Тип работы: Глава диплома

Предмет: Информатика (другое)

Введение

Актуальность темы исследования. Проблеме информационной безопасности сегодня уделяется пристальное внимание. Факт наличия скрытых каналов передачи информации и управление ими является важной составляющей в общей информационной безопасности личности, предприятия и даже государства. Кроме привычных задокументированных каналов передачи информации неизбежно будут существовать и скрытые каналы передачи, поскольку информационные ресурсы имеют самостоятельную коммерческую и иную ценность, и попытки эксплуатации всех возможных технических приемов получения незаконного доступа к информации исключить невозможно.

Грамотное администрирование информационных систем позволит значительно снизить влияние скрытых каналов передачи информации, предотвратить их возникновение.

Объектом исследования являются скрытые каналы передачи информации, их сущность и особенности.

Предметом исследования являются технологии создания, эксплуатации и администрирования скрытых каналов передачи информации.

Целью дипломного проекта является исследование способов скрытой передачи информации с использованием стандартных протоколов межсетевого взаимодействия.

Исходя из цели работы можно сформулировать следующие задачи:

• Изучить законодательную базу в области скрытых каналов передачи информации;

• Определить понятие и сущность скрытых каналов передачи информации;

• Изучить технологии создания и администрирования скрытых каналов передачи информации.

Научная новизна состоит в формализации теоретического материала и создании практических инструментов для оценки работы скрытых каналов передачи информации

Работа содержит __ страниц, __ таблиц и __ иллюстрации, содержит введение, __(две?) главы, заключение и список литературы.

В первой главе приводятся основные теоретические исследования, вводится понятие скрытых каналов информации, описаны технологии их создания и администрирования.

Во второй главе __(?)

1. Анализ скрытых каналов передачи информации

1.1 Понятие и сущность скрытых каналов передачи информации

Сегодня абсолютно все разработчики программного обеспечения для обеспечения информационной безопасности принимают во внимание сведения, раскрытые Сноуденом. Эти сведения позволяют сделать выводы о наличии, преднамеренной активации и функционировании каналов передачи информации, внедренных АНБ США для тайного доступа к информации, управления устройствами различных типов.

С учетом того, что сети передачи данных являются технологией, носящей сквозной характер, защита от скрытой передачи информации обретает в наше время вторую жизнь. Необходимость обособить методы скрытой передачи информации, - стеганографии, - связанные именно с цифровым представлением данных, в обиход был введен термин «компьютерная стеганография». Однако в работе Шнайера[_1] стеганографический метод передачи по каналам связи называется подсознательными каналами. В то же время появился термин "скрытый канал". Концепция скрытых проходов была впервые введена в работе Лэмпсона [_2] в 1973 году. Если канал не предназначен или не изначально предусмотрен для передачи информации в электронной системе обработки данных, он называется скрытым каналом. Таким образом,

термин "скрытый канал" больше относится к телекоммуникациям внутри компьютера.
В работе Цая[_3] дано следующее определение скрытых каналов: пусть в операционной системе I (M) построена модель недискреционной политики безопасности M. Тогда каждая связь между двумя субъектами I (Sh) и I (Si) в I (M) называется скрытой.
Современное законодательство РФ не оставляет без внимания контроль скрытых каналов передачи информации, для регламентации данной сферы деятельности разработаны ГОСТ Р53113.1-2008[_4] и ГОСТ Р53113.2-2009[_5].
В соответствии с ГОСТами определен термин «скрытый канал» – это непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности.
Поскольку все вышеперечисленные термины для скрытой передачи информации отличаются нюансами применения, мы будем называть способ скрытой передачи информации скрытым каналом, не ограничивая общность. Когда выделение соответствующего канала следует из контекста, мы вернемся к исходному термину в этих особых случаях.
ГОСТ вводит следующие категории скрытых каналов. По механизму передачи информации они делятся на:
- СК по памяти;
- СК по времени;
- скрытые статистические каналы.
Скрытый канал по памяти основан на существовании памяти, в которую отправляющий субъект записывает информацию, а принимающее тело считывает ее. Конфиденциальность канала памяти определяется тем фактом, что внешние наблюдатели не знают местоположения скрытой информации, записанной в памяти.
СК по памяти предполагает использование ресурсов памяти, однако способ использования памяти технологиями скрытых каналов не был учтен разработчиком системы защиты и, следовательно, не может быть обнаружен используемыми средствами защиты.
СК по памяти разделяют на:
• Каналы, использующие особенности информационных систем, работающих на структурированных данных. В отсутствии информации о структуре используемых данных несанкционированный программный агент встраивает данные в информационные объекты с формально описанными структурами и формальными правилами обработки.
• Каналы, использующие особенности информационных систем, использующие неструктурированные данны, эксплуатируют возможность встраивания данных в информационные объекты независимо от формально описанной структуры (например, запись скрытой информации в младшем значащем бите изображения.
Скрытый канал по времени побуждает субъекта, передающего информацию, модулировать некоторые привязанные ко времени процессы с помощью передаваемой информации, в то время как субъект, принимающий информацию, может демодулировать получаемый сигнал, наблюдая за процессом передачи информации во времени.
Скрытые статистические каналы используются для передачи информации об изменениях параметров распределения вероятностей любой характеристики системы. Эти характеристики можно считать случайными и описывать вероятностной статистической моделью.
Скрытость этого канала обеспечивается тем фактом, что получатель информации имеет меньшую стахостическую неопределенность параметров распределения наблюдаемых системой признаков, чем наблюдатель без знания структуры скрытого канала.
Например, появление реальной, но маловероятной комбинации в пакете передачи в заданный интервал времени может означать сигнал о сбое компьютерной системы.
Скрытый канал по пропускной способности может быть:
- Каналом с низкой пропускной способностью, если его пропускная способность достаточна для передачи наименьшего объема ценных информационных объектов (например, ключей паролей, паролей) или команд в течение периода времени, в течение которого эта передача актуальна;
- Каналом с высокой пропускной способностью, если его пропускная способность позволяет передавать информационные объекты среднего и большого размера (например, текстовые файлы, изображения, базы данных) в течение периода времени, когда эти информационные объекты являются ценными..
Для решения сложных задач могут использоваться комбинации скрытых каналов, основанные на различных механизмах передачи.
Скрытый канал передачи информации нарушает политику информационной безопасности. Общепринятое

определение политики информационной безопасности дано в стандарте TCSEC [_6]. В Российской Федерации концепция политики информационной безопасности приведена в ГОСТ Р53114-2008 [_7]: Политика информационной безопасности (организации) - это официальное изложение правил поведения, процедур, практических методов или руководящих принципов в области информационной безопасности, которыми руководствуется деятельность организации.
Многие политики безопасности выражаются через поток информации. Например, все информационные потоки в системе (включая потенциальные информационные потоки) разделены на два непересекающихся подмножества: разрешенные потоки и неразрешенные потоки. Затем система защиты должна обеспечивать поддержку разрешенных потоков и предотвращать запрещенные потоки. Многоуровневые стратегии (MLS) относятся к этому типу стратегий.
Многоуровневая политика безопасности (Политика MLS) была принята всеми развитыми странами мира. Российский государственный сектор также придерживается этой политики в своей повседневной тайной работе.
Злоумышленник может использовать скрытые каналы для реализации следующих нарушений политики безопасности:

_1. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, New York, 2nd edition, 1996.
_2. Lampson B.W. A Note of the Confinement Problem //Communications of ACM, 16:10, pp. 613-615, October 1973.
_3. Tsai C.-R., Gligor V.D., Chandersekaran C.S. A Formal Method for the Identification of Covert Storage Channels in Source Code// IEEE Transactions on Software Engineering, v.16:6, June 1990, pp. 569-580.
_4. ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. . Часть 1. Общие положения
_5. ГОСТ Р 53113.2-2009 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов»
_6. Department of Defense Trusted Computer System Evaluation Criteria, DoD, 1985.
_7. ГОСТ Р 53114-2008 Защита информации ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ Основные термины и определения
_8. Модель OSI и сетевые протоколы. qastack.ru. Дата обращения: 31 января 2022. https://qastack.ru/networkengineering/6380/osi-model-and-networking-protocols-relationship
_9. National Computer Security Center. A Guide to Understanding Covert Channel Analysis of Trusted Systems, 1993, NCSC-TG-030, ver. 1.
_10. Kemmerer R.A. Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels //ACM Transactions on Computer Systems, 1:3, pp. 256-277, August 1983.
_11. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации, М.: Агентство «Яхтсмен», 1996, 186 с
_12. Millen J.K. Security Kernel Validation in Practice/ Communications of ASM, 19:5, May 1976.
_13. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, New York, 2nd edition, 1996.
_14. Rowland C.H. Covert Channels in the TCP/IP Protocol Suite// 11-14-1996, Psionic Technologies Inc., 2002.
_15. National Computer Security Center. A Guide to Understanding Covert Channel Analysis of Trusted Systems, 1993, NCSC-TG-030, ver. 1.
_16. Huskamp J.C. Covert Communications Channels in Timesharing Systems/ Technical Report UCBCS-78-02, Ph.D. Thesis, University of California, Berkley, California, 1978.
_17. Гапонов, И. Ю. Сущность и методы функционирования скрытых каналов в пространственных областях изображения / И. Ю. Гапонов. — Текст : непосредственный // Молодой ученый. — 2013. — № 12 (59). — С. 68-70. — URL: https://moluch.ru/archive/59/8287/ (дата обращения: 03.05.2022).
_18. Грушо А.А. Скрытые каналы и безопасность информации в компьютерных системах // Дискретная математика, т.10, вып. 1, 1998.
19. Грушо А.А. О существовании скрытых каналов// Дискретная математика, т.11, вып. 1, 1999.
_20. Шипулин П.М., Козин В.В., Шниперов А.Н. Метод организации скрытого канала передачи информации на основе протокола потоковой передачи данных // Научно-технический вестник информационных

технологий, механики и оптики. 2018. Т. 18. № 5. С. 834–842. doi: 10.17586/2226-1494-2018-18-5-834-842
_21. Casner S., Frederick R., Jacobson V., Schulzrinne H. RFC 3550. RTP: A Transport Protocol for Real-Time Applications. Network Working Group, 2003, 25 p.
_22. Servetto S.D., Vetterli M. Communication using phantoms: covert channels in the Internet. Proc. IEEE Int. Symposium on Information Theory. Washington, 2001. doi: 10.1109/isit.2001.936092
_23. Cabuk S., Brodley C., Shields C. IP covert timing channels: design and detection. Proc. 11th ACM Conference on Computer and Communications Security. New York, 2004, pp. 178–187. doi: 10.1145/1030083.1030108
_24. Houmansadr A., Borisov N. CoCo: coding-based covert timing channels for network flows. Lecture Notes in Computer Science, 2011, vol. 6958, pp. 314–328. doi: 10.1007/978-3642-24178-9_22
_25. СКРЫТЫЕ ЛОГИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ | ЗАЩИТА ДАННЫХ ОТ УТЕЧКИ ПО СКРЫТЫМ ЛОГИЧЕСКИМ КАНАЛАМ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sluchai-utechki-informatsii/skrytye-logicheskie-kanaly-utechki-informatsii/