алгоритмы решения задачи о медиане графа-модели $G(X,E)$ противника, требующие для своей реализации $\underline{O}(|X|^2)$ арифметических операций.

Широко развитый математический аппарат теории графов, существующие эффективные численные методы их обработки позволяют говорить о значительных перспективах использования взвешенного графа в качестве математической модели при дальнейшем анализе деятельности и структуры различных криминальных групп.

Список литературы

1. *J. D. Farley.* Breaking al qaeda cells: A mathematical analysis of counterterrorism operations (a guide for risk assessment and decision making). Studies in Conflict & Terrorism, 26: 399411, 2003.

2. *Krebs V.E.* Mapping networks of terrorist cells. – Connections 24(3). – 2001. – Pp. 43-52.

3. *Carley K.M., Lee J.S., Krackhardt D.* Destabilizing networks. - Connections 24(3). – 2001. – Pp.79-92.

4. *J.Shetty, J.Adibi.* Discovering Important Nodes through Graph Entropy. The case of Enron Email Database/ In materials of the Eleventh ACM SIGKDD International Conference on knowledge Discovery and Data Mining.- August 21-24, 2005. – Chicago, IL, USA.

5. Brams S.J., Mutlu H., Ramirez S.L. Influence in Terrorist Networks: From Undirected to Directed Graphs. Studies in Conflict & Terrorism. – 2006. – 29. – Pp.703-718.

6. *Кобозева А.А., Хорошко В.А.* Использование взвешенного графа при моделировании террористической сети

7. *Иванов Б.Н.* Дискретная математика. Алгоритмы и программы. – М.: Лаборатория Базовых Знаний, 2001. – 288с.

8. *Новиков Ф.А.* Дискретная математика для программистов. – СПб.: Питер, 2006. – 364 с.

9. *Джордж А., Лю Дж.* Численное решение больших разреженных систем уравнений. – М.: Мир, 1984.- 333 с.

10. *Фихтенгольц Г.М.* Курс дифференциального и интегрального исчисления. – М. Наука, 1969.

11. *Харари Ф.* Теория графов. М.: Мир. - 1973. – 300с.

Надійшла 2.11.2007р.

УДК 004.681.3 **Мороз Е.С.**

СОВРЕМЕННЫЕ СЕТЕВЫЕ АТАКИ И ПРИНЦИПЫ АНОНИМНОСТИ В СЕТИ

Одной из важнейших задач обеспечения нормального функционирования сети Internet является построение сетевой маршрутизации. В Internet маршрутизация осуществляется на сетевом уровне (IP-уровень). Для ее обеспечения в памяти сетевой ОС каждого хоста существуют таблицы маршрутизации, содержащие данные о возможных маршрутах. Каждый сегмент сети подключен к глобальной сети Internet как минимум через один маршрутизатор, а, следовательно, все хосты в этом сегменте и маршрутизатор должны физически располагаться в одном сегменте. Поэтому все сообщения, адресованные в другие сегменты сети, направляются на маршрутизатор, который, в свою очередь, перенаправляет их далее по указанному в пакете IP-адресу, выбирая при этом оптимальный маршрут, используя специальные протоколы маршрутизации: RIP, OSPF и т. д.

Глубокие познания структуры сети и не совершенство протоколов маршрутизации позволяют злоумышленникам осуществлять различные виды сетевых атак. Одной из наиболее известной является типовая удаленная атака "Внедрение в распределенную ВС

ложного объекта путем навязывания ложного маршрута". Для осуществления этой удаленной атаки необходимо подготовить ложное ICMP Redirect Host сообщение, в котором указать конечный IP-адрес маршрута (адрес хоста, маршрут к которому будет изменен) и IP-адрес ложного маршрутизатора. Далее это сообщение передается на атакуемый хост от имени маршрутизатора. Для этого в IP-заголовке в поле адреса отправителя указывается IP-адрес маршрутизатора. На данном этапе реализация такой атаки возможна лишь на старых операционных системах (ОС), начиная с ОС класса Linux 2.0.0, становится практически не возможной.

Современные сетевые атаки столь же многообразны, как и системы, против которых они направлены. Для оценки типов атак необходимо знать некоторые ограничения, изначально присущие протоколу TPC/IP. Изначально сеть Интернет создавалась для связи между государственными учреждениями и университетами с целью оказания помощи учебному процессу и научным исследованиям. В результате в спецификациях ранних версий Интернет-протокола (IP) отсутствовали требования безопасности. Именно поэтому многие реализации IP являются изначально уязвимыми. Через много лет, после множества рекламаций (Request for Comments, RFC), наконец стали внедряться средства безопасности для IP. Однако ввиду того, что изначально средства защиты для протокола IP не разрабатывались, все его реализации стали дополняться разнообразными сетевыми процедурами, услугами и продуктами, снижающими риски, присущие этому протоколу. Рассмотрим типы атак, которые обычно применяются против сетей IP.

Сниффер пакетов - представляет собой прикладную программу, которая использует сетевую карту, работающую в режиме promiscuous mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки). При этом сниффер перехватывает все сетевые пакеты, которые передаются через определенный домен. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (Telnet, FTP, SMTP, POP3 и т.д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют единый пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме «клиент-сервер», а аутентификационные данные передаются по сети в читаемом текстовом формате, то эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам.

IP-спуфинг - происходит в том случае, когда злоумышленник, находящийся внутри корпорации или вне ее, выдает себя за санкционированного пользователя. Это можно сделать двумя способами: он может воспользоваться или IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример — атака DoS, которая начинается с чужого адреса.

Как правило, IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами. Для двусторонней связи злоумышленник должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Некоторые хакеры, однако, даже не пытаются получить ответ от приложений — если главная задача заключается в получении от системы важного файла, то ответы приложений не имеют значения.

Если же злоумышленнику удается поменять таблицы маршрутизации и направить трафик на ложный IP-адрес, он получит все пакеты и сможет отвечать на них так, как будто является санкционированным пользователем.

Отказ в обслуживании - Denial of Service (DoS), без сомнения, является наиболее известной формой атак. Кроме того, против атак такого типа труднее всего создать стопроцентную защиту. Простота реализации и огромные масштабы причиняемого вреда привлекают к DoS пристальное внимание администраторов, отвечающих за сетевую безопасность. Если вы хотите больше узнать об атаках DoS, вам следует рассмотреть их наиболее известные разновидности, а именно: TCP SYN Flood, Ping of Death, Tribe Flood Network (TFN) и Tribe Flood Network 2000 (TFN2K), Trinco, Stacheldracht, Trinity.

Атаки DoS отличаются от атак других типов. Они не нацелены ни на получение доступа к вашей сети, ни на получение из этой сети какой-либо информации, но атака DoS делает вашу сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения. В случае использования некоторых серверных приложений (таких как Web-сервер или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений, и держать их в занятом состоянии, не допуская обслуживания рядовых пользователей. В ходе атак DoS могут использоваться обычные Интернет - протоколы, такие как TCP и ICMP.

Парольные атаки - могут проводиться с помощью методов простого перебора, внедрения троянского коня, а так же применимы IP-спуфинг и сниффинг пакетов. Хотя логин и пароль зачастую можно получить при помощи IP-спуфинга и сниффинга пакетов, злоумышленники нередко пытаются подобрать пароль и логин, используя для этого многочисленные попытки доступа.

Man-in-the-Middle – для реализации данной атаки злоумышленнику нужен доступ к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, передаваемым от провайдера в любую другую сеть, может, к примеру, получить сотрудник этого провайдера. Для атак данного типа часто используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации. Атаки проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

Злоупотребление доверием - этот тип действий не является в полном смысле слова атакой или штурмом. Он представляет собой злонамеренное использование отношений доверия, существующих в сети. Классическим примером такого злоупотребления является ситуация в периферийной части корпоративной сети. В этом сегменте часто располагаются серверы DNS, SMTP и HTTP. Поскольку все они принадлежат к одному и тому же сегменту, взлом любого из них приводит к взлому всех остальных, так как эти серверы доверяют другим системам своей сети. Другим примером является установленная с внешней стороны межсетевого экрана система, имеющая отношения доверия с системой, установленной с его внутренней стороны. В случае взлома внешней системы злоумышленник может использовать отношения доверия для проникновения в систему, защищенную межсетевым экраном. Одной из разновидностей злоупотребления доверием, является переадресация портов - когда взломанный хост используется для передачи через межсетевой экран трафика, который в противном случае был бы обязательно отбракован.

Многие современные сетевые атаки базируются на методах социальной инженерии, к ним в первую очередь относится сетевая разведка.

Сетевая разведка - сбор информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети злоумышленник, как правило, пытается получить о ней как можно больше информации. Сетевая разведка проводится в форме запросов DNS, эхо-тестирования и сканирования портов. Запросы DNS помогают

понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, злоумышленник использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами.

Еще один из способов сетевой атаки заключается в том, что с помощью специальных программ на атакуемый сайт отправляются тысячи e-mail'ов, иногда в них содержатся вирусы, заражающие сайт. Однако, пока подобные акции оказываются малоэффективными — серверы восстанавливают обычный режим работы уже через несколько минут.

Анонимность в сети

Все действия по осуществлению описанных сетевых атак преследуются законом и как следствие, со стороны злоумышленников возникает задача анонимности. Данная задача реализуется, как правило, с помощью использования Tor- сетей и проксирования трафика.

Tor - это сеть, состоящая из виртуальных туннелей, позволяющая повышать степень своей конфиденциальности и безопасности в Интернет. Он также открывает перед разработчиками ПО широкие возможности для создания собственных средств коммуникаций со встроенной функциональностью, связанной с обеспечением повышенного уровня личной защищённости пользователей. Tor создаёт фундамент (основу) для целого класса приложений, позволяющих организациям и частным лицам обмениваться информацией посредством общедоступных сред передачи данных, не ставя при этом под удар собственную конфиденциальность.

Tor самостоятельно не решает всех проблем анонимности (приватности, конфиденциальности). Он фокусируется только на защите данных на этапе передачи. Необходимо использовать протокол-ориентированное ПО, не позволяющее получать от браузера любые сведения, необходимые для автоматической идентификации. Примером такого ПО являются различные веб-прокси, такие как Privoxy, которые могут быть использованы при веб-сёрфинге для блокирования передачи/установки закладок куки (cookies) веб-браузером и сокрытия информации о его типе.

Для защиты анонимности злоумышленнику нужно быть очень внимательным и осмотрительным. Как правило, они нигде не указывают своего настоящего имени или другую указывающую на них информацию в полях веб-форм.

Более эффективно задачу анонимности можно решить используя proxy сервера.

Прокси-сервер (от англ. proxy — «представитель, уполномоченный») — служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс, расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша (в случаях, если прокси имеет свой кэш).

Все типы Proxy-серверов можно разделить на три категории: *шлюзы*, *кэширующие* Proxy-сервера и *анонимные* Proxy-сервера.

Шлюзы чаще всего используются в локальных сетях –Proxy-сервер разделяет один канал между множеством пользователей. "Извне" остальные абоненты сети видят лишь один узел – Proxy-сервер этого провайдера. Клиент дает Proxy-серверу запрос на установку соединения с таким-то сервером и Proxy выполняет ее от своего имени, возвращая ответ сервера клиенту.

Шлюзы в свою очередь делятся на два подтипа – *SOCKS-Proxy* и *шлюзы уровня приложений.*

SOCKS-Proxy работают на сетевом уровне и невидимы для прикладных программ, которые даже не подозревают о существовании Proxy-сервера. От пользователя требуется всего лишь установить Proxy-клиента, выданного ему провайдером. Единственное условие – порты, через которые эти приложения работают, должны быть открыты на Proxy-сервере. *Шлюзы уровня приложений*, как и следует из их названия, работают на прикладном уровне

и взаимодействуют со строго определенными приложениями через заранее оговоренные порты. Причем, программное обеспечение должно быть спроектировано соответствующим образом и явно поддерживать

Кэширующие Proxy в основном представляют собой шлюзы уровня приложений, но, в отличие от них, используются факультативно, т.е. по желанию администратора. Использование таких Proxy позволяет значительно увеличить скорость обмена данными, особенно при соединении с далекими, загруженными серверами. Будучи подключенным к быстрому каналу, гораздо более быстрому, чем модемная линия, кэш-сервер сглаживает провалы и кратковременные "засыпания" удаленного сервера. Полученные данные Proxy сохраняет на своем диске – кэше и, если запрошенный клиентом ресурс уже был загружен какое-то время назад, он сразу же "отдается" ему без обращений к удаленному серверу. *Анонимные Proxy* – анонимными серверами называются те, которые выполняют запрос клиента от своего имени, не разглашая его IP-адреса.

Списки анонимных Proxy серверов доступны как на бесплатных, так и на платных сайтах сети.

Программы применяемые для анонимности

Proxy List Filter - преобразует списки прокси серверов из практически любых форматов (включая HTML) в стандартный вид, понимаемый практически всеми Proxy Checker'ами. Может работать с множеством файлов, объединяя их в один большой список и удаляя дубликаты. Proxy Checker - осуществляет проверку списка HTTP(S) proxy серверов. Позволяет брать списки proxy из файлов разных форматов (HTML & TXT), проверять proxy на анонимность, проверять HTTP proxy на поддержку FTP, HTTPS и proxy chaining. SocksCap - осуществляет SOCKS-ификацию программ (для программ, не умеющих работать с прокси), FreeCap - осуществляет соксификацию программ (для программ, не умеющих работать с proxy). Поддерживает цепочки прокси, умеет работать с SOCKS 4/5, HTTPS proxy и т.д.

Постоянно ведутся работы по созданию анонимных ОС. Так группой разработчиков "Kaos theory" предлагается ОС записанная на загрузочный CD-диск. На таких дисках исчезает проблема накопления "инкриминирующих" файлов в кэше браузера и других программ, опасность перезаписи системных файлов злонамеренными сайтами.

Система основана на одной из наиболее безопасных веток Unix – OpenBSD. Доступ к компьютеру пользователя заблокирован жёстким набором правил и политик безопасности, сетевые пакеты (чтобы не идентифицировать систему) маскируются под Windows XP. Анонимность работы обеспечивается полным туннелированием всех соединений через сеть TOR. При этом уже настроены TOR-соединения для почты, мессенджеров, FTP и других популярных программ.

В последующих версиях ожидается поддержка записи на USB-брелоки, использование Enigmail-GnuPG и Gaim Off-The-Record-мессенджера с возможностью отрицания аутентифицированных сеансов связи.

Защита от атак

Основной задачей разработчиков является усовершенствование сетевых протоколов. Значительное уменьшение количества сетевых атак стало возможным после появления IP Security - комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов; в его состав входят почти 20 предложений по стандартам и 18 RFC. Протокол IPSec является лучшим среди всех других протоколов защиты передаваемых по сети данных, разработанных ранее (включая разработанный Microsoft PPTP), но с другой стороны, в нем присутствует чрезмерная сложность и избыточность. На рынке представлены как программные реализации (например, протокол реализован в операционной системе Windows2000 компании Microsoft), так и программно-аппаратные реализации IPsec - это решения Cisco, Nokia. Несмотря на большое число различных решений, все они довольно хорошо совместимы друг с другом.

Для борьбы с сетевыми атаками используются персональные сетевые экраны. Наиболее известные и зарекомендовавшие себя продукты:

Outpost Firewall; KIS; Jetico Personal Firewall; Norton Personal Firewall; McAfee Firewall; Zone Alarm; Kerio WinRoute Firewall (относится именно к персональным);

Из пакетных сетевых экранов можно отметить Microsoft ISA (Internet Security and Acceleration Server).

Заключение

Интернет-преступность становится еще более сложной и продуманной. Это является результатом консолидации расширяющихся сетевых возможностей и социально-экономических факторов, таких, как экономическое развитие и отсутствие ИТ-занятости. Компьютерные преступники, избегают проблем с законом в тех странах, которые претерпевают серьезные политические проблемы и проблемы безопасности. Очевидно, что проблема надзора за информационными потоками в виртуальном пространстве уже назрела и требует своего решения. В противном случае в ближайшие годы мировому сообществу грозит «шквал» информационных атак, несанкционированных рассылок и даже предполагаются массовые «кибертерракты» как на государственные, так и на корпоративные сети.

Надійшла 16.11.2007р.

УДК 621.391

Дудыкевич В.Б., Томашевский Б.П.

ИССЛЕДОВАНИЕ НЕСИММЕТРИЧНЫХ КРИПТОСИСТЕМ НА АЛГЕБРАИЧЕСКИХ КОДАХ ДЛЯ КАНАЛОВ С АВТОМАТИЧЕСКИМ ПЕРЕСПРОСОМ

Введение

Обеспечение конфиденциальности и целостности передаваемых данных является одной из важнейших задач, стоящих при обмене информации между пользователями. Для ее обеспечения наиболее эффективными являются криптографические методы.

Проведенный анализ [1 - 8] показал, что перспективным направлением в развитии несимметричных криптоалгоритмов для обеспечения конфиденциальности и целостности данных является применение криптосистем с быстрыми (алгебраическими) алгоритмами декодирования, функционирующими в режиме маскирования кодовых слов под случайную последовательность. При этом дешифрование информации для неуполномоченного пользователя (несанкционированный доступ к информационной части сообщения) является NP-полной задачей - декодирование случайного кода. Уполномоченный пользователь, владеющий секретным ключом, расшифровует полученную последовательность быстрыми алгоритмами за полиномиальное время. Такие криптосистемы позволяют, интегрировано обеспечивать защиту и помехоустойчивость информационной части данных в каналах с прямым исправлением ошибок [5-8]. В тоже время большая часть модемных протоколов коррекции ошибок функционирует в режиме автоматического переспроса. Таким образом, актуальным направлением исследований является создание несимметричных кодовых криптосистем с быстрыми алгоритмами шифрования и расшифрования данных для каналов с автоматическим переспросом [7, 8].

Несимметричная кодовая криптосистема Нидеррайтера

В работе [1] впервые предложена кодовая криптосистема, основанная на маскировании проверочной матрицы алгебраического блокового кода. Основное достоинство несимметричной криптосистемы Нидеррайтера состоит в высокой скорости