УДК 681.3

ИСПОЛЬЗОВАНИЕ СМАРТ-КАРТ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ПРОЦЕССЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

М.И. Спирягин, В.И. Спирягин, С.А. Клюев, Е.А. Валуйский, Ф.П. Усенко

Восточноукраинский национальный университет им. В. Даля
кафедра “Компьютерные системы и сети”, 91034, г. Луганск, кв. Молодежный, 20а
munc@snu.edu.ua, volina@mail.dsip.net, sergeykluev@mail.ru

Описана технология создания программно-аппаратного комплекса для web-дистанционного процесса обучения с применением технологий SmartCard.

This article describes technology for creation of hard and software complex for web-distance process of education with applying SmartCard technology.

Постановка проблемы

Для обеспечения эффективной защиты информации, аутентификации пользователей, контролирования процесса дистанционного обучения необходимо разработать модель верификации. Следует обеспечить аутентификацию пользователя на уровне одного документа (студенческий, читательский билет) для доступа к электронным ресурсам (библиотека, комплект учебно-методической документации и т.д.), услугам Интернета, а также обеспечить целостность информации в процессе передачи и приема данных через Интернет при тестировании студента в процессе дистанционного обучения.

В настоящее время большая часть современных технологий проведения тестирования имеет один весомый недостаток. Все они хотя и допускают некоторую аутентификацию пользователя, однако не позволяют в полной мере проконтролировать этот процесс. Небрежность в данном вопросе снижает ценность результата теста, а также, чаще все, приводит к следующим проблемам:

1. Позволяет участникам предварительно ознакомиться со списком вопросов и вариантами ответов.
2. С помощью анализатора трафика дает возможность участникам определить ответы других.
3. Позволяет воспользоваться некорректными регистрационными данными.
4. Не исключает возможность подмены участника тестирования.

Невзирая на сравнительно небольшую вероятность использования каждого пункта отдельно, их совокупность уменьшает уровень доверия к тестам на основе современных компьютерных технологий. В некоторых же случаях их применение вообще становится нецелесообразным.

Технология SmartCard

Для устранения вышеописанных недостатков предлагается использовать технологию SmartCard.

Смарт-карты имеют ряд очевидных достоинств [1]. Прежде всего приставку "Smart" (интеллектуальная) карта получила не просто так. Имея вид обычной пластиковой кредитной карточки, она содержит в себе интегральную схему, которая наделяет ее способностями к хранению и обработке информации.

Смарт-карта, по своим размерам напоминающая кредитную, способна хранить и обрабатывать информацию с помощью полупроводниковых электронных схем, спрятанных внутри пластикового корпуса.

В зависимости от встроенной микросхемы все смарт-карты делятся на несколько основных типов, кардинально различающихся по выполняемым функциям:

- карты памяти;
- микропроцессорные карты;
- карты с криптографической логикой.

Карты памяти предназначены для хранения информации. Память на таких типах карт может быть свободной для доступа или содержать логику контроля доступа к памяти карты для ограничения операций чтения и записи данных.

Микропроцессорные карты также предназначены для хранения информации, но в отличие обычных карт памяти они содержат в себе специальную программу или небольшую операционную систему, которая позволяет преобразовывать данные по определенному алгоритму, осуществлять защиту информации хранящейся на карте при передаче, чтении и записи, выполнять криптографические преобразования информации (схемы шифрования, электронной цифровой подписи, аутентификации и др.). Кроме того, эти смарт-карты могут дополнительно обеспечиваться средствами аутентификации (как логического, так и биометрического характера), владельца смарт-карты.

Карты с криптографической логикой используются в системах защиты информации для принятия непосредственного участия в процессе шифрования данных или выработки криптографических ключей, электронных цифровых подписей и другой необходимой информации для работы системы.

Сейчас смарт-карты с микропроцессором получают все большее распространение во всем мире благодаря присущим им широким возможностям по аутентификации пользователей таких карт, компактности использования, быстроте и удобности работы с ними, а также стойкости применения в них криптографических алгоритмов, что обеспечивает высокую тайность конфиденциальной информации. Доступ к данным, сохраненным на карте, контролируется микропроцессором карты с помощью пароля.

Для реализации программно-аппаратного комплекса представляет интерес технология Java Card [2]. Данная технология использует смарт-карты, поддерживающие программы, написанные на языке Java.

Структура Java Card определяет набор классов прикладного программного интерфейса (API (Application Program Interface)), предназначенного для разработки приложений Java Card, и набор системных служб для нормального функционирования этих приложений. Необходимость дополнительных библиотек, которые реализуют расширенные служебные функции, обеспечивающие безопасность и описывающие системную модель, определяется спецификой решаемых задач. Приложения Java Card называются апплетами. На одной карте может выполняться несколько различных апплетов. Каждый однозначно определяется идентификатором приложения (application identifier, AID), который описывается в пятой части стандарта ISO 7816. Апплет не просто проигрывает один и тот же сценарий, а реагирует на действия пользователя и может динамически менять свое поведение.

Один из ключевых принципов разработки языка Java заключается в обеспечении защиты от несанкционированного доступа. Программы на Java не могут вызывать глобальные функции и получать доступ к произвольным системным ресурсам, что обеспечивает в Java уровень безопасности, недоступный для других языков.

Использование языка Java дает следующие преимущества:

- Java предоставляет для широкого использования свои апплеты (applets) — небольшие, надежные, динамичные, не зависящие от платформы активные сетевые приложения, встраиваемые в страницы Web. Апплеты Java могут настраиваться и распространяться потребителям с такой же легкостью, как любые документы HTML;
- Java высвобождает мощь объектно-ориентированной разработки приложений, сочетая простой и знакомый синтаксис с надежной и удобной в работе средой разработки. Это позволяет широкому кругу программистов быстро создавать новые программы и новые апплеты.

Устройство и механизм работы комплекса

Для реализации предлагаемого комплекса сервер должен отвечать ряду требований. Проведенный анализ рассматриваемой проблемы позволил сформулировать требования к программному обеспечению серверной части:

- ОС: Linux (версия ядра старше 2.4) или FreeBSD;
- Web-сервер: Apache 1.3 и выше с модулями openssl и PHP старше 4.1;
- БД: MySQL 4 и старше;
- программный или аппаратный фаервол.

Аппаратная часть сервера зависит от выбранной операционной системы и средней нагрузки на сервер. Кроме этого желательно дополнить сервер устройством резервного копирования и оснастить его аппаратным генератором случайных чисел.

Для работы клиентской части необходимо оснастить компьютеры кард-ридерами, а также должно быть установлено соответствующее программное обеспечение - браузер с поддержкой JavaScript 1.2 и виртуальная машина Java от Sun.

В качестве кард-ридера можно использовать внешнее устройство чтения/записи контактных смарт-карт ACR30U-CFC. Данный карт-ридер представляет собой компактное и удобное устройство, которое поддерживает все микропроцессорные смарт-карты, а также большинство карт памяти всех известных производителей.

Исходя из существующих задач по защите и достоверности информации, возникающих в процессе обучения, предлагается следующий алгоритм работы комплекса:

1. Каждый пользователь получает на руки персональную смарт-карту. Карта содержит логин, пароль и ключ пользователя. Технология снижает к минимуму возможность неправомерного перепрошивания карты с целью замены этих данных. Возможно, объединение такой смарт-карты с существующими студенческими и читательскими билетами. Это позволит больше всего широко внедрить технологию в существующий учебный процесс.
2. Перед началом теста пользователь вставляет свою смарт-карту в ридер. Клиентская часть приложения определяет наличие смарт-карты в ридере и считывает оттуда регистрационные данные. Выполняется базовая проверка этих данных (целостность и т.п.), после чего приложение устанавливает защищенное соединение с сервером. Клиент отправляет серверу регистрационные данные, считанные из смарт-

карты. В свою очередь сервер проверяет наличие в базе данных пользователей наличие подобной записи. С целью повышения защищенности системы пароли хранятся в базе в виде md5 отпечатков.

3. Если подобная запись в базе найдена, сервер выполняет также ряд дополнительных проверок. При проведении тестирования он проверяет наличие разрешения на сдачу теста в текущий промежуток времени (во избежание несанкционированной пересдачи теста в другое время).

4. Если пользователь авторизован успешно, сервер передает клиенту необходимые данные. Использование защищенного соединения сводит на нет возможность перехвата данных.

5. Апплет следит за наличием карты в ридере. В случае извлечения карты из ридера соединение клиента с сервером разрывается. При проведении тестирования сервер следит за тем, чтобы данные пользователя были отосланы в отведенный для теста промежуток времени. По окончании данного промежутка времени сервер также разрывает соединение. По окончании тестирования ответы пользователя подписываются его персональным ключом со смарт-карте и хранятся в БД сервера. Таким образом, преподаватель может проверить целостность результатов тестирования для каждого студента. Это делает невозможной несанкционированную вставку в БД ответов и результатов теста.

Рассматривая информационное взаимодействие студента и университета с точки зрения безопасности, следует качественно решить несколько задач [3]:

- защита подключенных к публичным каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий;
- защита информации (личных данных, контрольных заданий, результатов тестирования) в процессе передачи по открытым каналам связи.

Для решения первой задачи целесообразно использование межсетевых экранов (брандмауэров). На сегодня применение брандмауэров является стандартным не только в корпоративном секторе, но и в качестве защиты отдельного удаленного компьютера.

Решение второй задачи предполагает выполнение следующих функций [4]:

- аутентификация взаимодействующих сторон;
- криптографическое закрытие передаваемых данных;
- подтверждение подлинности и целостности доставленной информации;
- защита от повтора, задержки и удаления сообщений;
- защите от отрицания фактов отправления и приема сообщений.

Данные функции связаны друг с другом, их реализация основана на криптографической защите передаваемых данных. Эффективность такой защиты обеспечивается благодаря совместному использованию симметричных и асимметричных криптографических систем.

Такая технология объединения локальных сетей и отдельных компьютеров через открытую внешнюю среду в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих в ней данных, называется VPN (виртуальная защищенная сеть) [5]. Для независимости от прикладных протоколов и приложений VPN формируются на одном из более низких уровней модели OSI (Open System Interconnection) — канальном, сетевом или сеансовом. Чем ниже уровень, на котором реализуется защита, тем она прозрачнее для приложения и пользователя. Более высокий уровень модели OSI расширяет набор услуг безопасности и облегчает конфигурирование системы защиты, но в этом случае усиливается зависимость от используемых протоколов обмена и приложений.

Рассмотрим подробнее защищенное соединение (сеансовый уровень), на котором наибольшую популярность для шифрования информации получил протокол SSL/TLS (Secure Sockets Layer/Transport Layer Security). Ядром этого протокола является технология комплексного использования симметричных и ассиметричных криптосистем компании RSA Data Security. Для аутентификации взаимодействующих сторон и криптозащиты ключа симметричного шифрования используются цифровые сертификаты открытых ключей пользователей (в данном случае удаленного студента и сервера дистанционного обучения), заверенные цифровыми подписями специальных Сертификационных Центров. Сертификаты соответствуют общепринятому стандарту X.509. В качестве алгоритмов асимметричного шифрования используются алгоритмы RSA, а также Диффи - Хелмана. Допустимыми алгоритмами симметричного шифрования являются RC2, RC4, DES а также Triple DES. Для вычисления хеш-функций могут применятся MD-5 и SHA-1. В качестве альтернативы существующим и уже реализованным в протоколе алгоритмам поточного симметричного шифрования нами намечено применение собственного поточного шифра, работа над которым ведется в данное время.

Для стандартизации аутентифицированного прохода через брандмауэры консорциум IETF (Проблемная группа проектирования Интернет) определил протокол под названием SOCKS, в настоящее время 5-я версия этого протокола применяется для стандартизованной реализации посредников каналов. В протоколе SOCKS v.5 клиентский компьютер устанавливает аутентифицированный сокет (или сеанс) с сервером, выполняющим роль посредника (proxy). Этот посредник - единственный способ связи через межсетевой экран. Посредник проводит любые операции, запрашиваемые клиентом.

В качестве платформы для разработки клиентской части программного обеспечения нами выбрана технология JAVA CARD. Она позволяет разрабатывать как апплеты, исполняемые внутренним процессором смарт-карты, так и хост - приложение, которое поддерживает обмен информацией со смарт-картой, на языке

Java. Для работы по протоколам SSL\TLS в Java начиная с версии 1.4 в качестве базового расширения используется Java Secure Socket Extension (JSSE). Используя JSSE, можно установить безопасный обмен данными между клиентом и сервером, управляющим любым из прикладным протоколов типа HTTP, Telnet или FTP. Резюмируя сложные криптографические алгоритмы безопасности и механизмы "подтверждения связи", JSSE минимизирует риск создания тонкой, но опасной уязвимости безопасности. Кроме того, упрощается прикладная разработка, как стандартный блок, который разработчики могут непосредственно использовать в своих приложения.

В качестве преимуществ которые, дает использование JSSE, можно выделить следующее:

- 100% реализован на чистой Java;
- может экспортироваться в большинство стран;
- обеспечивает поддержку программного интерфейса приложений SSL версиям 2.0 и 3.0 и выполнение SSL 3.0;
- обеспечивает поддержку программного интерфейса приложений и выполнение для версии TLS 1.0;
- обеспечивает поддержку протоколу передачи гипертекста (HTTP), инкапсулированного в протоколе SSL (HTTPS), который предоставляет безопасный доступ к данным, веб-страницам, используя HTTPS;
- обеспечивает поддержку наиболее распространенных криптографических алгоритмов, включая перечисленные в табл. 1.

Криптографические алгоритмы, используемые для Java Secure Socket Extension Таблица

Криптографичекий алгоритм	**Длина ключа(Bits)**
RSA	2048 (authentication), 2048 (key exchange), 512(key exchange)
RC4	128, 128 (40 effective)
DES	64 (56 effective), 64 (40 effective)
Triple DES	192, (112 effective)
AES	256, 128
Diffie-Hellman	1024, 512
DSA	1024

Вышеприведенный алгоритм позволяет построить систему, лишенную подавляющего большинства недостатков, свойственным современным технологиям, применяемых в высших учебных заведениях. Она исключает подделку и изменение как со стороны студента, так и со стороны проверяющего технического персонала. Подобная технология отлично масштабируется и позволяет построить централизованную систему в рамках факультета и университета. В то же время система открыта для доработки и может быть дополнена другими возможностями, например статистическим анализом, распечаткой отчетов, сведений и др.

Выводы

Использование смарт-карт для защиты информации в процессе дистанционного обучения предоставляет следующие преимущества:

- возможность автоматизированно управлять и контролировать компьютерную сеть университета;
- предоставлять услуги Интернета студентам и техническому персоналу;
- универсальность системы позволяет соединять несколько компьютерных сетей кампусов в единственную управляемую структуру с одним центральным сервером;
- гибкое разграничение доступа к сетевым ресурсам для операторов, администраторов и др.;
- одновременная работа множества пользователей в системе посредством web-интерфейса;
- использование микропроцессорных смарт-карт в качестве студенческого и читательского билета гарантирует, что учетные записи используются лишь теми людьми, кому их предоставили. Смарт-карты защищены от подделки, их невозможно скопировать, потому что после персонализации карты ключи доступа никогда и нигде не появляются в открытом виде;
- пользователи уникально идентифицируют и аутентифицируют себя с использованием уникального имени пользователя и пароля;
- применение смарт-карт в университете во многом упрощает работу системного администратора и пользователя.

1. *ISBC* – Смарт-карты. - http://www.isbc.ru/products/smart/
2. *Sun Microsystem*. Java Technology. - http://java.sun.com/
3. *Столлингс В*. Криптография и защита сетей: принципы и практика: 2-е изд. - М.:"Вильямс", 2001. – 672 с.
4. *Зима В.М., Молдовян А.А., Молдовян Н.А*. Безопасность глобальных сетевых технологий. - СПб.: БХВ-Петербург, 2000. - 320 с.
5. *Галицкий А.В., Рябко С.Д., Шаньгин В.Ф.* Защита информации в сети - анализ технологий и синтез решений - М.: ДМК Пресс, 2004. - 616 с.