Разработка модели программно-аппаратного комплекса эмуляции уязвимостей систем ДБО

М.А. Кобилев, Е.С. Абрамов, И.Ю. Половко
Южный федеральный университет
kobilev@sfedu.ru, abramoves@sfedu.ru, iypolovko@sfedu.ru

Аннотация

В статье представлена модель программно-аппаратного комплекса эмуляции уязвимостей систем дистанционного банковского обслуживания. Данная модель рассматривается как основа лабораторного практикума для студентов направления подготовки информационная безопасность автоматизированных систем.
В качестве подхода к проведению лабораторных занятий предложен формат CTF (capture the flag) игры. В рамках таких лабораторных практикумов студенты получают знания не только о техниках, которые используются злоумышленниками при атаках на приложения ДБО, но и узнают о механизмах защиты, необходимых для обнаружения и предотвращения атак.
Актуальность данной тематики основывается на отчете крупных консалтинговых компаний, проводящих аудит систем ДБО. Основываясь на этих отчетах, можно говорить о востребованности рынка к специалистам по защите систем ДБО.
В работе был проведен анализ возможности реализации проекта и его дальнейшее внедрение в процесс обучения специалистов по направлению информационная безопасность автоматизированных систем.

Ключевые слова: дистанционное банковское обслуживание, электронные деньги, уязвимости ДБО, интернет банкинг, мобильный банкинг

1. Введение

В наше время интернет используется повсеместно – у каждого есть один, два, а то и три устройства, способные выйти в глобальную сеть. Настоящие деньги заменяются электронными. В погоне за удобством используют различные способы хранения и использования сбережений. Хранить деньги наличными не безопасно, но безопасно ли хранить их в банках, предоставляющих услуги дистанционного управления своим счетом?

Для специалистов направления подготовки информационная безопасность крайне важно понимать суть уязвимостей в реальных системах, оперирующих денежными средствами.

Чаще всего, объектом атаки злоумышленников является система ДБО, и в частности, мобильные приложения банка или сайт, предоставляющий услуг онлайн банкинга.

2. Системы дистанционного банковского обслуживания

Дистанционное банковское обслуживание (ДБО) – термин для технологий предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленным образом.

Технологии ДБО можно классифицировать по типам информационных систем, используемых для осуществления банковских операций.

Системы «Клиент-банк» (PC-banking, remote banking) – Это системы, доступ к которым осуществляется через персональный компьютер. Системы «Клиент-Банк» позволяют отправлять платежи в банк и получать выписки по счетам (информацию о движениях средств на счёте) из банка. Банк при этом предоставляет клиенту: техническую и методическую поддержку при установке системы, начальное обучение персонала клиента, обновление программного обеспечения и сопровождение в процессе дальнейшей работы.

В целях безопасности в системах «Клиент-Банк» используются различные системы криптографической защиты информации (СКЗИ), обеспечивающие шифрование и контроль целостности передаваемой в Банк информации. Системы «Клиент-Банк» принципиально подразделяются на 2 типа: толстый клиент и тонкий клиент.

Банк-клиент – или «толстый клиент» – на рабочей станции пользователя устанавливается отдельная программа-клиент. Программа-клиент хранит на компьютере все свои данные, как правило, это платёжные документы и выписки по счетам. Программа-клиент может соединяться с банком по различным каналам связи.

Интернет-клиент. Пользователь входит в систему через Интернет браузер. Система Интернет-Клиент размещается на веб-сервере банка. Все данные пользователя доступны на веб-сайте банка. По технологии Интернет-Клиент строятся также системы для мобильных устройств (mobile-banking). На основе Интернет-Клиента могут предоставляться информационные сервисы с ограниченным набором функций.

У дистанционного банковского обслуживания через Интернет есть ряд как преимуществ, так и недостатков. К преимуществам для организаций, предоставляющих такие услуги, можно отнести:

- невысокую стоимость эксплуатации интернет-системы;
- возможность интеграции с бухгалтерскими системами клиента;
- доступность интернет-услуг для конечного пользователя;
- поддержание лояльности клиентов, активно использующих данные услуги.

К недостаткам относится, в первую очередь, слабая защищённость интернет решений от несанкционированного доступа.

Поддержание уровня защиты на надлежащем уровне требует значительных материальных затрат, которые могут себе позволить, в основном, крупные банки, рассчитывающие на значительные доходы от предоставления подобных услуг.

Обслуживание с использованием банкоматов (ATM-banking) и устройств банковского самообслуживания. Технологии ДБО с использованием устройств банковского самообслуживания являются одними из наиболее популярных как в мире, так и в России.

Банкоматы и терминалы попадают в категорию ДБО, так как почти полностью предоставляют банковские услуги дистанционно, без посещения клиентом банковской организации. Кроме того, важным фактором для включения их в эту категорию является возможность дублирования основных функций стандартного банк-клиента, который банк предоставляет частным лицам для осуществления платежей.

3. Уязвимости систем ДБО

В основе данного анализа лежит отчет российской компании Positive Technologies, в котором приводилась статистика уязвимостей систем дистанционного банковского обслуживания за 2011 и 2012 годы, собранная специалистами этой компании в ходе проведения работ для ряда крупных российских банков.

По статистике, 55% рассмотренных систем ДБО построены на базе решений, поставляемых известными производителями, остальные же пользуются собственными разработками.

В ходе анализа выявлено большое количество уязвимостей различного уровня риска, при этом высокую степень риска имеют 8% уязвимостей, среднюю – 51%, и больше количество уязвимостей (41%) имеют низкую степенью риска.

Список уязвимостей коррелирует со списком OWASP top 10:

a) слабая парольная политика;
b) BruteForce;
c) утечка уязвимой информации;
d) XSS;
e) RCE;
f) SQLinjection.

Самые распространенные уязвимости имеют средний и низкий уровни риска. Однако сочетание подобных недостатков, а также наличие характерных для отдельной системы критических уязвимостей может привести к серьезным последствиям, в том числе к получению полного контроля над системой.

В ходе проведенного исследования было показано, насколько уязвимы современные системы дистанционного банковского обслуживания.

Реализация процесса безопасной разработки и регулярный контроль защищенности системы ДБО позволят снизить риски несанкционированного доступа к системе и сохранить в целости денежные средства клиентов банка

Степень защищенности систем ДБО выше, чем в среднем у других приложений, с которыми приходится сталкиваться специалистам Positive

Technologies, и критические уязвимости (RCE, SQL Injection) встречаются в них не так часто. Но, несмотря на это, комбинация некритических ошибок безопасности все равно может приводить к тому, что злоумышленник получает возможность обойти антифрод системы и совершать неавторизованные транзакции.

4. Модель системы ДБО

Разрабатываемая модель системы состоит из программной и аппаратной части. Программная часть представляет из себя уязвимое веб-приложение, реализующее функционал системы дистанционного банковского обслуживания, а аппаратная - сетевую инфраструктуру банка: доступ к демилитаризованной зоне, в которой находится уязвимое веб-приложение из внешней сети. Структурная схема стенда представлена на рисунке 1, а функциональное назначение каждого модуля описано в таблице 1.

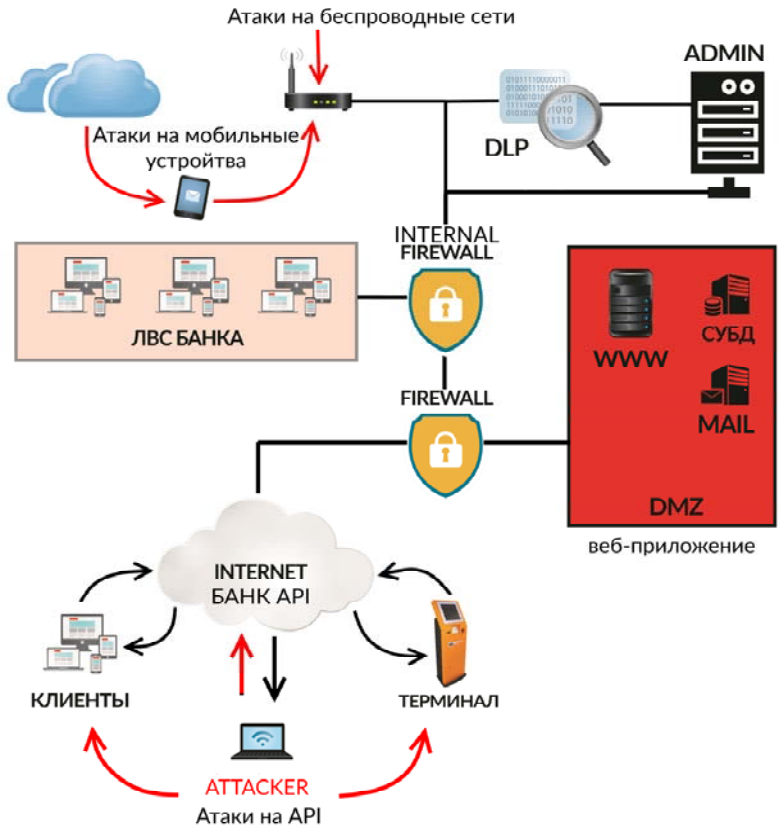

Рис. 1. Обобщенная схема компонентов модели

Таблица 1. Функциональное назначение модулей

Модуль	Функциональное назначение
Клиенты	Система "Клиент-БАНК". Кошёлек - приложение для управление личным, используя сетевые технологии, взаимодействую с сервером Банка, предоставляющим API. Реализована в виде: Web приложения для браузеров, Android, iOS, Windows Phone приложения для КПК. Приложения для ОС Windows, Linux, MacOS.
Банк API	Система ДБО.Web сервер, предоставляющий API. Реализует функции управления счетом, хранения данных о пользователях и операциях со счетами. Сервер БД.
Терминал	Банковский терминал самообслуживания. Выполняет функции приема платежей за услуги мобильной связи, перевод со счета на счет, оплата гос. услуг, пополнение счета и т.д.
FIREWALL	Межсетевой экран. Осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов из внешней сети в демилитаризованную зону в соответствии с правилами, заданными политикой безопасности.
INTERNAL FIREWALL	Внутренний межсетевой экран. Осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов во внутреннюю сеть банка в соответствии с правилами, заданными политикой безопасности.
DMZ (веб-приложение)	Демилитаризованная зона. Сегмент сети между пограничным и внутренним межсетевыми экранами. В этом сегменте находится веб сервер с уязвимым приложением банка, сервер базы данных и почтовый сервер.
DLP	Система предотвращения утечек информации
ADMIN	Администратор сети
ЛВС БАНКА	Внутренняя сеть банка
ATACKER	Атакующая сторона

5. Внедрение в образовательный процесс

Предлагаемый программно-аппаратный комплекс позволяет имитировать функционирование типовой системы ДБО. Данный комплекс является базой для проведения лабораторно-практических работ по курсам «Безопасность сетей ЭВМ», «Технологии обнаружения атак» и аналогичных курсах, в которых изучаются технологии и методы анализа защищённости автоматизированных систем управления от угроз информационной безопасности.

Создается заранее уязвимая система с типовым набором уязвимостей ДБО, которые предстоит найти студентам. Задачей студентов является поиск, эксплуатация уязвимостей системы и выработка контрмер. Целями являются мобильные приложения Интернет-клиентов банка, терминал обслуживания, коммуникационные каналы и имитируемая система ДБО.

Лабораторный комплекс можно использовать для тренировок в формате classic CTF. В таком игровом формате есть две стороны: атакующий и защищающий. Цель атакующей стороны – обнаружить уязвимости в системе и провести атаку, целью защищающей стороны является обнаружение уязвимостей и выполнение мер по их устранению.

Результатами работы с программно-аппаратным комплексом будет являться овладение навыками классификации и формализации уязвимостей, исследования защищённости банковских систем и автоматизированных систем управления.

Заключение

В работе описана модель программно-аппаратного комплекса для эмуляции уязвимостей система ДБО, а также рассмотрена возможность создания лабораторного стенда и последующее внедрение его в процесс обучения специалистов по направлению подготовки «Информационная безопасность».

Подобный лабораторный практикум позволит студентом получать знания о модели злоумышленника, техниках атак и механизмах защиты систем ДБО.

Практикум будет состоять из двух этапов – атака и защита, что в целом напоминает формат игры CTF.

Результатом данной работы стала модель системы, эмулирующая уязвимости программного обеспечения системы ДБО. Следующим этапом этой работы будет разработка программно-аппаратного комплекса, описанного в этой модели.

Литература

[1] Positive Technologies «Статистика уязвимостей систем дистанционного банковского обслуживания». URL: http://www.ptsecurity.ru/download/Analitika_ DBO.pdf (дата обращения: 08.05.2015).

[2] OWASP Top Ten Project «Популярные уязвимости веб-приложений». URL: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (дата обращения: 08.05.2015).

[3] iBank «Уязвимое банковское веб-приложение от PT». URL: http://blog.phdays.com/2012/05/once-again-about-remote-banking.html (дата обращения: 08.05.2015).

[4] Capture the flag «Формат соревнований по информационной безопасности». URL: https://en.wikipedia.org/wiki/Capture_the_flag (дата обращения: 08.05.2015).

[5] «Дистанционное банковское обслуживание». URL: https://ru.wikipedia.org/wiki/Дистанционное_банковское_обслуживание (дата обращения: 08.05.2015).

Model Emulate Vulnerability E-Banking Systems

Kobilev M.A., Abramov E.S., Polovko I.Yu.
Southern Federal University
kobilev@sfedu.ru, abramoves@sfedu.ru, iypolovko@sfedu.ru

The CTF format (capture the flag) of the competition is presented as the approach to the laboratory works. In the frames of such laboratory works students acquire knowledge not only about the techniques used by malicious users to attack on the remote banking services application, but also learn about the mechanisms of protection needed to detect and prevent attacks.

The relevance of this topic is based on the report of the major consulting firms conducting an audit of remote banking services. Based on these reports, we can say that the market demands for security specialists.

The relevance of this topic is based on the report of the major consulting firms conducting an audit of remote banking services. Based on these reports, we can talk about the demand of security specialists.

The article analyzed the feasibility of the project and its further implementation in the education process.

Keywords: remote banking, electronic money, vulnerability RBS, internet banking, mobile banking