УДК 519.816+519.712.6

Федюкович В. Е.

Инженер ООО «ИнтроПро» (г. Киев)

О НЕОБХОДИМОСТИ ДОПОЛНИТЕЛЬНОЙ ПРОВЕРКИ СЕРТИФИКАТА СХЕМЫ DAA

Выполнен анализ схемы DAA. Обнаружено, что схема допускает совместные действия Эмитента и Проверяющего с целью получить дополнительную информацию о Пользователе, которые не обнаруживаются Пользователем, следующим протоколу. Предложена дополнительная проверка Пользователем DAA сертификата, полученного от Эмитента, позволяющая обнаружить такую атаку и прекратить протокол.

Ключевые слова: DAA, анонимность, аутентификация, протокол доказательства знания, TPM.

ВВЕДЕНИЕ

Аппаратное обеспечение персонального компьютера состоит, с момента его появления, из унифицированных блоков, что допускает его самостоятельную сборку. Обратная сторона максимально упрощенной процедуры сборки заключается в фактическом отсутствии механизмов контроля целостности аппаратного обеспечения, что затрудняет обнаружение вмешательства на аппаратном уровне. Такое вмешательство, в свою очередь, может приводить к утечке конфиденциальных данных при их обработке на таком компьютере. Контроль целостности аппаратного и программного обеспечения компьютера является одной из основных целей, решаемых в рамках Trusted Computing

Group [1] (TCG). TCG анонсировала цели сохранности важной информации путем создания защищенного носителя данных; создания механизмов надежной аутентификации компьютеров, в том числе удаленной; контроля целостности и управления пользователем путей предоставления информации о целостности третьим лицам. Задача контроля целостности решается путем «измерения» параметров старта компьютера и сохранения их в микросхеме Trusted Platform Module (TPM). Предусмотрен механизм «накопления»: в регистр TPM помещается значение хэш-функции, аргументами которой являются текущее содержание регистра и очередное измерение. TPM предоставляет доступ на чтение к значению регистра, содержащему произвольные данные пользователя, при условии совпадения состояния такого компьютера, представленного регистром накопления, с состоянием на момент инициализации такого регистра. TCG также имеет надежную проверку состояния удаленного компьютера, с учетом ожидаемого конфликта интересов сторон, связанного с распространением персональных данных владельца компьютера. В версии 1.1 спецификаций TPM используется цифровая электронная подпись, выполняемая потенциально короткоживущими RSA ключами Attestation Identity Key (AIK). Такие ключи заверяются доверенной третьей стороной (Privacy CA), которая, в свою очередь, аутентифицирует компьютер по постоянному RSA ключу Endorsement Key (EK). Версия 1.2 спецификаций предусматривает схему Direct Anonymous Attestation (DAA) [2], в которой для скрытия связи между экземпляром подписи доверенной стороны и сертификатом пользователя используется вариант механизма затемнения (blinding) [3], полностью выполняемый на уровне программного обеспечения компьютера пользователя. Имеется свойство анонимности схемы: различные экземпляры подписи, созданные Пользователем, а также различными Пользователями, неотличимы.

Микросхема TPM серийно выпускается Infineon и другими компаниями, и устанавливается на некоторые системные платы и ноутбуки. Функциональность TPM включена в микросхему южного моста некоторых наборов логики (chipset) Intel. Дальнейшее развитие [4] схемы DAA предполагает использование эллиптических кривых, имеющих билинейные отображения (bilinear pairing).

Инициатива Trusted Computing в целом подверглась критике [5, 6] со стороны Фонда свободного программного обеспечения (FSF). Следует отметить, что ряд утверждений можно рассматривать как предположения о намерениях и планах участниках рынка. Так, например, в эссе Столлмена [5] содержится предположение о рисках для пользователей компьютеров, связанных с потерей возможности устанавливать и использовать свободное программное обеспечение; при этом делается ссылка на законодательные инициативы в США. Отдельного внимания заслуживает ссылка на программное обеспечение GNU Privacy Guard (GPG), а также утверждение о полезности GPG при пересылке информации по электронной почте, в форме противопоставления функциональности GPG и предполагаемых целей Trusted Computing. В материале Андерсена [6] корректно изложена идея мониторинга старта компьютера, на основании чего делается ряд предположений, в том числе о возможности избирательного блокирования компьютера, идентифицируемого на основании уникальных ключей. В статье [7] сформулировано утверждение о рисках, связанных с предоставлением третьим лицам точной информации о программном обеспечении Пользователя.

Ожидание анонимности пользователей при удаленной проверке целостности их компьютеров в рамках схемы DAA является решающим фактором, объясняющим интерес к изучению такого механизма проверки на уровне серийно выпускаемого оборудования. Ряд утверждений о возможностях TPM и рисках, возникающих при его использовании, следует рассматривать как необоснованные, а также игнорирующие возможности, предоставляемые протоколами доказательства знания для ограничения распространения персональной информации. С другой стороны, следует обратить внимание на ошибку, нередко встречающаяся при проектировании программного обеспечения: недостаточная проверка возвращаемого значения, что особенно важно в случае совместных вычислений и конфликта интересов участников вычислений. В этой работе изложены результаты независимого анализа схемы DAA, которые могут быть полезны при анализе рисков и выработке рекомендаций.

1. ОБЩАЯ ИНФОРМАЦИЯ О СХЕМЕ DAA

Участниками схемы являются Пользователи, Проверяющие и Эмитент. Схема состоит из алгоритма выбора параметров схемы (Setup), протокола выпуска Эмитентом сертификата Пользователя (Join), алгоритмов создания и проверки экземпляра подписи Пользователя (Sign и Verify). Пользователь создает экземпляр подписи, который является неинтерактивным вариантом [8] протокола доказательства знания ключей TPM, таких, что имеется экземпляр подписи Эмитента на экземпляре привязки к этим ключам. Предусматривается генерация микросхемой случайных значений (nonce), которые являются дополнительными аргументами хэш-функции при выборе значения запроса, отсутствующими в оригинальной работе [8]. Все вычисления с ключами TPM выпол-

няются на уровне микросхемы (TPM), операции с затемнением (blinding) и обмен cmoe e и случайное v'', вычисляет элемент группы A, такой, что

$$A^e US^{v''} = Z \pmod{n}, \quad (1)$$

где S, Z – элементы группы, параметры схемы. Используется подгруппа квадратичных вычетов мультипликативной группы кольца вычетов по модулю n для составного n, выбранного Эмитентом на этапе генерации параметров схемы. Эмитент пересылает пользователю (A, e, v'), что является экземпляром подписи вида Camenisch-Lysyanskaya [9]. Для создания экземпляра такой подписи необходимо знание факторизации n, что является ключом Эмитента. Исчерпывающая информация о схеме DAA приведена в оригинальной работе [1].

2. РЕЗУЛЬТАТЫ

Было замечено, что Пользователь использует полученные от Эмитента данные без предварительной проверки, удовлетворяют ли они уравнению (1) как экземпляр подписи Эмитента. Был обнаружен сценарий для Эмитента и Проверяющего (в дальнейшем называемых Соперником), в рамках которого Пользователь не достигает неотличимости событий аутентификации. Пусть Эмитент создал экземпляр подписи, который удовлетворяет уравнению (1) для некоторого произвольного уникального $\overline{Z}$, отличного от Z. Тогда Пользователь, следующий спецификациям, создает экземпляр подписи, успешно проверяемый уравнением (в обозначениях оригинальной работы)

$$T_1^e R_0^{f_0} R_1^{f_1} S^v h^{-ew} = \overline{Z} \pmod{n}, \quad (2)$$

Проверяющий, следующий спецификациям, отвергает такой экземпляр подписи как некорректный, так как значение запроса не совпадает со значением хэш-функции. Однако Проверяющий, имеющий список значений $\overline{Z}$, полученный от Эмитента, может попытаться воссоздать значение запроса, перебирая все значения из такого списка. А именно, при таком переборе следует использовать $\overline{T}_1$ при формировании аргумента хеш-функции вместо $\hat{T}_1$ в оригинальной работе:

$$\overline{T}_1 = \overline{Z}^{-c} T_1^{s_e + c2^{l_e - 1}} R_0^{s_{f_0}} R_1^{s_{f_1}} S^{s_v} h^{-s_{ew}} \pmod{n}. \quad (3)$$

Таким образом, Проверяющий всегда может распознать сертификат, выданный Пользователю действующим произвольно Эмитентом, при условии выдачи уникальных некорректных (т. е. не удовлетворяющих уравнению (1) проверки подписи) сертификатов. Такая конструкция позволяет такому Сопернику формировать историю событий аутентификации выбранных Эмитентом Пользователей, что делает заявленное свойство анонимности схемы DAA требующим уточнения. Схема DAA также допускает Пользователя, который всегда выполняет дополнительную проверку (1) полученного от Эмитента сертификата. Такой Пользователь всегда обнаруживает попытку нарушения анонимности путем предоставления некорректного сертификата и может прекратить протокол с таким Эмитентом. Кроме того, действия такого Пользователя неотличимы от действий Пользователя, следующего протоколу в случае, если Эмитент также следует протоколу. Дополнительная проверка предусматривает реализацию на уровне программного обеспечения и не требует каких-либо изменений в микросхеме Trusted Platform Module (TPM). Эти результаты были изложены в препринте IACR [10] и представлены на конференции РусКрипто [11]. В последовавших работах (например, [12]) предусмотрена проверка Пользователем корректности полученного экземпляра подписи Эмитента.

Необходимо также обратить внимание на дополнительные случайные значения, выбираемые TPM при формировании запроса при помощи хэш-функции. Как следствие, эти случайные значения необходимы для проверки корректности подписи Пользователя, что допускает скрытый канал передачи данных TPM – Проверяющий. Следует отметить, что предложенный способ формирования запроса не допускает механизма совместного выбора случайных значений, предложенного в модели «наблюдатель в кошельке» [13].

Формирование ответов Пользователя в виде экземпляра подписи может ограничивать возможности такого Пользователя в управлении доступностью информации о состоянии компьютера для третьих лиц. Определенный интерес может представлять интерактивная проверка состояния, в том числе с учетом схем с выбранным заранее Проверяющим (designated Verifier) или схем с подтверждением (confirmer signatures).

ВЫВОДЫ

Обнаружена уязвимость схемы Direct Anonymous Attestation в модели угроз, предусматривающей произвольные совместные действия Эмитента и Проверяющего. Уязвимость позволяет такому Сопернику исключить анонимность Пользователя, следующего спецификациям. Выпуск некорректных сертификатов может оставаться незамеченным в случаях использования программного обеспечения Эмитента и Проверяющего только одного производителя. Такая уязвимость может быть исключена дополнительной проверкой Пользователем полученного сертификата. Также отмечена возможность скрытого канала передачи путем генерации микросхемой TPM псев-

дослучайных чисел, которые должны быть получены Проверяющим в неизменном виде.

СПИСОК ЛИТЕРАТУРЫ

1. *Brickell, E.* Direct Anonymous Attestation[Электронный ресурс] / Brickell E., Camenisch J. and Chen L. // Cryptology ePrint Archive. – Report 2004/205. – Режим доступа: http://eprint.iacr.org/2004/205/.
2. Trusted Computing Group [Электронный ресурс]. – Режим доступа: http://www.trustedcomputinggroup.org/.
3. *Chaum, D.* Blind Signatures for Untraceable Payments / Chaum D., Rivest R. L. and Sherman A. T. (Eds.) // Advances in Cryptology : proceedings of CRYPTO'82. – Plemum, New York, 1983. – P. 89–105.
4. *Brickell, E.* Simplified security notions of direct anonymous attestation and a concrete scheme from pairings / Brickell E., Chen L. and Li J. // International Journal of Information Security. – 2009. – Vol. 8. – P. 315–330.
5. *Stallman, R.* Can You Trust Your Computer? [Электронный ресурс] / Richard Stallman // Free Software Free Society: selected essays of Richard M. Stallman. – Режим доступа: http://www.gnu.org/philosophy/can-you-trust.html.
6. *Anderson, R.* 'Trusted Computing' Frequently Asked Questions [Электронный ресурс] / Anderson R. – Режим доступа: http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html.
7. Trusted Computing: Promise and Risk [Электронный ресурс] // Electronic Frontier Foundation whitepaper. – Режим доступа: http://www.eff.org/wp/trusted-computing-promise-and-risk.
8. *Fiat, A.* How to Prove Yourself: Practical Solutions to Identification and Signature Problems / Fiat A. and Shamir A. // Lecture Notes in Computer Science. – 1987. – Vol. 263. – P.186–194.
9. *Camenisch, J.* A Signature Scheme with Efficient Protocols / Camenisch J. and Lysyanskaya A. // Lecture Notes in Computer Science. – 2003. – Vol. 2576. – P.268–289.
10. *Fedyukovych, V.* A strategy for any DAA Issuer and an additional verification by a Host [Электронный ресурс] / V. Fedyukovych // Cryptology ePrint Archive. – Report 2008/277. – Режим доступа: http://eprint.iacr.org/2008/277/.
11. *Федюкович, Е.* Восстановление анонимности при использовании протоколов DAA [Электронный ресурс] / В. Е. Федюкович // Рускрипто 2009. – Режим доступа: http://ruscrypto.ru/sources/conference/rc2009/.
12. *Brickell, E.* Enhanced Privacy ID from Bilinear Pairing [Электронный ресурс] / Brickell E. and Li J. // Cryptology ePrint Archive. – Report 2009/095. – Режим доступа: http://eprint.iacr.org/2009/095/.
13. *Chaum, D.* Wallet Databases with Observers / Chaum D. and Pedersen T. P. // Lecture Notes in Computer Science. – 1993. – Vol. 740/1993. – P. 89–105.

Надійшла 1.11.2010

Федюкович В. Є.

ПРО ДОДАТКОВУ ПЕРЕВІРКУ СЕРТІФІКАТА СХЕМИ DAA

Було виконано аналіз схеми DAA. Було знайдено, що схема не є анонімною: Емітент може випустити сертифікат, який завжди може впізнати Перевіряючий. Також було запропоновано додаткове рівняння перевірки, щоб уникнути такої атаки.

Ключові слова: DAA, анонімність, атрибуція, протокол доказу знання, TPM.

Fedyukovych V.

ON ADDITIONAL VERIFICATION OF DDA CERTIFICATE

A strategy for colluding Issuer and Verifier with DAA scheme was found to let such an adversary always distinguish honest Users that were issued 'tagged' certificates voiding anonymity property of DAA. Additional verification equation was introduced to detect such an attack.

Key words: DAA, anonimity, authentication, proof of knowledge, TPM.