Лекция 9

Скрытые каналы утечки информации.

Модели невлияния и невыводимости.

Понятие скрытых каналов утечки информации

Скрытый канал - механизм, посредством которого в КС может осуществляться информационный поток (передача информации) между сущностями в обход политики (правил) разграничения доступа

В моделях дискреционного доступа

- возможность осуществления доступа субъектов к объектам **вне области безопасного доступа, к примеру, вне явных разрешений, "прописанных" в матрице доступа** (потоки за счет "троянских программ" и неявные информационные потоки – за счет доступа к общим объектам).

В моделях мандатного доступа

- **потоки "сверху вниз"** – от сущностей с высоким уровнем безопасности к сущностям более низких уровней безопасности вне явного нарушения правил NRU и NWD (т.е. без непосредственного доступа к объектам на чтение или запись)

Скрытым каналом утечки информации в системах мандатного доступа называется механизм, посредством которого может осуществляться передача информации от сущностей с высоким уровнем безопасности к сущностям с низким уровнем безопасности без непосредственного нарушения правил NRU и NWD.

Проблемы анализа скрытых каналов

1) Выявление скрытых каналов;

2) Оценка пропускной способности скрытых каналов и оценка опасности, которую несет их скрытое функционирование;

3) Выделение сигнала или получение какой нибудь информации, передаваемой по скрытым каналам;

4) Противодействие реализации скрытого канала вплоть до его уничтожения.

Информационный поток (канал)

- Если осуществляется доступ на чтение (read) субъекта S к объекту O, то поток информации идет от O к S. Если S имеет доступ на запись (write) к O, то информационный поток направлен от S к O.

- Информационный поток между объектами X и Y существует, если средняя взаимная информация I(X,Y)>0.

- Информационным потоком от объектов {S} к объекту T можно считать тройку (T,{S},G), где T меняет свое состояние при условии, что логическое выражение G принимает значение истина.

Виды скрытых каналов утечки информации

- скрытые каналы ***по памяти*** (на основе анализа объема и других статических параметров объектов системы);
- скрытые каналы ***по времени*** (на основе анализа временных параметров протекания процессов системы);
- скрытые ***статистические каналы*** (на основе анализа статистических параметров процессов системы.

Примеры каналов по памяти

Простейшим скрытым каналом **по памяти** является возможность показа на уровне Low названий директорий и файлов, созданных на уровне High. В данном случае информация может передаваться в именах файлов, которые выбираются в соответствии с заранее условленным кодом, в атрибутах файлов, в которых информация может кодироваться, размерами файлов, датами изменения файлов и т.д.

И, наконец, существование файла с данным названием несет бит информации с верхнего уровня на нижний.

Другим примером канала **по памяти** является кодирование информации в сохраняемых настройках каких либо ресурсов общего пользования субъектов уровней High и Low. Настройки, проведенные на уровне High, доступны наблюдению на уровне Low и, следовательно, могут нести информацию, выраженную заранее условленным кодом.

Примеры каналов по времени

Скрытые каналы **по времени** впервые стали серьезно рассматриваться с 1976 г., когда один из создателей защищенной операционной системы Multics Миллен продемонстрировал своим коллегам скрытый канал по времени.

Скрытый канал по времени на изолированных машинах High и Low, подсоединенных к некоторым общим ресурсам ROM, других каналов или связей между ними не было. В подсистемах High и Low находились “Троянские кони”. На уровне High “Троянский конь” при нажатии букв на клавиатуре модулировал специальным кодом интервалы времен занятости реурса ROM. Время занятости библиотеки верхним уровнем сканировалось запросами в библиотеку “Троянским конем” нижнего уровня. Получившийся скрытый канал по времени позволял в реальном времени получать (печатать) информацию, получаемую через скрытый канал с клавиатуры подсистемы уровня High.

Примеры каналов по времени

В программно аппаратной схеме, реализующей интерфейс RS232 между Low и High, нет передатчика на уровне High и нет приемника на уровне Low. Вместе с тем для передачи байт с нижнего уровня на верхний машина верхнего уровня 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 на нижнем уровне и может таким образом передавать информацию от программно аппаратного агента на верхнем уровне к программно аппаратному агенту на нижнем уровне. Для этого агент на верхнем уровне кодирует сообщение различными по длине интервалами задержки выставления сигнала, а агент на нижнем уровне считывает эти сообщения с помощью таймера.

Примеры каналов по времени

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. На пример, 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.

«Скрытый канал» передачи информации через Интернет

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.

Статистический скрытый канал передачи информации

Существуют **скрытые статистические каналы**, которые не только трудны для обнаружения, но практически не выявляются.

Например, если T и S связаны между собой статистической зависимостью, то трудно выявить детерминированную связь между этими параметрами.

Так как «информационным потоком от объектов {S} к объекту T можно считать тройку (T,{S},G), где T меняет свое состояние при условии, что логическое выражение G принимает значение истина», и **пусть G случайная величина с характеристиками известными только источнику и приемнику**.

Пропускная способность скрытых каналов

- Пропускная способность скрытых каналов вычисляется методами теории информации.
- Часто пропускная способность скрытых каналов измеряется отношением количества скрытно переданной информации к количеству информации в легальном маскирующем скрытую передачу процессе или контейнере:
  - например в обычном цифровом изображении, содержащем 2,5 мегабит информации, манипуляцией последнего бита безопасно можно передать только 100 бит скрытого сообщения
  - скрытый канал потайного копирования интересующего файла на дискету обладает пропускной способностью, равной объему копируемого файла.

Борьба со скрытыми каналами

Наиболее эффективным способом борьбы со скрытыми каналами является их уничтожение.

Рандомизация.

На пример, в приведенных примерах скрытых каналов спуска информации при использовании интерфейса RS 232 встраивание между уровнями High и Low устройства, транслирующего байты и рандомизирующего задержку выставления сигнала на верхнем уровне, видимую на нижнем уровне, позволяет полностью уничтожить любой детерминированный скрытый канал по времени и существенно испортить скрытый статистический канал.

Борьба со скрытыми каналами

Технология "представлений".

"Представлением" информации КС называется процедура формирования и предоставления именованному пользователю после его входа в систему и аутентификации необходимого ему подмножества информационных объектов КС, в том числе, с возможным их количественным и структурным видоизменением исходя из задач разграничения доступа к информации.

- задача разграничения доступа решается автоматически, в буквальном смысле.
- техника "представлений" автоматически решает проблему скрытых каналов утечки информации первого вида («несанкционированный просмотр»).
- техника "представлений" широко применяется в реляционных СУБД, где "представления" формируют для пользователя "свое" представление базы данных.
- основные проблема в том, чтобы не выявили информацию о наличии в системе недоступной им информации

Борьба со скрытыми каналами

Техника "разрешенных процедур"

"Системой разрешенных процедур" называют разновидность интерфейса КС, когда при входе в систему аутентифицированным пользователям предоставляется только лишь возможность запуска и исполнения конечного набора логико-технологических процедур обработки информации без возможности применения элементарных методов доступа (read , write , append, create, delete и т. п.) к информационным объектам системы.

Таким образом, в системах с интерфейсом "разрешенных процедур" идеология разграничения доступа доведена, если так можно выразиться, до крайности, т. е. пользователи не "видят" информационные объекты системы вовсе, а имеют возможность только лишь "нажимать кнопки" и выполнять операции на уровне логико-технологических процедур предметной области КС.

Нетрудно заметить, что компьютерная система при этом для пользователей превращается в дискретный автомат, получающий команды на входе и выдающий обработанную информацию на выходе.

Основные положения теоретико-информационных моделей.

Свойства многоуровневой безопасности могут быть выражены многими способами, одним из них является **«невлияние».**

Эта концепция реализована для обеспечения гарантий того, что любые действия, происходящие на высоком уровне безопасности, не воздействуют (не влияют) на действия, происходящие на более низком уровне безопасности. Эта модель не имеет отношения к потокам данных, она относится к тому, что субъект знает о состоянии системы. Так, если сущность на высоком уровне безопасности выполняет некоторое действие, оно не может изменить состояние для сущности, находящейся на более низком уровне.

Основные положения теоретико-информационных моделей.

Если сущность на низком уровне безопасности узнает о том, что сущность на высоком уровне безопасности произвела определенные действия, из-за которых изменилось состояние системы для этой сущности на низком уровне, она (эта сущность) может догадаться (предположить) о дополнительной информации, относящейся к этим действиям на высоком уровне, что является разновидностью утечки информации.

Основные положения теоретико-информационных моделей.

Пусть, Фома и Катя одновременно работают на мейнфрейме, реализующем многоуровневую безопасность. Фома имеет допуск уровня «секретно», а Катя – «совершенно секретно». Соответственно терминал Фомы работает в контексте «секретно», а терминал Кати – «совершенно секретно». Эта модель утверждает, что никакие из действий Кати на своем терминале не окажут прямого или косвенного воздействия на домен Фомы (доступные ресурсы и рабочая среда). Независимо от выполняемых ею команд и используемых ресурсов, это никоим образом не повлияет на работу Фомы на этом мейнфрейме.

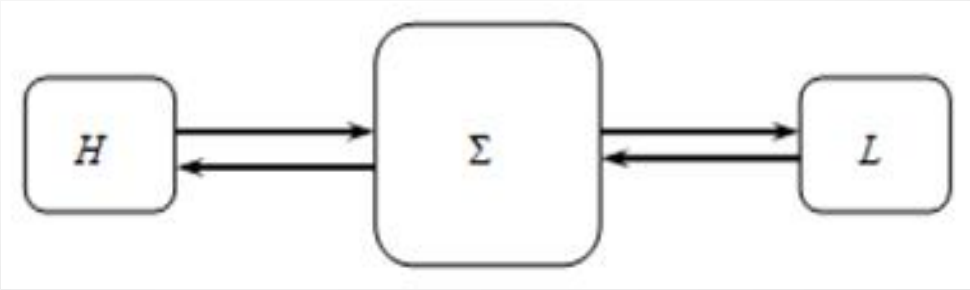
Основные положения теоретико-информационных моделей.

Реальный смысл этой модели состоит в учете скрытых каналов и атак посредством предположений о действиях.

Эта модель рассматривает общие ресурсы, которые будут использовать различные пользователи системы, и пытается идентифицировать способы, посредством которых информация может переходить от процессов, работающих с высоким уровнем допуска, к процессам с меньшим уровнем допуска. Данная модель содержит правила, гарантирующие, что Катя не сможет отправить данные Фоме посредством скрытых каналов (по памяти или по времени).

Основные положения теоретико-информационных моделей.

В рассматриваемой вероятностной модели безопасности информационных потоков анализируются КС, в которых реализована мандатная политика безопасности. В модели предполагается, что все объекты (в том числе и субъекты) КС объединены по трем группам: объекты Σ, реализующие систему защиты; объекты H, обрабатывающие информацию высокого уровня конфиденциальности; объекты L, обрабатывающие информацию низкого уровня конфиденциальности. Все информационные потоки между H и L проходят через систему защиты Σ.



Основные положения теоретико-информационных моделей.

1. КС рассматривается как совокупность двух непересекающихся множеств сущностей:
   - множества высокоуровневых объектов H;
   - множества низкоуровневых объектов L.
2. Состояние любого объекта $h \in H$ или $l \in L$ является случайным.

Понятие информационной невыводимости основывается на следующем определении "опасных" потоков:

Согласно требованиям мандатной политики безопасности любые информационные потоки от H к L запрещены. Однако в большинстве реальных систем реализовать данное жесткое требование не представляется возможным. В модели рассматриваются ряд подходов к определению возможных информационных потоков между H и L, основанных на понятиях информационной ***невыводимости*** *и информационного* ***невлияния****.*

Основные положения теоретико-информационных моделей.

Понятие информационной **невыводимости** основывается на следующем определении "опасных" потоков:

В системе присутствует информационный поток от высокоуровневых объектов к низкоуровневым, если некое возможное значение переменной в некотором состоянии низкоуровневого объекта невозможно одновременно с определенными возможными значениями переменных состояний высокоуровневых объектов.

Основные положения теоретико-информационных моделей.

КС *соответствует требованиям* ***информационной невыводимости****: если* $p(h)>0$, $p(l)>0$, то и $p(h|l)>0$, *где* $p(h)$, $p(l)$ – безусловные вероятности состояний, соответственно, высокоуровневого и низкоуровневого объектов; $p(h|l)$ – условная вероятность состояния высокоуровневого объекта.

В условиях определения из истинности неравенства $p(h|l)>0$ следует истинность $p(l|h)>0$, что предполагает отсутствие информационных потоков от низкоуровневых объектов к высокоуровневым: $p(l|h) = p(h,l) / p(h) = p(h|l)\ p(l)|p(h)$

Таким образом, требования информационной невыводимости являются более строгими, чем требования безопасности классической модели Белла-ЛаПадулы, и фактически предполагают изоляцию друг от друга высокоуровневых и низкоуровневых *объектов системы, что является чрезмерно жестким требованием.*

Основные положения теоретико-информационных моделей.

КС соответствует требованиям **информационного невлияния** (без учета времени), если для $p(h) > 0$, $p(l) > 0$, выполняется:

$$p(l|h) = p(l).$$

При $p(h) > 0$, $p(l) > 0$ условие определения равносильно усло*вию:*

$$p(h|l) = p(h).$$

Если ввести параметр времени, то возможно данное условие сделать в большей степени применимым для использования в реальных системах.

Основные положения теоретико-информационных моделей.

В системе присутствует информационный поток от высокоуровневых объектов к низкоуровневым, если имеется возможность накопления информации в низкоуровневых объектах о значениях высокоуровневых объектов

Невозможность накопления информации обеспечивается тем, что совместный анализ значений состояний низкоуровневого объекта в текущий момент времени $l(t)$ и в предшествующий $l(t-1)$ не дает никакой новой информации о состоянии высокоуровневого объекта в предыдущий момент времени $h(t-1)$.

$p(l(t)|h(t-1), l(t-1)) = p(l(t)|l(t-1))$ отсюда выводится

$p(h(t)|l(t), l(t-1)) = p(h(t)|l(t-1))$

что выражает незапрещенность потоков из $l(t)$ *в* $h(t+1)$.

Существования скрытого канала с верхнего уровня на нижний, хотя физически этот канал не существует

Для объяснения этой ситуации рассмотрим двухуровневую систему, в которой уровень High соответствует аналитической подсистеме, вырабатывающей варианты некоторого решения. Уровень Low соответствует подсистеме сбора информации из открытых источников и открытых сетей. Пусть подсистемы Low и High связаны однонаправленным каналом от Low к High, который позволяет реплицировать на верхнем уровне собранные на нижнем уровне данные.

Для того, чтобы понять суть таких каналов, представим себе, что на верхнем уровне секретное решение принимается с помощью некоторого известного алгоритма только на основании информации, реплицированной с нижнего уровня. Зная это противник на нижнем уровне может из той же информации с помощью того же алгоритма получить точно такое же решение.

Два важных вывода

- многоуровневая политика не является гарантией безопасности, так как секретная информация верхнего уровня может стать известной на нижнем уровне независимо от способа реализации многоуровневой политики.
- наиболее общая вероятностная трактовка информационного потока не позволяет просто разделить множество информационных потоков на разрешенные и не разрешенные.

Автоматная модель невлияния

Согласно описанию автоматной модели безопасности информационных потоков система защиты представляется детерминированным автоматом, на вход которого поступает последовательность команд пользователей.

Для каждого пользователя системы задана функция выходов, определяющая, что каждый из них «видит» на устройстве вывода в соответствующем состоянии системы.

Если всех пользователей системы разделить на две группы (низкоуровневые и высокоуровневые), то требование информационного невлияния автоматной модели является требованием независимости низкоуровневого вывода системы от ее высокоуровневого ввода.

Автоматная модель невлияния

Рассмотрим систему автоматной модели как совокупность 4-ех объектов: высокоуровневых и низкоуровневых портов ввода/вывода high-in, high-out, low-in, low-out. При этом системный вывод полностью определяется системным вводом. Вероятностные отношения исключаются. Однако, если интерпретировать детерминированность автомата, используя события с вероятностью {0, 1}, то информационное невлияние можно определить следующим образом:

Пусть система автоматной модели безопасности информационных потоков представляется совокупностью четырех событий с вероятностью {0, 1}: high-in$_t$, high-out$_t$, low-in$_t$, low-out$_t$ для t = 0, 1, 2, …. Тогда система автоматной модели соответствует требованиям информационного невлияния, если выполняется условие

$$p(\text{low-out}_t \mid \text{high-in}_s, \text{low-in}_s) = p(\text{low-out}_t \mid \text{low-in}_s),$$

где s, t = 0, 1, 2, … и s < t.

Автоматная модель невлияния Гогена-Месигера (GM-модель)

Особая (автоматная) разновидность класса моделей конечных состояний

- КС можно представить детерминированным автоматом, на вход которого поступает последовательность команд пользователей
- для каждой команды каждого пользователя задана функция вывода, определяющая то, что каждый пользователь "видит" на выходе (на устройстве вывода)

J.Goguen, J.Meseguer, 1982г.
Идеология невлияния (невмешательства) вводов (команд) одних пользователей на (в) выводы других пользователей
(выводы – то, что они «видят» на выходе)

- два уровня безопасности (решетка из 2-х элементов) – высокий (*high*) и низкий (*low*)
- соответственно в системе работает две группы пользователей – высокоуровневые и низкоуровневые

Критерий безопасности в GM-модели - **ввод** высокоуровневого пользователя не может смешиваться с **выводом** низкоуровневого пользователя

Автоматная модель невлияния Гогена-Месигера (GM-модель)

Для реализации критерия безопасности в модели GM вводится функция вывода (out), задающая вывод системы, в зависимости от команды пользователя, его уровня безопасности и команд ввода в системе. предыстории (traces)

Если при формировании вывода для низкоуровневого пользователя в предыстории команд наблюдается смешивание, т. е. присутствуют вводы высокоуровневых пользователей, то посредством применения специальной процедуры очищения (purge) строится подправленная трассировка (предыстория) поведения системы, по которой функция out формирует вывод низкоуровневому пользователю

Основные тезисы и определения GM-модели

1.Состояние системы описывается 4-мя элементами:

-высокий ввод (high-in)
-низкий ввод (low-in)
-высокий вывод (high-out)
-низкий вывод (low-out)

2.На множестве пользователей *u* вводится функция *cl(u)*, отражающая уровень доверия пользователю (низкий или высокий)

3.Переходы системы по командам пользователей описываются функцией:

- out(u, hist.command(u)),

где *hist.command(u)* - история вводов системы *(traces)* от момента, когда был осуществлен последний ввод *in(u)* пользователя *u.*

4.Вводится функция очищения ввода *purge* - очищает историю ввода *traces* от наличия в ней команд пользователей, чей уровень доверия ниже уровня доверия пользователя *u*

Основные тезисы и определения GM-модели

5. Формальное определение функции очищения :

purge: users,traces $\rightarrow$ *traces* (функция, отображающая историю ввода системы с момента действий конкретного пользователя *u* в область историй ввода), такая, что:

- *purge*(*u*, < >) = < >, где < > - пустая история ввода

- *purge*(*u*, *hist.command*(*u*)) = *hist.command*(*u*)/*command*(*w*), если *command*(*w*) - ввод, исполненный пользователем *w* с момента *in*(*u*) и *cl*(*u*)<*cl*(*w*)

- *purge*(*u*, *hist.command*(*u*))=*hist.command*(*u*) $\wedge$ *hist.command*(*w*), если *command*(*w*) - ввод, исполняемый пользователем *w* с момента *in*(*u*), и *cl*(*u*)$\geq$*cl*(*w*)

Основные тезисы и определения GM-модели

Система удовлетворяет требованию *невлияния* (*невмешательства*), если и только если:

для всех пользователей *u*,
всех историй *hist*,
и всех команд вывода *command*

***out*(*u*, *hist.command*(*u*)) = *out*(*u*, *purge*(*u*, *hist.command*(*u*)))**

т.е. когда вывод в системе организован так, что система всегда чиста по смешиванию высоких и низких вводов в предыстории каждого вывода)