Определение 8. Алгоритмическая процедура

$$AKG_z(G_z, \vec{X}'; A\lg_AkG_z; \vec{X}'') =$$

$$= G_z, \vec{X}' \frac{AKG_z}{A\lg_AkG_z} \to \vec{X}'' ,$$

реализующая преобразование с помощью графа G_z (z-ЛСВР) вектора входных сигналов $\vec{X}'$ (значения наблюдаемых признаков ОПР) в выходной вектор $\vec{X}''$ (значения целевого признака ОПР) посредством алгоритма $A\lg_AkG_z$, называется **оператором вывода решений (AKG_z –оператором).**

8. Примеры распознавания объектов с помощью запретной логической сети вывода решений

Пример 1. Задана база знаний в виде z-ЛСВР (см. рис. 3) и некоторый объект w со следующими наблюдаемыми признаками: $x_1 = x_{11}$, $x_2 = x_{21}$ и $x_3 = x_{31}$. Необходимо классифицировать объект, т.е. отнести его к одному из следующих классов: x_{41}, x_{42} или x_{43}. Решение задачи:

Шаг 1. Всем значениям целевого признака присвоить значение «1»: $\vec{X}'' = [111]$.

Шаг 2. Подать на вход сети вектор входных сигналов $\vec{X}' = [10:100:10]$.

Шаг 3. Активизировать 1-й уровень логической запретной сети вывода решений. Так как в результате активизации 1-го уровня запретной сети возникло противоречие (комбинация наблюдаемых значений признаков ОПР $x_2 = x_{21}$ и $x_3 = x_{31}$ является запретной), то выполнение алгоритма вывода решений по запретной сети останавливается.

Пример 2. Задана база знаний в виде z-ЛСВР (см. рис. 3) и некоторый объект w со следующими наблюдаемыми признаками: $x_1 = x_{11}$, $x_2 = x_{23}$ и $x_3 = x_{31}$. Необходимо классифицировать объект, т.е. отнести его к одному из следующих классов: x_{41}, x_{42} или x_{43}. Решение задачи:

Шаг 1. Всем значениям целевого признака присвоить значение «1»: $\vec{X}'' = [111]$.

Шаг 2. Подать на вход сети вектор входных сигналов $\vec{X}' = [10:001:10]$.

Шаг 3. Активизировать 1-й уровень логической запретной сети вывода решений. Противоречие не возникло.

Шаг 4. Активизировать И/ИЛИ граф G_z.

Шаг 5. С выходов логической запретной сети вывода решений снять вектор выходных сигналов $\vec{X}'' = [010]$. Делаем вывод, что целевой признак $x_4 = x_{42}$.

9. Выводы

Научная новизна полученных результатов заключается в том, что в рамках t-квантовой инженерии знаний впервые предложен метод принятия идентификационных решений, где в качестве решающего правила применяется запретная логическая сеть вывода решений, которая восстанавливается из импликативной базы квантов знаний. Данный метод позволяет, в отличие от t-квантового метода принятия решений на основе решающих деревьев, проверять ОПР при распознавании на противоречивость построенной БКЗ.

Предложенный метод был положен в основу программной разработки интеллектуального ядра знаниеориентированной системы поддержки принятия решений. Экспериментальные данные показали, что по сравнению с методом принятия решений на основе решающих деревьев точность распознавания повысилась на 40%.

Литература: 1. *Сироджа И.Б., Петренко Т.Ю.* Метод разноуровневых алгоритмических квантов знаний для принятия производственных решений при недостатке или нечёткости данных. К.: Наук. думка, 2000. 247с. **2.** *Сироджа И.Б.* Квантовые модели и методы искусственного интеллекта для принятия решений и управления. К.: Наук. думка, 2002. 427с. **3.** *Сироджа И.Б.* Квантовые модели и методы инженерии знаний в задачах искусственного интеллекта // Искусственный интеллект. 2002. №3. С.161-171.

Поступила в редколлегию 24.07.2004

Рецензент: д-р техн. наук, проф. Путятин Е.П.

Варфоломеева Илона Владимировна, аспирант, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ». Научные интересы: методы искусственного интеллекта для принятия решений в условиях неопределенности. Адрес: Украина, 61000, Харьков, ул. Чкалова, 1, к. 204, тел. 707-47-35, 707-40-64, e-mail: anoli_v@ukr.net.

УДК 681.324.01

ЗАЩИТА ИНФОРМАЦИИ В INTERNET-СЕТЯХ

НЕМЧЕНКО В.П., ДАО ТХУ ФЫОНГ

Рассматриваются вопросы техники осуществления атак на Internet с учетом уязвимостей существующих сетевых протоколов. Показываются пути предупреждения и устранения атак, в том числе и за счет перехода на протоколы стека нового поколения TCP/IPv6.

Введение. Широкое развитие и использование новых Internet-технологий в последнее время выдвигает на первый план вопросы, связанные с проблемами обеспечения безопасности информации в сетях. Среди новых Internet-приложений можно назвать такие как всевозможные банковские услуги, электронная коммерция (e-commerce), услуги различных туристических фирм и т.п. Естественно, что и организации, предоставляющие услуги, и их клиенты кровно заинтересованы в том, чтобы полностью избежать несанкционированного доступа третьих лиц к передаваемой по сети информации.

Вопросы классификации и анализа всевозможных сетевых атак достаточно подробно рассмотрены в публикациях, например в [1]. Подчеркнем, что исходя из семиуровневой модели OSI (Open System Interconnection) основной акцент в данной работе делается на анализе вопросов обеспечения инфор-

мационной безопасности в Internet-сетях, что представляет собой *цель* исследования.

Анализируя причины, по которым сетевые атаки могут иметь место, можно выделить три основных класса недостатков, встречающихся сегодня в области защиты сетевой информации. Это – недостатки, связанные с техническим обеспечением сетевых решений, уязвимости сетевых протоколов и, наконец, проблемы, вносимые человеческим фактором. Последними занимается новая область науки – социальный инжиниринг (Social Engineering). Естественно, что решать данные проблемы имеет смысл в соответствии с приведенной классификацией.

Топология сети типа "общая шина". Как известно, на сегодняшний день наиболее распространенной и применяемой на практике является Ethernet-технология, базирующаяся на топологии «общая шина». На рис. 1 показана структура сегмента, построенного по данной топологии. Как видим, вся информация в сегменте сети циркулирует по общей шине и для того, чтобы ее получить, не требуется никаких особых ухищрений. Достаточно быть подключенным к данной шине и активизировать программу "sniffer", которая позволяет «прослушивать» весь трафик в общей шине.

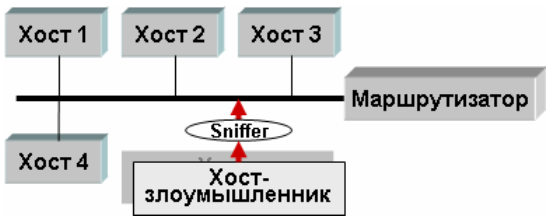

Рис. 1. «Прослушивание» трафика в Ethernet-сегменте

Предположим, на IP-адрес одного из узлов сегмента извне поступил пакет. Ближайший маршрутизатор, подключенный к данному сегменту, посылает на шину по ARP-протоколу (Address Resolution Protocol) так называемый ARP-запрос в виде IP-адреса, в соответствие которому требуется поставить MAC-адрес (адрес сетевой карты) искомого узла. Все узлы сегмента получают этот запрос, но лишь один узел, которому соответствует данный IP-адрес, посылает в шину ARP-ответ, т.е. свой MAC-адрес. В результате маршрутизатор доставит пакет данному узлу.

Теперь представим, что один из узлов сегмента является злоумышленником, который стремится перехватить пришедший пакет. Для этого он должен опередить запрашиваемый узел и первым послать свой ответ. Тогда пришедший после него истинный ARP-ответ будет проигнорирован маршрутизатором как ложный. В результате канал связи будет перехвачен злоумышленником и он сможет получить чужой пакет.

Естественно, здесь показана лишь суть атаки без анализа подробностей ее реализации. Но даже из этого примера видно, что угроза данного типа атаки является вполне реальной.

Для того чтобы исключить возможность прослушивания трафика в сегменте, нужно отказаться от топологии «общая шина» и перейти к топологии «выделенная линия», при которой каждый узел связан со всеми остальными выделенной линией. В этом случае полученный пакет доставляется маршрутизатором адресату напрямую. Следовательно, само понятие «прослушивание канала» теряет для злоумышленника всякий смысл, если он не находится непосредственно на пути следования пакета, поскольку в этом случае ему потребуется подключиться для прослушивания напрямую к каждой выделенной линии, что практически невыполнимо.

Вместе с тем, такая топология на практике труднореализуема, поскольку даже средней величины сегмент будет иметь весьма сложную и не гибкую структуру.

Структура сети типа "звезда". На практике, с точки зрения безопасности, имеет смысл использовать структуру типа «звезда», в центре которой находится коммутатор (свитч), к которому подсоединены узлы.

Вместе с тем, при реализации такой структуры будет нарушен один из основополагающих принципов сетевой реализации – живучесть, т.е. способность сети (в нашем случае сегмента) сохранять свою работоспособность даже при выходе из строя некоторого количества компонентов ее составляющих. В нашем случае выход из строя коммутатора полностью парализует работу сегмента.

Выделенные линии. Частичным выходом из сложившейся ситуации может быть компромиссное решение – разбиение подсетей на группы, связанные выделенными линиями, внутри которых узлы подключены к общей шине.

На рис. 2, а показана структура простейшего сегмента из четырех узлов, реализованного по принципу «выделенная линия». На рис. 2, б приведена структура типа «звезда» с коммутатором в качестве центральной точки.

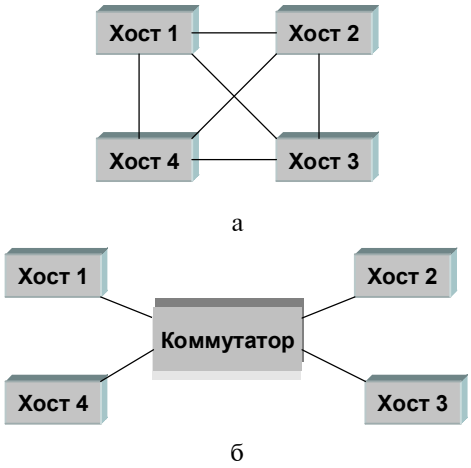

Рис. 2. Структура сегмента: а – выделенная линия; б – звезда с коммутатором в качестве центральной точки

Атаки и защиты от них на сетевом уровне. Рассмотрим теперь вопросы реализации атак и защиты от них на сетевом уровне.

Как известно, одним из наиболее защищенных протоколов транспортного уровня является TCP-протокол, поскольку на этапе установления связи в сети создается виртуальный канал в процессе так называемого «рукопожатия» (handshake) [2]. При этом узлы, устанавливающие связь, постоянно обмениваются аутентифицирующей информацией, базирующейся на некоторых исходных идентификаторах, сгенерированных «случайным» образом. Однако, как показала практика, приведенные выше меры безопасности не дают полной гарантии защиты от сетевых атак.

Наиболее эффективным методом защиты передаваемой по сети информации является ее криптографическая защита. Одним из применяемых в настоящее время криптографических стандартов является принятый относительно недавно стандарт SSL (Secure Socket Layer), использующий принцип открытого ключа и базирующийся на методе Дифи-Хелмана (Diffie−Hellman). Однако его использование в Internet-сетях поколения TCP/IPv4 (которые распространены сейчас повсеместно) не является обязательным и, следовательно, мы не можем говорить о гарантированной защите передаваемой по сетям информации.

В последнее время во всем мире осуществляется переход на сетевые технологии нового поколения, основанные на использовании стека протоколов TCP/IPv6. Характерной особенностью новой технологии является то, что вся информация в сети передается с использованием криптографической защиты, базирующейся на принципах, описанных выше. На рис. 3 показан процесс формирования криптографического контекста протоколом TCPv6.

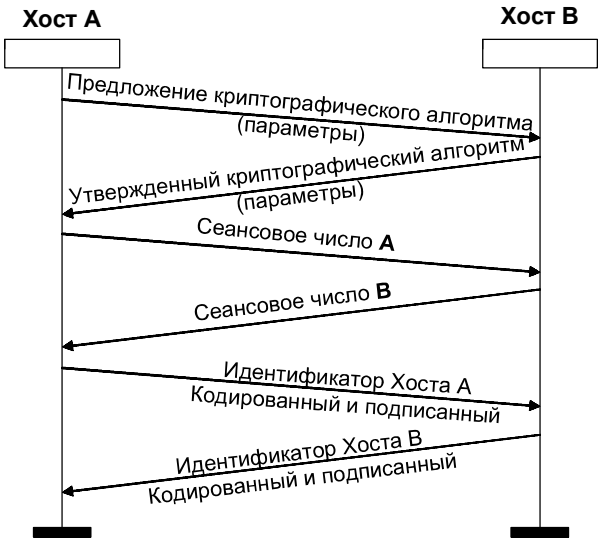

Рис. 3. Формирование криптографического контекста протоколом TCPv6

Как видно из рис. 3, фаза формирования криптографического контекста состоит из четырех последовательных шагов. Пусть хост А является инициатором установления связи с хостом В. Прежде всего, оба узла согласовывают общий криптографический алгоритм из числа наиболее распространенных и допускаемых стандартом. Предположим, это DES-алгоритм. Среди прочих параметров обсуждается также и сеансовый параметр g.

Затем хост А посылает хосту В число $A=g^x$, вычисленное на основе своего секретного ключа x. В свою очередь, хост В посылает хосту А число $B=g^y$, где y − секретный ключ хоста В. Таким образом, общий сеансовый открытый ключ будет равен g^{xy} [1].

После этого хосты обмениваются идентификаторами, подписанными своими секретными ключами и кодированными общим открытым ключом. Таким образом, фаза аутентификации, предшествующая обмену информацией, завершена. Далее вся информация будет передаваться в закодированном виде, что значительно снижает риск несанкционированного доступа к ней.

Что касается сетевой атаки на уровне маршрутизации, то практически все атаки данного вида основаны на фальсификации IP-адреса узла, сформировавшего пересылаемый по сети пакет. Имеется две возможности защититься от таких атак.

Прежде всего, необходимо, чтобы каждый маршрутизатор проверял, соответствует ли IP-адрес узла, сгенерировавшего пакет, IP-адресу его подсети. Если не соответствует − пакет должен быть отброшен маршрутизатором.

Вторая возможность заключается в том, чтобы в заголовке пересылаемого пакета были зарезервированы специальные поля, в которых каждый маршрутизатор, через который прошел пакет, оставлял информацию о своем IP-адресе. Таким образом, в конечной точке можно проанализировать весь пройденный маршрут и удостовериться, что пакет был сгенерирован именно тем узлом, чей IP-адрес прописан в заголовке. Однако здесь возникает проблема, связанная с тем, что мы наперед не можем знать количество проходимых маршрутизаторов, а следовательно, невозможно заранее определить количество резервируемых полей.

Заключение. В завершение анализа вопросов защиты информации в сетях отметим, что практически все распространенные современные операционные системы не предусматривают возможность защиты от так называемого «шторма запросов на связь TCP». А именно, нет ограничения на количество таких запросов, посылаемых в единицу времени одним и тем же узлом. Эта уязвимость операционных систем позволяет злоумышленнику переполнить входной стек запросов на связь с тем, чтобы вывести данный узел из рабочего состояния.

Следовательно, чтобы устранить угрозу атак подобного рода, следует ограничить количество запросов в очереди, сгенерированных одной и той же подсетью. А для этого, как было отмечено выше, нужно контролировать процесс маршрутизации в сетях.

В заключение отметим, что, несмотря на чрезвычайную важность, задача защиты информации в сетях до сих пор весьма далека от своего решения. Большой шаг в этом направлении будет сделан при переходе на сетевые протоколы нового поколения TCP/IPv6. Вместе с тем, авторы, руководствуясь древней мудростью «Кто осведомлен – тот вооружен», будут удовлетворены, если пользователи Internet, прочитавшие данную статью, задумаются о том, насколько хорошо защищен их хост.

Мы хотели бы обратить внимание читателей на то, что прежде чем разработать и внедрять на практике политику сетевой безопасности, следует задать себе вопрос – насколько адекватна цена защищаемой информации тем затратам, которые будут иметь место при ее защите. Необходимо принять во внимание следующую аксиому: требования обеспечения безопасности сетевой информации всегда находятся в противоречии с такими сетевыми характеристиками как функциональность, быстродействие, удобство работы и т.п. Поэтому приступать к осуществлению политики сетевой безопасности следует лишь хорошо взвесив все «за» и «против». При этом нужно проанализировать и определить возможность использования последних наработок в данной области. В частности тех, о которых шла речь выше.

Литература: 1. *Медведовский И.Д. и др.* Атака на Internet. Изд. ДМК, 1999. **2.** *Nemchenko V., Schaff A.* Vulnerabilities and test of Internet protocols / Radioelectronika i Informatika. 2003. No.3 P.194-195.

Поступила в редколлегию 28.09.2004

Рецензент: д-р техн. наук, проф. Кривуля Г.Ф.

Немченко Владимир Петрович, канд. техн. наук, профессор ХНУРЭ. Научные интересы: техническая диагностика, сетевые технологии. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 702-14-17, e-mail: vpn@kture.kharkov.ua.

Дао Тху Фыонг, магистрант ХНУРЭ. Научные интересы: использование сетевых технологий для решения экономических задач. Адрес: Украина, 61166, Харьков, пр. Ленина, 14; тел. 702-18-05.

УДК 681.326

МЕТОДЫ И СРЕДСТВА СОЗДАНИЯ ЦИФРОВЫХ СИСТЕМ НА КРИСТАЛЛАХ. АНАЛИТИЧЕСКИИЙ ОБЗОР

ХАХАНОВ В.И., ЕГОРОВ А.А., КАМИНСКАЯ М.А., ХАХАНОВА И.В.

Рассматриваются методы и средства создания и разработки цифровых систем на кристаллах. Приводится аналитический обзор существующих систем моделирования, верификации, синтеза и имплементации. Дается классификация чипов с позиции создания экономичных и высокопроизводительных цифровых систем. Показываются перспективные пути развития рынка электронных технологий и возможности их проникновения в Украину.

Введение

Цифровые системы (ЦС) управления, сбора, хранения, преобразования и анализа данных в настоящее время применяются во всех областях человеческой деятельности (производство, научные исследования, быт, офис, транспортные средства). В связи с этим к ЦС все более возрастают требования по уменьшению стоимости, размерности, энергопотреблению, аппаратурной избыточности. Последняя должна быть максимально подогнана под выполняемую задачу. Очевидно, что универсальные, мощные персональные компьютеры, потребляющие большое количество энергии и имеющие внушительные размеры и стоимость, не могут конкурировать на рынке специализированных устройств. Что же взамен?

Ответом на данный вопрос могут быть: Embedded Systems (встроенные системы), Systems on Chip (SoC – системы на кристаллах) [1], Networks on Chip (сети на кристаллах) [2]. Другими словами, чтобы добиться увеличения производительности, уменьшения потребляемой мощности и физических размеров, систему необходимо размещать не на плате, а на кристалле. При проектировании SoC проблема функциональной верификации и тестирования является одной из самых сложных: по оценкам ведущих зарубежных фирм и специалистов общества IEEE стоимость ее решения составляет 50 – 70% от совокупных затрат полного цикла разработки кристалла [3,4]. На рынке микроэлектроники для изготовления цифровых кристаллов наиболее популярными являются заказные БИС (cell based ASIC) и программируемые логические интегральные схемы – ПЛИС (PLD – CPLD, FPGA) [5]. Два других типа логических устройств постепенно уходят в прошлое – это SDL (дискретные логические микросхемы) и GA (вентильные матрицы) [6]. На базе ASIC и PLD существуют следующие направления разработки цифровых систем (рис. 1).