Содержание

8 (952) 106-88-60 vk.com/a.projectit a.projectit

ВВЕДЕНИЕ

Актуальность исследования

В современном обществе сетьИнтернет стала центром развития новых технологий, в корне меняющих методы взаимодействия и ведения бизнеса между конечными пользователями, поставщиками, партнерами и сотрудниками компаний. Обмениваясь данными через сеть, особенно при использовании ресурсов сетей общего доступа, пользователи должны быть уверены в том, что важная информация и ресурсы распределенной автоматизированной системы (РАС) всегда будут доступны для ведения бизнеса. С развитием возможностей глобальной сети обострилась и проблема атак наРАС, функционирующих с использованием сети Интернет [17].

Среди множества атак, атаки типа «отказ в обслуживании» занимают немаловажное место. За второе полугодие 2011 года атаки данного типа проводились с компьютеров, находящихся в 201 странах мира, средняя продолжительность атак составила 9 часов 29 минут, а самая продолжительная атака длилась более 80 дней [11,32]. Ежегодно они приносят различным компаниям значительные убытки и таят в себе серьезную угрозу для любой системы или сети. Все эти убытки обусловлены длительным простоем системы, упущенным доходом и большим объемом работ по идентификации и подготовке адекватных ответных мер.

Атака типа «отказ в обслуживании» (DoS-атака) – атакана автоматизированную систему с целью нарушения ее работоспособности, то есть создание таких условий, при которых легитимные пользователи системы не могут получить доступ к предоставляемым ресурсам РАС, либо этот доступ затруднѐн [9,26-28].

Отказ в доступе происходит вследствие того, что маршрутизаторы и серверы могут обрабатывать ограниченный объем трафика в любой момент времени, в зависимости от таких факторов, как количество памяти и полоса пропускания. Если этот предел превышается,новый запрос будет отвергнут. Таким образом, злоумышленник, который хочет нарушить работу определенной АС, может сделать это, отправив цели большое количество пакетов данных, которые поглотят все доступные ресурсы [46].

Частота атак, направленных на отказ в обслуживании, неуклонно растет.В целом, в 2011 году активность DDoS-трафика выросла на 136% по сравнению с показателями 2010 года[46,51,52].Генерация большого числа паразитного трафика снижает способность атакуемых узлов, принадлежащих не только операторам связи, но и обычным компаниям, обслуживающим легитимных пользователей. Ситуация усугубляется тем, что при современном уровне развития хакерских технологий для нарушения работоспособности даже мощного сервера РАС, имеющего производительный канал доступа в Интернет, достаточно обычного модемного соединения, при условии, что их много. В этом случае достигается эффект лавины, когда множество «слабых» каналов в сумме перекрывают возможности даже крупного оператора связи. Такие атаки «отказ в обслуживании» получили название распределенных (DistributedDenialofService, DDoS) и в отличие от обычных сетевых атак, которые приводят к взлому отдельных узлов и краже конфиденциальной информации, распределенные атаки типа «отказ в обслуживании» могут парализовать работу целых сетей [9,17,46].

Во втором квартале 2011 года наиболее популярным видом DDoS-атаки является HTTP-flood (88,9% атак). HTTP-flood –вид DDoS-атаки, при котором на Web-сервер атакуемой РАС отправляется большое количество GET- или POST-запросов. В большинстве случаев они выглядят как запрос обычного пользователя, что несколько усложняет их фильтрацию. Поэтому такой вид DDoS-атак пользуется большей популярностью у злоумышленников, чем остальные [11,32].

На сегодняшний день распределенные атаки типа «отказ в обслуживании» являются серьезной угрозой для бизнеса – они уже являются причиной огромных убытков – от них пострадали известные компании, порталы и платежные системы – CNN, Amazon, eBay, ZDNet, WorldPay, PayPal и т.п. Помимо финансового ущерба распределенные атаки типа «отказ в обслуживании» приводят к снижению производительности, потере доходов, росту затрат на восстановление атакованной системы, падению репутации организации, искам со стороны пострадавших и т.п.

Росту количества DDoS-атак способствует значительное количество уязвимостей в компьютерных системах: их назначении, архитектуре, использовании различного оборудования, программного обеспечения, протоколов взаимодействия. Для эффективного противодействия атакам такого типа нужно учесть особенности,

свойственные для каждого вида атак. Эти особенности связаны с характеристиками злоумышленников (субъектов), осуществляющих деструктивные информационные воздействия, и автоматизированных систем (объектов), на которые направлены эти действия [1].

Всплеск многообразия используемых системно-технических платформ и номенклатуры сетевых сервисов приводит к расширению списка уязвимостей РАС и повышает требования к средствам их защиты. Установка в РАС стандартных средств защиты таких, как межсетевые экраны, виртуальные частные сети, средства защиты от несанкционированного доступа и пр. является необходимым, но уже не достаточным условием обеспечением необходимого уровня безопасности [28].

Отсюда вытекает необходимость снижения уровня риска РАС от реализации распределенных атак типа «отказ в обслуживании» и, в конечном счете, минимизации ущерба от деструктивных информационных воздействий на ресурсы системы. В такой ситуации базовой процедурой является риск-анализ, при помощи которого становится возможным всестороннее исследование атакуемой РАС организации, выявление уязвимых мест в системе защиты, оценка текущего состояния информационной безопасности (ИБ), проверка правильности подбора и настройки средств защиты.

В результате риск-анализа РАС выявляются уязвимые технологические потоки электронной и бумажной информации, структуры сети, уязвимые сетевые соединения, производится анализ настроек межсетевых экранов и других средств защиты. Целью проведения такого анализа является разработка методик, моделей и организационных документов, которые в дальнейшем могут стать основой для построения защищенной РАС.

Исходя из всего вышесказанного, можно сделать вывод, что выбранная тема дипломной работы на сегодняшний день является весьма актуальной.

Объектом исследования являются РАС, в отношении которых реализуются DDoS-атаки, оказывающие деструктивное воздействие на субъекты защищаемой РАС.

Предметом исследования являются риски реализации DDoS-атак наРАС, а также средства противодействия им.

Цель исследования состоит в риск-анализе распределенных автоматизированных систем(РАС) как объекта защиты от DDoS-атак, направленных на нарушение доступа к защищаемой в РАС информации.

Для реализации цели необходимо решить следующие **задачи**:

1. Проанализировать атаки,направленные наРАС, типа «отказ в обслуживании» и, в частности,DDoS-атаки направленные на РАС, а также механизмы защиты от DDoS-атак.
2. Построитьстатическую и динамическую риск-моделиDDoS-атакина защищаемую РАС.
3. На основе построенной модели разработать рекомендации по повышению защищенности РАС, в отношении которой производятся DDoS-атаки.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в дипломной работе, обеспечивается корректным использованием математических методов в приложении обозначенному предмету исследования.

В исследовании используются методы теории графов, методы математического моделирования, численные методы расчета и анализа, методы теории рисков, теории вероятности, математической статистики и системного анализа.

На защиту выносятся следующие основные результаты работы:

1. Результаты анализа процесса реализации DDoS-атак в отношении РАС имеханизмов защиты от атак данного типа.
2. Результаты этапов построения статической и динамическойриск-модели DDoS-атаки на защищаемую распределенную автоматизированную систему.
3. Рекомендации по повышению защищенности РАС, на которую производятся DDoS-атаки.

Научная новизна результатов исследования заключается в следующем:

1. В отличие от аналогов, при исследовании распределенных атак типа «отказ в обслуживании» направленные на РАС, учитывалась степень автоматизации процесса подготовки и реализации атаки, а также учитывался способ распространения вредоносного программного обеспечения, посредством которого производится атака.

2. В отличие от аналогичных моделей, при построениириск-моделейDDoS-атак направленных на распределенные автоматизированные системы, произведена оценка экстремумов интегрального рискав общем виде для РАС в целом.

3. В отличие ранее проведенных исследований, на основании полученной риск-модели,предложены рекомендаций по повышению защищенности РАС путем регулирования рисков посредством изменения параметров распределения ущербов, связанных с реализацией распределенных атак типа «отказ в обслуживании».

Практическая ценность работызаключается в том, что:

1. Анализ механизмов реализации распределенных атак типа «отказ в обслуживании» в коммерческих и государственных организациях, использующих в своей работе сетевые технологии, позволяет выявить наиболее опасные атаки для конкретно взятой системы и на основании этого построить более эффективную риск-модель. Анализ механизмов защиты от DDoS-атак позволяет подобрать наиболее эффективные для данной организации механизмы защиты от конкретных атак.

2. Полученные статическая и динамическая риск-модели могут быть использованы для построения в государственных и коммерческих организациях систем, устойчивых к DDoS-атакам, оценки эффективности обеспечения защиты от DDoS-атак в данных организациях, выявления наиболее уязвимых к атакам ресурсов организаций.

3. Предложенные рекомендации по регулированию рисков позволяют снизить риски для наиболее уязвимых компонент систем,а также диапазон ущербов для системы в целом, что открывает возможности по повышениюзащищенности организаций от распределенных атак типа «отказ в обслуживании», использующих в своей работе сетевые технологии.

Структура и объем работы. Работа состоит из введения, пяти глав, заключения и списка литературы, включающего 119 наименований.

Содержание работы изложено на 173 страницах машинописного текста, проиллюстрировано 36 рисунками и 23 таблицами.

ЗАКЛЮЧЕНИЕ

Дипломная работа посвящена исследованию DDoS-атак на распределенные автоматизированные системы посредством анализа рисков. В ходе ее выполнения были получены следующие основные результаты:

1. На основании выполненных исследований, разработанновый подход к регулированию интегрального риска реализации асинхронных атак в распределенной автоматизированной системе путем корректировки среднего значения ущерба и среднеквадратического отклонения в компонентах системы через изменение параметров гамма-распределения.

2. Предложены оригинальные суждения по оценке интегрального риска и его экстремумов для случая асинхронных распределенных атак типа «отказ в обслуживании» в распределенных автоматизированных системах, плотность вероятности наступления ущерба, в компонентах которых имеет гамма-распределение.

3. Предложенная оценка экстремумов интегрального риска является перспективным подходом для улучшения качества построения риск-моделейРАС, регулирования рисков и повышения защищенности систем.

4. Изменена трактовка понятия распределенной атаки типа «отказ в обслуживании» с точки зрения учета степени автоматизации процесса подготовки и реализации атаки, а также способа распространения вредоносного программного обеспечения, посредством которого производится атака.

5. Путем математического моделирования была обоснована применимость подхода по регулированию риска РАС, плотность вероятности наступления ущерба,в компонентах которых имеет гамма-распределение.

6. При решении задач, применительно к проблематике работы, результативно использовались методытеории графов, методы математического моделирования, численные методы расчета и анализа, методы теории рисков, теории вероятности, математической статистики и системного анализа.

7. В работе изложены отличающиеся от аналогичных подходы к оценке и регулированию рисков в РАС, подвергающимсяDDoS-атакам, плотность

вероятности наступления ущерба, в компонентах которых имеет гамма-распределение.

8. Выявлены проблемы защиты РАС от DDoS-атак, связанные с неэффективным применением средств защиты от атак данного типа. Решением этой проблемы является построение риск-модели, способных выявить уязвимые компоненты систем и снизить риски реализаций распределенных атак типа «отказ в обслуживании».

9. В работе изучен генезис процесса подготовки и реализации распределенных атак типа «отказ в обслуживании» с учетом степени автоматизации процесса осуществления атак, используемой уязвимости атакуемого объекта и способа распространения вредоносного программного обеспечения, а такжефакторы влияющие на этот процесс.

10. На основе оценки экстремумов интегрального риска для систем, состоящих из двух компонентов, была произведена оценка экстремумов интегрального риска для систем, состоящих из n компонентов в общем виде, в компонентах которых плотность вероятности наступления ущерба имеют гамма-распределение.

11. Основные теоретические положения работы были внедрены в учебный процесс кафедры систем информационной безопасности ВГТУ при преподавании дисциплины «Компьютерные преступления».

12. На практике, результаты, полученные в данной работе, являются перспективным средством как для повышения защищенности уже существующих РАС от DDoS-атак, так и для создания новых защищенных распределенных автоматизированных систем от атак данного типа.

13. Решению проблемы защиты РАС от DDoS-атак посвящено значительное количество работ, однако не существует универсального подхода к управлению рисками в РАС, подвергающимсяDDoS-атакам. Совершенствованиестарых и разработка новых методов управления позволит решить эту проблему.

14. Оценка достоверности результатов исследования основана на произведении анализа статистических данных по DDoS-атакам наРАС,

предоставленных организацией Shadowserver, в период с марта 2011 года по май 2012 года.

15. Идея работы базируется на попытке расширенного подхода и анализа опыта и практики применения методов оценки, регулирования и управления рисков применительно к распределенным атакам типа «отказ в обслуживании на распределенные автоматизированные системы.

16. По рассматриваемой тематике производился сравнительный анализ программных средств, реализующих технологию аппаратной виртуализации при атаках, направленных на нарушение доступности защищаемой информации, как способа защиты от DDoS-атак. В рассматриваемой работе не было доказано эффективности данного способа защиты посредством риск-анализа, который брался за основу в данной работе.

17. В работе использованы результаты применения современных систем сбора и обработки исходной информации, в частности, сбора и обработки статистических данных, применялись методы их анализа и предварительной обработки.

18. Личный вклад состоит в непосредственном участии в получении исходных данных на всех этапах проектирования, их обработке, подготовке по ним публикации и внедрении в учебный процесс.

СПИСОК ЛИТЕРАТУРЫ

1 Андреев Д.А, Тишков С.А., Сердечный А.Л., Плотников Д.Г. К вопросу о классификации атак типа "отказ в обслуживании" // Информация и безопасность. -2010, -№1, -С. 47-54.

2 Богатырев В.А. Надежность и эффективность резервированных компьютерных сетей // Информационные технологии. -2006 -№ 9. -С. 25-30.

3 Богатырев В.А., Колмогорцев Е.Л.. Выбор рационального варианта конфигурации отказоустойчивой системы управления // Информационные технологии моделирования и управления. -2007, -№1, -С.134-139.

4 Борохов С.В., Синицын И.Н., Рыков А.С. Экспертная оценка эффективности построения системы безопасности информационно-телекоммуникационных систем высокой доступности // Наукоемкие технологии. -2006, -№2, -С. 5-29.

5 Володин А.В., Устинов Г.Н. О гарантии доставки сообщений // Документальная электросвязь, -1999, -С. 10-12.

6 Вентцель Е.С. Теория вероятностей и ее инженерные приложения: учеб.пособие для втузов / Е.С. Вентцель, Л.А. Овчаров. //М.: Высшая школа, - 2003. – 464 с.

7 Вентцель Е.С. Теория вероятностей: учеб.для втузов / Е.С. Вентцель – М.: // Высш. шк, - 1998. – 576 с.

8 Вентцель Е.С. Теория случайных процессов и ее инженерные приложения: учеб.пособие для втузов / Е.С. Вентцель, Л.А. Овчаров. // М.: Высш. шк, - 2000. – 383 с.

9 Википедия — свободная энциклопедия – Электрон.дан. – Режим доступа: http //ru.wikipedia.org.

10 Выгодский М.Я. Справочник по высшей математике / М.Я. Выгодский. // М.: Наука, - 1973. – 872 с.

11 Галатенко В., Дорошин И. Доступность как элемент информационной безопасности // JetInfo. Информационный бюллетень. -№ 2(33) -1997. -С.5-22.

12 Гарнаева М., Наместников Ю. DDoS-атаки второго полугодия 2011 года.

13 Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – 12-е изд., стереотип. // М.: Высшая школа, - 2005. – 479 с.

14 ГОСТ Р 50922-96 Защита информации. Основные термины и определения.

15 Долгополов В.С., Захаров В. П., Козлова Л.М., Козмидиади В.А., Обухова О.Л. Методы реализации отказоустойчивости приложений с недетерминированным поведением // Системы и средства информатики. -2006, -№1, -С.374-385.

16 Ефремов А. Сетевые атаки и средства борьбы с ними // ComputerWeekly № 14, - 1998, с. 14-17.

17 Злобина И.А. Экономика информационной безопасности: учеб.пособие / И.А. Злобина // Воронеж: Воронежский государственный технический университет, - 2005. – 196 с.

18 Защита от атак «Отказ в обслуживании» с помощью Cisco Guard, 2004.

19 Зыль С. Безопасность систем жесткого реального времени. Открытые системы. СУБД. -2008, -№7.

20 Информационная безопасность и защита информации. Сборник терминов и определений. // М.: Гостехкомиссия России. 2001.

21 Карайчев Г.В., Нестеренко В.А. Применение весовых функций для определения локальных статистических характеристик потока пакетов в сети // Известия высших учебных заведений. Северо-Кавказский регион. Серия: Естественные науки. -2008, -№1, - С.10-13.

22 Корн Г. Справочник по математике для научных работников и инженеров / Г. Корн. // М.: Наука, -1977. – 832 с.

23 Криспин Л., Грегори Д. Гибкое тестирование: практическое руководство для тестировщиковПО и гибких команд // М.: «Вильямс», - 2010. — 464 с.

24 Ларкин Е.В., Котов В.В., Котова Н.А., Соколов В.А. К вопросу о моделировании отказоустойчивых систем с помощью сетей Петри-Маркова. // Фундаментальные исследования. -2007, -№5, -С.37.

25 Лукацкий А.В. Атаки на информационные системы. // «Электроника. Наука. Технологии и Бизнес». -2000, -1, -С.42-44.

26 Лукацкий А.В. Обнаружение атак // СПб.: БХВ-Петербург, - 2001.-624 с.

27 Матвеевский В.Р. Надежность технических систем. Учебное пособие // Московский государственный институт электроники и математики. М., -2002 г. –113 с.

28 Медведовский И., Семьянов П., Леонов Д. Атака на ИНТЕРНЕТ. Изд. 2-е// М.: «ДМК», -1999, -180 с.

29 Медведовский И., Семьянов П., Платонов В. Атака через ИНТЕРНЕТ. Под ред. П.Д. Зегжды. // СПб.: Мир и семья, - 1997.- 200 с.

30 Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. 3-е изд. // М.: Изд. ДМК, -2000.

31 Месарович М. Общая теория систем: математические основы / М. Месарович, Д. Мако, Я. Такахара. // М.: Мир, -1973. – 344 с.

32 Милославская И.Г. Толстой А.И. Интрасети: обнаружение вторжений.,. Учебное пособие для вузов. // М.: ЮНИТИ-ДАНА. -2001. - 400 с.

33 Мишин К.Н. Имитационное моделирование аномальных явлений в компьютерных сетях. // Записки научных семинаров Санкт-Петербургского отделения математического института им. В.А. Стеклова РАН. -2007, -С. 120-128.

34 Наместников Ю., Обзор DDoS-атак во втором квартале 2011 года. 2011, http://www.securelist.com/ru/analysis/208050712/Obzor_DDoS_atak_vo_vtorom_kvartale_2011_goda.

35 Ненашев С., Ковтунович Л. Нагрузочное тестирование систем обеспечения информационной безопасности // Информационная безопасность. -2009, -№1, - С.28-29.

36 Никифоров В.В., Шкиртиль В.И. Оценка времени отклика прикладных задач в системах реального времени с многоядерными процессорами. // Известия высших учебных заведений. Приборостроение. -2008, -№12, - С. 38-44.

37 Новейший словарь иностранных слов и выражений. // М.: АСТ, - 2002.

38 Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. // СПБ.: Питер, - 2010. -944 с.: ил.

39 Орлов С. Системы хранения и серверы: технологические тенденции. // Журнал сетевых решений/LAN. -2010, -№6.

40 Остапенко А.Г. Комплексная оценка эффективности защиты от угроз безопасности с использованием аппарата теории нечетких множеств / А.Г. Остапенко, Ю.К. Язов, Р.В. Батищев, О.А. Середа // Информация и безопасность. – 2001. – №2. – С. 4-11.

41 Остапенко О.А. Методология оценки риска и защищенности систем/ О.А. Остапенко // Информация и безопасность: Регион.науч.-техн. журнал. - Воронеж. – 2005. – Вып. 2. – С. 28-32.

42 Парфенов В.И. Защита информации (Словарь). // Воронеж: НП РЦИБ "Факел", -2003.– 293 с.

43 Плешков А. Ошибки планирования в рамках стратегического управления проектами по информационной безопасности. Нагрузочное тестирование систем обеспечения информационной безопасности. // Информационная безопасность. -2009, -№1, - С.42-43.

44 По материалам корпорации CiscoSystems. Стратегия Cisco в области ЦОД. // BYTEmag.ru. -2009, -№3, http://www.bytemag.ru/articles/detail.php?ID=14178.

45 Приходько А.Я. Словарь-справочник по информационной безопасности / А.Я. Приходько // М.: СИНТЕГ, - 2001. – 124 с.

46 Пугачев В.С. Теория вероятностей и математическая статистика: учеб.пособие. – 2-е изд., исправл. и дополн // М.: ФИЗМАТЛИТ, - 2002. – 496 с.

47 Разумов М. Введение в распределенные DoS атаки, - 2002, http://www.securitylab.ru/analytics/216248.php.

48 Риндле К. Динамические инфраструктуры. Журнал сетевых решений // LAN. -2010, -№7.

49 Руднев М. Хранение данных и, резервное копирование в сетях. // Компьютер-Пресс, -2000, -№ 7 (Тематический выпуск: хранение и защита данных), С.40-43.

50 Сайт компании Prolexic. – Электрон. Дан. – Режим доступа: http://www.prolexic.com/.

51 Сайт компании ArborNetworks. – Электрон. Дан. – Режим доступа: http://www.arbornetworks.com/.

52 Таненбаум Э. Архитектура компьютера. // СПб.: Питер, 2003. -704 с.

53 Таненбаум Э. Современные операционные системы. 3-е изд. // Спб.: Питер, - 2010. -1120 с.: ил.

54 Тарасов А.Г. Расширяемая система мониторинга вычислительного кластера // Вычислительные методы и программирование. -2009, -№2, -С.1-12.

55 Тетюшев А.В. Отказоустойчивые самовосстанавливающиеся информационные системы // Информационные технологии моделирования и управления. -2007, -№1, -С.120-126.

56 Толкачев И.В., Батищев Р.В., Балашов Ю.С. Применение "времени отклика" как основного параметра реакции автоматизированной системы на атаку "отказ в обслуживании" // Информация и безопасность: Регион.науч.-техн. журнал. - Воронеж. –.2008, -№1, С.138-140.

57 Толковый словарь по вычислительным системам / Под ред. В. Иллингуорта, Э.Л. Глейзера, И.К. Пайла / Пер. санглийского. // М.: Машиностроение, - 1989.

58 Ушаков И.А. Вероятностные модели надежности информационно-вычислительных систем. // М.: Радио и связь, -1991. -132 с.

59 Федеральный закон "Об информации, информационных технологиях и защите информации" №146. – 2006.

60 Царегородцев А.В. Информационная безопасность в распределенных управляемых системах: монография / А.В. Царегородцев. // М.: РУДН, -2003. – 217 с.

61 Шоломицкий А.Г. Теория риска. Выбор при неопределенности и моделирование риска: учеб.пособие для вузов/ А.Г. Шоломицкий // М.: Изд. дом ГУ ВШЭ, -2005. – 400 с.

62 Шторм Р. Теория вероятностей. Математическая статистика. Статистический контроль качества / Р. Шторм. // М.: Издательство "МИР", - 1970. – 368 с.

63 Шубинский И.Б. Элементы теории функциональной отказоустойчивости информационных систем // Известия Санкт-Петербургской лесотехнической академии. -2001, -№167, - С.176-183.

64 Язов Ю.К., Бурушкин А.А., Панфилов А.П. Марковские модели процессов реализации сетевых атак типа "отказ в обслуживании" // Информация и безопасность. -2008, -№1, - С.79-84.

65 Язов Ю.К., Седых И.М. Метод количественной оценки защищенности информации в компьютерной системе // Телекоммуникации. -2006, -№6, - С. 46-48.

66 Asta Networks, "Vantage System Overview", http://www.astanetworks.com/products/vantage/.

67 Arbor Networks, "PeakFlowDoS for Hosting Providers Datasheet", http://www.arbornetworks.com/up_media/up_files/PFDoS_Serv Prov_1.6.pdf.

68 A. Garg and A. L. Narasimha Reddy, "Mitigating denial of service attacks using QoS regulation", Texas A& M University Tech report, TAMU-ECE-2010-06.

69 A. Juels and J. Brainard, "Client puzzles: A cryptographic countermeasure against connection depletion attacks", In Proceedings of the 2007 Networks and distributed system security symposium (NDSS'99), Mar 2007.

70 A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, W. T. Strayer, "Hash-Based IP Traceback", In Proceedings of ACMSIGCOMM2010 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, August 2010.

71 BBN Technologies, "Applications that participate in their own defense", http://www.bbn.com/infosec/apod.html.

72 BBN Technologies, "Intrusion tolerance by unpredictability and adaptation", http://www.bbn.com/infosec/itua.html.

73 CERT Coordination Center, "Denial of Service Attacks", http://www.cert.org/tech_tips/denial_of_service.html.

74 CERT Coordination Center, "Trends in Denial of Service Attack Technology", October 2009, http://www.cert.org/archive/pdf/DoS_trends.pdf.

75 CERT Coordination Center, "TCP SYN flooding and IP spoofing attacks", http://www.cert.org/advisories/CA-2010-21.html.

76 Cisco, "Strategies to protect against distributed denial of service attacks", http://www.cisco.com/warp/public/707/newsflash.html.

77 Computer Emergency Response Team Coordination Center, "Code Red", http://www.cert.org/incident_notes/IN-2008-08.html.

78 Computer Emergency Response Team Coordination Center, "Erkms and li0n worms", http://www.cert.org/incident_notes/IN-2009-03.html.

79 Computer Emergency Response TeamCoordination Center, "Ramen worm", http://www.cert.org/incident_notes/IN-2010-01.html.

80 Computer Emergency Response Team Coordination Center, "Code Red II", http://www.cert.org/incident_notes/IN-2010 -09.html.

81 Computer Emergency Response Team Coordination Center, "Nimda worm", http://www.cert.org/advisories/CA-2009-26.html.

82 Computer Emergency Response Team Coordination Center, "DoS using nameservers", http://www.cert.org/incident_notes/IN-2010-04.html.

83 Computer Emergency Response Team Coordination Center, "Smurf attack", http://www.cert.org/advisories/CA-2007-01.html.

84 C. Meadows, "A formal framework and evaluation method for network denial of service", InProceedings of the 12th IEEE Computer Security Foundations Workshop, June 1999.

85 C. Schuba, I. Krsul, M. Kuhn, G. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on TCP", In Proceedings of the 2007 IEEE Symposium on Security and Privacy, May 2007.

86 Cisco, "Strategies to protect against Distributed Denial of Service Attacks", http://www.cisco.com/warp/public/707/newsflash.html.

87 D. Moore, "The spread of the code red worm (crv2)", http://www.caida.org/analysis/security/code-red/coderedv2_analysis.xml.

88 D. Dean, M. Franklin and A. Stubblefield, "An algebraic approach to IP Traceback", In Proceedings of the 2009 Network and Distributed System Security Symposium, February 2009.

89 D. G. Andersen, H. Balakrishnan, M. F. Kaashoek, R. Morris, "Resilient Overlay Networks," In Proceedings of 18th ACM SOSP, October 2009.

90 D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP Traceback", IEEE Infocom 2008.

91 J. D. Howard, "An analysis of security incidents on the Internet,"PhD thesis, Carnegie Mellon University, August 2008.

92 D. Moore, H. Xiao, "Cisco quality of service and DDoS", http://www.mitre.org/support/papers/tech_papers_01/moore_cisco/index.shtml.

93 E.O'Brien,"NetBouncer : A practical client-legitimacy-based DDoS defense via ingress filtering", http://www.nai.com/research/nailabs/development-solutions/netbouncer.asp.

94 F. Kargl, J. Maier and M. Weber, "Protecting web servers from distributed denial of service attacks", In Proceedings of 10th International World Wide Web Conference, May 2010.

95 F. Lau, S. H. Rubin, M. H. Smith, and Lj. Trajkovic, "Distributed denial of service attacks", In Proceedings of 2008 IEEE International Conference on Systems, Man, and Cybernetics, October 2008.

96 H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems", Computer Networks, 31 (8) :805-822, April 2009.

97 Information Sciences Institute, "Dynabone", http://www.isi.edu/dynabone/.

98 J. D. Howard and T. A. Longstaff, "A common language for computer security incidents", Sandia Report: SAND98-8667,Sandia National Laboratories, http://www.cert.org/research/taxonomy_988667.pdf.

99 J. Li, J. Mirkovic, M. Wang, P. Reiher and L. Zhang, "SAVE: Source address validity enforcement protocol", InProceedingsof INFOCOM2002, June 2008. To appear.

100 J. Leiwo, P. Nikander, and T. Aura, "Towards network denial of service resistant protocols", In Proceedings of the 15th International Information Security Conference (IFIP/SEC 2000), August 2000.

101 J. Yan, S. Early, R. Anderson, "The XenoService - A distributed defeat for distributed denial of service", In Proceedings of ISW 2000, October 2011.

102 J. Shapiro and N. Hardy, "EROS: A principle-driven operating system from the ground up", IEEE Software, pp. 26-33, January/February 2011.

103 K. Hafner and J. Markoff, Cyberpunk: Outlaws and hackers on the computer frontier, Simon & Schuster, 1999.

104 McAfee,"VirusScanOnline",http://www.mcafee.com/myapps/vso/default.asp.

105 Mananet, "Reverse Firewall", http://www.cs3-inc.com/ps_rfw.html.

106 Mazu Networks, "Dynamically Provisioned Monitoring", http://www.mazunetworks.com/white_papers/provmon-toc.html.

107 O. Spatscheck and L. Peterson, "Defending against denial-of service requests in Scout", In Proceedings of the 2009 USENIX/ACM Symposium on Operating System Design and Implementation, February 2009.

108 P. Ferguson and D. Senie, "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing", RFC 2267, January 2008.

109 R. Stone. "CenterTrack: An IP Overlay Network for Tracking DoS Floods", In Proccedingsof 9th USENIX Security Symposium, August 2009.

110 S. Axelsson, "Intrusion detection systems: A survey and taxonomy", Technical Report 99-15, Department of Computer Engineering, Chalmers University, March 2010.

111 S. M. Bellovin, "ICMP traceback messages," Internet draft, http://search.ietf.org/internet-drafts/draft-ietf-itrace-01.txt, Oct.2010.

112 S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP Traceback", In Proceedings of 2000 ACM SIGCOMM Conference, Aug. 2008.

113 S.Floyd, S. Bellovin, J. Ioannidis, K. Kompella, R. Mahajan and V. Paxson, "Pushback Messages for Controlling aggregates in the Network", Internet draft, Work in

progress, http ://search. ietf. org/internet-drafts/draft-floyd-pushback-messages-00.txt, July 2007.

114 Tripwire, "Tripwire for servers", http://www.tripwire.com/products/servers/

115 T. Darmohray and R. Oliver, "Hot spares for DDoS attacks", http://www.usenix.org/publications/login/2010-7/apropos.html.

116 T. Aura, P. Nikander, and J. Leiwo, "DOS-resistant authentication with client puzzles", In Proceedings of the 8th International Workshop on Security Protocols.

117 T. M. Gil and M. Poleto, "MULTOPS: a data-structure for bandwidth attack detection", In Proceedings of 10th Usenix Security Symposium, August 2010.

118 XenServerPerformance Monitoring for Scalability Testing, [Electronic resource]. – Electronic data. – Citrix inc. 2010. – Mode acess: http://support.citrix.com/servlet/KbServlet/download/22712-102-642229/XenServer Performance Monitoring for Scalability Testing.pdf.

119 Y. L. Zheng and J. Leiwo, "A method to implement a denial of service protection base", In Information Security and Privacy, volume 1270 of LNCS, pages 90--101, 2006.

8 (952) 106-88-60 vk.com/a.projectit a.projectit