МЕТОДЫ СЕТЕВОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ JAVA-КАРТ

С. А. Маталыцкий

Введение

Аутентификация пользователей в компьютерных системах всегда была актуальной и острой проблемой. Одним из наиболее распространенных и эффективных методов аутентификации является аутентификация с использованием пластиковых карточек, выступающих в качестве носителя персональной информации. В данной работе рассматриваются варианты построения систем аутентификации на основе перспективной технологии JavaCard, проведен анализ известных протоколов аутентификации с использованием пакета JCDK (Java Card Development Kit) фирмы Sun, предложены эффективные алгоритмы аутентификации, реализуемые на основе JavaCard.

Смарт-карта – это пластиковая карточка, содержащая микрокомпьютер, позволяющий обрабатывать и хранить информацию. Как правило, смарткарта содержит в себе микропроцессор (чаще всего 8-разрядный), ОЗУ (256 байт – 2 Кб), ПЗУ (2–8 Кб), энергонезависимую память (2–16 Кб). Часто в современную смарткарту встраивают математический сопроцессор, выполняющий операции с большими числами и позволяющий эффективно реализовывать различные криптографические алгоритмы. JavaCard – это смарткарта, в ПЗУ которой находится java-машина, позволяющая загружать и выполнять java-программы. Главные достоинства такого подхода – аппаратная независисимость и простота разработки приложений. Согласно спецификации JavaCard2.2 от компании Sun MicroSystems (разработчика данной технологии), JavaCard должна содержать библиотеки классов, реализующие различные криптографические алгоритмы, что позволяет строить на основе JavaCard надежные протоколы аутентификации.

Исследуемая модель и протоколы аутентификации

При исследовании протоколов аутентификации акцент ставился на устойчивость алгоритмов к воздействиям на канал связи смарткарты и терминала, так как именно этот участок связи может с легкостью контролироваться третьим лицом. Также предполагалась полная открытость используемых алгоритмов, так как современные системы безопасности не могут основываться на засекречивании протоколов обмена данными и должны опираться только на используемые секретные ключи. Целью процесса аутентификации предполагалось удостоверение подлинности сторон и получение сеансового ключа для обмена данными с использованием симметричных алгоритмов шифрования. В работе было уделено внимание только тем алгоритмам аутентификации, которые могут быть эффективно реализованы в JavaCard, т. е. основанных на стандартных криптографических алгоритмах шифрования данных.

Результаты

В работе был проведен анализ протоколов аутентификации, построенных на базе односторонних функций, симметричных и несимметричных алгоритмов шифрования данных.

По мнению автора, надежные протоколы аутентификации должны строиться на основе несимметричных алгоритмов шифрования (исключают проблему распределения секретных ключей) с обязательным использованием случайных данных в передаваемых пакетах информации (исключает возможность подбора сеансового ключа по пе-

рехваченному открытому ключу терминала или смарткарты), а также с использованием авторизационного сервера в качестве посредника при проверке подлинности сторон терминалом и смарткартой (исключает возможность атаки «человек-в-середине», основанной на перехвате и подмене открытых ключей терминала и смарткарты).

Заключение

Эффективность систем аутентификации на основе карточек на сегодняшний день проверена временем и не вызывает сомнений. Использование в качестве носителя информации JavaCard позволит поднять безопасность таких систем на новый уровень и расширить спектр их применения, особенно в области аутентификации в компьютерных системах и сетях (минимальные требования к аппаратному обеспечению).

В заключение хотелось бы отметить постоянно снижающуюся стоимость JavaCard. Смарткарта, поддерживающая стандарт JavaCard 2.2, на сегодняшний день в розницу стоит 14$, а при поставках свыше 1 000 штук – 8$, что является доступным для большинства потребителей.