

Защита информации от утечки по скрытым каналам

Лабораторная работа №1. Способы построения скрытых каналов.

Содержание

1. Теория.....	3
2. Задание	7
3. Варианты	9

1. Теория

Целью данной лабораторной работы является изучение способов построения скрытых каналов.

Скрытый канал — это канал связи (коммуникационный канал), изначально не предназначенный для передачи информации, нарушающий установленную политику безопасности информации.

Скрытые каналы по механизму передачи информации делятся на:

- скрытые каналы по памяти;
- скрытые каналы по времени.

Скрытые каналы по памяти основаны на наличии памяти, в которую передающий субъект записывает информацию, а принимающий — считывает ее. В скрытых каналах по времени передающий информацию субъект модулирует с помощью передаваемой информации некоторый изменяющийся во времени процесс, а субъект, принимающий информацию, в состоянии демодулировать передаваемый сигнал, наблюдая несущий информацию процесс во времени.

Более детальная классификация скрытых каналов в случае IP сетей представлена на рисунке ниже.

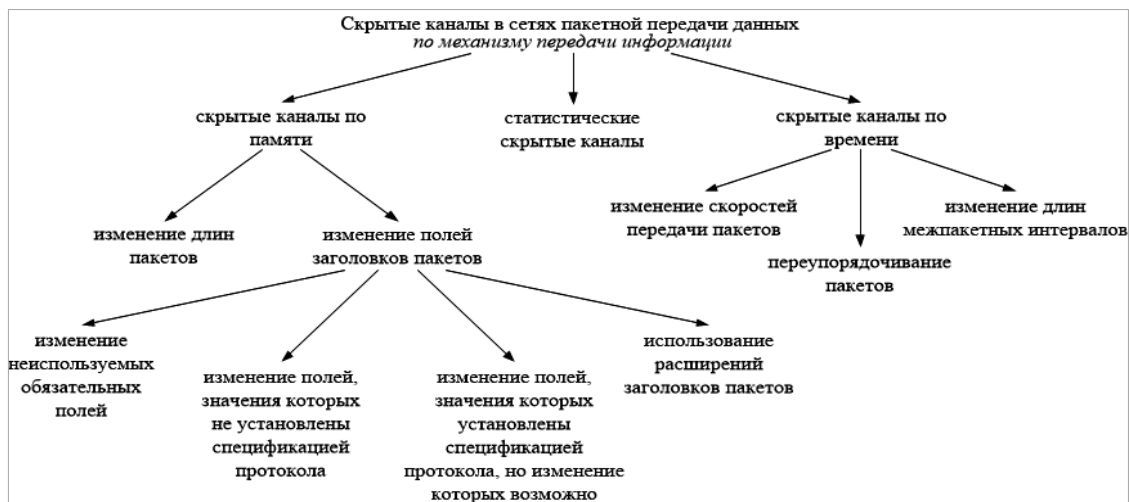


Рисунок 1. — Классификация скрытых каналов в сетях пакетной передачи данных

Закладка, реализующая скрытый канал, может обладать следующими возможностями:

- Буферизовать трафик;
- Модифицировать трафик;
- Генерировать фиктивный трафик.

Ниже приведены примеры различных сетевых скрытых каналов

- **Пример 1. Скрытый канал, основанный на изменении поля TTL заголовка пакета IPv4**

Определяется диапазон значений поля TTL, соответствующий единице, и диапазон значений, соответствующий нулю. В начальный момент времени нельзя передавать длинные последовательности, состоящие только из нулей или только из единиц, так как получателю необходимо понять разброс значений для определения, в каком диапазоне находятся ноль и единица.

- **Пример 2. Скрытый канал, основанный на изменении поля QoS заголовка пакета IPv4**

В данном поле последние два бита не используются и могут служить для негласной передачи информации. Зачастую маршрутизаторы игнорируют значение данного поля, следовательно, для передачи скрытой информации могут служить все 8 бит.

- **Пример 3. Скрытый канал, основанный на изменении поля Checksum заголовка пакета IPv4**

В данном случае используются неиспользуемые поля заголовка, заполняемые таким образом, чтобы получить требуемое значение в поле checksum.

- **Пример 4. Скрытый канал, основанный на изменении поля Hop Limit заголовка пакета IPv6**

Идея построения данного скрытого канала аналогична построению скрытого канала, основанного на изменении поля TTL заголовка пакета IPv4

- **Пример 5. Скрытый канал, основанный на изменении длин передаваемых пакетов**

Пусть L — максимальная длина пакета в битах. Предлагается разбить отрезок $[1, L]$ на $\frac{L}{n}$ диапазонов, где n — параметр скрытого канала, $n|L$. Пусть нарушитель имеет алфавит из $\frac{L}{n}$ символов, тогда для отправки символа с номером $i, i = \overline{1, \frac{L}{n}}$, злоумышленник посылает пакет, длина l которого удовлетворяет неравенству $(i - 1)n < l \leq in$.

- **Пример 6. Модифицированный скрытый канал, основанный на изменении длин передаваемых пакетов**

Пусть $S = s_0 \dots s_{k-1}$ — секретное сообщение, представляющее собой k -битную строку. Данная строка разбивается на подстроки перед отправкой. $W_i = s_{iw} \dots s_{iw+w-1}$ — $i^{\text{ая}}$ битовая подстрока строки S . SUM_i — десятичное представление W_i , вычисляемое по правилу:

$$SUM_i = \begin{cases} [W_i]_{10} - 2^{w-1}, i(mod 2) = 0, \\ [W_i]_{10} - (2^{w-1} - 1), i(mod 2) = 1. \end{cases} \quad (1)$$

Представим алгоритм передачи информации по скрытому каналу [18]:

- шаг 1 — А и В общаются в обычном режиме, записывают длины передаваемых пакетов в Справочник;
- шаг 2 — А и В случайным образом выбирают длину l из Справочника;
- шаг 3 — во время i ой отправки сообщения А отправляет В сообщение длины $l_{next} = l + SUM_i$, Справочник обновляется добавлением в него l_{next} ;
- шаг 4 — В восстанавливает i ое сообщение: $SUM_i = (l_{next} - l)$ и вычисляет W_i ;
- шаг 5 — шаги два и три повторяются до тех пор, пока секретное сообщение не передается до конца.

Замечания:

- А и В знают k, w, i ;
- если L_{max} — максимальная длина сообщений в начальном заполнении Справочника, то должно выполняться соотношение $L_{max} > 2^w$;
- на третьем шаге, если $l_{next} < 0$, то $l_{next} = l_{next} + L_{max}$.

• **Пример 7. Простейший скрытый канал, основанный на изменении скоростей передаваемых пакетов**

В данном скрытом канале по времени информация кодируется посредством прибытия/отсутствия пакета в течение каждого временного интервала t .

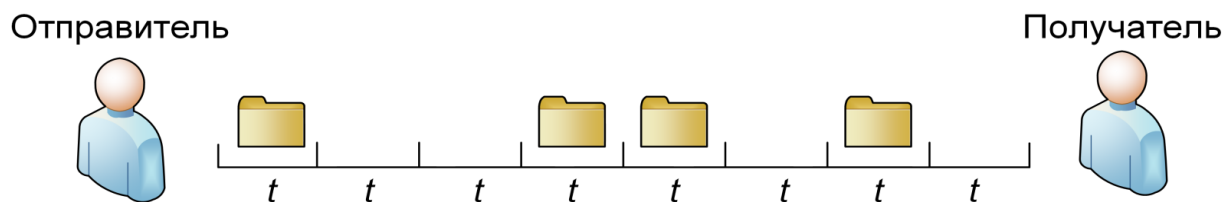


Рисунок 2. — Пример передачи сообщения «10011010» по скрытому каналу, основанному на изменении скоростей передаваемых пакетов

• **Пример 8. Скрытый канал, основанный на изменении длин межпакетных интервалов**

В данном случае измеряется время между приходами двух последовательных пакетов (другими словами, измеряются длины межпакетных интервалов). Информация кодируется в значениях длин межпакетных интервалов, схема кодирования оговаривается

заранее (в простейшем случае — выбирается пороговое значение, все значения ниже которого соответствуют «0», выше — «1»).

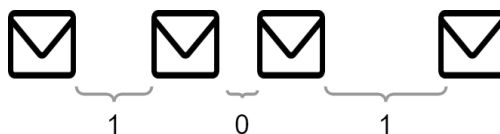


Рисунок 3. — Кодирование информации в скрытом канале, основанном на изменении длин межпакетных интервалов

- **Пример 9. Time Relay Covert Channel**

Исходя из измерения возможных значений задержек между пакетами в открытом трафике, определяется медианное значение этого множества, и при передаче скрытого сообщения для кодирования 0 выбирается значение межпакетного интервала из подмножества значений, которые больше медианного, а для 1 — которые меньше.

- **Пример 10. Модификация скрытого канала, основанного на изменении длин межпакетных интервалов**

Значение Δ используется для модификации межпакетного интервала, учитывая при этом базисную величину межпакетной задержки t_b . Если кодируется 0, то время между пакетами не изменяется, а если кодируется 1, то либо увеличивается, либо уменьшается на величину Δ . В таблице ниже приведена схема кодирования.

Таблица 1. — Схема кодирования информации в модифицированном скрытом канале, основанном на изменении длин межпакетных интервалов

Передаваемый бит	Предыдущий интервал	Текущий интервал
0	t_b	t_b
0	$t_b + \Delta$	$t_b + \Delta$
1	t_b	$t_b + \Delta$
1	$t_b + \Delta$	t_b

В качестве информации, которую можно передать по скрытому каналу, может выступать любая чувствительная информация.

2. Задание

1) Разработать стенд, имитирующий информационное взаимодействие двух пользователей по разрешенному каналу связи, который контролируется устройством защиты. В данное устройство защиты внедрена закладка, реализующая скрытый канал. Разрешенный канал связи прослушивает злоумышленник, выделяя из трафика передаваемое закладкой скрытое сообщение. Схема стенда представлена на рисунке ниже.

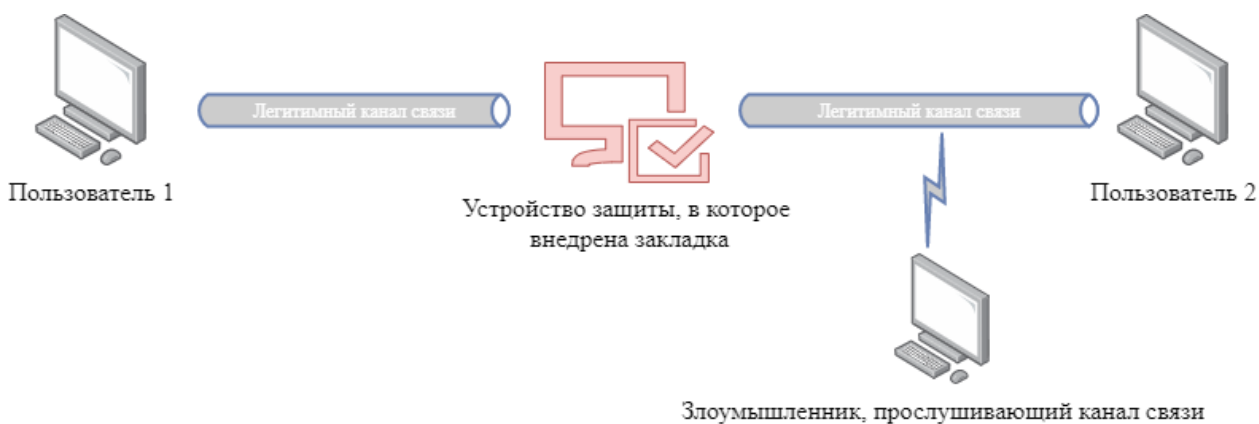


Рисунок 4. — Схема лабораторного стенда

- Пользователь 1, Устройство защиты и Пользователь 2 — отдельные логические устройства в сетевом взаимодействии (должны быть реализованы отдельными программными средствами).
 - Для простоты реализации Злоумышленник может считаться отдельным модулем в рамках устройства Пользователь 2.
 - У закладки должна иметься возможность передавать ей в качестве параметра необходимое скрытое сообщение. Злоумышленник должен иметь возможность корректно декодировать передаваемое скрытое сообщение.
- 2) Предоставить анализ того, как меняется трафик в зависимости от активности закладки, реализующей скрытый канал.
- 3) Продемонстрировать процесс кодирования и декодирования скрытой информации на сторонах отправителя и получателя соответственно. Продемонстрировать принцип работы закладки.

Примечания:

1) Рекомендуемый язык программирования — Python. Удобным средством в языке программирования Python для передачи параметров скрипту является библиотека `argparse`. В листинге ниже представлен пример кода, реализующего возможность передачи параметров программному средству.

```
import argparse

def parse_arguments():
    parser = argparse.ArgumentParser(description='Covert channel emulation',
                                     formatter_class=argparse.ArgumentDefaultsHelpFormatter
    )
    parser.add_argument('-f', '--filename', help='data to tranfer via covert channel',
                        required=True, dest='filename', type=str, default='test')
    return parser.parse_args()

def main():
    args = parse_arguments()
    fname = args.filename

if __name__ == "__main__":
    main()
```

Листинг 1. — Передача параметров

2) В качестве средства анализа трафика рекомендуется использовать ПО Wireshark (<https://www.wireshark.org/>). В процессе сдачи лабораторной работы оно должно быть установлено на ПК сдающего. Также в отчете при описании построенного скрытого канала необходимо привести скриншоты трафика с пометкой, где расположена скрытая информация.

3) Для защиты лабораторной работы необходимо предоставить отчет, содержащий в себе описание хода выполнения и результатов всех указанных в задании пунктов.

3. Варианты

Модели штатной (без наличия скрытого канала) передачи информации:

- Модель 1. Пакеты фиксированной длины передаются в фиксированные моменты времени.
- Модель 2. Пакеты фиксированной длины передаются в случайные моменты времени.
- Модель 3. Пакеты случайной длины передаются в фиксированные моменты времени.
- Модель 4. Пакеты случайной длины передаются в случайные моменты времени.

№	Модель штатной передачи информации	Скрытый канал	Возможности закладки
1	Модель 1	Пример 7	<ul style="list-style-type: none">• Буферизация трафика• Генерация фиктивного трафика
2	Модель 3	Комбинация из Пример 1, Пример 2 и Пример 3. В качестве доп. параметра для скрытого канала указывается, в какие поля встраивать секретное сообщение	Модификация трафика
3	Модель 3	Пример 5. Максимальная длина пересылаемого пакета задается через параметр Пользователя 1.	Модификация трафика
4	Модель 2	Пример 10	<ul style="list-style-type: none">• Буферизация трафика• Генерация фиктивного трафика
5	Модель 1	Пример 4	Модификация трафика
6	Модель 4	Пример 6	<ul style="list-style-type: none">• Буферизация трафика• Модификация трафика
7	Модель 4	Пример 9	<ul style="list-style-type: none">• Буферизация трафика• Генерация фиктивного трафика
8	Модель 4	Пример 8	<ul style="list-style-type: none">• Буферизация трафика

№	Модель штатной передачи информации	Скрытый канал	Возможности закладки
			<ul style="list-style-type: none"> Генерация фиктивного трафика
9	Модель 4	Пример 10	<ul style="list-style-type: none"> Буферизация трафика Генерация фиктивного трафика
10	Модель 4	Пример 6	<ul style="list-style-type: none"> Буферизация трафика Модификация трафика
11	Модель 1	Пример 5. Максимальная длина пересылаемого пакета задается через параметр Пользователя 1.	Модификация трафика
12	Модель 2	Пример 7	<ul style="list-style-type: none"> Буферизация трафика Генерация фиктивного трафика
13	Модель 3	Пример 9	<ul style="list-style-type: none"> Буферизация трафика Генерация фиктивного трафика

Номер варианта определяется по формуле $(N \bmod 13) + 1$, где N – номер в списке группы.