10.7256/2305-6061.2013.4.11092

КОДИРОВАНИЕ И ЗАЩИТА ИНФОРМАЦИИ

Савинов А.Н., Меркушев О.Ю.

ЗАЩИТА БИОМЕТРИЧЕСКИХ ПОДСИСТЕМ УПРАВЛЕНИЯ ДОСТУПОМ

Аннотация: *В статье рассматривается протокол аутентификации с нулевым разглашением на основе биометрического нечеткого экстрактора и криптосистемы Эль-Гамаля. Рассмотрены преимущества, недостатки и аспекты практического применения этого протокола. Описываются виды биометрических криптографических систем: системы с освобождением ключа, системы со связыванием ключа и системы с генерацией ключа, приводятся их краткие описания с рассмотрением возможных атак. Говорится, что существуют два подхода, позволяющие генерировать из биометрических данных ключи, удовлетворяющие требованиям современной криптографии, и обладающие при этом низкой вероятностью ошибки второго рода. Одним из основных факторов, определяющих состояние защищенности той или иной ключевой системы информационной инфраструктуры, является эффективность функционирования подсистемы управления доступом ее системы защиты информации. Предложен протокол биометрической аутентификации с нулевым разглашением. Главное условие надежности протокола – однократное использование сессионного ключа k. Преимуществом протокола является отсутствие необходимости хранения конфиденциальных пользовательских данных на стороне подсистемы управления доступом.*

Ключевые слова: *биометрическая криптографическая система, нечеткий экстрактор, криптосистема Эль-Гамаля, защита биометрических подсистем, управление доступом, протокол биометрической аутентификации, сессионный ключ, надежность, процесс аутентификации, угрозы*

Введение

Необходимо отметить, что первоначальной целью биометрической криптографии являлась защита криптографических ключей с помощью биометрических данных, однако, как будет показано далее, основными ее практическими применениями стали защита биометрических образцов и генерация криптографических ключей.

Эффективным функционированием подсистемы будем считать такое функциониро-

10.7256/2305-6061.2013.4.11092

вание, при котором обеспечиваются максимально возможные надежность и скорость процесса аутентификации, а также конфиденциальность обрабатываемых данных. Поэтому важным аспектом практической реализации подсистемы управления доступом являются методы защиты ее от актуальных угроз, в том числе от несанкционированного доступа к аутентификационным данным ее пользователей. В частности, для биометрических подсистем управления доступом одним из вариантов является применение так называемой биометрической криптографии[1].

В настоящее время существуют следующие виды биометрических криптографических систем: системы с освобождением ключа (англ. key release cryptosystems), системы со связыванием ключа (англ. key binding cryptosystems) и системы с генерацией ключа (англ. key generation cryptosystems)[2]. Ниже приведены их краткие описания с рассмотрением возможных атак.

1. Биометрические криптографические системы с освобождением ключа.

В режиме освобождения ключа биометрическая аутентификация осуществляется независимо от механизма освобождения ключа, биометрический эталон и ключ хранятся отдельно друг от друга, сам ключ освобождается после успешной биометрической аутентификации.

Такие системы непригодны для применения в приложениях, требующих высокой степени защиты, поскольку они имеют две основные уязвимости. Во-первых, биометрические эталоны не являются защищенными, поскольку они хранятся локально и к ним требуется доступ в процессе сравнения биометрических данных. Во-вторых, поскольку аутентификация и освобождение ключа абсолютно не связаны между собой, то представляется возможным заменить модуль сравнения при выполнении аутентификации, используя вредоносное программное обеспечение. В случае реализации этой уязвимости будет принято неверное решение об аутентификации и, соответственно, получен доступ к секретному ключу.

2. Биометрические криптографические системы со связыванием ключа.

Данный вид биометрических криптосистем изначально был разработан для за-

1 Бардаев С.Э., Финько О.А. “Многофакторная биометрическая пороговая криптосистема”, Известия ЮФУ. Технические науки, 2010, №4, С. 148–155.

2 Куликова О.В. “Биометрические криптографические системы и их применение”, Безопасность информационных технологий, 2009, № 2009-3.

10.7256/2305-6061.2013.4.11092

щиты криптографических ключей. Впоследствии такие криптосистемы стали применять и в целях защиты биометрических эталонов. Одной из наиболее часто применяемых в этих целях стала схема, предложенная в работе[3], названная «нечетким контейнером» (англ. fuzzy vault). Рассмотрим кратко принцип ее функционирования. Пусть X - биометрический образец с r элементами. Пользователь выбирает ключ K, преобразует его в полином P степени n и вычисляет значение полинома P для всех элементов X. Точки, принадлежащие P (назовем их подлинными), скрывают среди большого количества (обозначенного s) случайных точек, которые не принадлежат P (назовем их случайными); объединение наборов подлинных и случайных точек составляет контейнер V. В случае отсутствия биометрических данных пользователя в вычислительном отношении трудно определить подлинные точки в V. В ходе аутентификации пользователь предоставляет биометрический образец X'. Если X' значительно схож с X, пользователь может определить много точек в V, принадлежащих полиному. Если количество несоответствий между X и X' меньше чем $(r—n)/2$, то для восстановления P может быть применено декодирование Рида-Соломона, т.е. аутентификация пройдет успешно. С другой стороны, если X и X' недостаточно схожи, то невозможно восстановить P, т.е. аутентификация неуспешна. Существуют варианты схемы нечеткого контейнера для нескольких биометрических образцов, например, представленный К. Нандакумаром и А.К. Джейн[4]. В обоих случаях для каждого пользователя, зарегистрированного в подсистеме управления доступом, создается индивидуальный нечеткий контейнер.

Трудность вычисления подлинных точек в V при отсутствии биометрических данных пользователя обеспечивает безопасность образца. Однако схема нечеткого контейнера не является совершенным способом защиты биометрических образцов. В. Шейрер и Т. Боулт выделяют несколько классов атак схемы нечеткого контейнера[5]: 1) корреляционные атаки (англ. correlation attacks, attacks via record multiplicity (ARM), 2) атаки с инверсией ключа (англ. surreptitious key-inversion attacks (SKI) и 3) атаки подстановки со смешиванием (англ. blended substitution attacks). Корреляционная атака основана на перехвате зашифрованных данных во время сеансов аутентификации и последующем их соотнесении. Атака с инверсией ключа предполагает получение атакующим закры-

3 Juels A., Sudan M. "A Fuzzy Vault Scheme", in Proc. of IEEE Intl. Symp. on Info. Theory, Lausanne, Switzerland, 2002, p. 408.

4 Nandakumar K., Jain A.K. "Multibiometric Template Security Using Fuzzy Vault", in Proc. IEEE Int. Conf. Biometrics: Theory, Applications and Systems, Arlington, VA, Sep. 2008, pp. 1-6.

5 Scheirer W. J., Boult T. E. "Cracking Fuzzy Vaults and Biometric Encryption", in Proc. of Biometrics Symposium, September 2007.

10.7256/2305-6061.2013.4.11092

того ключа пользователя (в том числе, посредством социальной инженерии[6], и др.) и последующее извлечение биометрических данных из соответствующего контейнера. Атака подстановки со смешиванием основана на свойстве аддитивности нечеткого контейнера и состоит в несанкционированном добавлении в него биометрических данных злоумышленника. После такой инжекции и зарегистрированный пользователь, и злоумышленник будут успешно проходить аутентификацию по одной учетной записи.

3. Биометрические криптографические системы с генерацией ключа.

В такой биометрической криптосистеме ключ извлекается непосредственно из биометрических данных пользователя и не хранится в базе данных. Возможность не хранить ключ, полученный из биометрических данных, является неоспоримым преимуществом метода генерации криптографических ключей из биометрических данных пользователя по сравнению с другими существующими методами.

Использование для генерации криптографических ключей биометрических данных осложняется тем, что они неточно воспроизводимы и не имеют равномерного распределения, тогда как большинство криптографических преобразований требуют точного значения длины ключа. Кроме того, биометрические данные обладают следующими особенностями:

1) биометрические характеристики могут изменяться со временем, а некоторые зависят от физического и эмоционального состояния их владельца;

2) проблема смены ключей – биометрические данные неотзываемы;

3) невозможность держать многие биометрические данные в тайне (например, отпечатки пальцев могут быть оставлены на различных поверхностях).

На данный момент существуют два подхода, позволяющие генерировать из биометрических данных ключи, удовлетворяющие требованиям современной криптографии, и обладающие при этом низкой вероятностью ошибки второго рода[7]: использование специально обученных больших искусственных нейронных сетей и применение «нечетких экстракторов».

1. *Нейронные сети.*

Нейросетевой преобразователь «биометрия-код» – заранее обученная искусствен-

6 Касперски К. “Секретное оружие социальной инженерии” [Электронный ресурс] // Режим доступа: http://www.insidepro.com/kk/004r.shtml.

7 Бардаев С.Э., Финько О.А. “Многофакторная биометрическая пороговая криптосистема”, Известия ЮФУ. Технические науки, 2010, №4, С. 148–155.

10.7256/2305-6061.2013.4.11092

ная нейронная сеть с большим числом входов и выходов, преобразующая частично случайный вектор входных биометрических параметров «СВОЙ» в однозначный код криптографического ключа (длинного пароля) и преобразующая любой иной случайный вектор входных данных в случайный выходной код[8].

2. *Нечеткие экстракторы (англ. fuzzy extractors).*

Данный способ, впервые предложенный в работе[9], позволяет однозначно восстанавливать секретный ключ из неточно воспроизводимых биометрических данных при участии так называемых «вспомогательных данных» (англ. helper data), являющихся открытыми. При этом качество нечетких экстракторов определяется качеством применяемых в них кодов, исправляющих ошибки. Несомненным достоинством способа является отсутствие необходимости хранения секретного ключа, однако требуется хранение вспомогательных данных. Еще одним недостатком способа можно назвать то, что он позволяет получить из одних биометрических данных только один ключ. Однако это свойство является положительным с точки зрения применения данного способа в протоколах аутентификации, поскольку, таким образом, устанавливается однозначное соответствие биометрических данных конкретного пользователя ключу, который из них получен. Кроме того, качество выходной ключевой последовательности удовлетворяет всем критериям качества криптографических ключей.

Нечеткие экстракторы подвержены тем же классам атак, что и нечеткие контейнеры[10]. В то же время, атаки сложнее в реализации, а некоторые из них становятся невозможными в случае применения предложенных в более новых работах усовершенствований. Но и они не лишены недостатков: в частности, решение, предложенное Х. Бойеном, требует участия независимой доверенной третьей стороны[11].

Наиболее уязвимы нечеткие экстракторы к атакам со стороны квалифицированного персонала, напрямую связанного с функционированием подсистемы управления доступом (например, администратор сервера базы данных пользователей). Т.е. не исключена вероятность, что в роли злоумышленников могут оказаться указанные лица. Исходя из сказанного, в подсистеме управления доступом крайне нежелательна обработка вспомогательных данных, поскольку в этом случае если злоумышленнику известен алгоритм

8 ГОСТ Р 52633-2006 “Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации”.

9 Dodis Y., Reyzin L., Smith A. “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data” // April 13, 2004.

10 Scheirer W. J., Boult T. E. “Cracking Fuzzy Vaults and Biometric Encryption”, in Proc. of Biometrics Symposium, September 2007.

11 Boyen X. “Reusable cryptographic fuzzy extractors” // Eleventh ACM Conference on Computer and Communication Security. ACM, October 25–29 2004. P. 82–91.

10.7256/2305-6061.2013.4.11092

работы экстрактора, то, скомпрометировав биометрические данные, он сможет легко сгенерировать секретный ключ пользователя. Если аутентификация с помощью нечеткого экстрактора осуществляется по незащищенному каналу связи, мы должны исключить возможность перехвата любых данных, с использованием которых злоумышленник будет способен успешно осуществить атаку. Т.е. необходимо исключить передачу как биометрических данных, так и ключевой последовательности, сгенерированной на их основе, а также вспомогательных данных нечеткого экстрактора.

Эффективным решением поставленной выше задачи является использование некоторого протокола аутентификации, обладающего доказательством с нулевым разглашением (ZK-протокола). ZK-протоколы позволяют произвести процедуры идентификации, обмена ключами и другие основные криптографические операции без утечки любой секретной информации в течение информационного обмена[12]. Этой цели можно добиться при помощи демонстрации знания секрета, однако проверяющий должен быть лишен возможности получать дополнительную информацию о секрете. Следуя ZK-протоколу, участвующие стороны создают сеанс интерактивного доказательства, в ходе которого проверяющий и доказывающий обмениваются многочисленными запросами и ответами. Целью доказывающего является убеждение проверяющего в истинности утверждения. Поверяющий отклоняет или принимает доказательство. Таким образом, ZK-протоколы носят вероятностный, а не абсолютный характер. Сторона A владеет секретом s и пытается убедить сторону B в знании секрета.

Основные характеристики ZK-протокола:

— проверяющий не может ничего узнать из протокола;

— доказывающая сторона не может обмануть проверяющую сторону.

Если сторона A не знает секрета s и пытается доказать стороне B его знание, то после нескольких раундов протокола данный факт может быть установлен настолько точно, насколько это необходимо. Протокол также является «Cut AND Choose", т. е. после первого неудачного раунда сторона B точно знает, что A нелегальна. Проверяющая сторона не может обмануть доказывающую сторону. Сторона B не может вынести из протокола какой-либо информации, даже если она не следует протоколу. Единственное, что может сделать сторона B, это убедить себя, что сторона A знает секрет.

В данной работе предлагается ZK-протокол, основанный на идентификации по

12 Шнайдер Б. "Прикладная криптография". М.: Триумф, 2002.

10.7256/2305-6061.2013.4.11092

открытому ключу криптосистемы Эль-Гамаля[13]: проверяющая сторона шифрует произвольное число с помощью открытого ключа доказывающей стороны, и если доказывающая сторона сможет верно расшифровать его с помощью своего секретного ключа, сгенерированного нечетким экстрактором, то подтвердит свою подлинность. Чем больше произвольных чисел, зашифрованных проверяющей стороной, сможет расшифровать доказывающая сторона, тем выше вероятность того, что она подлинная. Чтобы скрыть возвращаемое расшифрованное значение, используется однонаправленная хеш-функция. Таким образом, проверяющая сторона фактически проверяет только соответствие присланного доказывающей стороной значения хеш-функции от выбранного числа.

Рассмотрим подробно процессы регистрации и аутентификации, основанные на предложенном протоколе.

1. *Регистрация.*

1) нечеткий экстрактор генерирует ключ $x>1$ из биометрических данных пользователя, вспомогательные данные сохраняются у пользователя (например, на карту памяти или др. носитель);

2) генерируется случайное простое число $p>x$;

3) выбирается целое число g, являющееся первообразным корнем по модулю p;

4) вычисляется $y=g^x \bmod p$;

5) открытый ключ $(p;g;y)$, который впоследствии будет использоваться в качестве идентификатора, высылается регистрирующей стороне и сохраняется у пользователя;

6) регистрирующая сторона выбирает сессионный ключ k, взаимно простой с p-1, т.е. НОД(k, p-1)=1;

7) вычисляются $a= g^k \bmod p$ и $b= y^k M \bmod p$, где M – случайное сообщение;

8) шифротекст $(a;b)$ высылается регистрируемому пользователю;

9) на стороне пользователя вычисляется $M'= b(a^x)^{-1} \bmod p$, регистрирующей стороне высылается $h(M')$ - значение хеш-функции от M';

10) регистрирующая сторона продолжает повторять пункты 6-10 до достижения требуемой вероятности подлинности регистрируемого пользователя, либо отказывает в регистрации в зависимости от верности равенства $h(M)= h(M')$.

2. *Аутентификация.*

1) нечеткий экстрактор восстанавливает ключ x из биометрических данных пользователя по сохраненным вспомогательным данным;

13 Мухачев В.А., Хорошко В.А. "Методы практической криптографии". – Киев, ООО "Полиграф-Консалтинг", 2005. 215 с.; Коробейников А.Г.,Воробьев А.О. ,Сидоркина И.Г., ПылинВ.В. Анализ криптографической стойкости алгоритмов асимметричного шифрования информации. Изв.ВУЗОВ. Приборостроение. 2007. Т. 50. № 8., стр. 28-32.

10.7256/2305-6061.2013.4.11092

2) открытый ключ *(p;g;y)* высылается проверяющей стороне на проверку наличия его в базе; если ключ отсутствует в базе, сеанс заканчивается, в ином случае выполняются шаги аналогично пунктам 6-10 регистрации.

В данном случае пользователь является доказывающей стороной, а подсистема управления доступом – проверяющей стороной. Если хотя бы на одном из раундов не будет выполнено равенство *h(M)= h(M')*, в аутентификации будет отказано.

Поскольку проверяющей стороне не известен секретный ключ доказывающей стороны, шифрование сообщений в ходе последующего обмена информацией между ними будет осуществляться с использованием других ключей. Возможна передача общего секретного сеансового ключа в сообщении *M*. В этом случае возникает дополнительное требование к стойкости хеш-функции *h*.

Таким образом, получен простой и эффективный протокол биометрической аутентификации с нулевым разглашением. Главное условие надежности протокола – однократное использование сессионного ключа *k*. Преимуществом протокола является отсутствие необходимости хранения конфиденциальных пользовательских данных на стороне подсистемы управления доступом. В отличие от некоторых реализаций, не требуется участие третьей стороны. Основным недостатком можно считать то, что пользователям необходимо хранить носители с их открытыми вспомогательными данными. С другой стороны, информационный носитель является дополнительным фактором аутентификации. Кроме того, в сохранности собственных данных пользователи заинтересованы обычно в большей степени, чем персонал систем информационной инфраструктуры.

Предложенный протокол может быть усовершенствован заменой криптосистемы Эль-Гамаля криптосистемой, основанной на эллиптических кривых.

Библиография:

1. Бардаев С.Э., Финько О.А. "Многофакторная биометрическая пороговая криптосистема", Известия ЮФУ. Технические науки, 2010, №4, С. 148–155.
2. Куликова О.В. "Биометрические криптографические системы и их применение", Безопасность информационных технологий, 2009, № 2009-3.
3. Juels A., Sudan M. "A Fuzzy Vault Scheme", in Proc. of IEEE Intl. Symp. on Info. Theory, Lausanne, Switzerland, 2002, p. 408.
4. Nandakumar K., Jain A.K. "Multibiometric Template Security Using Fuzzy Vault", in Proc. IEEE Int. Conf. Biometrics: Theory, Applications and Systems, Arlington, VA, Sep. 2008, pp. 1-6.
5. Scheirer W. J., Boult T. E. "Cracking Fuzzy Vaults and Biometric Encryption", in Proc. of Biometrics Symposium, September 2007.

6. Касперски К. “Секретное оружие социальной инженерии” [Электронный ресурс] // Режим доступа: http://www.insidepro.com/kk/004r.shtml.
7. ГОСТ Р 52633-2006 “Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации”.
8. Dodis Y., Reyzin L., Smith A. “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data” // April 13, 2004.
9. Boyen X. “Reusable cryptographic fuzzy extractors” // Eleventh ACM Conference on Computer and Communication Security. ACM, October 25–29 2004. P. 82–91.
10. Шнайдер Б. “Прикладная криптография”. М.: Триумф, 2002.
11. Мухачев В.А., Хорошко В.А. “Методы практической криптографии“. – Киев, ООО “Полиграф-Консалтинг“, 2005. 215 с.
12. Коробейников А.Г.,Воробьев А.О. ,Сидоркина И.Г., ПылинВ.В. Анализ криптографической стойкости алгоритмов асимметричного шифрования информации. Изв.ВУЗОВ. Приборостроение. 2007. Т. 50. № 8., стр. 28-32.

References:

1. Bardaev S.E., Fin’ko O.A. “Mnogofaktornaya biometricheskaya porogovaya kriptosistema”, Izvestiya YuFU. Tekhnicheskie nauki, 2010, №4, S. 148–155.
2. Kulikova O.V. “Biometricheskie kriptograficheskie sistemy i ikh primenenie”, Bezopasnost’ informatsionnykh tekhnologii, 2009, № 2009-3.
3. Juels A., Sudan M. “A Fuzzy Vault Scheme”, in Proc. of IEEE Intl. Symp. on Info. Theory, Lausanne, Switzerland, 2002, p. 408.
4. Nandakumar K., Jain A.K. “Multibiometric Template Security Using Fuzzy Vault”, in Proc. IEEE Int. Conf. Biometrics: Theory, Applications and Systems, Arlington, VA, Sep. 2008, pp. 1-6.
5. Scheirer W. J., Boult T. E. “Cracking Fuzzy Vaults and Biometric Encryption”, in Proc. of Biometrics Symposium, September 2007.
6. Kasperski K. “Sekretnoe oruzhie sotsial’noi inzhenerii” [Elektronnyi resurs] // Rezhim dostupa: http://www.insidepro.com/kk/004r.shtml.
7. GOST R 52633-2006 “Zashchita informatsii. Tekhnika zashchity informatsii. Trebovaniya k sredstvam vysokonadezhnoi biometricheskoi autentifikatsii”.
8. Dodis Y., Reyzin L., Smith A. “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data” // April 13, 2004.
9. Boyen X. “Reusable cryptographic fuzzy extractors” // Eleventh ACM Conference on Computer and Communication Security. ACM, October 25–29 2004. R. 82–91.
10. Shnaider B. “Prikladnaya kriptografiya”. M.: Triumf, 2002.
11. Mukhachev V.A., Khoroshko V.A. “Metody prakticheskoi kriptografii“. – Kiev, OOO “Poligraf-Konsalting“, 2005. 215 s.
12. Korobeinikov A.G.,Vorob’ev A.O. ,Sidorkina I.G., PylinV.V. Analiz kriptograficheskoi stoikosti algoritmov asimmetrichnogo shifrovaniya informatsii. Izv.VUZOV. Priborostroenie. 2007. T. 50. № 8., str. 28-32.

