

УДК 004.93(062):[57.087.1:519.21](062)

Параметры биометрических систем

Гончаров В.Ю. Орел ГТУ, 12-Р,

E-mail: goncharov.v.u@rambler.ru

Рук. Абашин В.Г.

Актуальность: В наши дни люди стали активно уделять внимание биометрическим параметром, в связи внедрение новых технологий.

Цель: Повысить уровень знаний, изучить подробно данную тему.

Биометрия — раздел вариационной статистики, с помощью методов которого производят обработку экспериментальных данных и наблюдений, а также планирование количественных экспериментов в биологических исследованиях.

Вероятность возникновения ошибок FAR/FRR, то есть коэффициентов ложного пропуска (False Acceptance Rate — система предоставляет доступ незарегистрированному пользователю) и ложного отказа в доступе (False Rejection Rate — доступ запрещен зарегистрированному в системе человеку). Необходимо учитывать взаимосвязь этих показателей: искусственно снижая уровень «требовательности» системы (FAR), мы, как правило, уменьшаем процент ошибок FRR, и наоборот. На сегодняшний день все биометрические технологии являются вероятностными, ни одна из них не способна гарантировать полное отсутствие ошибок FAR/FRR, и нередко данное обстоятельство служит основой для не слишком корректной критики биометрии. FRR(False Rejection Rate) — процент ошибочных отказов, когда система отказывает в доступе авторизованному пользователю; FAR(False Acceptance Rate) — процент ошибочных допусков, когда доступ к системе ошибочно предоставляется неавторизованному пользователю. Необходимо

знать оба параметра системы (FRR и FAR), особенно если они были получены в результате лабораторных тестов либо скрупулёзного анализа результатов ежедневного использования. Кроме того, намереваясь приобрести ту или иную биометрическую систему, вы должны вначале выяснить ее уязвимые места:

1) Атака путём повторной передачи корректной информации. Аппаратные компоненты биометрической системы должны передавать информацию на обработку программным компонентам для аутентификации пользователя. Если эти передаваемые данные в определённый момент перехватить, то в будущем можно попытаться повторно симулировать их передачу от аппаратных компонентов, чтобы получить доступ к системе. К примеру, при использовании сканера для проверки отпечатков пальцев, подключенного через порт USB, последовательность передаваемых во время верификации данных может быть перехвачена, и позднее повторно передана тому же порту.

2) Фальсификация. Поскольку принцип работы биометрических устройств идентификации сводится к распознаванию некоторых физических характеристик человека, можно попытаться создать точную копию характеристики. Например чтобы обмануть систему распознавания по голосу, достаточно воспроизвести речь этого человека, записанную на пленку.

3) Манипуляции с базой данных. Биометрическая информация должна храниться в некоторой базе данных, чтобы поступившие данные можно было сравнивать с некоторым образцом в процессе аутентификации пользователя. Поэтому, проникнув в базу данных, шпион может добавить характеристики пользователя, ранее не имевшего доступ к системе.

4) Инженерный анализ. Любое устройство биометрической аутентификации состоит из аппаратной и программной части, которые взаимодействуют с операционной системой или приложениями. Можно проанализировать программный код приложения, чтобы в дальнейшем создать программную «заплату», позволяющую всегда идентифицировать пользователя как легального, даже если на самом деле его данные вообще отсутствуют в системе. Ведь в течение многих лет компьютерные пираты успешно

игнорировали, например, схемы защиты программного обеспечения от копирования, изменяя значения шестнадцатеричных кодов на ассемблере в операторах условного выбора либо заменяя фрагменты кода холостыми командами (NOP). И если подростки в состоянии дизассемблировать приложение и убрать нетривиальные средства защиты программы от копирования, то, очевидно, что защита системы биометрической аутентификации также может быть взломана.

Таблица 1. Основные технические характеристики на биометрические системы HandKey II

Параметры	Значения
Время верификации	менее 1 с
Размер шаблона	9 байт
Срок хранения данных в памяти	до 5 лет при использовании встроенной стандартной литиевой батареи
Идентификационный номер	1-10 цифр с клавиатуры или считывателя карт
Объем памяти событий	5120 событий
Виды связи	RS-485 (4-проводной и 2-проводной интерфейсы); RS-232 подключение к принтеру или к сети
Скорость в бодах	от 300 до 28800 бод/с
Количество пользователей	512 пользователей, возможно расширение до 32512 пользователей
Частота возникновения ошибки первого рода	0,001%
Частота возникновения ошибки второго рода	0,000001%
Вход считывателя карт доступа	proximity, wiegand, магнитная карта или штрих-код
Выход эмуляции считывателя карт	wiegand, магнитная карта или штрих-код
Код принуждения	1 цифра, назначаемая пользователем
Количество временных зон	62
Питание	12 - 24 В постоянного или переменного тока
Размер	22 (Ш) x 30 (В) x 22 (Г) см
Вес	2,7 кг
Опции	BB-200 - внутренний аккумулятор бесперебойного питания; MD-500 - высокоскоростной внутренний модем; EN-200 - модуль для связи по сети Ethernet;

Таблица 1 продолжение

	EM-801 - расширение памяти до 9728 пользователей; EM-803 - расширение памяти до 32512 пользователей; DC-102 - конвертер RS-232/RS-485; KP-201 - дополнительная клавиатура; встраиваемый проксимити-считыватель фирмы HID
--	---

Рынок биометрических систем бурно развивается. Несмотря на это, лишь несколько российских компаний могут предложить комплексные биометрические решения.

Вывод: Подробно изучили данную тему, самое интересное, что параметры биометрических систем распространились настолько широко, что в настоящее время используются не только в серьезных учреждениях типа банков или аэропортов, но и в университетах, школах и даже дома. Данные технологии применяются чаще в Западной Европе и США.

Список литературы:

1. Эра биометрики [электронный ресурс]/ <http://www.osp.ru/text/print/302/173069.html> (с изм. и доп.)- режим доступа: (дата обращения 22.02.10)
2. Биометрические системы доступа [электронный ресурс]/ http://www.amosystems.ru/system/biometric_system_handkey_II.ahtm (с изм. и доп.)- режим доступа: (дата обращения 25.02.10)
3. Биометрические технологии [электронный ресурс]/ http://www.ru.wikipedia.org/wiki/Биометрические_технологии (с изм. и доп.)- режим доступа: (дата обращения 25.02.10)
4. Биометрическая идентификация в масштабах компании [электронный ресурс]/ <http://www.elsys.ru/review7.php> (с изм. и доп.)- режим доступа: (дата обращения 25.02.10)