Защита информации от утечки по скрытым каналам

Лабораторная работа №3. Методы противодействия утечке информации по сетевым скрытым каналам

Содержание

1. Теория

Целью данной лабораторной работы является изучение способов противодействия утечке информации по сетевым скрытым каналам.

Общая схема противодействия представлена на рисунке ниже.

Рисунок 1. — Общая схема противодействия

После идентификации скрытого канала, то есть оценки возможности встраивания агента нарушителя, и определения степени опасности идентифицированного скрытого канала, идет этап принятия решения о необходимости противодействия угрозе. Меры противодействия делятся на превентивные — ограничение пропускной способности вплоть до устранения возможности построения скрытого канала, и не превентивные — обнаружение.

У обоих подходов есть свои преимущества и недостатки. Превентивные меры влияют на характеристики основного канала связи, например на пропускную способность этого канала. При этом, при использовании превентивных мер отсутствует вероятность ошибок первого и второго рода, то есть таких ошибок, как не распознавание функционирующего скрытого канала, и принятие легитимного трафика за функционирование скрытого канала соответственно.

Решение о применении защитных мер применяется исходя из вида скрытого канала. Так, превентивные меры для противодействия скрытым каналам по памяти влияют на канал связи меньше, чем превентивные меры для противодействия скрытым каналам по времени.

Однако, оценку эффективности применяемых мер защиты необходимо проводить для каждого из скрытых каналов в отдельности.

Кроме того, необходимо исходить из допущений при построении методов противодействия:

– противнику известна вся необходимая для организации скрытого канала информация о характеристиках сети пакетной передачи данных, в которой планируется его построение: топология сети, применяемое сетевое оборудование, пропускная способность каналов связи и так далее;

– противнику известны значения всех статических параметров метода противодействия;

– противнику неизвестны значения всех динамических параметров метода противодействия;

– задано значение пропускной способности скрытого канала *v0*, такое что функционирование скрытых каналов с пропускной способностью, не превосходящей *v0*, является допустимым.

Классически, при построении системы защиты необходимо исходить из модели нарушителя и модели угроз для защищаемой системы. В частности, для задачи защиты от утечки информации по скрытым каналам необходимо исходить из возможностей нарушителя, требуемых для построения скрытого канала.

На рисунке ниже продемонстрирована связь возможностей нарушителя и способов построения сетевых скрытых каналов.

Возможности нарушителя, необходимые для построения скрытого канала	**Способы построения скрытых каналов**				
	Изменение полей заголовков передаваемых пакетов (К1)	Изменение длин передаваемых пакетов (К2)	Изменение скорости передачи пакетов (К3)	Изменение длин межпакетных интервалов (К4)	Переупорядочивание пакетов, подлежащих отправке (К5)
Изменение содержимого полей пакетов	Да	Нет	Нет	Нет	Да
Изменение длин передаваемых пакетов	Нет	Да	Нет	Нет	Нет
Формирование фиктивных пакетов	Да	Да	Да	Да	Нет
Буферизация пакетов, подлежащих отправке, и передача в определенный момент времени	Нет	Да	Да	Да	Да
Добавление временных задержек при передаче пакетов	Нет	Нет	Да	Да	Нет

Рисунок 2 — Связь возможностей нарушителя и способов построения

Исходя из возможностей нарушителя, можно выделить основные превентивные способы противодействия, которые могут иметь три варианта, обозначенные на рисунке ниже:

– «+» — устранение возможности построения скрытого канала;
– «±» — ограничение пропускной способности скрытого канала;
– «-» — пропускная способность скрытого канала не ограничена.

Способы подавления и ограничения пропускной способности скрытых каналов	Способы построения скрытых каналов				
	К1	К2	К3	К4	К5
Нормализация значений полей заголовков пакетов	+	—	—	—	±
Нормализация длин передаваемых пакетов	—	+	—	—	—
Нормализация длин межпакетных интервалов	—	—	+	+	—
Фрагментация и агрегирование пакетов	—	±	±	±	±
Шифрование трафика	+	—	—	—	±
Генерация фиктивного трафика	±	±	±	±	±
Увеличение длин пакетов случайным образом перед отправкой пакетов	—	±	—	—	—
Введение дополнительных случайных задержек перед отправкой пакетов	—	—	±	±	±
Использование промежуточных шлюзов	+	+	±	±	+
Установление нескольких допустимых скоростей передачи пакетов	—	—	+	+	—

Рисунок 3. — Связь способов противодействия и способов построения скрытых каналов

В свою очередь методы обнаружения делятся на статистические и интеллектуальные (на основе алгоритмов машинного обучения). Статистические используют как классические математические способы обнаружения предсказуемости в трафике, означающей работу скрытого канала, так и специально разработанные новые способы. Часть статистических методов представлена на рисунке ниже.

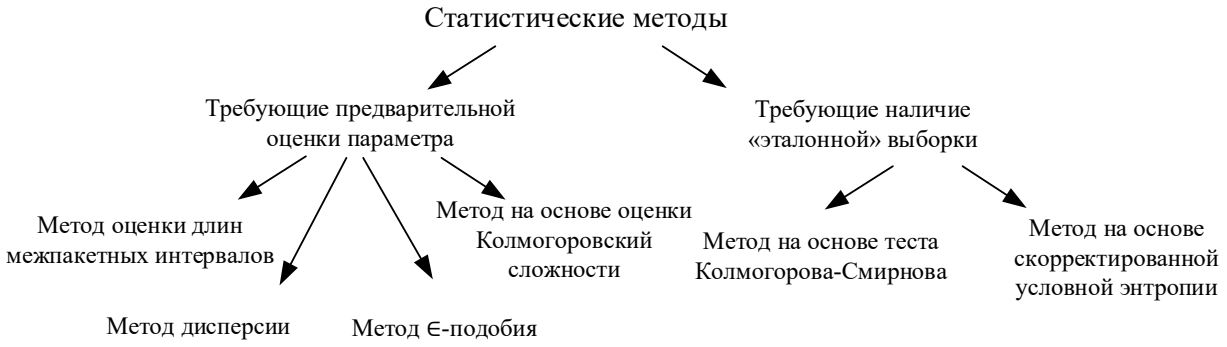

Рисунок 4. — Статистические методы обнаружения скрытых каналов по времени

Ключевой проблемой для многих методов обнаружения является требование наличия «эталонного» трафика, то есть трафика, в котором гарантированно отсутствует функционирующий скрытый канал.

2. Задание

Модифицировать стенд, разработанный в первой лабораторной работе таким образом, что устройство с закладкой и устройство защиты являются двумя логически отдельными устройствами.

Средство защиты теперь не является «заглушкой». Выбрать две схемы превентивного противодействия для разработанного скрытого канала, и реализовать их. Первая схема ограничивает пропускную способность скрытого канала. Вторая схема полностью устраняет возможность построения скрытого канала.

В отчете необходимо:

– Продемонстрировать работу средства защиты.

– Оценить эффективность выбранной схемы противодействия для двух случаев. Оценка заключается в анализе того, насколько сильно падает пропускная способность скрытого канала.

– Оценить влияние выбранной схемы противодействия для двух случаев на основной канал связи. Оценка заключается в анализе того, насколько сильно падает пропускная способность основного канала связи.

– Сделать вывод о возможности применения выбранных схем противодействия для задачи защиты от утечки информации по реализованному скрытому каналу.