Александр Б. Саттаров, Наталья Г. Милославская
Национальной исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: zdarovyak-007@yandex.ru, http://orcid.org/0000-0001-8993-4317
e-mail: ngmiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805

УЧЕБНО-ЛАБОРАТОРНЫЙ КОМПЛЕКС ПО ИЗУЧЕНИЮ АТАК ТИПА «ЧЕЛОВЕК ПОСЕРЕДИНЕ» И СПОСОБОВ ЗАЩИТЫ ОТ НИХ

DOI: http://dx.doi.org/10.26583/bit.2018.4.06

Аннотация. Для реализации образовательной программы подготовки магистров по направлению 10.04.01 «Информационная безопасность» под названием «Обеспечение непрерывности и информационной безопасности бизнеса» в НИЯУ МИФИ разработана программная оболочка учебно-лабораторного комплекса (УЛК), предназначенная для изучения сетевых атак типа «Человек посередине». В УЛК смоделированы четыре основные атаки данного типа: UDP Hijacking, Session Hijacking, TCP Hijacking и Bucket brigade attack. В статье представлены два приложения УЛК: приложение преподавателя и приложение студента. Для оценки знаний студентов после выполнения лабораторной работы создан модуль оценки знаний «Тестирование», который включает в себя вопросы для проведения тестирования с помощью программной оболочки УЛК. Составлены методические указания по выполнению лабораторной работы. В рамках дисциплины «Защищенные информационные системы» кафедры «Информационная безопасность банковских систем» НИЯУ МИФИ, реализующих выше указанную программу подготовки магистров, проведена успешная апробация разработанного УЛК. В заключении статьи указаны пути дальнейшего совершенствования УЛК.
Ключевые слова: учебно-лабораторный комплекс, атака типа «Человек посередине», UDP Hijacking, Session Hijacking, TCP Hijacking, Bucket brigade attack.
Для цитирования: САТТАРОВ, Александр Б.; МИЛОСЛАВСКАЯ, Наталья Г. УЧЕБНО-ЛАБОРАТОРНЫЙ КОМПЛЕКС ПО ИЗУЧЕНИЮ АТАК ТИПА «ЧЕЛОВЕК ПОСЕРЕДИНЕ» И СПОСОБОВ ЗАЩИТЫ ОТ НИХ. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 63-74, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1162>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.06.

Alexander B. Sattarov, Natalia G. Miloslavskaya
National Research Nuclear University "MEPhI",
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: zdarovyak-007@yandex.ru, http://orcid.org/0000-0001-8993-4317
e-mail: ngmiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805

Educational and Laboratory System for Studying Man-in-the-Middle Attacks and Ways to Protect against Them

DOI: http://dx.doi.org/10.26583/bit.2018.4.06

Abstract. For the implementation of the Master's program "Business Continuity and Information Security Maintenance" in the field of specialty 10.04.01 "Information Security", a software shell of the educational laboratory complex (ELC) designed to study the "Man in the middle" network attacks has been developed in the NRNU MEPhI. In the framework of the ELC four basic attacks of this type are modeled: UDP Hijacking, Session Hijacking, TCP Hijacking and Bucket brigade attack. The paper presents two ELC applications: the instructor's application and the student's application. To assess the students' knowledge after performing laboratory work, the "Testing" module for assessing progress testing has been created, which includes questions for testing using the ELC software shell. Methodical instructions on performance of laboratory work have been written. Within the framework of the "Protected Information Systems" discipline of the Information Security of Banking Systems Department of the NNIU MEPhI, implementing the above-mentioned Mastre's program, a successful approbation of the developed ELC has been carried out. In conclusion the ways to further improvement of the ELC are suggested.
Keywords: Educational and Laboratory System, Man-in-the-middle attack, MITM, UDP Hijacking, Session Hijacking, TCP Hijacking, Bucket brigade attack.

For citation: SATTAROV, Alexander B.; MILOSLAVSKAYA, Natalia G. Educational and Laboratory System for Studying Man-in-the-Middle Attacks and Ways to Protect against Them. IT Security (Russia), [S.l.], v. 25, n. 4, p. 63-74, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1162>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.06.

Введение

Современный мир предъявляет к грамотному специалисту повышенные требования, которые не существовали в старых образовательных программах. Эти требования отличает большая универсальность, и согласно компетентностному подходу, впервые зародившемуся в начале 80-х годов XX века, они называются базовыми профессиональными компетенциями, включающими знания, умения и навыки. Компетентностный подход, реализуемый в современных российских образовательных стандартах, предполагает создание фондов оценочных средств, предназначенных для объективного контроля появления, развития и совершенствования заданного набора компетенций у выпускников вузов. При этом оценивание сформированности каждой компетенции как способности успешно применять знания, умения, навыки при решении задач профессиональной деятельности является важной задачей. Нередко для решения подобных задач в учебном процессе применяются электронные информационно-образовательные системы и среды, которые позволяют организовать и проводить мониторинг, контроль и управление процессом обучения.

В рамках образовательной программы «Обеспечение непрерывности и информационной безопасности бизнеса» подготовки магистров по направлению 10.04.01 «Информационная безопасность» кафедра «Информационная безопасность банковских систем» НИЯУ МИФИ реализует дисциплину «Защищенные информационные системы». Эта дисциплина формирует следующие общекультурные (ОК), общепрофессиональные (ОПК) и профессиональные компетенции (ПК) выпускников [1]:

- «способность к саморазвитию, самореализации, использованию творческого потенциала» (ОК-2);
- «способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой профессиональной деятельности» (ОК-3);
- «способность к самостоятельному обучению и применению новых методов исследования» (ОПК-2);
- «способность понимать и анализировать направления развития информационно-коммуникационных технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты в соответствии со стратегией развития информационных систем» (ПК-1);
- «способность проектировать и разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности» (ПК-2);
- «способность проводить обоснование выбора принципов организации и функциональной структуры программного, программно-аппаратного и технического обеспечения систем и средств обеспечения информационной безопасности объектов защиты на основе отечественных и международных стандартов» (ПК-3);
- «способность разрабатывать программы и методики испытаний программных, программно-аппаратных и технических средств и систем обеспечения информационной безопасности» (ПК-4);
- «способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента» (ПК-7);

- «способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи» (ПК-8);
- «способность организовать выполнение работ по созданию, монтажу, наладке, испытанию и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности» (ПК-15).

Для формирования компетенций ОК-3, ОПК-2 и ПК-1 разработан учебно-лабораторный комплекс (УЛК) по моделированию атак типа «Человек посередине» (англ. Man-in-the-Middle), который состоит из программной оболочки (включает приложение преподавателя и приложение студента), самих лабораторных модулей, модуля оценки знаний и методических указаний по выполнению лабораторных работ. В результате успешного прохождения лабораторных работ, реализованных в качестве модулей УЛК, студенты будут:

знать:

- основные методы и средства реализации атак типа «Человек посередине»;
- протоколы передачи данных TCP и UDP;

уметь:

- определять наличие уязвимостей информационных систем (ИС), подверженных атакам типа «Человек посередине»;

владеть:

- навыками распознавания атак типа «Человек посередине» на ИС для выбора адекватной защиты от них.

Суть атак типа «Человек посередине» широко освещена в англоязычных источниках, однако в русскоязычных практически не встречается. Проведение интерактивных лабораторных работ по данной теме возможно двумя способами: изучая реальные атаки в изолированной среде – песочнице (примеры учебных заведений, выбравших этот способ – Университет Тренто [https://securitylab.disi.unitn.it/lib/exe/fetch.php?media=teaching:netsec:2016:network_security_lab_report_-_group_1.pdf], Мичиганский технологический университет [http://pages.mtu.edu/~xinlwang/itseed/labs/Spoof_MiTM.pdf], Исламский университет Газы [http://site.iugaza.edu.ps/nour/files/lab4-MITM1.pdf], Университет Петры [http://lms.uop.edu.jo/lms/pluginfile.php/401/mod_resource/content/0/Lab-MITM.pdf] и другие университеты) или полностью эмулируя их. Мы выбрали второй путь. Ни одного описания аналогичных лабораторных работ для данной атаки в открытой печати не найдено.

Целью данной статьи является описание разработанного УЛК по изучению атак типа «Человек посередине» и опыта его использования в рамках учебного процесса НИЯУ МИФИ.

Общие сведения об атаке «Человек посередине»

Атака типа «Человек посередине» впервые была применена еще задолго до появления современных компьютеров в 1586 г. в заговоре Боббингтона, в котором шифровки передавались на бумаге, а также позднее – во время Второй мировой войны, для чего использовался радиопередатчик «Aspidistra». При данной атаке возникает ситуация, в которой атакующий способен читать и изменять сообщения, передающиеся между атакуемыми [2, 3]. Такой метод компрометации канала позволяет злоумышленнику незаметно для атакуемых осуществлять активное вмешательство в протокол передачи данных, удаляя, искажая, навязывая ложную информацию или создавая сообщения от имени атакуемых. Очевидно, что такое вмешательство в канал связи открывает широкие возможности для атакующего и позволяет влиять на ситуацию, оставаясь незамеченным.

Первое упоминание атаки в сфере информационной безопасности (ИБ) появилось в 1981 г. в труде «Password authentication with insecure communication» автора Лесли Лампорта (Leslie Lamport) [4]. С тех пор сетевые технологии значительно шагнули вперед, а атака приобрела более отчетливые черты и стала использоваться во множестве случаев. Атака активно применяется до сих пор и будет применяться до тех пор, пока компьютеры

будут передавать информацию между собой незащищенным образом. Поэтому этой теме посвящено много работ современных исследователей: уязвимости анализируются, например, в [5], новые разновидности, особенно связанные с беспроводным доступом и протоколом IPv6, - в [6 - 8]. Вопросам защиты от этих атак посвящены, например, работы [9, 10].

В настоящее время известны четыре основные реализации названной атаки.

1. Bucket brigade attack – это разновидность атаки «Человек посередине», в которой атакующий перехватывает сообщения атакуемых при обмене ключами, используемыми для создания защищенного канала. Атакующий встает посередине между ними при обмене сообщениями (рис. 1). Свое название разновидность атаки получила из-за сходства с пожарными бригадами во время тушения пожара – они передавали ведро с водой от человека к человеку, чтобы доставить его до конца цепочки из людей и обратно. В сетевой атаке цепочка состоит из трех участников, где посередине находится атакующий, а по краям – атакуемые [11].

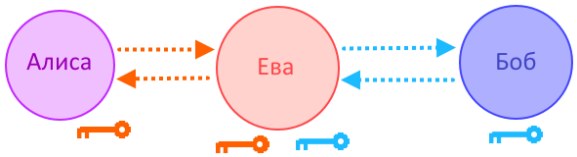


Рис. 1. Bucket brigade attack
(Fig. 1. Bucket brigade attack)

2. Session Hijacking (перехват сессии). В эпоху цифровых технологий люди активно используют поисковые системы, социальные сети и другие возможности Интернета. Но часто доступ к некоторой информации требуется разрешить только определенному кругу лиц. Многие сайты предоставляют возможность оставлять комментарии к новостям и общаться с другими пользователями. Для того чтобы наделить пользователя правом представляться тем, за кого он себя выдает, интернет-ресурсы ввели систему аутентификации: требуется ввести имя и пароль пользователя. Но время показало, что это удобно и необременительно не для всех пользователей. Сохранять же аутентификационные данные в браузере – небезопасно, поскольку при получении физического доступа к компьютеру они попадают в руки злоумышленника. Так появились сессии пользователя: при успешном прохождении процедуры аутентификации браузер пользователя сохраняет не введенные пользователем данные, а уникальную строку (характеризующую текущую сессию пользователя), которую ему сообщает посещаемый сайт. В будущем при каждом обращении к сайту браузер сообщает сайту ранее сохраненную сессионную строку, что подтверждает подлинность пользователя. Строка является уникальной для каждой сессии и исчезает необходимость сохранять пароль в браузере – требуется ввести его единожды при входе на сайт. Но и это открывает возможность без знания аутентификационных данных получить авторизованный доступ к интернет-ресурсу, если каким-либо образом узнать уникальную сессионную строку. Именно поэтому данная разновидность атаки и получила название Session Hijacking.

Если в момент запроса к сайту атакующий перехватит сессию, которую браузер атакуемого автоматически добавляет в запрос к сайту, то он сможет подставить ее в свой браузер. В таком случае атакующий без знания аутентификационных данных получает авторизованный доступ к сайту от лица атакуемого [12], что проиллюстрировано на рис. 2.

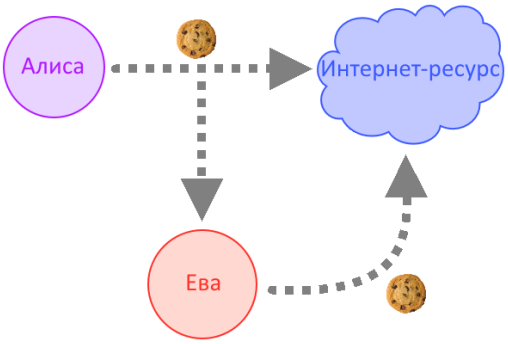
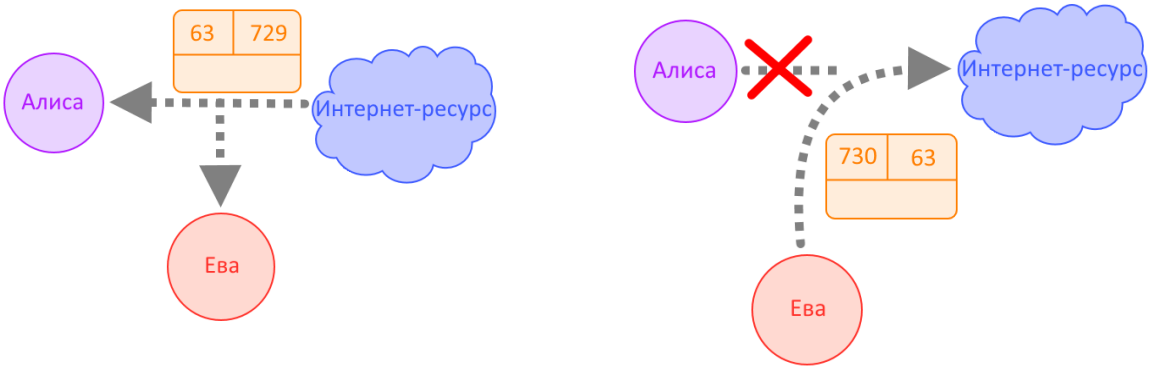


Рис. 2. Session Hijacking
(Fig. 2. Session Hijacking)

3. TCP Hijacking. С развитием технологий и появлением новых протоколов передачи данных существует вероятность возникновения и новых возможностей для проведения атак. Так произошло и с протоколом транспортного уровня TCP [13], который используется для гарантированной доставки информации от одного узла сети к другому. Известно, что для контроля обмена пакетами при TCP-соединении в пакетах предусмотрено два поля (Sequence number и Acknowledge number) по 32 бита каждое. Эти два поля являются единственными идентификаторами, с помощью которых сервер различает TCP-соединения и TCP-абонентов. С их помощью при обмене пакетами клиент с сервером ведут учет пакетов. Если атакующий сможет узнать эти поля, то у него появится возможность составить ложный TCP-пакет, который будет обработан сервером или клиентом [14]. Более того, будет возможно и дальше продолжать обмен ложными TCP-пакетами. Однако следует обратить внимание на очевидную закономерность при внедрении ложного TCP-пакета – получатель пакета при ответе будет использовать Acknowledge number, отличный от того, что ожидает его TCP-собеседник. Произойдет десинхронизация, и соединение между сервером и клиентом в рамках текущей TCP-сессии будет невозможно, но оно останется открытым для атакующего. И эта проблема решаема, если атакующий полностью контролирует все пакеты между клиентом и сервером – он может самостоятельно изменять значения идентификационных полей на корректные и пропускать модифицированный пакет дальше.

Для проведения рассматриваемой атаки злоумышленнику требуется узнать Sequence number. После он должен составить ложный пакет, который в поле Acknowledge number будет содержать Sequence number, увеличенное на единицу. В таком случае отправленный пакет будет корректно обработан (рис. 3).



А) Б)

Рис. 3. TCP Hijacking: А) перехват TCP-пакета; Б) захват соединения атакующим
(Fig. 3. TCP Hijacking: A) TCP packet interception; Б) connection capturing by attacker)

4. UDP Hijacking. Многие приложения (например, при передаче голоса или в играх реального времени с несколькими игроками по сети) используют протокол UDP из-за его

легковесности. Потеря пакетов при доставке их клиенту или на сервер в таких случаях не существенна, ведь следом за ним придет пакет с актуальной информацией, а потерянный пакет уже будет не нужен. Это и является отличным условием для передачи атакующим атакуемому своего собственного ложного пакета. При этом пакет, который придет от сервера, уже будет не нужен – он считается устаревшим. На этом и основана атака UDP Hijacking (рис. 4). Атакующий, просматривая информацию, которой обмениваются атакуемый и сервер, ждет, когда атакуемый запросит у сервера некоторые данные по протоколу UDP. Если в этот момент отправить атакуемому ложный пакет в ответ на его запрос до того, как он получит ответ от сервера, то он его примет как действительный ответ на свой запрос [15]. С помощью этого можно скомпрометировать поведение атакуемого.

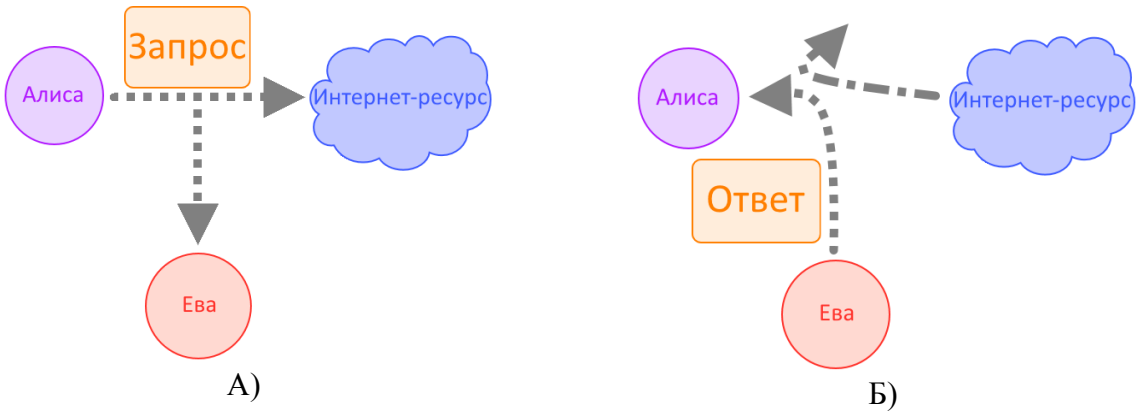


Рис. 4. UDP Hijacking: А) перехват запроса; Б) отправка ответа атакующим
(Fig. 4. UDP Hijacking: A) request interception; Б) sending of response by attacker)

Программная оболочка учебно-лабораторного комплекса

На основе рассмотренных выше видов атак составлены требования к УЛК, а также детально описаны его особенности. Описание было формализовано в виде технического задания. Для возможности расширения набора лабораторных модулей архитектура УЛК спроектирована таким образом, чтобы при написании кода сторонние разработчики могли использовать наработки УЛК с максимальным удобством и минимальными временными затратами.

В составе УЛК разработана программная оболочка, состоящая из двух приложений – преподавателя и студента.

Графический интерфейс приложения студента представлен на рис. 5 – 7. Это аутентификация студента, выбор им лабораторной работы и ее выполнение соответственно.

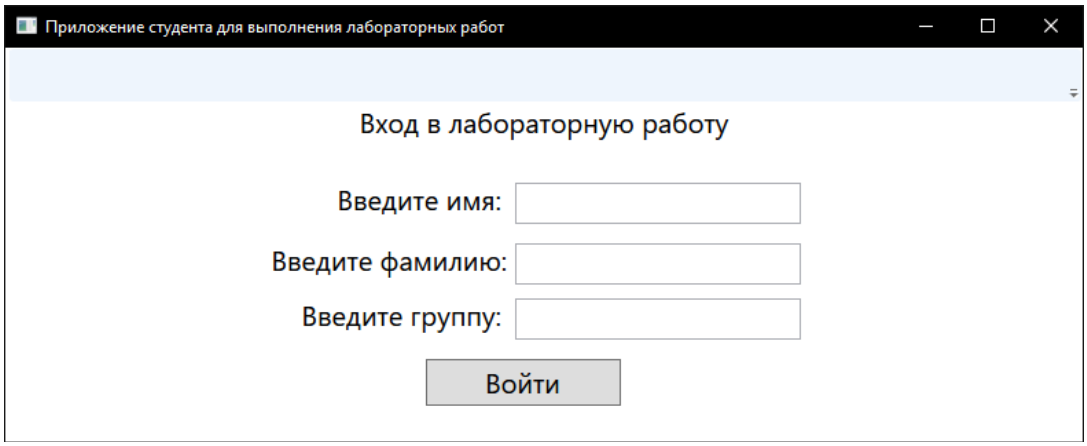


Рис. 5. Экран приложения студента для входа в лабораторную работу
(Fig. 5. The student application screen for entering the laboratory work)

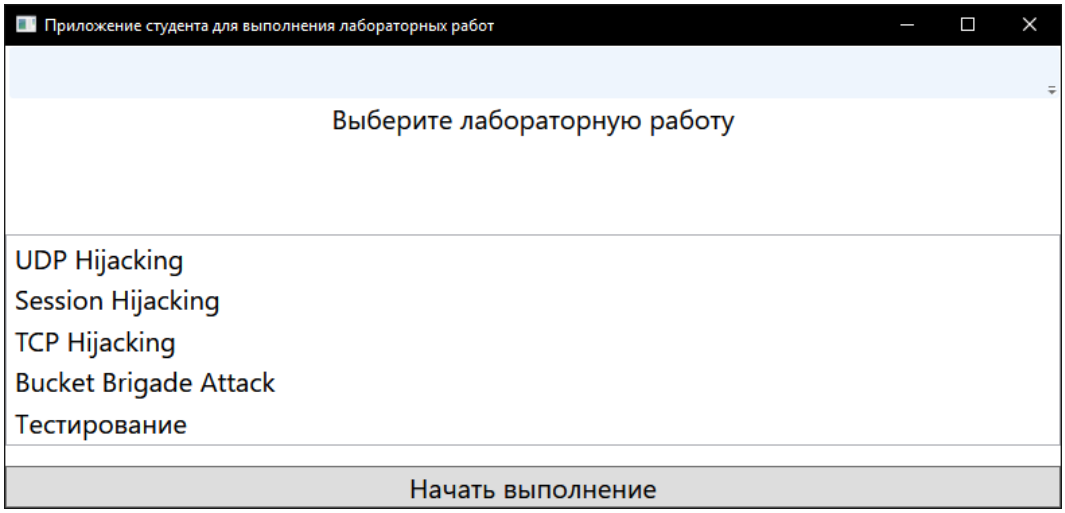


Рис. 6. Экран выбора лабораторной работы
(Fig. 6. Screen for selecting laboratory work)

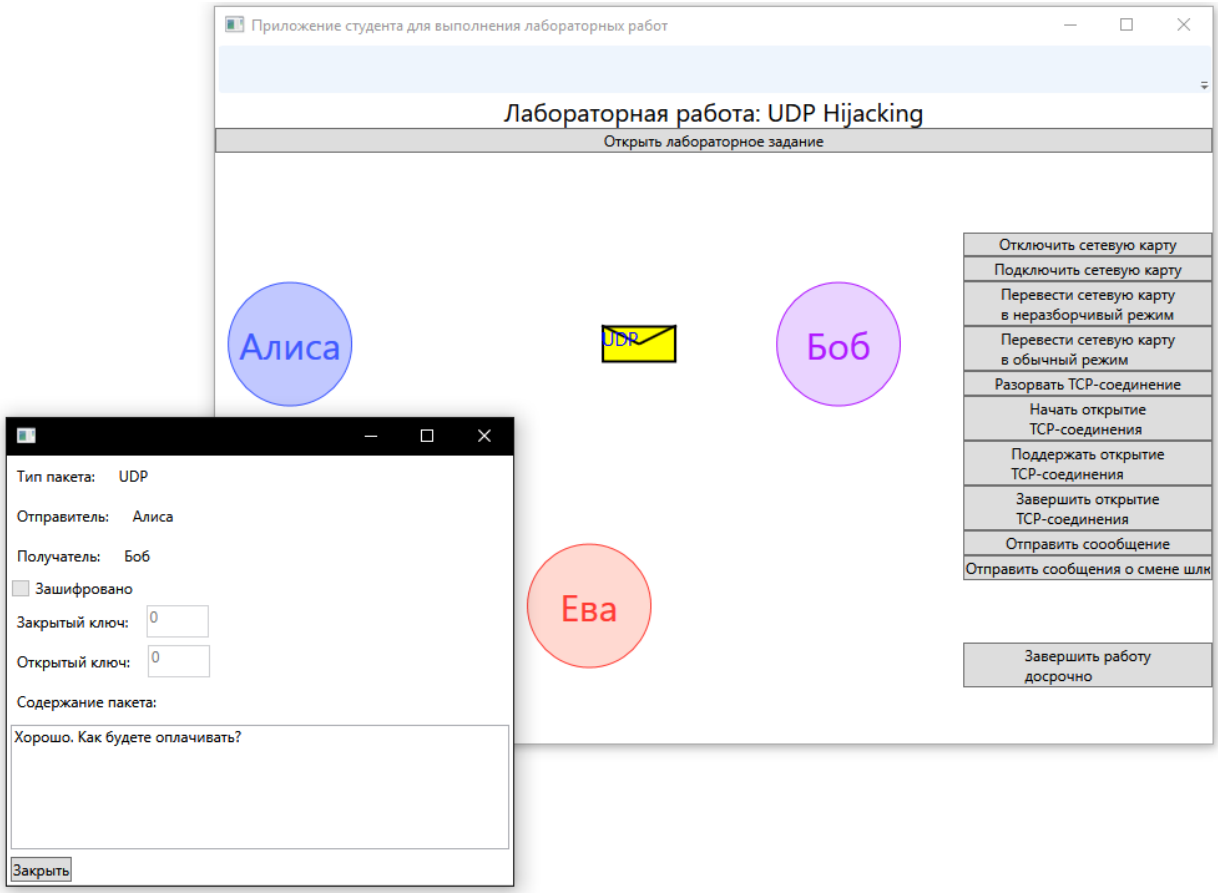


Рис. 7. Экран выполнения лабораторной работы
(Fig. 7. The screen of laboratory work implementation)

Если студент случайно закрывает свое приложение, то ему следует ввести те же самые идентификационные данные, так как встроенная система их контроля не позволит перейти к этапу выбора лабораторной работы, если они не совпадут с введенными в первый раз. Это сделано для предупреждения аутентификации студентов под чужими именами для «пробных» попыток прохождения лабораторных работ.

По завершении лабораторной работы в дополнительном окне отображается результат ее выполнения, выраженный целым числом по пятибалльной шкале.

Графический интерфейс приложения преподавателя отображает аутентифицировавшихся студентов (фамилию, имя, группу) и элементы управления для допуска к лабораторным работам, просмотра результатов их выполнения, а также сохранения в виде «*.CSV»-файла статистики выполнения четырех модулей лабораторной работы по каждому студенту в отдельности или статистики по всем студентам и всем модулям (рис. 8).

Если студент закроет свое приложение, то строка с его идентификационными данными станет серой, а при повторной аутентификации – снова зеленой.

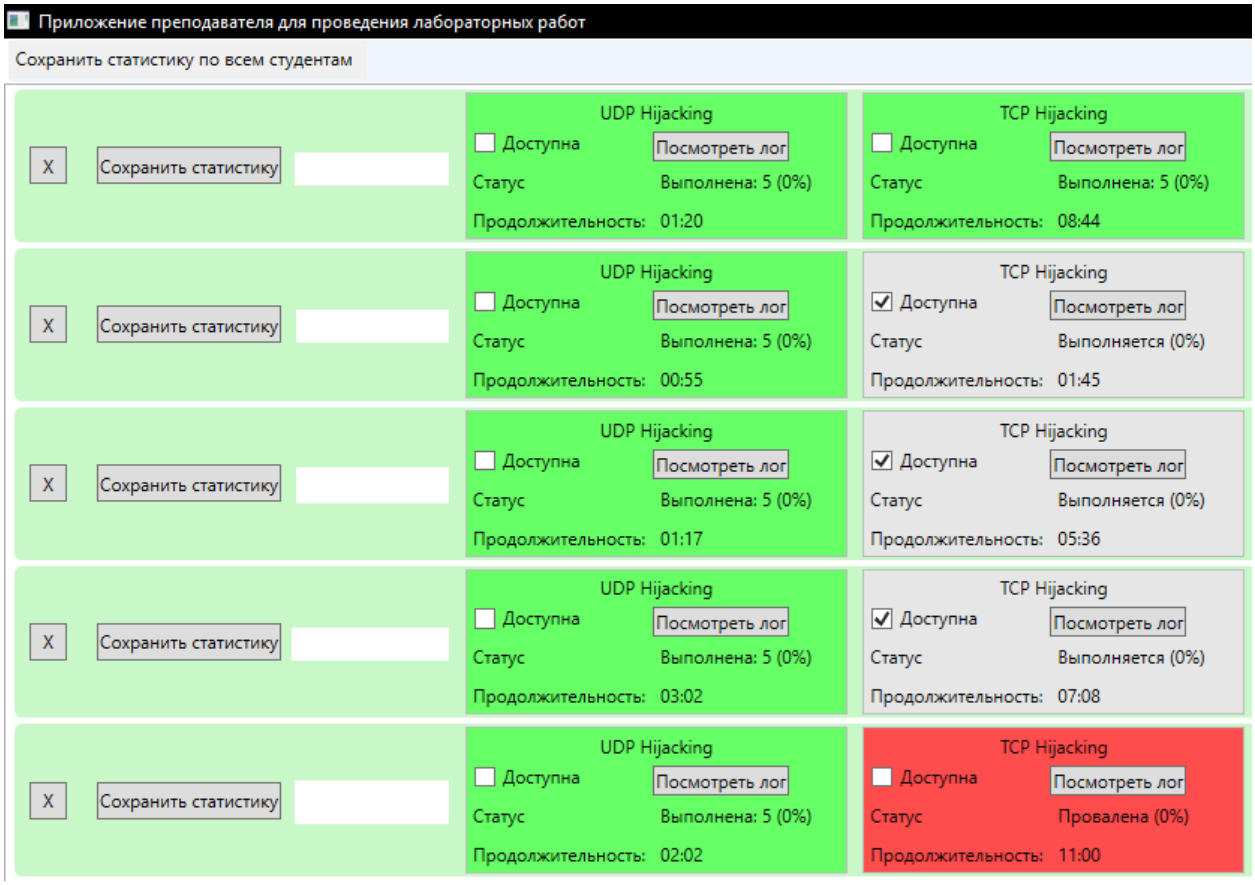


Рис. 8. Графический интерфейс приложения преподавателя
(Fig. 8. The graphical interface of the instructor's application)

В каждом блоке, соответствующем четырем модулям лабораторной работы, доступен элемент типа «CheckBox» с текстом «Доступна». При установке его в состояние «выбран» модуль лабораторной работы по сети передается в приложение соответствующего студента, а при установке в состояние «недоступна» – отзывается из приложения соответствующего студента. Таким образом, студент не сможет при получении несанкционированного доступа к лабораторным компьютерам (так называемым автоматизированным рабочим местам (АРМ) студента) получить модули для подготовки дома или заменить их на скомпрометированные. Также для предотвращения перехвата модулей по сети приложения преподавателя и студента используют протокол TCP с TLS 1.2 (Transport Layer Security). TLS-сертификат должен располагаться в папке «Certificate», а модули лабораторных работ в папке «Labs». Папки «Certificate» и «Labs» расположены в директории, в которую установлено приложение преподавателя.

Также в программной оболочке присутствует подсистема журналирования. Журналы индивидуальны для каждого модуля у каждого студента и позволяют вести журналирование при помощи метода Log (string message) объекта radio, которые передаются в конструктор лабораторного модуля при создании. Для просмотра журналов предназначена кнопка «Посмотреть лог» в блоке модуля, после нажатия на которую

содержимое журнала появится в отдельном окне. Также сами блоки окрашиваются в салатовый цвет, если студент успешно завершил выполнение модуля, в светло-красный, если завершил, но не успешно, и в светло-голубой на сером фоне, если студент находится в процессе выполнения лабораторной работы. В последнем случае в блоке присутствует секундомер, показывающий длительность выполнения студентом лабораторной работы. По завершении выполнения лабораторной работы в соответствующем блоке будет отображен результат выполнения: «Выполнена» с оценкой выполнения по пятибалльной шкале, если она успешно завершена, и «Провалена», если нет.

Представленная программная оболочка разработана на языке программирования C# с использованием платформы «.NET Framework», так как она является предустановленной на компьютерах с ОС «Windows» версий 7, 8.1 и 10, которые используются на компьютерах лаборатории кафедры. Разработка велась с использованием графической подсистемы Windows Presentation Foundation (WFP), входящей в состав «.NET Framework», что в случае необходимости расширения ее функционала позволяет гибко модифицировать исходный код программной оболочки. Также WPF позволяет использовать для этого не только элементы WFP, но и интегрировать распространенные до сих пор «Windows Forms» элементы, если разработчик не будет владеть WPF в достаточной мере.

Суммарное количество строк кода УЛК составляет порядка 11 тыс.

Шаблон «LabTemplate» и модули лабораторной работы

На платформе «.NET Framework» версии 4.0 был разработан шаблон «LabTemplate» в виде динамической библиотеки, содержащей одноименный класс в пространстве имен «LabTemplateNamespace», который необходимо использовать для реализации модуля лабораторной работы и переопределить методы, создающие графические элементы с заданием лабораторной работы и самой лабораторной работой.

Результатом компиляции модуля лабораторной работы является динамическая библиотека, исходный код которой также написан с использованием платформы «.NET Framework» версии 4.0.

Для переопределения доступны следующие методы:

- getUIControl: графический элемент, предназначенный для взаимодействия с пользователем, он будет отображен в центре приложения студента для выполнения лабораторных работ;
- getName: наименование лабораторной работы, которое будет отображено в заголовке лабораторной работы;
- getMission: графический элемент, предназначенный для отображения в отдельном окне лабораторного задания.

На языке программирования C# были разработаны пять модулей лабораторной работы, представляющие собой динамические библиотеки: модули «UDP Hijacking», «Session Hijacking», «TCP Hijacking» и «Bucket brigade attack» и модуль «Тестирование».

Апробация разработанного УЛК в учебном процессе НИЯУ МИФИ

Вышеописанный УЛК был установлен в двух учебно-лабораторных кабинетах на лабораторных компьютерах кафедры «Информационная безопасность банковских систем» НИЯУ МИФИ. Его апробация происходила на 63 магистрантах трех групп первого года обучения в рамках дисциплины «Защищенные информационные системы».

Для подготовки студентов к лабораторным работам были составлены методические указания, включающие в себя как информацию о самих лабораторных работах, так и теоретическую справочную информацию в виде описания протоколов TCP и UDP, трехэтапного установления соединения по протоколу TCP, протокола Диффи-Хеллмана, шифра Цезаря, режимов работы сетевой карты и информации об ARP-таблице. Также в методических указаниях приведены способы защиты от моделируемых студентами атак типа «Человек посередине».

Условия выполнения лабораторных работ были следующие: количество попыток и время прохождения модулей не ограничены, допуск к модулям происходит последовательно – доступ к следующему модулю открывается при прохождении предыдущего, модули выполняются в следующей последовательности: «UDP Hijacking»; «Session Hijacking»; «TCP Hijacking»; «Bucket brigade attack»; «Тестирование».

Модуль «Тестирование» содержит список вопросов, из которых выбираются случайные 20. Каждый вопрос представлен в виде текста и нескольких вариантов ответа, среди которых можно выбрать один и более.

В табл. 1 указано среднее время прохождения каждого модуля и среднее количество попыток, совершенное студентами для его прохождения. Собрана следующая статистика: в среднем на прохождение модуля «UDP Hijacking» требуется 3 попытки по 4.1 мин каждая, модуля «Session Hijacking» – 2 попытки по 3.8 мин каждая, модуля «TCP Hijacking» – 3 попытки по 8.9 мин каждая, модуля «Bucket brigade attack» – 3 попытки по 21.4 мин каждая, модуля «Тестирование» – 1 попытка длительностью 17.1 мин.

Таблица 1. Средние показатели прохождения каждого модуля УЛК

	UDP Hijacking	Session Hijacking	TCP Hijacking	Bucket Brigade Attack	Тестирование
Среднее время прохождения модуля, мин	4.1	3.8	8.9	21.4	17.1
Среднее количество попыток прохождения модуля	3	2	3	3	1

Согласно этим данным, в среднем на проведение лабораторной работы требуется 127.9 минуты (чуть меньше трех академических часов). Однако показатель – средний, а значит будут присутствовать студенты, выполняющие лабораторную работу несколько дольше.

На рис. 8 представлен скриншот с графическим интерфейсом приложения преподавателя во время проведения лабораторной работы у одной из групп (идентификационные данные студентов искажены умышленно). Он показывает, что первый студент успешно выполнил три лабораторные работы, последний студент успешно выполнил первые две работы, но не смог выполнить третью, а остальные студенты успешно выполнили первые две работы и находятся в процессе выполнения третьей.

Заключение

Использование информационных технологий в сфере образования значительно ускоряет процесс передачи знаний за счет их более наглядного и динамического представления. Однако эта сфера настолько обширна, что создать для каждой учебной дисциплины поддержку в виде преобразования знаний в цифровой формат до сих пор является проблемой. Целью данной работы было оптимизировать процесс проведения лабораторных работ с помощью разработанного УЛК. В рамках представленной работы разработан и апробирован УЛК, состоящий из шаблона «LabTemplate» модуля лабораторной работы, программной оболочки (приложение преподавателя и приложение студента для проведения лабораторных работ), четырех модулей лабораторных работ («UDP Hijacking», «Session Hijacking», «TCP Hijacking», «Bucket brigade attack»), модуля оценки знаний «Тестирование» и методических указаний к лабораторной работе.

Апробация разработанного УЛК прошла успешно, что показало его работоспособность и соответствие поставленным целям, а также позволило собрать статистику прохождения студентами отдельных лабораторных модулей. В среднем студенту требуется 127.9 минут для того, чтобы пройти четыре модуля УЛК и протестировать полученные теоретические знания и практические навыки.

В текущей работе смоделированы вышеописанные атаки, однако в рамках работы отсутствуют реализации наглядных демонстраций способов защиты от них. Таким

образом, продолжение работы будет заключаться в расширении списка лабораторных работ, в которых будет реализовано моделирование способов защиты от вышеописанных атак.

СПИСОК ЛИТЕРАТУРЫ:

1. Образовательный стандарт высшего образования Национального исследовательского ядерного университета «МИФИ». 10.04.01 «Информационная безопасность». 2017.
2. Лапонина О. Р. Основы сетевой безопасности. Часть 1. Межсетевые экраны: Учебное пособие. 2014. 16 с.
3. Müller L. Man in the Middle Attack. 2010. URL: http://jusit.eu/wp-content/uploads/2011/08/mitm.pdf (дата обращения 03.05.2018)
4. Lamport L. Password authentication with insecure communication. Communications of the ACM. ACM New York, NY, USA. Volume 24 Issue 11, Nov. 1981. Pages 770-772.
5. Kaka S., Sastry, V.N., Maiti, R.R. On the MitM vulnerability in mobile banking applications for android devices. 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2016. DOI: 10.1109/ANTS.2016.7947811.
6. Gelernter N., Kalma S., Magnezi B., Porcilan H. The Password Reset MitM Attack. 2017 IEEE Symposium on Security and Privacy, SP 2017. San Jose; United States. Pages 251-267. DOI: 10.1109/SP.2017.9.
7. Vondráček M., Pluskal J., Ryšavý O. Automation of MitM attack on Wi-Fi networks. Proceedings of the 9th International Conference on Digital Forensics and Cyber Crime, ICDF2C 2017. Prague, Czech Republic. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST. Volume 216, 2018, Pages 207-220. DOI: 10.1007/978-3-319-73697-6_16.
8. Huang Y., Jin L., Wei H., Lou Y., Kang X. Pilot Contamination with MITM Attack. Proceedings of the 5th IEEE Vehicular Technology Conference, VTC Spring 2017. Sydney, Australia. DOI:10.1109/VTCSpring.2017.8108523.
9. Ouseph C., Chandavarkar, B.R. Prevention of MITM attack caused by rogue router advertisements in IPv6. Proceedings of the 2016 IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2016, Pages 952-956. DOI: 10.1109/RTEICT.2016.7807969.
10. Al Abri D. Detection of MITM attack in LAN environment using payload matching. Proceedings of the 2015 IEEE International Conference on Industrial Technology, ICIT 2015. Seville; Spain. Pages 1857-1862. DOI: 10.1109/ICIT.2015.7125367.
11. Bucket Brigade. SearchSecurity. URL: http://searchsecurity.techtarget.com/tip/Bucket-Brigade (дата обращения: 03.05.2018).
12. Study And Analysis On Session Hijacking Computer Science Essay. UK Essays. URL: https://www.ukessays.com/essays/computer-science/study-and-analysis-on-session-hijacking-computer-science-essay.php?utm_expid=309629-38._Nb6m1ixT_aGX1K3CVQTDw.0 (дата обращения: 03.05.2018).
13. RFC 793, Transmission Control Protocol. URL: https://tools.ietf.org/html/rfc793 (дата обращения: 03.05.2018).
14. Wegener C., Dolle W. Hijack Prevention – Understanding and preventing TCP attacks. Linux-Magazine, 09/2005; pages 66-71; ISSN 14715678.
15. Basta A., Basta N., Brown M. Computer Security and Penetration Testing. Cengage Learning. 2013. 400 p.

REFERENCES:

[1] Obrazovatel'nyj standart vysshego obrazovanija National Research Nuclear University «MEPhI». 10.04.01 «Information security». 2017.
[2] Laponina O. R. Fundamentals of network security. Part 1. Mezhsetevye jekrany: Uchebnoe posobie. 2014 (in Russian).
[3] Müller L. Man in the Middle Attack. 2010. Available at: http://jusit.eu/wp-content/uploads/2011/08/mitm.pdf (accessed 15.05.2018)
[4] Lamport L. Password authentication with insecure communication. Communications of the ACM. ACM New York, NY, USA. Volume 24 Issue 11, Nov. 1981. Pages 770 - 772.
[5] Kaka S., Sastry, V.N., Maiti, R.R. On the MitM vulnerability in mobile banking applications for android devices. 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2016. DOI: 10.1109/ANTS.2016.7947811.
[6] Gelernter N., Kalma S., Magnezi B., Porcilan H. The Password Reset MitM Attack. 2017 IEEE Symposium on Security and Privacy, SP 2017. San Jose; United States. Pages 251 - 267. DOI: 10.1109/SP.2017.9.
[7] Vondráček M., Pluskal J., Ryšavý O. Automation of MitM attack on Wi-Fi networks. Proceedings of the 9th International Conference on Digital Forensics and Cyber Crime, ICDF2C 2017. Prague, Czech Republic. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST. Volume 216, 2018, Pages 207 - 220. DOI: 10.1007/978-3-319-73697-6_16.
[8] Huang Y., Jin L., Wei H., Lou Y., Kang X. Pilot Contamination with MITM Attack. Proceedings of the 5th IEEE Vehicular Technology Conference, VTC Spring 2017. Sydney, Australia. DOI:10.1109/VTCSpring.2017.8108523.

[9] Ouseph C., Chandavarkar, B.R. Prevention of MITM attack caused by rogue router advertisements in IPv6. Proceedings of the 2016 IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2016, Pages 952-956. DOI: 10.1109/RTEICT.2016.7807969.
[10] Al Abri D. Detection of MITM attack in LAN environment using payload matching. Proceedings of the 2015 IEEE International Conference on Industrial Technology, ICIT 2015. Seville; Spain. Pages 1857-1862. DOI: 10.1109/ICIT.2015.7125367.
[11] Bucket Brigade. SearchSecurity. No Author Available at: http://searchsecurity.techtarget.com/tip/Bucket-Brigade (accessed: 03.05.2018).
[12] Study And Analysis On Session Hijacking Computer Science Essay. UK Essays. Available at: https://www.ukessays.com/essays/computer-science/study-and-analysis-on-session-hijacking-computer-science-essay.php?utm_expid=309629-38._Nb6m1ixT_aGX1K3CVQTDw.0 (accessed: 03.05.2018).
[13] RFC 793, Transmission Control Protocol. Available at: https://tools.ietf.org/html/rfc793 (accessed: 03.05.2018).
[14] Wegener C., Dolle W. Hijack Prevention – Understanding and preventing TCP attacks. Linux-Magazine, 09/2005; pages 66-71; ISSN 14715678.
[15] Basta A., Basta N., Brown M. Computer Security and Penetration Testing. Cengage Learning. 2013. 400 p.

Поступила в редакцию – 06 мая 2018 г. Окончательный вариант – 01 ноября 2018 г.
Received – May 06, 2018. The final version – November 01, 2018.