В. Келдыша, 2016. — С. 290-297. — doi:10.20948/abrau-2016-24
15. Ubuntu 16.04. — URL: http://www.ubuntu.com/.
16. Windows Server 2012 R2. — URL: https://www.microsoft.com
17. IETF RFC 4186, H. Haverinen, J. Salowey “Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)”, January 2006.
18. JavaTESK. — URL: http://www.unitesk.ru/content/category/5/25/60/.
19. А.В.Никешин, Н.В.Пакулин, В.З.Шнитман "Мутационное тестирование сетевых протоколов с использованием формальных моделей" // Научный сервис в сети Интернет: труды XVII Всероссийской научной конференции (21-26 сентября 2015 г., г. Новороссийск). - М.: ИПМ им. М.В.Келдыша, 2015. ISBN 978-5-98354-015-6. С. 259-266.
20. А.В.Никешин, Н.В.Пакулин, В.З. Шнитман "Тестирование реализаций клиента протокола TLS" // Труды Института системного программирования РАН. Том 27. Выпуск 2. 2015 г. Стр. 145-160. ISSN 2220-6426 (Online), ISSN 2079-8156 (Print).