СПОСОБ МУЛЬТИБИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ

Меркушев О. Ю.,Кубашев Д. Ю.,Кубашева Е. С.
Кафедра информационно-вычислительных систем, Поволжский государственный технологический университет
Йошкар-Ола, Российская Федерация
E-mail: lem11x@mail.ru

В мультибиометрических системах управления доступом эффективное решение задачи распознавания особенно актуально, поскольку злоумышленник потенциально может завладеть данными одновременно о нескольких биометрических характеристиках пользователя. Предложена реализация метода мультибиометрической аутентификации с нулевым разглашением на основе нечеткого экстрактора и криптосистемы Эль-Гамаля. Рассмотрены преимущества и аспекты практического применения этого метода

Введение

Методы аутентификации по биометрическим параметрам, ввиду неотъемлемости этих параметров от конкретного человека, способны обеспечить повышенную, в сравнении со способами проверки соответствия по известной человеку информации и/или физическим компонентам, точность, невозможность отказа от авторства и удобство для пользователей, а применение для аутентификации одновременно нескольких биометрических параметров способствуют снижению уровня ошибок первого и второго рода, а также негативного влияния таких факторов, как возможности повреждения или утраты биометрической характеристики, излишней схожести либо слабой считываемости отдельных биометрических характеристик некоторых людей [1].

Помимо обеспечения необходимой точности проверки соответствия, для биометрических подсистем управления доступом актуальна задача защиты аутентификационных данных пользователей. Одним из наиболее перспективных вариантов решения этой задачи является применение метода «нечеткий экстрактор» [2], генерирующего при каждом считывании биометрических параметров некоторого конкретного человека идентичную равномерно распределенную последовательность из данных, получаемых при считывании, с использованием «вспомогательных данных», сохраняемых при первом считывании (регистрации). Нечеткий экстрактор позволяет получить из одних биометрических данных только одну последовательность, благодаря чему устанавливается однозначное соответствие биометрических данных конкретного пользователя и последовательности. Кроме того, достигается низкая вероятность ошибки второго рода [3]. Также разработан метод генерации равномерно распределенной последовательности из нескольких биометрических параметров [4].

I. Описание реализации

Биометрические подсистемы управления доступом, в которых применяются нечеткие экстракторы, подвержены различным внутренним и внешним атакам, особенно со стороны квалифицированного персонала, напрямую связанного с их функционированием [5]. Следовательно, для обеспечения защиты биометрической подсистемы управления доступом на основе нечеткого экстрактора, использующей незащищенные каналы связи, как от внутренних, так и от внешних угроз необходимо исключить передачу и хранение биометрических данных и последовательности, сгенерированной на их основе, а также передачу вспомогательных данных нечеткого экстрактора. Для достижения этой цели можно использовать некоторый протокол аутентификации, обладающий доказательством с нулевым разглашением: в ходе сеанса демонстрируется знание секрета без раскрытия его самого или какой-либо информации о нем [6].

В качестве варианта реализации протокола биометрической аутентификации с нулевым разглашением предлагается применение асимметричной криптографии: установление подлинности основывается на расшифровании доказывающей стороной своим секретным ключом случайных сообщений от проверяющей стороны, шифруемых открытым ключом доказывающей стороны. Рассмотрим действия проверяющей и доказывающей сторон в процессах регистрации и аутентификации на примере протокола с нулевым разглашением, основанном на криптосистеме Эль-Гамаля [7].

1. *Регистрация.*

1. проверяющая сторона генерирует случайное простое число p, которое должно быть больше максимально возможного значения, генерируемого нечетким экстрактором;
2. проверяющая сторона выбирает целое число g, являющееся первообразным корнем по модулю p;

3. нечеткий экстрактор доказывающей стороны генерирует ключ $x>1$ из биометрических данных пользователя, вспомогательные данные сохраняются на некоторый носитель пользователя;
4. доказывающая сторона вычисляет $y = g^x \ mod \ p$;
5. y, который впоследствии будет использоваться в качестве идентификатора, сохраняется у обеих сторон.

2. *Аутентификация.*

1. нечеткий экстрактор доказывающей стороны генерирует ключ x из биометрических данных пользователя и вспомогательных данных;
2. y высылается проверяющей стороне для выяснения наличия его в базе; если ключ отсутствует в базе, сеанс заканчивается, в ином случае — переход к следующему пункту;
3. проверяющая сторона выбирает сессионный ключ k, взаимно простой с $p-1$, т.е. НОД(k, $p-1$)=1;
4. проверяющая сторона вычисляет $a=g^k \ mod \ p$ и $b=y^k M \ mod \ p$, где M – случайное сообщение, $M<p$;
5. шифротекст $(a;b)$ высылается доказывающей стороне;
6. доказывающая сторона вычисляет $M'=b(a^x)^{-1} \ mod \ p$, проверяющей стороне высылается $h(M')$ - значение хеш-функции от M';
7. проверяющая сторона продолжает повторять пункты 2-5 до достижения требуемой вероятности подлинности регистрируемого пользователя, либо отказывает в регистрации в зависимости от верности равенства $h(M)= h(M')$.

II. Биометрический нечеткий экстрактор

При каждом считывании биометрических параметров некоторого конкретного человека нечеткий экстрактор генерирует идентичную равномерно распределенную последовательность из данных, получаемых при считывании, с использованием «вспомогательных данных», сохраняемых при первом считывании (регистрации), если данные, полученные при очередном считывании близки к данным, полученным при регистрации. Нечеткий экстрактор позволяет получить из одних биометрических данных только одну последовательность, благодаря чему устанавливается однозначное соответствие биометрических данных конкретного пользователя и последовательности. Кроме того, достигается низкая вероятность ошибки второго рода. Также разработан метод генерации равномерно распределенных последовательностей с использованием нескольких биометрических параметров.

Биометрические системы управления доступом, в которых применяются нечеткие экстракторы, подвержены различным внутренним и внешним атакам, особенно со стороны квалифицированного персонала, напрямую связанного с их функционированием. Следовательно, для обеспечения защиты биометрической системы управления доступом на основе нечеткого экстрактора, использующей незащищенные каналы связи, как от внутренних, так и от внешних угроз необходимо исключить передачу и хранение биометрических данных и последовательности, сгенерированной на их основе, а также передачу вспомогательных данных нечеткого экстрактора. Для достижения этой цели можно использовать некоторый протокол аутентификации, обладающий доказательством с нулевым разглашением: в ходе сеанса доказывающая сторона (субъект доступа) демонстрирует знание секрета проверяющей стороне (системе управления доступом) без раскрытия его самого или какой-либо информации о нем.

III. Заключение

Таким образом, предложен способ мультибиометрической аутентификации с нулевым разглашением, позволяющий безопасно подтверждать подлинность при использовании не защищенных от перехвата каналов связи. Кроме того, вследствие отсутствия необходимости хранения биометрических данных пользователей на стороне сервера исключается ответственность ее персонала за обеспечение конфиденциальности таких данных.

IV. Список литературы

1. Jain A.K., Ross A. “Multibiometric Systems” // January 2004/Vol. 47 No. I COMMUNICATIONS OF THE ACM).
2. Dodis Y., Reyzin L., Smith A. "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data"// April 13, 2004.
3. Бардаев С.Э., Финько О.А. "Многофакторная биометрическая пороговая криптосистема Известия ЮФУ. Технические науки, 2010, №4.
4. Zhang M., Yang B., Zhang W., Takagi T. “Multibiometric based secure encryption and authentication scheme with fuzzy extractor”, International Journal of Network Security, Vol. 12, No. 1, 2011, pp. 50-57.
5. Scheirer W. J., Boult T. E. "Cracking Fuzzy Vaults and Biometric Encryption in Proc. of Biometrics Symposium, September 2007.
6. Шнайдер Б. "Прикладная криптография". М.: Триумф, 2002.
7. Мухачев В.А., Хорошко В.А. “Методы практической криптографии“. – Киев, ООО “Полиграф-Консалтинг“, 2005. 215 с.