УДК 004.934.8’1

А.Н. Ручай

Модель атак и защиты биометрических систем распознавания диктора

Приведена общая модель атак на биометрическую систему распознавания диктора, представлены классификация возможных атак на данную систему, а также методы защиты от них.

Ключевые слова: биометрическая аутентификация, биометрическая система, распознавание диктора, атаки, защита.

При массовом внедрении биометрических систем возникает проблема в безопасности использования таких систем. Исследователи большое внимание уделяют в основном решению прямой задачи биометрики [1, 2], т.е. непосредственно распознаванию человека по биометрическим характеристикам, чем оценкам надежности, возможным атакам на реализуемые системы и обратной задаче биометрики [3, 4].

В работе [5] были систематизированы только основные типы атак, в статье [6] была предложена модель, которая описывала общие атаки на биометрические системы через угрозы на отдельные элементы. Имеется целый ряд обзорных статей с подробным описанием атак и мер защиты на биометрические системы на основе статических характеристик [7–11]. В данной статье представлен обзор существующих атак и мер защиты, которые относятся к системам с динамическими характеристиками и, в частности, к системам распознавания диктора [12].

Модель атак и классификация сценариев атак

Любую атаку на биометрическую систему нужно моделировать с учетом параметров, соответствующих реальной системе. В работе [3] была представлена классификация атак по степени возможных действий:

• активные – существует возможность записывать, модифицировать, читать и перехватывать как на программном уровне, так и на аппаратном уровне данные в биометрической системе;

• пассивные – существует возможность только подменять данные на уровне устройства ввода.

Также в [3] было введено понятие злоумышленника, который является в некотором смысле специалистом в различных областях и которому присущи следующие знания и умения:

• знание недостатков оборудования и аппаратной реализации в целом;

• знание протокола взаимодействия и передачи данных;

• знание структуры и способа хранения информации;

• знание методов и алгоритмов, заложенных в реализованную систему;

• навыки синтезирования данных и использования этих данных;

• умение выбрать более эффективную и результативную атаку.

Самыми распространенными злоумышленниками являются пассивные, так как активные действия достаточно трудны в реализации. Однако в работе [3] были классифицированы сценарии атак по действиям злоумышленника, которые связаны в основном с активным воздействием:

• использование неавторизированного биометрического оборудования или легального оборудования нестандартным способом;

• использование процедуры извлечения шаблона;

• использование уровня порогового значения при принятии решения;

• использование протокола аутентификации;

• использование неправомочной модификации шаблона;

• использование протокола передачи данных.

Опишем систему распознавания диктора через общую схему биометрической аутентификации [1, 7, 8] (рис. 1). В данной схеме каждый элемент может создавать угрозу, приводящую к реализации атаки, и с каждой угрозой связаны свой тип атаки и мера предотвращения ее.

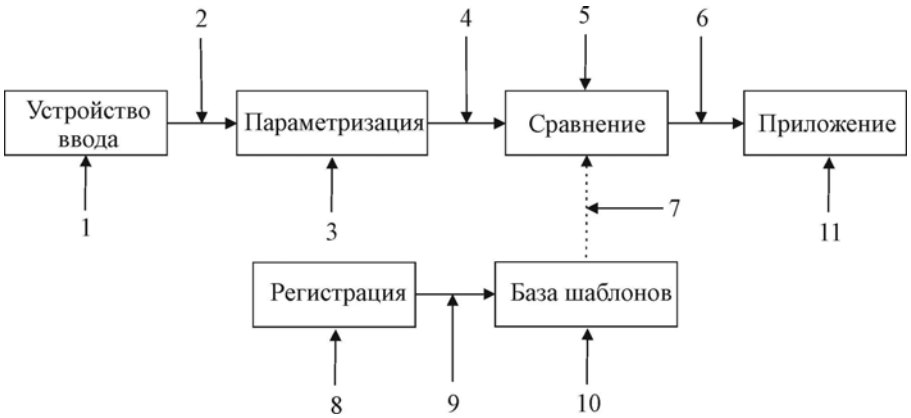

Рис. 1. Общая схема аутентификации с обозначенными атаками

Приведем все типичные атаки, связанные с угрозами на элементы системы аутентификации диктора, которые могут быть в равной степени применены и для других биометрических систем (см. рис. 1):

1) атака на устройство ввода;
2) атака на канал связи между сенсором и биометрической системой;
3) атака на параметризацию речевого сигнала;
4) атака на канал передачи параметризованного сигнала;
5) атака на элемент сравнения вектора параметра и шаблона;
6) атака на элемент результата сравнения;
7) атака на канал связи с базой шаблонов;
8) атака на элемент регистрации пользователя;
9) атака на канал между элементом регистрации и базой шаблонов;
10) атака на элемент базы шаблонов;
11) атака на приложение.

Все перечисленные выше атаки, кроме атаки на устройство ввода, являются общими для всех биометрических систем [1, 7, 8]. Защита от подобных атак заключается в использовании цифрового кодирования, временных меток и шифрования открытого канала передачи данных.

Больший интерес представляет атака на устройство ввода в биометрической системе распознавания диктора, так как эта атака создает реальную угрозу.

Атака на устройство ввода

Данная атака направлена на устройство ввода и возникает, когда злоумышленник предоставляет нелегитимные биометрические данные сенсору. Данную атаку можно разделить на три вида:

• принудительная атака – предоставление биометрических данных подлинного пользователя на нелегитимных основаниях, например с применением насилия;

• имитационная атака – изменение биометрических характеристик злоумышленника с целью имитации биометрических данных зарегистрированного пользователя;

• атака воспроизведения – предоставление ранее записанных биометрических данных подлинного пользователя.

Рассмотрим подробно каждый вид атак на устройство ввода, которые являются наиболее вероятными для угрозы биометрической системы распознавания диктора.

1. Принудительная атака

В принудительной атаке под угрозой подлинный пользователь произносит фразу, необходимую для доступа к системе. Для этого варианта атаки существует несколько способов защиты:

• использование параллельно с системой аутентификации говорящего голосового «детектора лжи», т.е. системы, обнаруживающей возбуждение и напряженность говорящего [13];

• использование дополнительной парольной фразы, так называемой «тревожной кнопки», при распознавании которой система реагирует внешне нормально, но на самом деле оповещает службу безопасности [1];

• видео- и аудионаблюдение за всеми попытками входа в систему [1].

2. Имитационная атака

Также возможно использовать имитацию голоса зарегистрированного пользователя [12]. Для предотвращения подобной атаки необходимо использовать в системе плохо имитируемые признаки. Большинство автоматических систем аутентификации диктора используют признаки, отличные от тех, которые использует речеслуховая система. Связано это с тем, что имитироваться могут либо медленно меняющиеся параметры, либо отдельные акустические события или просодические характеристики речи (мелодика, ритмика, динамика). Однако признаки, используемые автоматической системой, являются достаточно быстро меняющимися и не связаны с произнесением в целом. Это дает гарантию невозможности имитации голоса.

Дадим определение синтезированным данным как поддельным биометрическим данным, которые максимально соответствуют оригинальным. Существует два класса синтезированных данных [3, 4]:

• данные, в некотором смысле соответствующие оригиналу, т.е. для речевого сигнала должны сохраняться структура и разборчивость речи;

• данные, не имеющие никакого соответствия с оригиналом, т.е. для речевого сигнала не сохраняется никакой структуры, что легко можно определить на слух.

Использование синтезированных данных для осуществления атаки на биометрическую систему аутентификации диктора является более возможной, чем имитация голоса, так как существует возможность искусственного синтеза речи конкретного человека.

Синтез речи начал свое развитие в 60-е годы XX в. с первых экспериментов [14]. В наши дни решение данной задачи продвинулось достаточно далеко, однако до сих пор она полностью не решена. Синтез голоса должен учитывать возраст, пол, эмоциональное состояние, индивидуальные черты, физиологическую и социальную окраску диктора. Синтез голоса также должен включать индивидуальные просодические характеристики голоса человека, которые имитируют более правдоподобную речь.

Для успешной реализации атаки необходимо использовать систему речи с учетом индивидуальных характеристик диктора, которые используются для аутентификации диктора, однако до сих пор таких готовых систем не существует.

3. Атака воспроизведения

При атаке воспроизведения в основном используются записи зарегистрированного диктора, полученные тем или иным способом. Существует несколько способов защиты от такой атаки:

• Простейший способ защиты системы – это ограниченное время реакции пользователя на произнесение фразы. Даже при использовании современного звукового оборудования мгновенная реакция злоумышленника практически невозможна.

• Другой способ защиты – это требование повторного произнесения пароля, когда «живым голосом» точное воспроизведение одного и того же речевого сигнала невозможно.

• Более сложные системы идентификации используют некоторую базу паролей, сформированную системой на этапе обучения. В данном случае система аутентификации диктора случайным образом выбирает пароль из этой базы и предлагает пользователю каждый раз произнести новую фразу.

В последнее время проводятся активные исследования по возможности построения систем идентификации диктора на основе паролей, что делает вероятность взлома системы с помощью записи речи диктора практически невозможной. Можно предложить несколько эффективных методов аутентификации диктора на основе паролей:

1. На основе парольной фразы [15]. На этапе регистрации диктор несколько раз произносит парольную фразу, после чего формируется биометрический эталон. При аутентификации диктор заново произносит ту же самую парольную фразу, после чего принимается решение о совпадении сформированного эталона и предъявленного шаблона. Достоинства: простота реализации. Недостатки: существует реальная возможность осуществления атаки воспроизведения, невозможность смены парольной фразы без процедуры обучения. Такой способ аутентификации можно использовать в том случае, когда ценность данных не очень высока, но требуется увеличить надежность системы по сравнению со стандартными методами аутентификации.

2. На основе множества парольных фраз [16, 17]. Основное отличие от предыдущего способа заключается в том, что на этапе регистрации пользователю предлагается произнести не одну, а 5–15 парольных фраз, и на этапе аутентификации диктору предлагается произнести парольную фразу, выбранную случайным образом из базы. Достоинства: увеличение надежности от атаки воспроиз-

ведения при небольшом усложнении алгоритма. Недостатки: увеличение времени обучения и объема памяти. Такой способ аутентификации можно использовать либо в общественных местах, либо при разграничении доступа в помещениях, ведущих дополнительно видеонаблюдение над пользователем. Также необходимо осуществлять контроль зоны проведения процедуры аутентификации на предмет установки звукозаписывающей аппаратуры.

3. На основе множества ключевых слов [18]. Парольная фраза случайным образом формируется из словаря небольшого объема. Достоинства: более защищена от атаки воспроизведения, чем другие способы аутентификации. Недостатки: увеличение времени обучения и трудности в переобучении.

4. На основе динамического изменения множества ключевых слов. Данный метод был предложен и описан в статье [19]. Суть метода заключается в том, что множество ключевых слов может быть динамически изменен без этапа обучения. Достоинства: самая высокая защита от атаки воспроизведения. Недостатки: нет достаточных оценок надежности данного метода.

Заключение

Многие статьи и публикации обличают биометрические системы как ненадежные и подверженные серьезным уязвимостям в связи с продемонстрированными возможностями атак на данные системы [1, 7, 8].

Многие проблемы и атаки можно предотвратить с помощью цифрового кодирования, временных меток и шифрования открытого канала передачи данных. Иными словами, создаются специальные криптографические протоколы, позволяющие предотвратить различные атаки.

Также для предотвращения атак используют следующие методы:

• используют специальные методы обнаружения живучести биометрических образцов [9];

• применяют для повышения безопасности систем различные подходы к организации базы данных шаблонов и к структуре шаблона [20, 21];

• используют для повышения надежности биометрических систем многофакторную аутентификацию [1];

• для устранения проблемы конфиденциальности и защиты информации используют специальную технологию сокращения биометрических параметров и «шифрование личности» [22].

Однако существование угрозы атаки на устройство ввода биометрической системы на основе распознавания диктора является актуальной и требует дополнительных мер защиты.

Литература

1. Руководство по биометрии / Р.М. Болл, Дж.Х. Коннел, Ш. Панканти и др. – М. : Техносфера, 2007. – 368 с.

2. Dunstone T. Biometric system and data analysis: design, evaluation, and data mining / T. Dunstone, N. Yager. – Boston, Ma: Springer, 2009. – 268 p.

3. Inverse Problems of Biometrics / S. Yanushkevich, V. Shmerko, A. Stoica, D. Popel // CRC Press, Taylor and Francis Group. – 2005. – 386 p.

4. Image pattern recognition: synthesis and analysis in biometrics / S. Yanuschkevich, P. Wang, M. Gavrilova, S. Srihari // Series in Machine Perception and Artifical Intelligence. – Vol. 67. New Jersey–London–Singapore: World Scientific Publishing Co., 2007. – 430 p.

5. Wayman J. Technical testing and evaluation of biometric devices // Biometrics – personal identication in networked society. – N.Y.: Kluwer Academic Publisher, 2002. – P. 345–368.

6. Ratha N.K. Enhancing security and privacy in biometrics–based authentication systems / N.K. Ratha, J.H. Connell, R.M. Bolle // IBM Systems Journal. – 2001. – № 40(3). – P. 614–634.

7. Roberts C. Biometric attack vectors and defences // Computers and Security. – 2007. – Vol. 26, № 1. – P. 14–25.

8. Schneier B. The uses and abuses of biometrics // Communications of the ACM. – 1999. – № 42(8). – 136 p.

9. Алгулиев Р.М. Методы обнаружения живучести в биометрических системах / Р.М. Алгулиев, Я.Н. Имамвердиев, В.Я. Мусаев // Вопросы защиты информации. – 2009. – № 3(86). – С. 16–21.

10. Galbally J. Bayesian hill-climbing attack and its application to signature verification / J. Galbally, J. Fierrez, J. Ortega Garcia // Lecture Notes Comput. Sci. 4642. – 2007. – P. 386–395.

11. Uludag U. Attacks on biometric systems: a case study in fingerprints / U. Uludag, A. Jain // Proc. SPIE. – 2004. – Vol. 5306. – P. 622–633.

12. Рамишвили Г.С. Автоматическое опознавание говорящего по голосу. – М.: Радио и связь, 1981. – 224 с.

13. Hansen J. Speech under stress: Analysis, Modeling and Recognition / J. Hansen, S. Patil // Speaker Classification 1, LNAI 4343 / S. Müller (Ed.). – Berlin; Heidelberg: Springer–Verlag, 2007. – P. 108–137.

14. Лобанов Б.М. Компьютерный синтез и клонирование речи / Б.М. Лобанов, Л.И. Цирульник. – Минск: Белорусская наука, 2008. – 316 с.

15. Campbell J.P. Speaker recognition: a tutorial / J.P. Campbell // Proceedings of the IEEE. – 1997. – № 85(9). – P. 1437–1462.

16. Higgins A. Password-based voice verification using SpeakerKey / A.L. Higgins, L.G. Bahler [Электронный ресурс]. – Режим доступа: http://www.isca-speech.org/archive_open/archive_papers/odyssey/odys_031.pdf, свободный (дата обращения: 05.05.2011).

17. Rodriguez–Linares L. A novel technique for the combination of utterance and speaker verification systems in a text–dependent speaker verification task / L. Rodriguez-Linares, C. Garcia-Mateo // Proceedings of the international conference on spoken language processing (ICSLP). – 1998. – № 2. – P. 213–216.

18. Markowitz J. Voice biometrics / J. Markowitz // Communications of the ACM. – 2000. – № 43(9). – P. 66–73.

19. Бабенко Л.К. Аутентификация диктора с использованием изменяемого множества ключевых слов / Л.К. Бабенко, В.М. Федоров, П.Ю. Юрков // Известия ТРТУ. Спец. вып.: Матер. науч. конф. ТРТУ. – Таганрог : Изд-во ТРТУ, 2004. – № 1(36). – С. 128.

20. Biometric Device Protection Profile (BDPP) // Technical Report, UK Government Biometrics Working Group. – 2001 [Электронный ресурс]. – Режим доступа: http://www.cesg.gov.uk/policy_technologies/biometrics/media/bdpp082.pdf, свободный (дата обращения: 05.05.2011).

21. Biometric System Protection Profile for Medium Robustness Environments // Technical Report, US Department of Defence and Federal. – 2002. – [Электронный ресурс]. – Режим доступа: https://www.biometricscatalog.org/2003gbw/downloads/PP_BSPP-MR_V0.02.pdf, свободный (дата обращения: 05.05.2011).

22. Иванов А. Высоконадежная биометрическая аутентификация пользователя: последний дюйм первой мили / А. Иванов, А. Малыгин // Первая миля. – 2007. – №2. – С. 20–24.

Ручай Алексей Николаевич
Аспирант каф. компьютерной безопасности и прикладной алгебры ЧелГУ, г. Челябинск
Тел.: (351) 977-92-92
Эл. почта: ruchai@pochta.ru

Ruchay A.N.
The model of attacks and protection of the speaker recognition biometric system

The paper discusses the general model of attacks to the speaker recognition biometric system, classification of attacks to this system and protection from these attacks are given.
Keywords: biometric authentication, biometric system, speaker recognition, attack, protection.
