БИОМЕТРИЧЕСКИЕ МЕТОДЫ В КРИПТОГРАФИИ: проблемы и перспективы

Е.Карпиков, инженер компании DNA Distribution

Статья посвящена биометрии как перспективному инновационному механизму криптографической защиты информации. Практическое применение уникальных биометрических параметров человека для защиты от несанкционированного доступа к конфиденциальной информации имеет ряд сложностей и ограничений. Тем не менее, биометрические системы по многим параметрам являются удобным и достаточно надежным способом обеспечения безопасности защищаемой среды.

Понятие "конфиденциальная информация" возникло задолго до появления первых письменных документов. Человечество изо дня в день старалось совершенствовать системы и методы защиты своих личных данных, чтобы уберечь их от посягательства посторонних лиц и тем более мошенников. Существует множество мощных аппаратных и программных средств защиты информации, но зачастую их недостаточно для того, чтобы с полной уверенностью заявить о стопроцентной безопасности защищаемой среды.

Даже самая надежная система безопасности не может работать автономно, она нуждается в постоянном авторизованном управлении. Для получения доступа к системе нужно пройти аутентификациию: система должна удостовериться в том, что именно вы являетесь подлинным офицером ее безопасности.

Существует много способов аутентификации, в числе которых парольная аутентификация, а также аутентификация с помощью всевозможных токенов – компактных устройств, предназначенных для обеспечения информационной безопасности пользователя. В последнее время большую популярность получила биометрическая аутентификация. Ее ключевая особенность состоит в том, что элементами авторизации являются биометрические параметры человека: отпечатки пальцев, черты лица, структура сетчатки и узор радужной оболочки глаза, параметры голоса, способ подписи, манера походки и многие другие.

В отличие от парольной аутентификации, проблемами которой являются утерянные, украденные либо забытые пароли, биометрическая аутентификация обладает рядом значительных преимуществ. Биометрический идентификатор практически невозможно утратить или забыть, как пароль, или потерять, как токен. Для самого процесса аутентификации необходимо обязательное присутствие самого владельца биометрических параметров. Уникальность таких параметров человека, как узор сетчатки глаза или отпечатки пальцев, в разы повышает достоверность аутентификации. Эти параметры довольно трудно фальсифицировать. Методы биометрической аутентификации хорошо зарекомендовали себя и успешно применяются в различных системах контроля доступа. По своей природе биометрические данные имеют следующие особенности, затрудняющие их использование в криптографии:

- они могут меняться со временем и в зависимости от физического и психологического состояния владельца. Например, сетчатка глаза может

изменяться со временем; голос и почерк человека могут меняться в зависимости от его состояния. В связи с этим возникает проблема с идентичной воспроизводимостью данных;
- они находятся в открытом доступе и не являются секретной информацией. Например, можно сделать копию отпечатков пальцев с поверхности;
- они неотзываемы. Другими словами, они не могут быть легко изменены, так как присущи определенной личности. Отсюда возникает проблема смены ключей при желании иметь различные ключи для доступа к различным приложениям;
- есть проблема конфиденциальности личных данных: многие люди не хотят хранить свои биометрические эталоны в базах данных.

Несмотря на перечисленные трудности, биометрия в криптографии постоянно развивается и совершенствуется. Биометрическая аутентификация стала применяться не только в качестве защиты от несанкционированного доступа, но также в качестве источника уникальной персонифицированной информации для формирования ключей. Однако применение биометрического материала в качестве ключей сталкивается с принципиальной сложностью: в криптографии требуется точное значение ключа, в то время как биометрические данные всегда имеют естественную погрешность при воспроизведении в цифровом виде.

В зависимости от целей и задач, можно выделить несколько видов биометрических криптографических систем:
- системы с освобождением ключа (Key Release Cryptosystems). В этих системах биометрическая аутентификация осуществляется независимо от использования ключа шифрования, т.е. биометрический эталон и ключ хранятся отдельно друг от друга, а ключ становится доступным после успешной биометрической аутентификации. Такие системы непригодны для применения в приложениях, требующих высокой степени защиты, поскольку имеют две основные уязвимости. Во-первых, биометрические эталоны не являются защищенными, так как 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, представляется возможным заменить модуль сравнения при выполнении аутентификации, используя вредоносное ПО. В случае реализации этой уязвимости будет принято неверное решение

об аутентификации и, соответственно, получен доступ к секретному ключу;

- системы со связыванием ключа (Key Binding Cryptosystems). В таких криптографических системах ключ и биометрический эталон непосредственно связаны между собой и представляют единое целое. Каждому биометрическому эталону соответствует только один ключ. Декодирование ключа из биометрического эталона без знания биометрических данных пользователя является вычислительно сложной задачей и практически невозможно. Для корректного извлечения ключа из эталона используются специальные коды, исправляющие ошибки. Они позволяют извлечь ключ даже в случае, если биометрические данные пользователя отличаются от эталона, но не более чем на определенное количество бит. Добиться этого можно с помощью избыточной информации в эталоне, но повышение устойчивости к ошибкам означает снижение криптографической стойкости. Другими словами, ключ закрывается (зашифровывается) биометрическим эталоном пользователя и сохраняется именно в таком виде в базе данных. Если сравнение биометрических данных было успешным, то ключ извлекается из биометрического эталона и может дальше использоваться в системе. В данном методе безопасность зависит от степени секретности алгоритмов закрытия и восстановления ключа. Когда алгоритмы известны, их можно легко скомпрометировать. Однако по сравнению с криптографическими системами с освобождением ключа, эти системы более безопасны, но и более сложны в реализации с учетом изменения биометрических данных во времени;
- системы с генерацией ключа (Key Generation Cryptosystems). В таких биометрических криптосистемах ключ извлекается непосредственно из биометрических данных пользователя и не хранится в базе данных. Из биометрических данных человека извлекаются параметры, из которых при помощи специального алгоритма генерируется секретный ключ пользователя. Возможность не хранить ключ, а получать его из биометрических данных пользователя является неоспоримым преимуществом по сравнению с другими существующими методами. Использование для генерации криптографических ключей биометрических данных осложняется тем, что они неточно воспроизводятся, тогда как все криптографические преобразования требуют точного значения ключа.

За последние несколько лет было разработано множество методов генерации ключей из самых различных биометрических параметров. Однако, как показала практика, длина ключа очень мала в силу ограниченности уникальных биометрических признаков. Вероятность ошибки второго рода (случай, когда за истину принимается ложное значение какого-либо параметра) при этом превышает 20%, что исключает на текущем этапе развития практическое применение таких систем для защиты действительно ценной информации. Но и это не мешает биометрии развиваться быстрыми темпами, и, возможно, уже в самом ближайшем будущем появятся надежные биометрические системы, которые отодвинут привычные нам повседневные пароли на второй план. ■

В Барселоне будет представлена сеть Wi-Fi операторского класса с автоматическим роумингом

На Всемирном конгрессе мобильной связи 2014 в Барселоне будет впервые развернута широкомасштабная сеть стандарта Hotspot 2.0, которой смогут воспользоваться десятки тысяч посетителей. Над созданием сети следующего поколения Wi-Fi Hotspot совместно работали компании AT&T, Cisco и Accuris Networks и несколько международных операторов мобильной связи, включая Bell Mobility, China Mobile, Korea Telecom, MEO, Mobily, NTT DOCOMO, PCCW-HKT, SK Telecom и True.

Абоненты операторов-участников, пользующиеся новейшими совместимыми телефонами, будут автоматически и безопасно аутентифицированы в сети Hotspot 2.0 Wi-Fi на территории проведения конференции с той же легкостью, с какой они переключатся в роуминг, приземлившись в барселонском аэропорту.

Стандарт Hotspot 2.0 стал результатом многолетней работы и сотрудничества операторов мобильной связи с производителями сетевого оборудования и мобильных телефонов. В сущности, он обеспечивает ту же бесшовную, исключительно безопасную аутентификацию в сети Wi-Fi, с которой пользователи уже знакомы по роумингу в сетях мобильной связи. Технология Hotspot 2.0 соответствует требованиям данного стандарта и сертифицирована по программе Wi-Fi Certified Passpoint международным альянсом Wi-Fi Alliance.

http://www.cisco.com