МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Институт информационных технологий и телекоммуникаций
Северо-Кавказского федерального университета (г. Ставрополь)

Институт компьютерных технологий и информационной безопасности
Инженерно-технологической академии Южного федерального университета (г. Таганрог)

Поволжский государственный университет телекоммуникаций и информатики (г. Самара)
Ростовский государственный экономический университет «РИНХ» (г. Ростов-на-Дону)

СТУДЕНЧЕСКАЯ НАУКА ДЛЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

СБОРНИК МАТЕРИАЛОВ
III ВСЕРОССИЙСКОЙ НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ

(Ставрополь, 14-18 декабря 2015)

Часть 2

Ставрополь
2015

УДК 004.2/.9
ББК 32.97
С 88

Организаторы конференции:

Министерство образования и науки Российской Федерации
Институт информационных технологий и телекоммуникаций
Северо-Кавказского федерального университета (г. Ставрополь)
Институт компьютерных технологий и информационной безопасности Инженерно-технологической академии Южного федерального университета (г. Таганрог)
Поволжский государственный университет телекоммуникаций и информатики (г. Самара)
Ростовский государственный экономический университет «РИНХ»
(г. Ростов-на-Дону)

Оргкомитет конференции:

Председатель:

Лиховид А.А. – проректор по научной работе и стратегическому развитию СКФУ, доктор географических наук, кандидат биологических наук, профессор.

Члены оргкомитета:

Чипига А.Ф. – директор Института информационных технологий и телекоммуникаций СКФУ, заведующий кафедрой информационной безопасности автоматизированных систем, кандидат технических наук, профессор.

Мезенцева О.С. – заместитель директора по учебной работе Института информационных технологий и телекоммуникаций СКФУ, кандидат физико-математических наук, доцент.

Петренко В.И. – заместитель директора по научной работе Института информационных технологий и телекоммуникаций СКФУ, заведующий кафедрой организации и технологии защиты информации, кандидат технических наук, доцент.

Веселов Г.Е. – директор Института компьютерных технологий и информационной безопасности Инженерно-технологической академии Южного федерального университета, полномочный представитель ректора по развитию инженерного направления, доктор технических наук, доцент.

Самойлов А.Н. – заместитель директора Института компьютерных технологий и информационной безопасности Инженерно-технологической академии Южного федерального университета по научной и международной деятельности, кандидат технических наук, доцент.

Маслов О.Н. – заведующий кафедрой экономических и информационных систем Поволжского государственного университета телекоммуникаций и информатики, доктор технических наук, профессор.

Тищенко Е.Н.– заведующий кафедрой информационных технологий и защиты информации Ростовского государственного экономического университета (РИНХ), доктор экономических наук, доцент.

Ответственный секретарь:

Толстова Н.А. – доцент кафедры межинститутской базовой кафедры СКФУ, кандидат педагогических наук.

С 88 **Студенческая наука для развития информационного общества:** сборник материалов III Всероссийской научно-технической конференции. Часть 2. – Ставрополь: Изд-во СКФУ, 2015. – 374 с.

ISBN 978-5-9296-0813-1

Материалы конференции посвящены вопросам развития инновационных образовательных и инфокоммуникационных технологий, проблемам информационной безопасности объектов информатизации, изучению информационных систем и технологии. Изложены результаты научных исследований в области разработки информационных технологий решения экономических задач, затрагиваются вопросы создания и использования робототехнических систем.

УДК 004.2/.9
ББК 32.97

ISBN 978-5-9296-0813-1

Современные отечественные операционные системы могут пойти по двум реальным направлениям развития. В первую очередь хочется отметить вполне оправданную заинтересованность военных. Именно для них важно защищенное отечественное программное обеспечение. Второй путь можно отметить в качестве «патриотической разработки»[4].

Иногда в интернете встречаются проекты, которые разработаны авторами, анонсирующими российскую операционную систему. Стоит упомянуть о таких операционных системах, как «Роса», «Патриот ОС», «Фантом», PhantomOS, KolibriOS. Операционная система PhantomOS (http://www.dz.ru/solutions/phantom) от Дмитрия Завалишина система наиболее подходит под громкое звание российской операционной системы. Но она настолько оригинальна, а заложенные в её основу идеи настолько необычны, что она лет на 10 опередила своё время[4].

Литература

1. Википедия. Хамелион. [Электронный ресурс] URL: https://ru.wikipedia.org/wiki/Хамелеоны (дата посещения 29.11.2015)
2. Интернет ресурс: [Электронный ресурс] URL http://l4os.ru/ (дата посещения 29.11.2015)
3. Hameleon [Электронный ресурс] URL http://habrahabr.ru/company/hameleon/profile/ дата посещения 29.11.2015
4. Phantom. [Электронный ресурс] URL: http://www.dz.ru/solutions/phantom) дата посещения 30.11.2015)

РАЗРАБОТКА АЛГОРИТМА ЗАЩИТЫ СЕТИ ОТ DOS-АТАК НА ОСНОВЕ КАЧЕСТВЕННОГО АНАЛИЗА ТРАФИКА

З. А. Носиров, А. А. Честнов
руководитель, ассистент кафедры информационной безопасности ***О. М. Князева***
Астраханский государственный университет, г. Астрахань

Быстрое и повсеместное распространение Интернета привело к бурному развитию компьютерных сетей, что позволило существенно расширить возможности для компаний, предоставляющих свои услуги через глобальную сеть. К глобальной сети подключены миллионы устройств и пользователей, благодаря чему множество фирм и потребителей взаимодействуют между собой. Для реализации своих услуг компании используют информационные ресурсы, которые позволяют выполнять обработку информации, относящуюся к их клиентам. Некорректная работа или недоступность сервисов может повлечь значительные потери, как финансовые, так и клиентские. Именно по этим причинам в последние годы информационные ресурсы и сервисы все чаще сталкиваются с вредоносным воздействием, осуществляемым с использованием протоколов межсетевого взаимодействия – удаленной сетевой атакой.Частой причиной нарушения доступности ресурсов являются DDos-атаки на сервер, где физически расположен сайт. Уязвимости, через которые реализуются DDos-атаки сводятся к:

- Ошибкам в программном обеспечениикоторая работает на атакуемом сервисе
- Недостаткам протоколов сети [1]
- Ограничениям в пропускной способности канала связи.

Источником DDoS-атаки является определенное количество заражённых компьютеров, объединённых в сеть, именуемую «ботнет». Зараженные компьютеры, управляютсяопределённым портом или же откликами на команды в IRC-чате (англ. InternetRelayChat — протокол прикладного уровня для обмена сообщениями в режиме реального времени). Впрочем, в настоящее время получили распространение ботнеты, управляемые через сайт или же по принципу p2p-сетей.

Согласно отчёту [2], размещенному фирмой Arbor Networks, предоставляющей одни из наилучших решений для обеспечения стабильной работы информационной системыи имеющей большой навык в вопросах борьбы с DDoS-атаками, число DDoS-атак со скоростью 20 Гбит/с в 2014 году, по сопоставлению с аналогичным периодом 2013 года увеличилось вдвое. Больше 100 DDoS-атак со скоростью 100Гбит/с были зафиксированы за 2014 год. 46% атак относились к всеохватывающим DDoS-атакам, использующим отправку мусорного трафика, SYN-флуд и UDP Flood, а также атаки с использованием протоколов уровня приложений. Впрочем, в сопоставлении с прошлыми годами соотношения заявленных атак этого типа практически не изменились по отноше-

нию к большинству служб, таких как HTTP, DNS и SMTP. Есть определённая обеспокоенность по поводу компрометации (факта доступа постороннего лица к защищаемой информации) рабочих станций. Есть вероятность того, что компьютеры, принадлежащие к корпоративной сети, имеют все шансы быть частью ботнета. Эта обстановка приводит к усилению эффекта от атаки, так как защита может быть направленна только на внешнюю сеть, игнорируя внутрисетевой корпоративный трафик. Повышение числа хостов, входящих в ботсети, не вызывает удивление, беря во внимание численность и сложность существующих на сегодняшний день вирусов, темпы их развития и исходящую из этого невозможность построить надежную систему защиты на основе антивирусных программ и систем обнаружения проникновений.

Рассмотрим принципы, по которым была произведена самая мощная DDos-атака. Согласно проведенному отчету [3] в основе данной атаки лежит UDP-флуд(сетевая атака типа «отказ в обслуживании», использующая без сеансового режима протокола UDP),который сопровождается SYN-флудом. Это указывает на наличие достаточно большого числа подконтрольных серверов.

В ходе данной атаки осуществлялось умножение первоначального вредоносного трафика за счёт отражения DNS-запросов через DNS-резолверы, которые установлены у каждого Интернет-провайдера. Обычно DNS-резолверы сконфигурированы так, чтобы обрабатывать только запросы своих пользователей, но существует большое количество компаний, которые неправильно их сконфигурировали, так что резолверы принимают запросы от любого пользователя интернета. Любопытно заметить, что в значительной мере усиление происходило благодаря большим ключам DNSSEC, которые включены в тело ответа, а ведь протокол DNSSEC внедрялся с целью повысить безопасность системы DNS.

Рис.1 Схематическое представление DDos-атаки

Существуют три основных решений по защите от атак:

- Программные решения;
- Аппаратные решения;
- Облачные решения.

Программные решения – самое распространённое на рынке информационных технологий, представляет собой набор правил фильтрации трафика, которые составлены разработчиком. Данное решение достаточно просто установить прямо на сервер, на котором работает ресурс, но поможет только от малозаметных атак.

Аппаратные решения – это распределенная сетевая структура с большим запасом пропускаемого трафика. Используются в масштабных сетевых структурах, таких как: точки обмена трафиком, дата-центры, крупные региональные провайдеры.

Облачные решения представляют сетевую структуру с большой пропускной способностью, в состав которой вводятся сервера для фильтрации вредоносного трафика. Таким образом, такая сеть постепенно будет отфильтровывать негативный трафик и снижать количество вредоносных пакетов.

Анализ трафика является достаточно сложной задачей, поэтому некоторые компании патентуют свои алгоритмы, например, компания “Black Lotus” запатентовала алгоритм «Human Behavior Analysis» [4], который определяет, кто генерирует трафик, человек или бот. Определив причины возникновения и проблемы, которые подлежат решению при борьбе с данным видом атак, появляется возможность найти методы решения данных проблем.

Рассмотрим атаку на предприятие со следующей топологией сети (рис.2).

Вредоносный и полезный трафик поступает во внутреннюю сеть. Сперва данные поступают на устройство анализа трафика. На данном этапе применяются простые алгоритмы фильтрации – статические таблицы, с помощью которых появляется возможность блокировать вредоносный трафик от определенных узлов. Управление данным узлом (заполнение таблиц) осуществляет сервер, который находится в сети за устройством анализа трафика. Этот сервер выполняет активную верификацию данных и собирает статистические данные о вредоносном трафике и его источниках возникновения. После установления источника вредителя он передает информацию о нем в устройство анализа трафика и блокирует его. Чтобы к заблокированным узлам не попали доверенные и другие рабочие устройства, сервер выполняет постоянный активный анализ всего трафика. Далее сервер выполняет лимитирование скорости и перенаправление проверенного трафика в сеть предприятия. Проверенный трафик доставляется до узлов назначения по корпоративной сети без проблем и перегрузок.

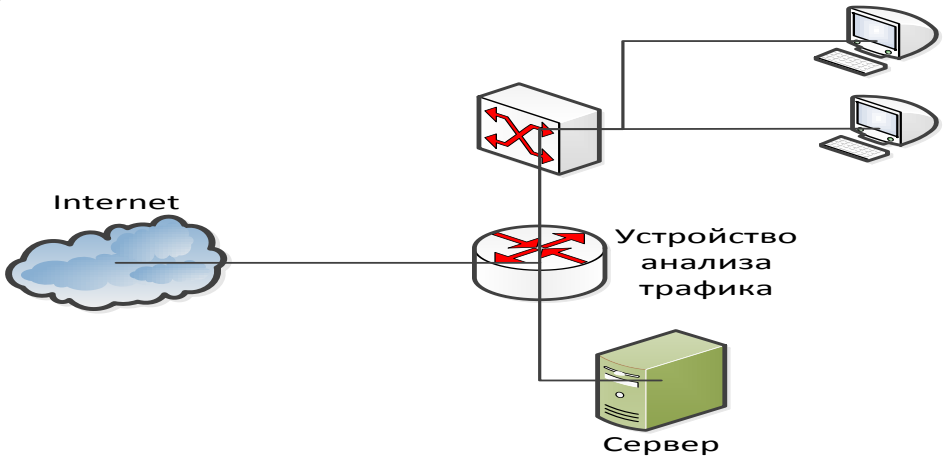

Рис.2 Схематическое представление моделируемой сети

Хотя существуют лидеры рынка в данной области, предлагаемый ими продукт является полностью закрытым. В отличие от решений с закрытым исходным кодом, открытые рекомендации позволяют привести методы и алгоритмы к единому стандарту, что сделает данные решения более гибкими и позволит пользоваться ими с большей эффективностью.

Несмотря на все передовые методы защиты от хакеров, методы проведения атак на шаг опережают тех, кто разрабатывает защиту от уязвимостей. Поэтому владельцам веб-приложений необходимо быть начеку вследствие постоянного появления новых угроз

Литература

1. Лейкин А.В. Протоколы транспортного уровня UDP, TCPиSCTP достоинства и недостатки [Электронный ресурс] – Санкт-Петербург: СПбГУТ, 2013. – Режим доступа: http://niits.ru/public/2013/2013-007-pp.pdf

2. Максим зайцев. Статистика глобальной сетевой активности [Электронный ресурс] – Москва:KasperskyLab,2014 –Режим доступа: http://qps.ru/z1PWV

3. Abliz M. Internet Denial of Service Attacks and Defense [Электронный ресурс] – Pittsburgh : University of Pittsburgh,2011– Режим доступа: http://people.cs.pitt.edu/~mehmud/docs/abliz11-TR-11-178.pdf

4. BlackLotus. Patent Pending Technology [Электронный ресурс] – Сан-Франциско, 2012. – Режим доступа: https://www.blacklotus.net/learn/technology/

ЧИСЛЕННОЕ ИССЛЕДОВАНИЕ КРИВОЙ НАМАГНИЧИВАНИЯ МАГНИТОДИЭЛЕКТРИЧЕСКОГО ДАТЧИКА ПЕРЕМЕННОГО ТОКА

И. А. Орлов, О. А. Пурчина, Д. Д. Фугаров, С. В. Ефремов
руководитель – д-р техн. наук, профессор, заведующий кафедрой автоматизации и математического моделирования в нефтегазовом комплексе ***Ю. Я. Герасименко***
Донской государственный технический университет, г. Ростов-на-Дону

Для обеспечения гальванической развязки силовых цепей переменного тока и измерительной схемы наиболее целесообразно применение измерительных преобразователей индукционного типа, однако применение трансформаторов тока не обеспечивает заданный диапазон линейности для всей шкалы задания величин переменных токов больших амплитуд при приемлемых массогабаритных характеристиках [1]. Решением является использование датчиков тока с магнитодиэлектрическим сердечником (МДТ) на основе порошковых материалов *(Iron Powder)* фирмы *Magnetics* (США). В литературных источниках описываются МДТ, созданные на основе порошков карбонильного железа марок Р10, Р20, Р100 или ПС, которые применялись в корабельных энергетических системах [2]. Применение современных материалов даёт возможность обеспечить улучшенные характеристики МДТ при приемлемой погрешности преобразования первичных токов.

На рис. 1 представлена основная кривая намагничивания смеси Magnetics 60. В данном случае задача аппроксимации основной кривой намагничивания, с требуемой точностью простыми выражениями является крайне актуальной [2]. Предлагается основную кривую намагничивания магнитодиэлектриков на основе *Iron Powder* аппроксимировать формулой [3]:

$$B = A\ln(\alpha H + 1), \qquad (1)$$

где B и H – координаты кривой намагничивания; A и α – коэффициенты аппроксимации.

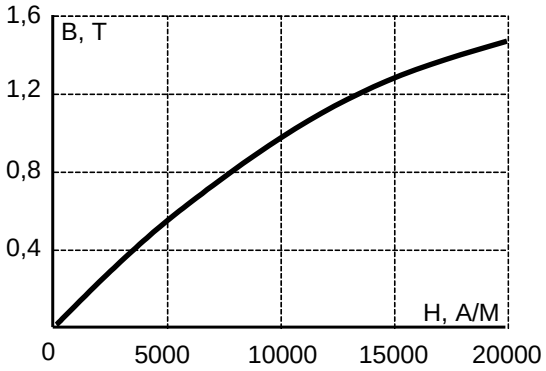

Рис. 1. Основная кривая намагничивания магнитодиэлектрика на основе смеси Magnetics 60

Для дальнейших расчетов выходных напряжений датчиков тока с магнитодиэлектрическим сердечником с наименьшей погрешностью необходимо достичь максимально возможного совпадения экспериментальной кривой и аппроксимирующей функции на начальном участке кривой намагничивания, в связи с чем на все аппроксимируемые выражения наложим дополнительные ограничения:

$$\lim_{H\to 0} B(H) = 0,\ \lim_{H\to 0}\frac{dB}{dH} = \mu_H\ ,(2), \qquad (3)$$

где μн – начальная магнитная проницаемость основной кривой намагничивания.

Из основной формулы (1) в общем виде получим:

$$\frac{dB}{dH} = \frac{A\alpha}{\alpha H + 1}, \qquad (4)$$

откуда при Н →0 имеем

$$\lim_{H\to 0}\frac{dB}{dH} = A\alpha\,. \qquad (5)$$

С учетом выражений (3) и (5) можем записать:

$$A = \frac{\mu_H}{\alpha}\,. \qquad (6)$$

СОДЕРЖАНИЕ

ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ РЕШЕНИЯ ЭКОНОМИЧЕСКИХ ЗАДАЧ

Научное издание

СТУДЕНЧЕСКАЯ НАУКА ДЛЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

СБОРНИК МАТЕРИАЛОВ
III ВСЕРОССИЙСКОЙ НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ
(Ставрополь, 14-18 декабря 2015)
Часть 2

Издается в авторской редакции

Компьютерная верстка М. И. Толмачёв

Подписано в печать 16.12.2015

Формат 60x84 1/8	Усл. п. л. 43,48	Уч.-изд. л. 42,72
Бумага офсетная	Заказ 295	Тираж 500 экз.

Отпечатано в Издательско-полиграфическом комплексе
ФГАОУ ВПО «Северо-Кавказский федеральный университет»
355028, г. Ставрополь, пр-т Кулакова, 2.