Обман, выполненный мафией

Материал из Википедии — свободной энциклопедии

Обман, выполненный мафией (англ. *Mafia fraud attack*) — один из способов злоупотребления доказательством с нулевым разглашением. Впервые данный метод был описан Иво Десмедтом (англ. *Yvo Desmedt*)[1]. Своё название способ получил благодаря высказыванию Ади Шамира[2], сделанному им во время обсуждения протокола идентификации с нулевым знанием Файга-Фиата-Шамира[3]:

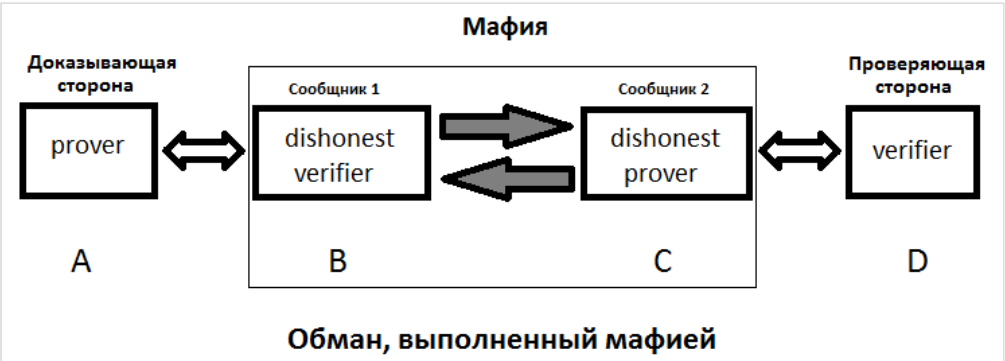
> Я могу ходить в принадлежащий мафии магазин хоть миллион раз подряд, а они все ещё не смогут выдать себя за меня.
>
> **Оригинальный текст (англ.)**
>
> *I can go to a Mafia-owned store a million successive times and they still will not be able to misrepresent themselves as me.*

Но на самом деле подобное мошенничество возможно.

Содержание

Описание

Пусть имеется 4 участника: **A**, **B**, **C**, **D**. Причём **B** и **C** сотрудничают между собой («принадлежат одной мафии»). **A** доказывает свою личность **B**, а **C** хочет выдать себя за **A** перед **D**. Обычно, мошенничество описывают следующей ситуацией: **B** владеет рестораном, принадлежащим мафии, **C** — также представитель мафии, **D** — ювелир. **A** и **D** не знают о предстоящем мошенничестве. В момент, когда **A** готов заплатить за



Описание Обмана, выполненного мафией

обед и идентифицировать себя перед **B**, **B** извещает **C** о начале мошенничества. Это возможно, благодаря наличию радио-канала между ними. В это время, **C** выбирает бриллиант, который хочет купить, и **D** начинает идентифицировать личность **C** (а на самом деле **A**). **C** передаёт вопрос по протоколу **B**, а тот, в свою очередь, задаёт его **A**. Ответ передаётся в обратном порядке. Таким образом, **A** заплатит не только за обед, но и за дорогой бриллиант[4].

Как видно из вышеописанного, существуют определённые требования для подобного мошенничества. Например, моменты, когда **A** начинает доказывать свою личность перед **B**, а **C** — перед **D** должны быть точно синхронизированы[2].

Обман, выполненный мафией, оказывается действенным в ситуациях, когда нужно совершить атаку на систему, в которой аутентификация является успешной только при условии, что доказывающий участник находится в непосредственной близости от проверяющей стороны, и успешная аутентификация позволяет доказывающему получить некий сервис, предоставляемый проверяющей стороной[5].

Примеры применения

- Обман, выполненный мафией, широко применяется для атаки на RFID-системы. RFID-система (англ. *Radio Frequency IDentification, радиочастотная идентификация*) состоит из считывающего устройства (ридера) и транспондера (RFID-метки). Предположим, злоумышленник собирается получить несанкционированный доступ к автомобилю. Доступ обеспечивается посредством RFID (в данном случае транспондером будет бесконтактная карта). Злоумышленник, у которого есть поддельная карта («rogue card»), располагается рядом с автомобилем и устанавливает связь между своей картой и ридером RFID-системы автомобиля («legitimate reader»). В то же время сообщник, обладающий ещё одним считывающим устройством («rogue reader»), находится рядом с владельцем автомобиля и устанавливает соединение с картой легитимного владельца. Таким образом, тот из злоумышленников, кто обладает поддельной картой, передает сообщения, полученные от легитимного ридера, своему подельнику, который пересылает эти сообщения карте (транспондеру) владельца автомобиля. Ответ, полученный с легитимного транспондера, пересылается по той же цепи в обратном направлении и, в конечном итоге, доходит до ридера, установленного на автомобиле[6].
- Mafia fraud attack также может применяться для атаки на систему радиолокационного опознавания «Свой-чужой» (IFF — Identification Friend or Foe). Многие IFF-системы используют способ аутентификации «вызов-ответ» («challenge — response authentication»). Например, два самолета **W** и **B** могут идентифицировать друг друга посредством IFF, в то время, как два вражеских самолета **A1** и **A2** пытаются выдать себя за «своих». В этом случае применяется схема, аналогичная схеме для атаки на RFID-системы. Например, **W** посылает запрос **A1**, для того чтобы он подтвердил свою личность, **A1** пересылает сообщение **A2**, **A2** в свою очередь отправляет этот запрос самолету **B**, который, являясь «своим» для **W**, отвечает верным сообщением. Данный ответ по тому же пути передается **W**. Таким образом, **W** и **B** будут считать «своими» **A1** и **A2** соответственно[7].

Способы предотвращения

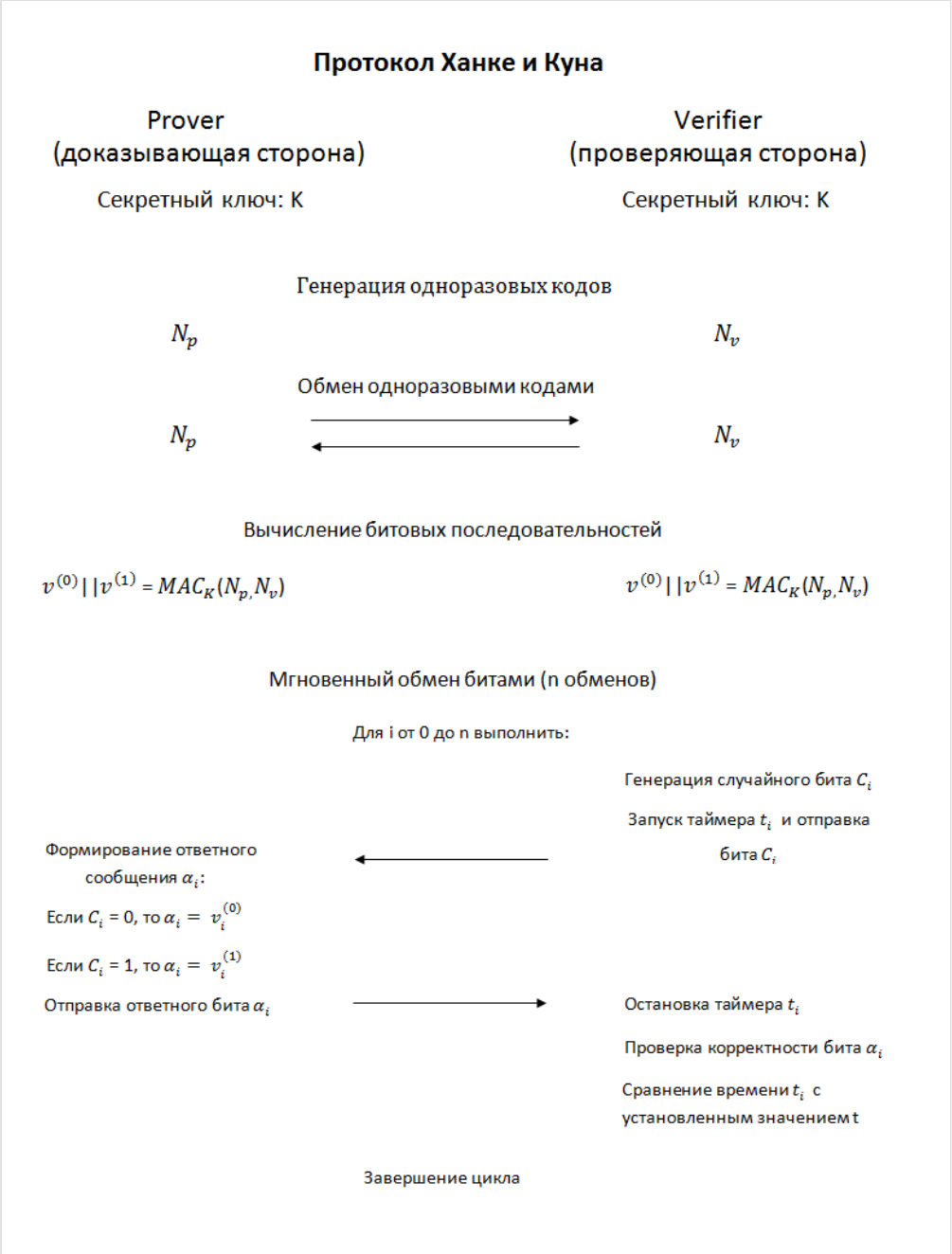
Дистанционно-ограниченные протоколы (Distance-bounding protocols)

Техника предотвращения обмана, выполненного мафией, задействующая, так называемые, дистанционно-ограниченные протоколы («distance-bounding protocols»), впервые была приведена в работе Стефана Брандса (Stefan Brands) и Дэвида Чаума (David Chaum). Данная техника применяется, когда одной из взаимодействующих согласно некоторому криптографическому протоколу сторон необходимо знать, что другой участник находится на расстоянии, не более определенного. Например, если человек применяет электронный пропуск на входе в здание, система аутентификации должна определить, что человек находится от входа на расстоянии, не большем определенного. Согласно

Брандсу и Чауму основной элемент дистанционно-ограниченного протокола прост. Он основывается на принципе «вызов-ответ». Происходит **k** мгновенных обменов битами («rapid bit exchanges») между участниками **P** и **V**, **P** («Prover») — тот, кто доказывает свое знание, **V** («Verifier») — тот, кто проверяет подлинность того, что доказывает **P**. Параметр **k** является секретным параметром протокола. Обмен битами является мгновенным в том смысле, что **P** после получения бита от **V** отправлет ответный бит незамедлительно[8].

Пример дистанционно-ограниченного протокола

Одним из распространенных дистанционно-ограниченных протоколов является протокол Герхарда Ханке (Gerhard P. Hancke) и Маркуса Куна (Markus G. Kuhn) [9], широко применяемый в RFID-системах[10]. На первом этапе протокола **P** (Prover) и **V** (Verifier) обмениваются одноразовыми кодами, сгенерированными случайным образом (Nonce) (то есть **P** и **V** генерируют и передают последовательности бит N_p и N_v соответственно). Затем обе стороны вычисляют одинаковые битовые последовательности $v^{(0)}$ и $v^{(1)}$, используя псевдослучайную функцию (обычно это MAC или Криптографическая хеш-функция), то есть $MAC_K(N_v, N_p) = v^{(0)} \,||\, v^{(1)}$, здесь **K** — это секретный ключ, известный обеим сторонам. Далее производится серия из **n** мгновенных обменов битами между двумя сторонами. В каждом отдельно взятом обмене **V** отправляет бит C_i («вызов») доказывающей стороне **P**. Если этот бит равен 0, то **P** отправит в качестве ответного сообщения бит под номером **i** из последовательности $v^{(0)}$. Если же C_i равен 1, то ответным сообщением будет бит с номером **i** из последовательности $v^{(1)}$. В свою очередь после каждого обмена битами **V** проверяет все полученные сообщения на корректность, а также сравнивает время, прошедшее с момента отправки сообщения C_i до момента получения ответного бита, с некоторым установленным значением **t**. Если все полученные сообщения и времена корректны, то обмен считается успешным[11].



Описание протокола Ханке и Куна

Для того чтобы осуществить атаку, злоумышленник встраивается в данную схему и до того, как **V** отправил сообщение C_i, угадывает соответствующий бит C_i', затем сразу передает его стороне **P**. Когда злоумышленник получает сообщение от **P**, то он сравнивает C_i и C_i'. Если биты совпадают (вероятность совпадения равна 1/2), значит злоумышленник передаст корректное сообщение $v_i^{(C_i)}$ проверяющей стороне **V**, в оставшейся половине случаев, когда биты не совпали, мошенник пробует угадать значение теперь уже $v_i^{(C_i)}$ и передает его **V**. Таким образом, вероятность, что злоумышленник выдаст правильное значение $v_i^{(C_i)}$ равна 3/4. Для **n** обменов битами получаем, что вероятность успешной атаки равна $\left(\frac{3}{4}\right)^n$ [10].

С момента публикации работы Ханке и Куна было предложено несколько решений для увеличения эффективности протокола, например, Ту (Yu-Ju Tu) и Пирамуту (Selwyn Piramuthu) предложили свой дистанционно-ограниченный протокол, который задействует некоторые принципы протокола Ханке и Куна, но позволяет снизить вероятность успешной атаки до 9/16 (для одного обмена битами)[12].

Другие способы

1. Идентификация должна проходить в клетке Фарадея. Если в магазине ювелира будет клетка Фарадея, то мафиози не смогут обмениваться сообщениями[2].
2. Иво Десмедт и Томас Бет (англ. *Thomas Beth*) предложили использовать точные часы. Если каждый этап протокола будет проходить за точный период времени, то Мафиози просто не успеют передавать сообщения друг другу. Стоит также учитывать, что сообщения между доказывающей и подтверждающей стороной передаются не мгновенно, а с некоторой задержкой. Эта задержка связана с тем, что скорость света не бесконечна, поэтому на передачу сообщений тратится время, равное l/c, где **l** — расстояние между сторонами, а **c** — скорость света[13].

Другие методы злоупотребления доказательством с нулевым разглашением

Интересным расширением обмана, выполненного мафией, является атака типа «обман, выполненный террористами»[5]. В данном виде атаки злоумышленник **A** (adversary) и доказывающая сторона состоят в сговоре, то есть, доказывающий участник **P** является нечестным участником взаимодействия (dishonest prover). **P** использует помощь мошенника, чтобы доказать проверяющей стороне **V**, что находится поблизости. Злоумышленник не знает значение секретного ключа, которым обладает **P**. В этом нет ничего удивительного, так как обычно на практике, **A** — это малое устройство, обладающее некоторой вычислительной мощностью и памятью. Данное устройство должно быть расположено вблизи **V** (проверяющей стороны). Доказывающая сторона не имеет полного контроля над злоумышленником, таким образом, **P** не может доверить свой пароль устройству **A**. В противном случае, например, какой-нибудь другой мошенник может совершить атаку на устройство, завладеть секретным ключом, принадлежащим **P**, и выдать себя за **P**[14].

Основным способом предотвращения обмана, выполненного террористами, также является применение дистанционно-ограниченных протоколов. Однако избежать такой атаки поможет не любой дистанционно-ограниченный протокол, применимый в случае обмана, выполненного мафией. Например, протокол Ханке и Куна, упомянутый выше, является уязвимым для обмана террористов. Доказывающий участник протокола, находящийся далеко от проверяющей стороны **V**, может попросту передать злоумышленнику, расположенному вблизи от **V**, вычисленные последовательности $v^{(0)}$ и $v^{(1)}$. Тогда мошенник сможет корректно отвечать на запросы проверяющего участника, укладываясь при этом во временные рамки. Стоит отметить, что даже обладая последовательностями бит $v^{(0)}$ и $v^{(1)}$, злоумышленник не сможет в будущем выдавать себя за **P**, поскольку он не знает

секретного ключа, а последовательности N_p и N_v являются одноразовыми[15]. Одним из известных дистанционно-ограниченных протоколов, применимых для предотвращения обмана, выполненного террористами, является, например, протокол Рэйда (Reid et al.'s protocol)[15].

Существует ещё несколько методов злоупотребления доказательством с нулевым разглашением, таких как обман с несколькими личностями и проблема гроссмейстера[16].

Примечания

1. Desmedt, 1988.
2. Bengio, Brassard, Desmedt et al., 1991.
3. Feige, Fiat, Shamir, 1988.
4. Шнайер, 2003, с. 93.
5. Singelee, Preneel, 2005.
6. Zhang, Kitsos, 2009, с. 151-156.
7. Alkassar, Stuble, 2002.
8. Brands, Chaum, 1994, с. 344-359.
9. Hancke, Kuhn, 2005, с. 67-73.
10. Chong Hee Kim et al, 2008, с. 98-115.
11. Singelee et al, 2007, с. 101-115.
12. Tu, Piramuthu, 2007.
13. Beth, Desmedt, 1991.
14. Cremers et al, 2012.
15. Reid et al, 2007.
16. Шнайер, 2003, с. 92.

Литература

- *Desmedt Y. G., Goutier C., Bengio S.* Special Uses and Abuses of the Fiat-Shamir Passport Protocol (extended abstract) (http://bengio.abracadoudou.com/cv/publications/pdf/desmedt_1988_crypto.pdf) (англ.) // *Advances in Cryptology — CRYPTO '87*: *A Conference on the Theory and Applications of Cryptographic Techniques, Santa Barbara, California, USA, August 16-20, 1987, Proceedings* / C. Pomerance — Berlin: Springer Berlin Heidelberg, 1987. — P. 21—39. — (Lecture Notes in Computer Science; Vol. 293) — ISBN 978-3-540-18796-7 — ISSN 0302-9743 (https://www.worldcat.org/issn/0302-9743); 1611-3349 (https://www.worldcat.org/issn/1611-3349) — doi:10.1007/3-540-48184-2_3 (https://dx.doi.org/10.1007/3-540-48184-2_3)
- *Desmedt Y. G.* Major Security Problems with the "Unforgeable" (Feige)-Fiat-Shamir Proofs of Identity and How to Overcome Them (англ.) // *SECURICOM 88*: *6th Worldwide Cong.Computer and Communications Security and Protection* — Groupe Blenheim-SEDEP, 1988. — P. 147—159.
- *Feige U., Fiat A., Shamir A.* Zero-Knowledge Proofs of Identity (http://www.fi.muni.cz/~xslaby/jiri_slaby/kr/9/p210-fiege.pdf) (англ.) // *Journal of Cryptology* / I. Damgård — Springer Science+Business Media, International Association for Cryptologic Research, 1988. — Vol. 1, Iss. 2. — P. 77–94. — ISSN 0933-2790 (https://www.worldcat.org/issn/0933-2790); 1432-1378 (https://www.worldcat.org/issn/1432-1378) — doi:10.1007/BF02351717 (https://dx.doi.org/10.1007/BF02351717)
- *Beth T., Desmedt Y. G.* Identification Tokens — or: Solving The Chess Grandmaster Problem (http://link.springer.com/content/pdf/10.1007%2F3-540-38424-3_12.pdf) (англ.) // *Advances in Cryptology — CRYPTO '90*: *10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings* / A. J. Menezes, S. A. Vanstone — Berlin, Heidelberg, New York City, London: Springer Berlin Heidelberg, 1991. — P. 169—176. — (Lecture Notes in Computer Science; Vol. 537) — ISBN 978-3-540-54508-8 — ISSN 0302-9743 (https://www.worldcat.org/issn/0302-9743); 1611-3349 (https://www.worldcat.org/issn/1611-3349) — doi:10.1007/3-540-38424-3_12 (https://dx.doi.org/10.1007/3-540-38424-3_12)

- *Bengio S., Brassard G., Desmedt Y. G., Goutier C., Quisquater J.* Secure implementation of identification systems (англ.) // *Journal of Cryptology* / I. Damgård — Springer Science+Business Media, International Association for Cryptologic Research, 1991. — Vol. 4, Iss. 3. — P. 175—183. — ISSN 0933-2790 (https://www.worldcat.org/issn/0933-2790); 1432-1378 (https://www.worldcat.org/issn/1432-1378) — doi:10.1007/BF00196726 (https://dx.doi.org/10.1007/BF00196726)
- *Alkassar A., Stüble C.* Towards Secure IFF: Preventing Mafia Fraud Attacks (https://www.researchgate.net/publication/4003248_Towards_Secure_IFF_Preventing_Mafia_Fraud_Attacks) // *MILCOM 2002. Proceedings* — IEEE, 2002. — Т. 2. — ISBN 978-0-7803-7625-0
- *Singelee D., Preneel B.* Location verification using secure distance bounding protocols (https://securewww.esat.kuleuven.be/cosic/publications/article-760.pdf) (англ.) // *Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on* — IEEE, 2005. — ISBN 978-0-7803-9465-0
- *Zhang Y., Kitsos P.* Security in RFID and Sensor Networks (англ.) — Boston: Auerbach Publications, 2009. — 560 p. — (Wireless Networks and Mobile Communications) — ISBN 978-1-4200-6839-9
- *Stefan Brands, David Chaum.* Distance-Bounding Protocols // Advances in Cryptology — EUROCRYPT ’93. — Springer Berlin Heidelberg, 1994. — С. 344-359.
- *Gerhard P. Hancke, Markus G. Kuhn.* An RFID Distance Bounding Protocol (http://modsec.zimmerle.org/wireless-sec-papers/An%20RFID%20Distance%20Bounding%20Protocol.pdf) // SECURECOMM '05 Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks. — IEEE Computer Society Washington, DC, USA, 2005. — С. 67–73. Архивировано (https://web.archive.org/web/20161021070402/http://modsec.zimmerle.org/wireless-sec-papers/An%20RFID%20Distance%20Bounding%20Protocol.pdf) 21 октября 2016 года.
- *Chong Hee Kim, Gildas Avoine, Fran¸cois Koeune, Fran¸cois-Xavier Standaert, Olivier Pereira.* The Swiss-Knife RFID Distance Bounding Protocol (https://link.springer.com/chapter/10.1007%2F978-3-642-00730-9_7#page-1) // Information Security and Cryptology – ICISC 2008. — Springer Berlin Heidelberg, 2008. — С. 98-115.
- *Yu-Ju Tu, Selwyn Piramuthu.* RFID Distance Bounding Protocols (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.387.1511&rep=rep1&type=pdf) // In 1st International EURASIP Workshop in RFID Technology, Vienna, Austria. — 2007.
- *Cas Cremers, Kasper B. Rasmussen, Benedikt Schmidt, Srdjan Capkun.* Distance Hijacking Attacks on Distance Bounding Protocols (https://eprint.iacr.org/2011/129.pdf) // Proceedings of the 2012 IEEE Symposium on Security and Privacy. — IEEE Computer Society Washington, DC, 2012. — С. 113-127.
- *Брюс Шнайер.* Развитые протоколы // Прикладная криптография. — 2-е изд. — Триумф, 2003. — С. 92-93. — 816 с. — 3000 экз. — ISBN 5-89392-055-4.
- *Jason Reid, Juan M. Gonz´alez Nieto, Tee Tang, Bouchra Senadji.* Detecting Relay Attacks with Timing-Based Protocols (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.70.5584&rep=rep1&type=pdf) // Proceeding ASIACCS '07 Proceedings of the 2nd ACM symposium on Information, computer and communications security. — ACM New York, NY, USA, 2007. — С. 204-213.
- *Thomas Beth, Yvo Desmedt.* Identification Tokens — or: Solving The Chess Grandmaster Problem (https://link.springer.com/chapter/10.1007%2F3-540-38424-3_12#page-1). — Springer Berlin Heidelberg, 1991.
- *Dave Singelee, Bart Preneel.* Distance bounding in noisy environments (https://link.springer.com/chapter/10.1007%2F978-3-540-73275-4_8#page-1) // Proceeding ESAS'07 Proceedings of the 4th European conference on Security and privacy in ad-hoc and sensor networks. — Springer Berlin Heidelberg, 2007.