Капшук О.А., Старосельский А.Я.
УНК "ИПСА" НТУУ "КПИ", Киев, Украина

Проблемы хранения биометрических параметров в базах данных систем идентификации личности

При использовании биометрических технологий для установления личности являются актуальными задачи обеспечения безопасности хранения и использования биометрических данных.

Биометрические системы идентификации работают по стандартному алгоритму. Первый шаг, система запоминает образец биометрической характеристики. Второй, система делает несколько образцов для того, чтобы составить наиболее точную цифровую модель биометрической характеристики. Третий, полученная информация обрабатывается и преобразовывается в биометрический код, который заносится в БД и используется в дальнейшем для идентификации человека в системе. Проблема состоит в том, что биометрический код хранится в незашифрованном виде.

Исходя из опыта известных систем и новой законодательной платформы (оператор системы не может своевольно менять персональные данные человека без его присутствия) можно выделить основную проблему – проблема защиты биометрического кода, а так же БД, где он хранится.

Для решения проблемы защиты БД можно предложить пакет программ Oracle Advanced Security [1], что является наиболее подходящей системой защиты для самой СУБД. Недостаток: система актуальна только для БД семейства Oracle. Существуют и другие пакеты расширения с похожими функциями, такие как: InfoSphere Guardium 8 (разработан IBM) и DbProtect (разработан Application Security Inc).

Биометрические данные необходимо хранить в БД в зашифрованном виде, чтобы доступ к ним можно было получить только в присутствии их владельца (необходимо использовать методы шифрования основанные на биометрических данных [2]). Биометрическая криптографическая система со связыванием ключа – один из самых популярных методов защиты биометрического кода. В криптографических системах такого типа ключ и биометрический код связываются между собой и представляют единое целое. Для обеспечения возможности извлечения ключа из биометрического кода используются методы кодирования, которые позволяют извлекать ключ в случае, если биометрические данные пользователя отличаются от биометрического кода (не более чем на заданное количество бит). Так же можно построить систему хранения и использования биометрических данных, используя метод нечетких экстракторов (использование биометрических данных для формирования ключей в идентификационных криптосистемах).

Исследование различных методов защиты биометрического кода позволяет сделать вывод, что наиболее подходящим является метод криптозащиты с использованием биометрических параметров, который позволяет жестко связать биометрический код и его владельца.

В докладе рассмотрены различные методы защиты биометрической информации и методы защиты БД различными программными средствами. Даны рекомендации относительно выбора метода шифрования на основе биометрических данных.

Литература

1. Oracle Advanced Security [Электронный ресурс] / Режим доступа: http://www.interface.ru/home.asp?artId=24676 Дата обращения: 23.02.11.
2. О.В. Куликова. Биометрические Криптографические Системы и их применение./ Режим доступа: статья.

International conference on System Analysis and Information Technologies SAIT 2011
Institute for Applied System Analysis of National Technical University of Ukraine "KPI", Kyiv, Ukraine, May 23–28, 2011
ISBN 978-966-2153-57-6, revision 0.9.2 (2011.05.12), available at http://sait.kpi.ua/books/sait2011.ebook.pdf