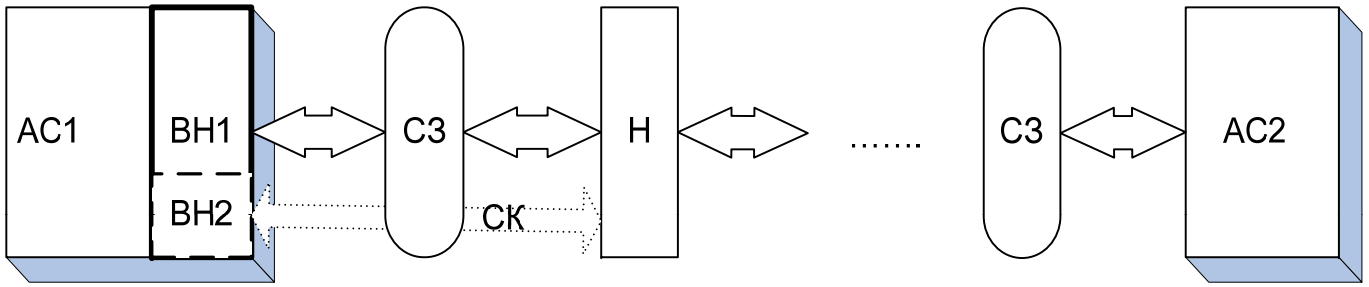
Скрытые каналы в автоматизированных системах и оценка пропускной способности скрытого канала при одном из возможных способов противодействия.

Матвеев Сергей Васильевич
Пензенский филиал ФГУП «НТЦ «Атлас», г.Пенза

Скрытые каналы

- Определение
  - Скрытый канал - это коммуникационный канал, который может быть использован для нарушения политики безопасности системы
- Виды скрытых каналов
  - по памяти (storage channels)
  - по времени (timing channels)
  - статистические

Схема взаимодействия скрытого канала с автоматизированной системой и средствами защиты



- АС1, АС2 – сегменты автоматизированной системы
- ВН1 – внутренний нарушитель системы обладающий полным контролем над коммуникационным каналом между сегментами АС
- ВН2 – внутренний нарушитель системы обладающий частичным контролем над коммуникационным каналом между сегментами АС
- СЗ – средства защиты АС
- Н – внешний нарушитель
- СК – скрытый канал

Угрозы, которые влечет за собой наличие или возможность построение скрытых каналов в автоматизированной системе

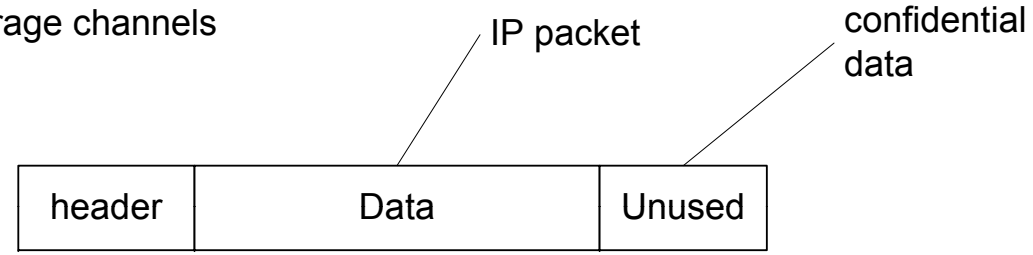
- У1 - утечка конфиденциальной информации из АС
- У2 - негативное, возможно деструктивное влияние извне, на деятельность АС

Механизмы построения скрытых каналов

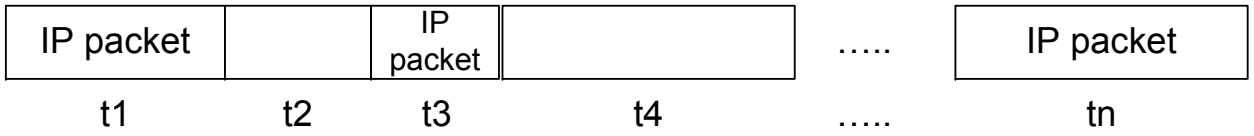
- К1 - внедрение данных в неиспользуемые поля передаваемых или принимаемых объектов (пакетов);
- К2 - внедрение данных в информационные объекты приводящее к внешне невидимым изменениям данных объектов;
- К3 - изменение длин передаваемых пакетов;
- К4 - изменение длин межпакетных интервалов;
- К5 - манипуляция адресами отправителя или получателя.

Примеры построения скрытых каналов в IP-сетях

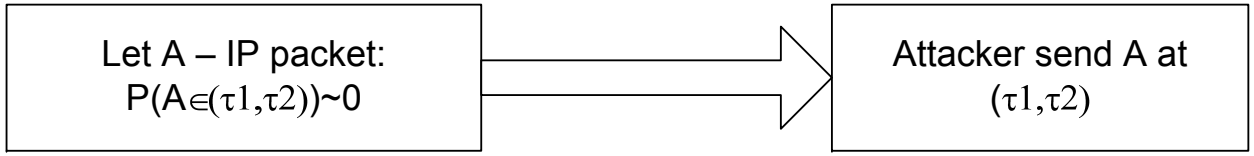
1) Storage channels



2) Timing channels



3) Statistic channels



Возможности внутреннего нарушителя необходимые для построения скрытых каналов

- В1 - возможность изменять содержимое служебных полей любого истинного передаваемого пакета (для построения каналов типа К1);
- В2 – возможность изменять информационное содержимое любого истинного передаваемого пакета (для построения каналов типа К2);
- В3 - возможность изменять длину любого пакета (для построения каналов типа К3);
- В4 - возможность формировать собственные ложные IP-пакеты произвольной длины (для построения каналов типа К3, К4, К5);
- В5 - возможность буферизовать все пакеты, подлежащие передаче из внутренней или внешней сети, и передавать из в канал в заранее определенный момент времени (для построения каналов типа К3, К4, К5);
- В6 – возможность получить полную информацию о топологии используемой сети связи (для построения каналов типа К5).

Применяемые механизмы для обеспечения защиты от скрытых каналов

- 31- нормализация неиспользуемых полей пакетов трафика;
- 32 - нормализация длин пакетов;
- 33 - нормализация длин межпакетных интервалов;
- 34 - нормализация процесса передачи пакетов различным адресатам;
- 35 - контроль и фильтрацию пакетов по заданным правилам (межсетевое экранирование);
- 36 - переформирование пакетов передаваемых или принимаемых из коммуникационной среды (использование прокси-серверов);
- 37 - туннелирование трафика с использованием алгоритмов криптографической защиты, таких как шифрование и имитозащита.

Соответствие между возможностями нарушителя и алгоритмами реализованными в средствах защит

	31	32	33	34	35	36	37
B1	+	-	-	-	±*	±*	+
B2	-	-	-	-	-	±	+
B3	-	+	-	-	±*	±*	-
B4	-	-	±	-	±*	-	+
B5	-	-	+	-	-	-	-
B6	-	-	-	+	-	-	-

- \+ - обозначает полную защиту от построения скрытых каналов в случае наличия у противника данной возможности от угроз У1(У2).
- ± - обозначает частичную защиту или защиту при определенных ограничениях на возможности нарушителя от угроз У1(У2).
- – - защита не обеспечивается.
- * – в зависимости от заданных правил.

Модель скрытого канала при одном способе противодействия

- существует внутренний нарушитель осуществляющий полный контроль внутреннего исходящего трафика (возможности В1-В6)
- все передаваемые граничным маршрутизатором пакеты имеют одну длину
- при необходимости для поддержания постоянной скорости в канал передаются маскирующие пакеты
- имеется возможность изменить скорость передачи данных в зависимости от реальной потребности
- возможность изменения скорости передачи данных происходит через административно заданный интервал времени n

Математическая модель скрытого канала

- $n_1, n_2, k, M \in Z$
- Передается n_1+k единичных символов и n_2 нулевых разделительных символов
- n_1, n_2 – фиксированные
- k – используется для кодирования информации
- $n_1+n_2=n>0$
- $k \in [0,M-1]$
- $P(k=i)=1/M, i \in [0,M-1]$

Оценка пропускной способности

Пропускная способность канала
C= W((2n-1)/e)/(n-½)/ln(2), где W(x) –функция Ламберта
W(x) – функция Ламберта, определяемая, как корень уравнения
y·exp(y)=x

$$C \approx \frac{\log_2 2n}{n} - \frac{\log_2(e \cdot \ln 2n)}{n}\left(1 - \frac{1}{\ln 2n}\right)$$, при $n \to \infty$

Значения пропускной способности для некоторых значений n

n	5	10	20	50	100
C	0.36	0.2314	0.14	0.07	0.045
C*	0.16	0.09	0.04	0.02	0.01

C – пропускная способность скрытого канала при кодировании информации длительностью интервала передачи
C* - пропускная способность скрытого канала при кодировании информации фактом смены скорости передачи данных

Выводы

- существует возможность передачи информации из частной сети по скрытому каналу даже при неполной нормализации скорости исходящего трафика
- изменяя параметры выравнивания трафика можно понизить скорость передачи по скрытому каналу

Литература

- 1. ГОСТ Р 53113.1-2008, "Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения."
- П.Волобуев. "Безопасность SCADA: Stuxnet – что это такое и как с ним бороться?", SecurityLab, 2010г.
- Матвеев С. В., "Пропускная способность некоторых видов скрытых каналов", Интеграл, №5, 2011г.