



СКРЫТЫЕ И ПОТАЙНЫЕ КАНАЛЫ

Бесланеева Татьяна Юрьевна

студент, Северо-Кавказский федеральный университет, РФ, г. Ставрополь

Впервые термин скрытый канал был использован американским ученым Батлером Лэпсоном в его работе “Заметка о проблеме ограничения”, где он определяет скрытые каналы как каналы, которые совершенно не предназначены для информационной передачи.

ГОСТ Р 53113.1-2008 “Информационная технология (ИТ). Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения”, гласит о том, что скрытый канал – это непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности.

Более традиционным и обширным определением является следующая формулировка. Пусть M – политика безопасности, а $R(M)$ – реализация политики M . Если взаимосвязь между субъектами в реализации $R(M)$, не разрешена в модели M , такая связь называется скрытым каналом.

Принцип работы скрытых каналов заключается в том, что изменение состояния некоего объекта несет информацию. И определить данную закономерность, зачастую довольно проблематично. Но за скрытность, приходится расплачиваться невысокой скоростью передачи информации.

Для наглядности рассмотрим пример: возьмем два процесса, A и B , и обозначим что A имеет более высокий уровень допуска чем B , B – не имеет доступа к данным высокого уровня, в свою очередь A – не может передавать данные на нижний уровень. Может ли в таком случае процесс A найти обходной способ передачи информации процессу B , который не будет вызывать подозрений? Например, таким способом может являться варьирование заполнения буфера при легальном выводе данных, когда A при выводе, кодирует данные, т.е. изменяет их объем в соответствии с кодировкой которую знает B , притом что B имеет возможность анализировать буфер. В таком случае процесс A , вполне легально имеет возможность, в обход установленной модели безопасности передавать информацию, не предназначенную для процесса B . Именно на этой идее основываются скрытые каналы.

Одна из главных опасностей скрытых каналов заключается в том, что передача информации по подобным каналам не контролируется стандартными механизмами безопасности, такими как авторизация и аутентификация.

Принято выделять два типа скрытых каналов: скрытый канал памяти и скрытый временной канал. В первом случае для скрытой передачи информации используется модулирование характеристик памяти, таких как адреса, объем свободной памяти и др.

Процесс использует скрытый временной канал, если для кодирования информации он варьирует временные характеристики, связанные с его собственным выполнением, например, в мультипрограммном режиме, это может быть использованная доля кванта процессорного времени.

Проблема скрытых каналов — это проявление более общей проблемы сложности современных информационных систем. В сложных системах неизменно будут присутствовать скрытые каналы, так что бороться нужно с причиной, а не со следствием. В самом общем виде борьбу со сложностью систем можно представить, как "проведение объектного подхода с физическими границами между объектами". Пользовательская и административные сети должны быть физически отделены друг от друга. Также, компоненты системы должны не доверять друг другу, поднимать тревогу и применять защитные меры при выявлении подозрительной активности (дисковый контроллер может зашифровать файлы, сетевой контроллер — блокировать коммуникации и т.п.). Если организовать физические границы невозможно, следует воспользоваться виртуальными, формируемыми в первую очередь криптографическими средствами.

Потайными каналами называются нестандартные способы передачи информации по легальным каналам (так же называемыми обертывающими). Такие каналы используют в случаях, когда имеется легальный коммуникационный канал, но политика безопасности запрещает по нему передавать определенные данные. Важно понимать, что скрытые и потайные каналы имеют несколько существенных различий. В отличие от скрытых каналов, потайные каналы существуют только тогда, когда о нем не знает противник. Время передачи данных по тайному каналу зависит от характеристик обертывающего (легального) канала, то есть имеет ограничения, в то время скрытые каналы нет.

Для примера рассмотрим реализацию сети анонимизаторов с помощью HTTP-серверов и клиентов. Web-серфинг служит обертывающим каналом. В роли узлов сети анонимизаторов выступают HTTP-серверы, а взаимодействие между ними осуществляется по скрытым каналам в HTTP/HTML при посредничестве ничего не подозревающих клиентов (в первую очередь — с помощью средств перенаправления запросов и активного содержимого, встроенных, например, в рекламные баннеры, присутствующие на посещаемой Web-странице). В результате можно достичь не только невозможности ассоциации между отправителем и получателем сообщений, но и реализовать более сильное свойство — скрытность (даже в присутствии глобального наблюдателя). Оказывающиеся невольными посредниками Web серферы пополняют подлежащее анализу множество анонимности, затрудняя тем самым получение наблюдателем полезной информации.

Разумеется, и злоумышленники, и разработчики защитных средств осознают возможности и проблемы, связанные с использованием HTTP в качестве обертывающего канала. В целом, потайные каналы гораздо практичнее скрытых, поскольку у них есть легальная основа — обертывающий канал. Потайные (а не скрытые) каналы — наиболее подходящее средство для управления враждебной многоагентной системой. Но в них нуждаются не только злоумышленники. Потайные каналы могут эффективно применяться поставщиками информационного наполнения, встраивающими в него скрытые "цифровые водяные знаки" и желающими контролировать его распространение, соблюдение потребителями цифровых прав.

Еще один пример, ставший классическим, — применение потайного канала премьер-министром Великобритании Маргарет Тэтчер, которая, чтобы выяснить кто из ее министров виновен в утечках информации, раздала им варианты одного документа с разными межсловными промежутками.

Побочные каналы являются частным случаем скрытых. В роли передатчиков выступают компоненты информационных систем, а в роли приемников — внешние наблюдатели с соответствующим оборудованием. С помощью побочных каналов измеряется время видимых операций, их энергопотребление или побочные электромагнитные излучения и наводки, но помимо этого, для атак могут применяться и акустические каналы. Побочные каналы представляют собой наиболее наглядное проявление многоаспектности современной информационной безопасности.

Роль атакующих на информационные системы берут на себя как правило их владельцы, которые располагают временем и необходимым инструментарием. В сочетании с принципиальной невозможностью управления физическим доступом, перечисленные факторы делают атаки с использованием побочных каналов особенно опасными. Объектами атак с использованием побочных каналов чаще всего становятся криптографические компоненты информационных систем, точнее, их секретные ключи.

Кардинальное решение проблемы побочных каналов возможно при соблюдении следующего основополагающего принципа: данные об операциях, которые можно получить из побочных каналов, должны быть статистически независимы от входных и выходных данных и информации ограниченного доступа. На практике системы укрепляются "по мере сил", а у мотивированных злоумышленников остается масса возможностей для результативных атак. Подводя итог, можно сказать, что появление скрытых каналов практически неизбежно в современных условиях быстрого развития информационных систем. В связи с этим, в целях информационной безопасности разработчикам важно знать о возможных местах и причинах возникновения этих каналов для минимизации возможных утечек. Это же можно сказать и о потайных каналах, несмотря на их принципиальную разницу.