УДК 004.056

Н. В. Бритвин[1], специалист, e-mail: britvin.nickita@yandex.ru,
Е. О. Карпухин[1, 2], канд. техн. наук, ст. науч. сотр., e-mail: ret1987@yandex.ru
[1] Федеральное государственное бюджетное учреждение науки
Центр информационных технологий в проектировании Российской академии наук, Одинцово
[2] Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования "Московский авиационный институт
(национальный исследовательский университет)", Москва

Разработка имитационной модели атаки "человек посередине" для исследования эффективности протоколов информационного взаимодействия

Задачи, связанные с оценкой и повышением эффективности применения протоколов и средств защиты от различных атак, актуальны для большинства предприятий, в том числе авиационной и ракетно-космической промышленности. Совершенствование протоколов информационного взаимодействия, а также средств защиты, основанных на детектировании аномалий в сети путем наблюдения за меняющимися характеристиками информационных потоков при воздействии на них злоумышленника, требует разработки адекватной модели для описания реализации такой актуальной атаки, как "человек посередине". Проведен анализ основных характеристик процесса передачи данных по сети, на которые оказывает влияние атака "человек посередине". Определены принцип воздействия атакующего на моделируемую систему передачи данных и последствия реализации атаки. Результатом работы является программное средство для имитации присутствия злоумышленника в сети, позволяющее исследовать влияние атакующего на процесс информационного взаимодействия между абонентами в виде задержек, потерь, искажений пакетов и снижения скорости передачи данных. Также приводятся методы и особенности применения разработанной модели.

Ключевые слова: *атака "человек посередине", информационное взаимодействие, оптимизация протоколов, модель злоумышленника, TCP, UDP*

Введение

Популярность и распространенность мобильных и сетевых технологий с каждым годом растет. Однако вместе с проникновением технологий в повседневную деятельность возрастают угрозы, связанные с перехватом данных при информационном взаимодействии двух сторон, что может повлечь за собой серьезные последствия. Одним из результатов реализации такого рода угроз является атака "человек посередине". Атака "человек посередине" (англ. Man in the middle, MitM-атака) представляет собой ситуацию, когда злоумышленник может читать, видоизменять, замещать, удалять информацию, которой обмениваются два адресата, при этом взаимодействующие стороны не ощущают присутствия третьего лица [1]. Этот вид атаки остается популярным среди хакеров, так как предоставляет возможность модификации информации в любых сферах (банковские транзакции, личная переписка, вторжение в частную жизнь).

Чтобы предупредить последствия данной атаки, необходимо комплексное решение, состоящее не только из средств защиты информации от несанкционированного доступа, но и систем обнаружения и предотвращения вторжений. Последние могут обнаруживать злоумышленника по аномалиям в сети, которые возникают из-за изменения характеристик информационных потоков в результате деятельности атакующего. К этим характеристикам следует отнести потери и искажения пакетов, увеличение задержек при передаче данных по сети, а также снижение скорости передаваемой информации. Имитация данных характеристик сети позволит воспроизвести атакующие воздействия со стороны злоумышленника на процесс информационного взаимодействия и повысить эффективность систем обнаружения вторжений.

Для имитации воздействия злоумышленника, реализующего атаку "человек посередине", на потоки данных, передаваемых по сети, можно вос-

пользоваться различными моделями, включая математические и имитационные.

Математические модели базируются на графах атак [2], а также на системах массового обслуживания [3]. Однако для применения моделей на основе графов атак требуются экспертные оценки вероятностей реализации того или иного проявления атаки (потерь, перемешивания пакетов и т. д.), которые отсутствуют для рассматриваемого вида атаки. Модель злоумышленника на основе систем массового обслуживания позволяет воспроизвести только один параметр — задержку, вносимую атакующей стороной.

Имитационная модель атаки "человек посередине" в силу возможности усложнения модели злоумышленника при сохранении принципов построения модели позволяет воспроизвести основные характеристики проявления этого вида атаки на систему передачи информации и поэтому будет рассмотрена в данной работе.

1. Особенности разработки имитационной модели атаки "человек посередине"

Наша задача состоит в разработке модели, имитирующей характеристики сети, в которой находится злоумышленник. Данная модель не предполагает операций по дешифровке сетевого трафика, если таковой зашифрован, перехват паролей и иных деструктивных действий, которые могут нарушить работоспособность сети. Разрабатываемая модель может быть использована для имитации не только действий третьего лица — злоумышленника, но и процессов, происходящих в сетях. Примерами таких процессов являются потери пакетов в беспроводных сетях из-за искажения данных при их передаче по физическому каналу, увеличение времени передачи пакетов до получателя и обратно при смене маршрута между передающей и принимающей сторонами.

Для создания приложения, которое будет имитировать атаку "человек посередине", необходимо провести анализ особенностей реализации программного обеспечения (ПО) данного типа. Были выбраны и исследованы следующие программы:

- *Dsniff* — мониторинг сети для сбора паролей, файлов и т. д.;
- *Cain&Abel* — выявление паролей путем перехвата информационных пакетов;
- *Ettercap* — ПО для перехвата и прослушивания сетевых пакетов.

Dsniff [4] специализируется на перехвате паролей, сеансов, сообщений электронной почты и адресов веб-страниц. Данная программа работает в локальных сетях и позволяет извлекать информацию из пакетов. На извлечение информации затрачивается некоторое время, что приводит к появлению задержек при передаче пакетов по сети и ограничению скорости передаваемых данных [5], а в ряде случаев и к потерям пакетов.

Рис. 1. Общая схема модели, имитирующей поведение злоумышленника в сети

Cain&Abel [6] — утилита для восстановления паролей, использующихся при входе в систему, и перехвата данных. Основной интерес представляет функция подмены связки IP и MAC адресов (ARP Spoofing), осуществление которой приводит к перенаправлению информационных потоков между абонентами через злоумышленника, что влечет модификацию сетевых пакетов с возможностью отправки дубликатов некоторых из них.

Ettercap [7] является более мощным решением в проведении атак "человек посередине". Данное ПО обладает возможностью анализа сетевого трафика и фильтрации контента, а также модификации пакетов в реальном времени. Применение фильтра приводит к перемешиванию пакетов в исходящем от злоумышленника потоке данных по сравнению с входным.

По результатам проведенного анализа представленных выше программ было решено обеспечить имитационную модель злоумышленника (рис. 1) следующим функционалом: искажение пакетов, потеря пакетов, перемешивание пакетов, повтор пакетов, ограничение пропускной способности, предоставление возможности модифицирования полезной нагрузки пакета в "реальном" времени.

Имитатор атаки "человек посередине" реализован в виде программы на языке высокого уровня C# [8] и использует четыре сокета: два на прием данных от отправителя и получателя и два на передачу данных — к получателю и отправителю. Далее будут рассмотрены основные функции имитационной модели злоумышленника на примерах работы отдельных алгоритмов.

2. Модификация пакетов в "реальном" времени

Так как наша имитационная модель работает на прикладном уровне стека TCP/IP, то это позволяет

Рис. 2. Модель модификации сетевых пакетов с использованием сторонних средств

обрабатывать трафик любого типа — от HTML-страниц до сообщений, передаваемых по сети. Основной идеей данного алгоритма является запись передаваемых данных между абонентами в текстовый файл — логирование пакетов. С помощью разработанной программы можно модифицировать пакеты с их последующей отправкой получателю (PC 2 на рис. 2) с привлечением сторонних средств. Это позволит более гибко использовать данный имитатор атаки, моделируя процесс передачи данных для абонентов в режиме "реального" времени.

3. Ограничение пропускной способности канала между абонентами

Во время атаки "человек посередине" злоумышленник вносит временну́ю задержку, которая связана с анализом передаваемого трафика. Увеличение времени обработки каждого пакета снижает скорость передачи данных и приводит к эффекту ограничения пропускной способности канала между абонентами.

Алгоритм ограничения пропускной способности канала приближает нашу модель к функционированию реальной сети с находящимся в ней злоумышленником. Особенностью данного алгоритма является предотвращение проблем, которые характерны для стандартных решений по ограничению трафика. В стандартных алгоритмах существует проблема переполнения буфера. Это происходит в том случае, если буфер, отведенный под пакеты, заполняется быстрее, чем опустошается. Мы решили избежать данных проблем путем создания "виртуального" буфера — в нем может храниться только один пакет, который сразу же передается получателю. В случае ожидания отправки нескольких пакетов под каждый из разрешенных к передаче пакетов создается свой "виртуальный" буфер. По достижении максимального числа разрешенных к отправке пакетов за 1 с наша программа отбрасывает вновь приходящие. Число сетевых пакетов, которое наше приложение обрабатывает за 1 с определяет пропускную способность канала (рис. 3). Такой подход позволяет более практично подойти к задаче ограничения трафика.

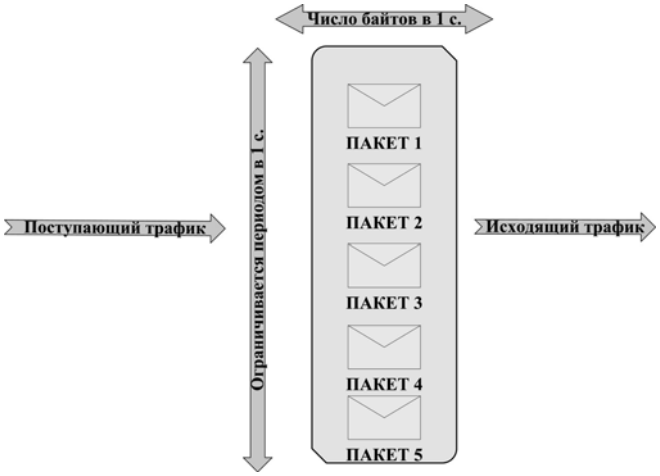

Рис. 3. Схема работы "виртуального" буфера

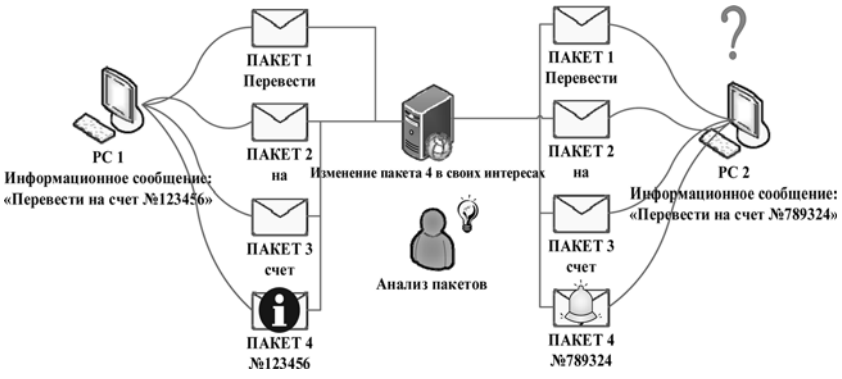

Рис. 4. Модель искажения пакетов злоумышленником

4. Искажение пакетов злоумышленником

Довольно интересно проявляет себя алгоритм искажения пакетов. Его практическая ценность для исследования воздействия атакующего на информационные потоки в сети состоит в том, что злоумышленник может сфальсифицировать содержимое пакета в личных целях. Отличие данного алгоритма от модификации пакетов в "реальном" времени состоит в том, что при включении данного параметра от пользователя не требуется никакого вмешательства и предварительной записи набора пакетов. Программа сама изменит пакет, имитируя действие третьего лица (рис. 4).

5. Имитация воздействия атакующего на информационный поток в виде потерь, повторов и перемешивания пакетов

Потери, повторы и перемешивание сетевых пакетов происходят в результате деструктивной деятельности злоумышленника и являются следствием внедрения атакующего между абонентами. Эти функции нежелательны для злоумышленника, так как позволяют обнаружить его, но в то же время интенсивная обработка сетевого трафика требует от него огромных ресурсов, из-за чего и возникают указанные выше потери, повторы и перемешивания пакетов.

В некоторых случаях злоумышленник, анализируя трафик, может посчитать ненужным ретрансляцию пакета адресату. Это приведет к снижению скорости передачи данных между абонентами, что повысит эффективность обработки информационного потока атакующим (рис. 5). Данную функцию также можно расценивать как один из параметров, характеризующих сеть, — ведь в обычном информационном взаимодействии возможна потеря пакетов.

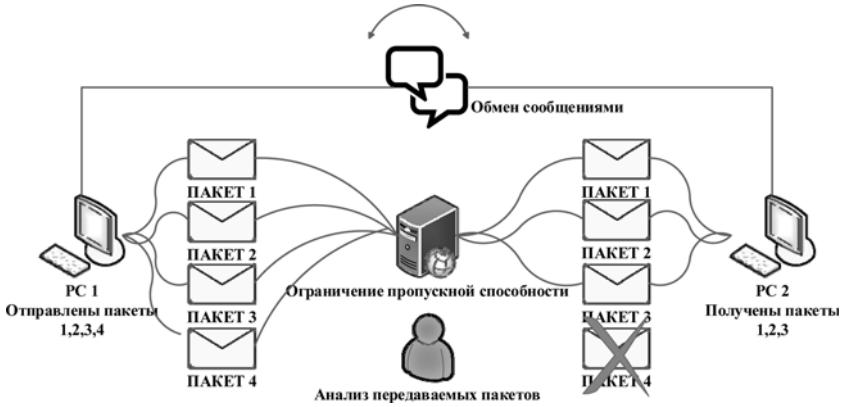

Рис. 5. Модель системы передачи информации с потерями пакетов

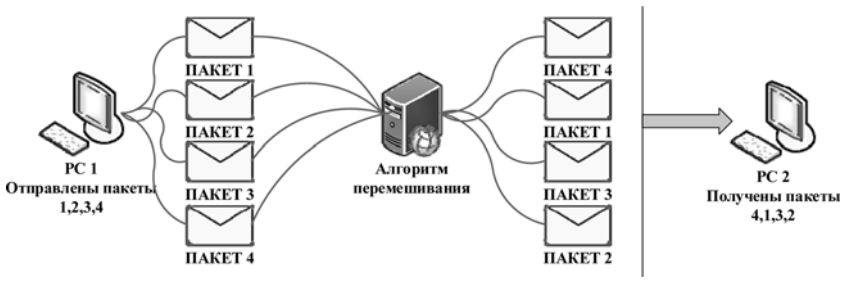

Рис. 6. Схема реализации алгоритма перемешивания пакетов

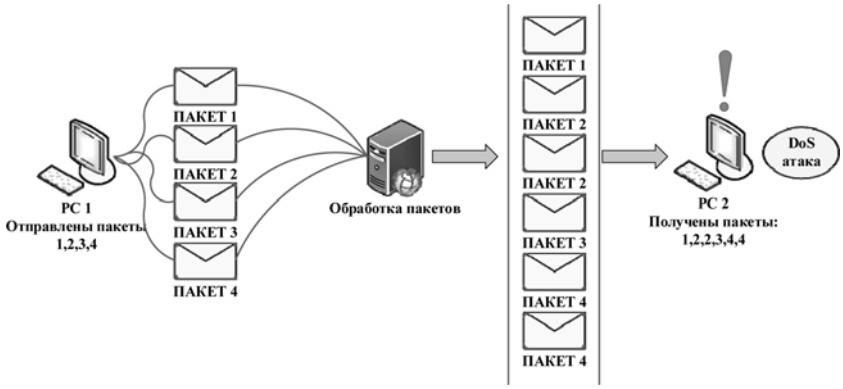

Рис. 7. Реализация алгоритма повтора пакетов

Для того чтобы как можно дольше не привлекать к себе внимание, злоумышленник должен обеспечить непрерывное взаимодействие между адресатами. В связи с этим время, потраченное на модификацию пакетов, влечет за собой перемешивание последовательности пакетов (рис. 6).

Принимающая сторона будет осуществлять прием пакетов, адресованных только ей и, возможно, по определенной маске пакета. Злоумышленник, прослушивающий трафик, может провести атаку "отказ в обслуживании" путем многократной отправки повторяющихся пакетов, причем принимающая сторона ничего не заподозрит (рис. 7).

6. Основные характеристики разработанной программы

Все изложенные выше алгоритмы имитационной модели атаки "человек посередине" реализованы в одном приложении MITM.exe (рис. 8).

В меню "Настройка" можно указать следующие характеристики имитатора атаки:

- потеря пакетов;
- повтор пакетов;
- перемешивание пакетов;
- искажение пакетов;
- ограничение скорости передаваемых данных (рис. 9).

В меню "Конфигурация" пользователь может выбрать вид используемого протокола (TCP или UDP), поменять порты и IP-адреса отправителя и получателя. После выбора и установки параметров работы имитатора атаки "человек посередине" необходим его запуск путем нажатия кнопки "Start".

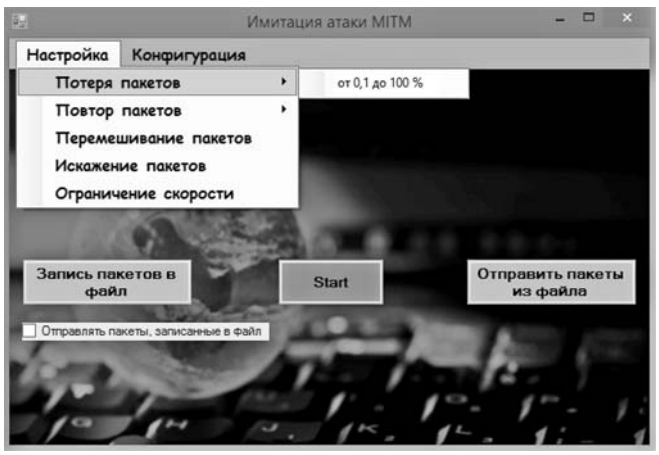

Рис. 8. Основные настройки приложения

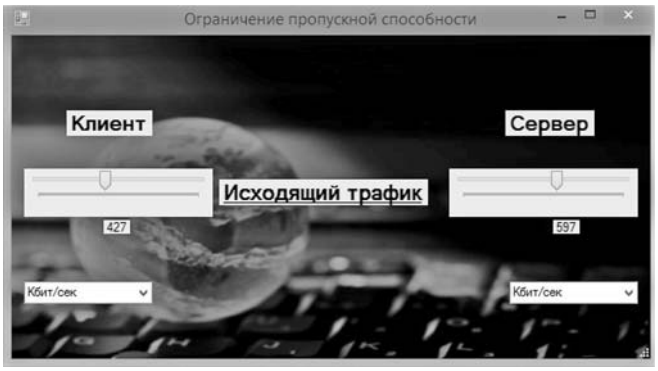

Рис. 9. Настройка ограничения скорости передаваемых данных

7. Методы и особенности применения разработанной модели

Один из вариантов применения разработанной модели, который представлен на рис. 10, заключается в передаче данных между отправителем и получателем через имитатор атаки, который расположен между ними и воспроизводит воздействие злоумышленника на сетевые протоколы, такие как TCP и UDP, в виде потерь, повторов, перемешивания и искажения пакетов, а также ограничения скорости передаваемых данных. Чтобы симулировать атаку, необходимо подключить отправителя и получателя к имитатору атаки "человек посередине", указав IP-адрес и порт последнего в одной из программ, протоколы которой предполагается протестировать, например iperf. Для имитации атаки в программе MITM.exe указывается процент пакетов (от 0,1 до 100 %), которые будут отброшены или продублированы, число искаженных и перемешанных пакетов, а также проводится ограничение скорости передаваемых данных (см. рис. 9). Меняя данные параметры на имитаторе атаки "человек посередине", можно изучить влияние атакующего на такие характеристики, как скорость и надежность информационного взаимодействия между абонентами, которые, в свою очередь, определяются механизмами управления перегрузкой и контроля целостности заголовков сетевых пакетов и данных, расположенных в этих пакетах. Рассмотренный метод применения имитационной модели атаки "человек посередине" пригодится для исследования новых протокольных элементов и компонентов на предмет их эффективности противодействия атакующему.

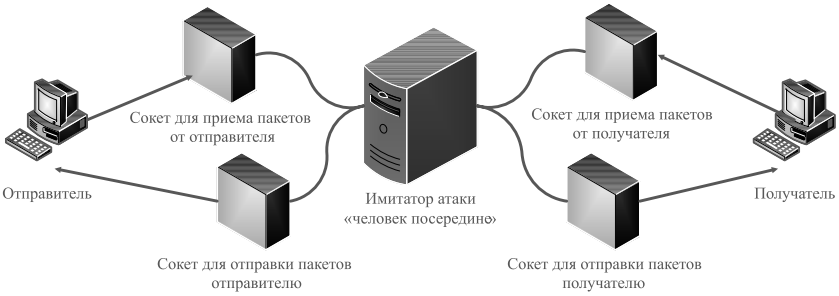

Рис. 10. Структурная схема имитатора атаки для исследования влияния воздействия злоумышленника на протоколы информационного взаимодействия

Еще одним вариантом применения разработанной имитационной модели является перехват данных с их последующей записью и ретрансляцией записанных пакетов в сеть. Для этого осуществляется перехват сеанса между взаимодействующими сторонами с помощью программы-сниффера, а затем эти пакеты через некоторое время воспроизводятся с помощью опции "Отправлять пакеты, записанные в файл". Для записи пакетов также можно использовать разработанную программу MITM.exe, предварительно выполнив настройку отправителя и получателя, как было описано в первом варианте применения имитационной модели. При использовании в сети коммутаторов фирмы Cisco серий 4500 и 6500, повторной отправкой пакетов можно протестировать работу системы противодействия ключевым узлам атаки "человек посередине", таким как DHCP Snooping [9] и IP Source Guard [10].

Заключение

Поставленная во введении задача по разработке имитационной модели атаки "человек посередине" была достигнута полностью. Ее результатом является программа MITM.exe. Она написана под ОС Windows со средой .NET Framework 4.5. Данная модель может использоваться для исследования методов и средств защиты, основанных на детектировании аномалий в сети, путем наблюдения за меняющимися характеристиками информационных потоков при воздействии на них злоумышленника. Также она будет полезна разработчикам сетевых протоколов, так как позволяет оценить воздействие злоумышленника на работу протокольной машины и вносить необходимые дополнения в ее функционирование.

Стоит отметить, что компонент программы, описанный в п. 2, делает ее актуальной в течение длительного времени. Не важно, какие протоколы прикладного уровня будут использовать абоненты, так как злоумышленник всегда сможет обрабатывать пакеты по своему усмотрению в силу функционирования имитационной модели на транспортном уровне. Также необходимо отметить, что со скорым выходом Visual Studio 2015 программа получит кроссплатформенность. Этот статус позволит использовать ее на большинстве современных вычислительных устройств.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 14-07-31247 мол_а.

Список литературы

1. **Понятие** термина MITM-атака [Электронный ресурс] // Сайт It-Sektor: [Электронный ресурс], 2015. URL: http://it-sektor.ru/ponyatie-termina-mitm-ataka.html (дата обращения 06.03.2015).

2. **Sheyner O., Haines J., Jha S., Lippmann R., Wing J.** Automated Generation and Analysis of Attack Graphs // Proceedings of the IEEE Symposium on Security and Privacy. Oakland, CA, USA, 2002. P. 273—284.

3. **Мазепа Р. Б., Михайлов В. Ю., Большов О. А., Карпухин Е. О., Корнилов А. М.** Методы обеспечения безопасности информационных процессов. М.: МАИ-ПРИНТ, 2012. 168 с.

4. **Сниффинг** сети на коммутаторах [Электронный ресурс] // Сайт Nag.ru: [Электронный ресурс], 2015. URL: http://nag.ru/articles/reviews/15770/sniffing-seti-na-kommutatorah.html (дата обращения 06.03.2015).

5. **Шоуэнберг Р.** Атака на банки. Аналитическая статья "Лаборатории Касперского" [Электронный ресурс], 2015. URL: http://www.itsec.ru/articles2/Inf_security/ataka-na-banki (дата обращения 06.03.2015).

6. **Использование** сниффера Cain & Abel [Электронный ресурс] // Сайт Записки it Guy: [Электронный ресурс], 2015. URL http://itguy-note.blogspot.de/2010/03/cain-abel.html (дата обращения: 06.03.2015).

7. **Анализ** безопасности компьютерных сетей [Электронный ресурс] // Сайт Zen Way: [Электронный ресурс], 2015. http://zenway.ru/page/ettercap (дата обращения 06.03.2015).

8. **Нейгел К., Ивьен Б., Глинн Д., Уотсон К., Скиннер М.** C# 5.0 и платформа .Net 4.5 для профессионалов: Пер. с англ. М.: Издат. дом "Вильямс", 2014. 1440 с.

9. **Конфигурация** DHCP Snooping [Электронный ресурс] // Сайт Cisco.com: [Электронный ресурс], 2015. URL: .cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_dhcpsnoop.html (дата обращения 05.11.2015).

10. **Конфигурация** IP Source Guarde [Электронный ресурс] // Сайт Cisco.com: [Электронный ресурс], 2015. URL:http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/soft ware/release/3e/security/configuration_guide/b_sec_3e_3650_cg/b_sec_3e_3650_cg_chapter_01101.pdf (дата обращения 05.11.2015).

N. V. Britvin[1], expert, britvin.nickita@yandex.ru,
E. O. Karpukhin[1, 2], Senior Staff Scientist, ret1987@yandex.ru
[1] Design Information Technologies Center, Russian Academy of Sciences
[2] Moscow Aviation Institute (National Research University)

Development a Simulation Model of the Attack "Man in the Middle" for Studies the Effectiveness Data-Driven Interaction Protocols

The tasks, related to evaluating and improving the effectiveness of protocols and protection means from various attacks, are relevant for majority of enterprises, including aerospace industry. Improving data-driven interaction protocols and protection means, based on the detection of anomalies in the network by monitoring the changing characteristics of information flows when exposed to an attacker, requires the development of an adequate model to describe the actual implementation of such an attack, as a "man in the middle". To achieve this target, in this work was carried the analysis of the main characteristics of the process data transferring over a network, that are affected by the attack "man in the middle". It defines the principles of attacks to simulated data transmission system and the implications of this attack. The result of this work is a software tool to simulate the presence of attacker in the network, allowing the attacker to investigate the influence on the process of information exchange between subscribers in the form of delays, loss, distortion and reduce packet data rate. It also provides methods and features of application developed model.

Keywords: *attack "man in the middle", data-driven interaction, protocol optimization, model of the attacker, TCP, UDP*

References

1. **Ponjatie** termina MITM-ataka [Definition of the term MITM-attack]. Site It-Sektor: [electronic resource], 2015. URL: http://it-sektor.ru/ponyatie-termina-mitm-ataka.html (date of the application 06.03.2015).

2. **Sheyner O., Hames J., Jha S., Lippmann R., Wing J. M.** Automated Generation and Analysis of Attack Graghs // *Proceedings of the IEEE Symposium on Security and Privacy*. Oakland, CA, USA, 2002. P. 273—284.

3. **Mazepa R. B., Mihajlov V. Ju., Bol'shov O. A., Karpuhin E. O., Kornilov A. M.** *Metody obespechenija bezopasnosti informacionnyh processov* [Methods of safety information processes]. Moscow: MAI-PRINT, 2012, 168 p.

4. **Sniffing** seti na kommutatorah [Sniffing network switches] // Site Nag.ru: [electronic resource], 2015. URL: http://nag.ru/articles/reviews/15770/sniffing-seti-na-kommutatorah.html (date of the application; 06.03.2015).

5. **Shouenberg R.** *Ataka na banki. Analiticheskaja stat'ja "Laboratorii Kasperskogo"* [Attacks on banks. The analytical article "Kaspersky Lab"], 2015. URL: http://www.itsec.ru/articles2/Inf_security/ataka-na-banki (date of the application 06.03.2015).

6. **Ispol'zovanie** sniffera Cain & Abel [Using sniffer Cain & Abel]. Site Zapiski it Guy: [electronic resource], 2015. URL http://itguy-note.blogspot.de/2010/03/cain-abel.html (date of the applications 06.03.2015).

7. **Analiz** bezopasnosti komp'juternyh setej [Analysis of the security of computer networks]. Site Zen Way: [electronic resource], 2015. http://zenway.ru/page/ettercap (date of the application 06.03.2015).

8. **Nejgel K., Iv'en B., Glinn D., Uotson K., Skinner M.** *C# 5.0 i platforma* .Net 4.5 dlja professionalov: Per. s angl. Moscow: OOO "I.D. Vil'jams", 2014. 1440 pp.: il. [Christian Nagel, Bill Iven, Jay Glynn, Karli Watson, Morgan Skinner. C # 5.0 and .Net 4.5 platform for professionals, Trans, from English. M.: OOO "ID Williams"]

9. **Konfiguracija** DHCP Snooping [Configuring DHCP Snooping]. Site Cisco.com: [electronic resource], [2015]. URL: .cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_dhcpsnoop.html (date of the application 05.11.2015).

10. **Konfiguracija** IP Source Guarde [Configure IP Source Guarde]. Site Cisco.com: [electronic resource], 2015. URL: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/3e/security/configuration_guide/b_sec_3e_3650_cg/b_sec_3e_3650_cg_c hapter_01101.pdf (date of the application 05.11.2015).