УДК 004

Писарчик А.Ю.

СКРЫТЫЕ КАНАЛЫ ПЕРЕДАЧИ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Впервые понятие скрытого канала было введено в работе Лэмпсона «A Note of the Confinement Problem» в 1973 году. Канал является скрытым, если он не проектировался, не предполагался для передачи информации в электронной системе обработки данных [1-13]. Иными словами, это некий способ скрытой (замаскированной) несанкционированной передачи информации стороннему лицу, нарушающий действующую политику безопасности. При этом для организации передачи данных могут использоваться атрибуты, не предназначенные для этого: задержки между регистрируемыми событиями, порядок следования сообщений, длины передаваемых блоков данных и т.п.

Пик теоретических исследований в области скрытых каналов приходится на середину 1980-х годов, когда была опубликована «Оранжевая книга» Министерства обороны США, в которой, начиная с класса безопасности B2, было введено требование анализа скрытых каналов. Эффективность скрытого канала оценивалась при помощи сравнения его пропускной способности с пороговым значением. Канал, обладающий меньшей пропускной способностью, считался неопасным. Примерно в это же время в работе Кеммерера [2], было дано формальное определение двух типов скрытых каналов. Скрытый канал по памяти определяется, как канал, в котором информация передается через доступ отправителя на запись и получателя на чтение к одним и тем же ресурсам или объектам. Скрытый канал по времени характеризуется доступом отправителя и получателя к одному и тому же процессу или изменяемому во времени атрибуту. Кроме того, в этой работе была также впервые предложена методика борьбы с приведенными типами скрытых каналов, основанная на принципе построения и анализа матрицы разделяемых ресурсов (“Shared Resources Matrix”).

К сожалению, наличие соответствующих требований в «Оранжевой книге» помимо начального положительного импульса, в долгосрочной перспективе привело к значительному торможению исследований по данной проблематике. Это произошло по причине того, что бороться со скрытыми каналами стали, в основном, не ради реальной безопасности, а ради успешной сертификации. Кроме того, скрытые каналы из-за, в общем-то, случайной ассоциации с классами B2 и выше исследовались почти исключительно в контексте соответствующих этим классам систем. Поэтому сравнительно долгое время и теоретические и практические исследования в области скрытых каналов являлись уделом сравнительно небольшой группы специалистов, ведущих свои исследования в рамках узкой проблематики.

Тем не менее, в начале XXI века начали появляться теоретические работы, систематизирующие часть накопленных знаний, и предлагающие новые способы и методы организации и противодействия скрытых каналов. Здесь можно отметить работу Е.В. Тимониной, в которой, в частности, был проведен

обзор наиболее актуальных, по мнению автора, типов скрытых каналов, и предложены два новых типа – каналы по порядку и статистические каналы. Передача информации в каналах по порядку осуществляется при помощи изменения порядка следования информационных пакетов и анализе этого порядка на приемной стороне. Принцип работы статистических каналов заключается в модуляции определенных статистических характеристик информационного потока, и их анализе на приемной стороне. Наряду с этим, в данной работе были описаны основные методы борьбы со скрытыми каналами и поставлен вопрос о формировании способа качественной оценки различных методов их реализации. Примерно в то же время вышла работа А.В. Галатенко, иллюстрирующая другой подход к проблематике скрытых каналов. В ней автор делает акцент не на общетеоретические аспекты их создания, а на оценку применимости данного подхода в различных типах реальных систем. В связи с этим автором предлагается альтернативная классификация существующих скрытых каналов, базисом которой является учет особенностей, затрудняющих или упрощающих их создания в реальных системах.

Следует отметить, что, несмотря на усилия отдельных авторов, к сожалению, в настоящее время вопросы оценки эффективности различных способов организации скрытых каналов, практически не исследованы. Наиболее часто используемым методом оценки качества и опасности скрытого канала попрежнему остается предложенный более 20 лет назад метод оценки пропускной способности, и ее сравнения с пороговым значением. Кроме того, в силу определенной инерционности, по-прежнему продолжается исследование скрытых каналов в рамках требований и ограничений, применимых для сравнительно небольшого класса систем, описанных в «Оранжевой книге» и работах Кеммерера и Лэмсона.

Что касается описания практических примеров реализации скрытых каналов, то еще в 1976 году один из создателей защищенной операционной системы Multics Миллен [3] продемонстрировал своим коллегам скрытый канал по времени, реализованный на изолированных машинах А и В. Обе машины были подсоединены к некоторым общим ресурсам ROM, других каналов или связей между ними не было. На обеих машинах находились «Троянские кони». В системе А «Троянский конь» при нажатии букв на клавиатуре модулировал специальным кодом интервалы времен занятости библиотеки ROM. Время занятости библиотеки верхним уровнем сканировалось запросами в библиотеку «Троянским конем» системы В. Получившийся скрытый канал по времени позволял в реальном времени печатать информацию, получаемую через скрытый канал с клавиатуры системы А.

Рассмотрим еще один пример скрытого канала по времени. Пусть в программно-аппаратной схеме, реализующей интерфейс RS 232 между двумя системами А и В, нет передатчика в системе А и нет приемника в системе В. Вместе с тем для передачи байт от системы В системе А последняя выставляет сигнал готовности к приему информации. Очередной байт передается только тогда, когда выставлен сигнал готовности приема. Тогда задержка в выставлении

сигнала после очередного переданного байта считается таймером системы B и может таким образом передавать информацию от программно-аппаратного агента в системе A к программно-аппаратному агенту в системе B. Для этого один из программных агентов кодирует сообщение различными по длине интервалами задержки выставления сигнала, другой считывает эти сообщения с помощью таймера.

В ряде скрытых каналов по времени, порожденных работой процессора, особо следует выделить два примера каналов по времени, использующих возможности изменять длительности занятости в работе центрального процессора. В первом примере отправитель информации меняет время занятости CPU в течение каждого фрагмента времени, выделенного для его работы. Например, для передачи 0 и 1 одна длина промежутка времени кодирует 1, а другая - 0. В другом случае отправитель использует промежутки времени между обращениями к процессору. Более подробно об этих каналах можно прочитать в работе Хаскампа [4]

Пример скрытого канала по памяти можно найти в работе Шнайера [5]. Скрытый канал передачи информации через Интернет строится с помощью вписывания сообщения вместо последнего бита оцифрованного изображения, которое передается в качестве легального сообщения. Поскольку последний бит мало влияет на качество изображения, передача информации оказывается скрытой от субъекта ведущего перехват и допускающего передачу только легальных изображений. Хорошо известен метод борьбы с данным методом стеганографии, заключающийся в изменении формата изображения, например, с помощью компрессии. Данный метод уничтожает скрытый канал указанного вида.

Нельзя не отметить также массу работ, основанных на особенностях, используемых в сети Интернет универсальных протоколах. Это программный инструмент для безопасного тунелирования данных Active Port Forwarder [6], использущий SSL, инструмент для создания туннелей Firepass, позволяющих обойти ограничения брандмауэра и инкапсулировать потоки данных в легитимные HTTP POST запросы, система скрытой передачи данных при помощи неиспользуемых полей протокола TCP – NUSHU и многие, многие другие.

Рассмотрим подробнее историю развития термина «стеганография».

Несмотря на многочисленные открытые публикации и ежегодные конференции, длительное время стеганография не имела сложившейся терминологии. С середины 80-х гг. прошлого столетия для описания модели стеганографической системы (сокращенно — стегосистемы или, что по мнению авторов этой работы является более правильным определением, стеганосистемы, поскольку приставка «стего» в переводе с латыни означает «крыша» или «черепица» и искажает смысл используемого понятия) использовалась так называемая «проблема заключенных», которую предложил в 1983 г. Симмонс (G.J. Simmons) [7].

Основные понятия стеганографии были согласованы в 1996 г. на 1-й Международной конференции по скрытию данных — Information Workshop on

Information Hiding*96. Тем не менее, даже такое основополагающее понятие как «стеганография» разными специалистами трактуется неодинаково. Например, некоторые специалисты понимают под стеганографией только скрытую передачу информации, другие же относят к ней такие приложения как, например, метеорная радиосвязь, радиосвязь с псевдослучайным перестраиванием частоты, широкополосную радиосвязь.

В работе «Цифровая стеганография» Грибунина В.Г. приводится следующее определение цифровой стеганографии: «...наука о незаметном и надежном скрытии одних битовых последовательностей в других, имеющих аналоговую природу». Упоминанием об аналоговой природе цифровых данных подчеркивается факт встраивания информации в оцифрованные непрерывные сигналы. Таким образом, в сравнении с ЦС, компьютерная стеганография имеет более широкий смысл, поскольку в ее пределах рассматриваются вопросы ввода данных в заголовки IP-пакетов, в текстовые сообщения и файлы других форматов.

Слово «незаметное» в представленном выше определении цифровой стеганографии подразумевает обязательное включение человека в систему стеганографической передачи данных. То есть, человек рассматривается как специфический приемник данных, предъявляющий к системе передачи требования, которые достаточно тяжело формализовать [8].

Опыт показывает, что скрытую передачу информации обнаружить сложней. Как правило, канал утечки информации путем ее скрытой передачи обнаруживается только после его длительной эксплуатации инсайдером. Таким образом, наиболее опасной угрозой можно считать скрытую утечку конфиденциальной информации, которая может быть весьма продолжительной.

В случае, когда объединение компьютеров в ЛВС предполагает подключение этой сети к внешним сетям, возникает ряд возможностей образования скрытых каналов утечки конфиденциальной информации.

Основные каналы утечки конфиденциальной информации, характерные для таких сетей:

- несанкционированное копирование конфиденциальной информации на внешние носители, ее вынос за пределы контролируемой зоны;
- вывод на печать конфиденциальной информации и ее вынос на распечатанных документах за пределы контролируемой зоны;
- несанкционированная передача конфиденциальной информации по сети во внешние сети за пределы контролируемой зоны;
- хищение носителей конфиденциальной информации.

При скрытой передаче информации скрывается сам факт ее передачи. Обнаружить такой канал утечки очень непросто. А значит, злоумышленник может вновь и вновь использовать его в своих целях. Возможностей скрыто передавать информацию бесконечно много, достаточно просто проявить фантазию.

Организовать скрытую передачу информации может как злоумышленник извне, так и сотрудник компании. Совсем не обязательно обладать правами

администратора, достаточно иметь доступ к информации, желание ее продать и человека, готового ее купить.

Можно привести простой пример. Два пользователя договариваются, что, если слово в сообщении содержит нечетное количество букв, передается бит, равный 1, а если четное — 0.

В случае, когда в роли злоумышленника выступает администратор, возможно внедрение программы-закладки, которая будет скрытым образом передавать информацию или позволит управлять сетью извне.

Бывает и так, что разработчики программного обеспечения внедряют в код недокументированные функции, исполнение которых может привести к нарушению целостности корпоративной информации.

Борьба с намеренными утечками - задача весьма сложная. Эффективность такой борьбы в основном заведомо ниже, чем борьбы со случайными утечками, в силу того что предстоит противодействовать злонамеренным ухищрениям инсайдеров, на вооружении которых имеется ряд интересных возможностей скрытой передачи, а также программных и даже аппаратных средств ее реализации.

Все большую опасность приобретают следующие способы скрытой передачи информации:

- возможность скрытого канала утечки информации возникает при использовании инсайдерами анонимных https и других защищенных прокси-серверов: туннелирование, которое позволяет злоумышленнику, используя разрешенный протокол, передавать по нему конфиденциальную информацию, минуя межсетевой экран;
- стеганографические способы сокрытия информации;
- шифрование инсайдером конфиденциальной информации перед ее отправкой;
- использование инсайдером вредоносных программ для реализации скрытой передачи информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] Butler W. Lampson. A Note of the Confinement Problem — Communications of ACM, 1973.

[2] R.A. Kemmerer. Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels — ACM Transactions on Computer Systems, 1983.

[3] J.K. Millen. Security Kernel Validation in Practice — Communications of ASM. May I.S. Moscowitz, M.H. Kang. Covert Channels — Information Technology Division Naval Research Laboratory, Washington, DC 20375, 1995.

[4] J.C. Huskamp. Covert Communications Channels in Timesharing Systems. Technical Report UCB-CS-78-02, Ph.D. Thesis — University of California, Berkley, California, 1978.

[5] B. Schneier. Applied Cryptography: Protocols, Algorithms, and Source

Code in C. 2nd edition — John Wiley & Sons, 1996.

[6] D.J. Pack, W. Streilein, S. Webster. Detecting HTTP Tunneling Activities, 2002.

[7] Грибунин, В.Г. Цифровая стеганография. — М.: Солон-Пресс, 2002. — 272 с.

[8] B. Pfitzmann, Information Hiding Terminology In: Information Hiding, Springer Lecture Notes in Computer Science, 1996.

[9] D. Kahn. The Code-Breakers: The Story of Secret Writing. MacMillan Publishing Company. New York. USA, 1996.

[10] W. Bender, D. Grulil, N. Morimoto, A. Lu. Techniques for Data Hiding IBM: Systems Journal. 35(3&4), 1996. — pp. 313-336.

[11] Savateev E. O. Design of Steganography System Based on the Version 4 Internet Protocol // IEEE International Siberian Conference on Control and Communications (SIBCON-2005). Tomsk, 2005.

[12] Postel J. RFC 791. Internet Protocol. USC/Information Sciences Institute. September, 1981. — pp. 117-120.

[13] Алексеев, А.П. Сокрытие сообщений путем их распыления в пространстве // ИКТ, Т.6, №3, 2008. – с.52-56.