А. А. Миронов
Инженер первой категории ПАО «Интелтех», кандидат технических наук, доцент

Н. Л. Томилин
Ведущий инженер ПАО «Интелтех», кандидат технических наук

АНАЛИЗ ВОЗМОЖНОСТЕЙ ФОРМИРОВАНИЯ СТЕГОСИГНАЛА ПРИ ПЕРЕДАЧЕ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ПАРАМЕТРОВ СЕТЕВОГО IP ПРОТОКОЛА

АННОТАЦИЯ. Дается краткий анализ возможностей скрытой передачи информации с использованием штатных средств защищенных мультисервисных *IP* сетей и общий подход к обеспечению защиты от формирования стегосигнала при передаче информации.

КЛЮЧЕВЫЕ СЛОВА: стеганография, стегосигнал, эхо-запросы ping, IP –пакет, специальное программное обеспечение

Введение

К числу основных параметров *IP* протокола, посредством которых возможно формировать стегосигнал при передаче информации, следует отнести:

1) Манипуляция длиной пакетов («морзянка пакетов»).

2) Манипуляция длиной заголовка пакета (частный случай «морзянки»).

3) Непосредственное кодирование бит в полях заголовка, неиспользуемых в ходе информационного обмена.

4) Изменение отдельных бит заголовка по заранее известному закону («моргание» битами).

5) Манипуляция количеством посланных эхо-запросов *ping*.

> ***Примечание:*** стегосигнал от слова «стеганогра́фия» (от греч. στεγανός «скрытый» + γράφω «пишу»; написание букв, «тайнопись») — способ передачи или хранения информации с учетом сохранения в тайне самого факта такой передачи (хранения).

Рассмотрим каждый вариант стегосигнала в отдельности.

1. Манипуляция длиной пакетов («морзянка» пакетов)

Способ тайной передачи информации путем изменения длин передаваемых пакетов по заранее известному закону.

Одним из примеров такого закона является код Морзе. В этом случае короткий пакет является «точкой», а длинный пакет — «тире». Аварийный сигнал *SOS*, передаваемый кодом Морзе имеет вид: ... —- ... (3 «точки» — 3 «тире» — 3 «точки»). Этот же сигнал, переданный посредством IP пакетов с использованием «морзянки пакетов» может выглядеть следующим образом: IP-пакет [500 байт] — IP-пакет [500 байт] — IP-пакет [500 байт] — IP-пакет [1500 байт] — IP-пакет [1500 байт] — IP-пакет [1500 байт] — IP-пакет [500 байт] — IP-пакет [500 байт] — IP-пакет [500 байт]. Естественно, все пакеты однозначно определяются как принадлежащие одному сеансу передачи информации.

Законы формирования «морзянки» могут быть различными и зависят только от воображения и способностей разработчика. Чем сложнее применяемый для стегосигнала алфавит, тем выше вероятность скрыть его в передаваемой информации.

Реализация данного способа требует обязательного наличия на сторонах передачи и приема специального программного или аппаратно-программного обеспечения, которое непосредственно будет осуществлять перехват пакетов и их модуляцию по заранее заложенному закону.

Способы борьбы с «морзянкой пакетов»:

– выравнивание длин пакетов на границе с транспортной сетью — технический способ;

– осуществление контроля за внедрением специального программного (аппаратно-программного) обеспечения (СПО, САПО) в тракт передачи пакетной информации — административно-технологический способ.

На самом деле, исходя из обязательности наличия СПО (САПО), реализация данного способа достаточно затруднительна, так как СПО можно внедрить только на автоматизированном рабочем месте должностного лица (АРМ ДЛ). В сетевое оборудование внедрение практически маловероятно, по причине закрытости программного обеспечения самого оборудования. АРМ ДЛ специального назначения, в свою очередь, имеют средства защиты от установки посторонних программных продуктов. В случае установки САПО сложностей возникает еще больше, так как требуется включение САПО непосредственно в тракт, с обеспечением доступа к нему для ввода передаваемой (модулирующей) информации. В таком случае, устройство может быть обнаружено визуально.

2. Манипуляция длиной заголовка пакета (частный случай «морзянки»)

Способ, отличающийся от первого только тем, что манипуляциям подвергается только длина заголовка за счет поля *IP* пакета — «параметры и выравнивание (*Options&Padding*)». В этом случае длина заголовка *IP* пакета может варьироваться от 20 байт (минимальное значение) до 60 байт (максимальное значение). Реализация данного способа намного сложнее первого, а с учетом того, что не все сетевое оборудование (в частности, маршрутизаторы) могут обрабатывать пакеты с длиной заголовка более 20 байт, то и вовсе маловероятна.

Способы борьбы аналогичны «морзянке пакетов».

3. Непосредственное кодирование бит в полях заголовка, неиспользуемых в ходе информационного обмена

Данный способ заключается в скрытой передаче информации посредством кодирования бит полей заголовка, незадействованных в передаче пакетов. К таким битам можно отнести:

– поле *TOS* (*type of service* — тип сервиса), биты 7–8 (как зарезервированные в большинстве случаев);

– поле *TTL* (*time to live* — время жизни пакета), биты 1–3 (так как, чаще всего *TTL* устанавливается не более 32);

– поле *Options&Padding* (параметры и выравнивание), фактически можно использовать все биты, хотя есть ограничения. Количество бит в этом случае может быть до 320 (40 байт по 8 бит).

Данный способ, как и все остальные, требует наличия СПО (САПО) и, в ряде случаев, не гарантирует доставки скрываемой информации, так как на промежуточных узлах сети оборудование может полностью изменять содержание указанных полей (в частности, маршрутизаторы могут изменять поле *TTL*, устанавливая свое значение (помимо уменьшения на единицу), а криптомаршрутизаторы могут устанавливать значение поля *TOS* в «неопределенность»). Пакеты с полем *Options&Padding* могут вообще отбрасываться рядом сетевого оборудования.

Способы борьбы:

– явная установка на граничном с транспортной сетью устройстве значений бит полей *TTL* и *TOS*;

– запрет обработки на граничном устройстве и транзитных узлах пакетов с полем *Options&Padding* (этот же способ является одним из основных в случае «морзянки» заголовка пакета).

В целом, способ требует больших трудозатрат и, с большой долей вероятности, не обеспечивает доставку информации нарушителю.

4. Изменение отдельных бит заголовка по заранее известному закону («моргание» битами)

Является частным случаем третьего способа. Отличается тем, что кодируется не группа бит вышеуказанных полей заголовка, а осуществляется манипуляция одним конкретным битом вышеуказанных полей в потоке пакетов. Например, значение 7 бита поля *TOS* в 3-х первых пакетах

будет равно «0», затем в 3-х последующих «1» и в следующих 3-х пакетов опять равны «0». На приемной стороне получим последовательность 000–111–000, то есть аварийный сигнал *SOS*. По сути данный способ является прямой реализацией бинарного кода Морзе одним битом заголовка.

Реализация и способы противодействия аналогичны способу 3.

5. Манипуляция количеством посланных эхо-запросов *ping*

Способ, не требующий на передающей стороне СПО (САПО), легко реализуемый (так как любое сетевое оборудование и любая операционная система имеют такой функционал), заключающийся в передаче скрываемой информации комбинаций посылок эхо-запросов типа *ping*. Подавляющее большинство сетевого оборудования и операционных систем позволяют устанавливать количество посылок *ping* от 1 до 255, что и позволяет использовать данный способ при передаче информации. Например, совокупность команд *Linux*-подобной ОС:

$*ping* — с 3 < *IP*-адрес получателя>
пауза 10 сек.
$*ping* — с 6 < *IP*-адрес получателя>
пауза 10 сек.
$*ping* — с 3 < *IP*-адрес получателя>

приведет к тому, что получающая сторона увидит комбинацию: 3 *ping*-пакета, пауза 10 сек, 6 *ping*-пакетов, пауза 10 сек, 3 *ping*-пакета.

При заранее установленном алфавите комбинаций *ping*-проб получатель получит сигнал *SOS*.

Бороться с таким каналом утечки информации возможно простым запретом передачи и обработки *ping*-проб на всех типах сетевого оборудования. Но, как показывает практика, посылка *ping*-проб является единственным способом проверки доступности сетевого оборудования и канала для администраторов сети и данную блокировку чаще всего снимают.

Выводы

1) Формирование стегосигнала посредством управления параметрами *IP* пакета является достаточно сложной технологией, требующей от нарушителя максимальных прав доступа к передаваемой информации, оборудованию и тракту ее прохождения. Также требует наличия специального программного продукта и хорошего уровня знаний операционных систем, сетевого оборудования и функционирования сетевых протоколов. В системах с высокими требованиям по информационной безопасности, тем не менее, должны быть предусмотрены организационные и технические меры, исключающие возможность нарушителю формировать стегосигнал при передаче информации.

2) Формирование стегосигнала посредством *ping*-проб требует доступа к сетевому оборудованию (но не обязателен максимальный уровень прав доступа), Он не требует специального программного обеспечения СПО (САПО) и высокого уровня подготовки нарушителя. Противодействовать данному способу утечки тайной информации значительно проще, так как любое сетевое оборудование и любая операционная система имеют возможность блокировать отправку и обработку *ping*-проб.

ЛИТЕРАТУРА

1. **Ричард СтивенсУ.** Протоколы TCP/IP. Практическое руководство. — СПб.: «Невский Диалект» — «БХВ-Петербург». 2003 г.

2. **Таненбаум Э., Уэзеролл А.** Компьютерные сети. — СПб.: Питер, 2017.