ОРГАНИЗАЦИЯ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ СКРЫТОМУ ОБМЕНУ ИНФОРМАЦИЕЙ МЕЖДУ ОБЪЕКТАМИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Дорошенко Я.В.
Харьковский Национальный Университет Радиоэлектроники
(61166 Харьков, пр.Ленина,14, кафедра ТКС, т.702-13-20)
E-mail: slavon85@mail.ru

This work considers actual problem of network security is control system defense against forming of control hiding channels for data exchange between network elements. A complexity for solving this problem consists of heterogeneity of elements, telecommunication multitasking, randomicity of processes, dynamic character and dependency of control functions. There are steganographic detecting of hiding channels, estimation of attack potential, signals detection and erasing described as methods for developing countermeasures.

Введение

Одной из актуальных на сегодняшний день проблем сетевой защиты является противодействие формированию скрытых каналов управления отдельными объектами телекоммуникационных сетей (ТС). Сложность противодействия связана, прежде всего, со сложностью, возникающей при проектировании и анализе ТС, а конкретней:

- разнородностью составляющих элементов, каждый из которых решает свою частную задачу в рамках единой цели функционирования всей ТС;
- сложность взаимосвязей между отдельными элементами ТС и описывающими их параметрами;
- многоплановость решения телекоммуникационных задач;
- случайный характер протекающих в системе процессов;
- зависимость функции управления от множества случайных фактов и т. д.

Злоумышленник, используя агентную концепцию построения систем управления (СУ) ТС, с использованием нескольких каналов передачи данных, разнесенно во времени, передает и активирует код, приводя этим к новым возможностям воздействия на функции ядра СУ ТС (рис. 1).

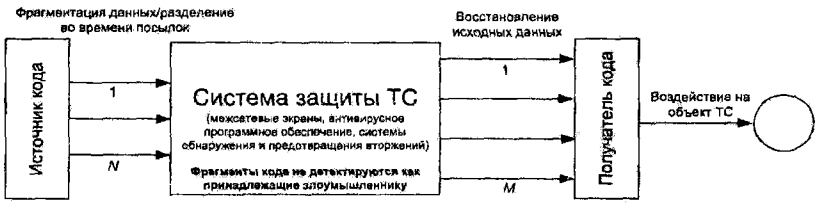

Рис. 1. Передача информации злоумышленником в обход системы защиты ТС с применением пространственно-временного разделения данных

Скрытые каналы эффективно создаются при помощи стеганографических методов. Это может быть:

- передача нейтральной по отношению к управляющей информации, не относящейся к процедурам управления, одновременно с основной и дальнейшее восстановление новых последовательностей команд;
- передача дополнительного управляющего кода в виде измененной последовательности высокоуровневых управляющих команд или низкоуровневых инструкций;
- активация с помощью нефильтруемых команд программ-закладок в СУ, ответственных за отладку отдельных процедур управления для запуска потенциально опасного кода.

Противодействие с использованием анализа скрытой пропускной способности подканала

Классическим подходом, который используются на сегодняшний день в системах противодействия скрытой передаче информации, является ограничение пропускной способности скрытого подканала путем ухудшения помеховой обстановки. В таком случае модель противодействия можно описать с помощью теории игр в виде противодействия злоумышленника (З) и защитника системы (ЗС), выбирающих решения исходя из условий:

- немодификации каналов, не используемых для скрытой передачи информации (З, ЗС);
- точного помехового воздействия на скрытый подканал при различных предположениях о методе внедрения, путем выбора преобразований, инвариантых для канала и существенно изменяющих характеристики скрытого подканала (ЗС);
- снижения пропускной способности подканала до той степени, когда увеличение уровня шума будет воздействовать не только на подканал, но и на канал в целом (З).

Однако, в современных системах скрытой передачи информации исходящий поток данных разделяется в демультиплексоре на N потоков для обработки и передачи по отдельным каналам. На приемной стороне имеется M приемных каналов, данные с которых проходят через мультиплексор и обрабатывается по специальным алгоритмам, позволяющим снизить число ошибок приема, вызванных искажениями в канале передачи и пространственной корреляцией сигналов.

В связи с этим возникла проблема многоканального анализа скрытых подканалов, который предполагает решение пяти взаимосвязанных задач:

1) выявление возможности организации скрытых подканалов;
2) оценка пропускной способности скрытых подканалов и оценка опасности, которую несет их скрытое функционирование;
3) оценка возможности изменения характеристик канала таким образом, чтобы внедренная информация не могла быть выделена;
4) определение характеристик сигнала на основе данных всех наблюдаемых каналов информационного обмена;
5) формирование стираемых воздействий для противодействия скрытой передачи информации.

Метод многоканального анализа данных с целью выявления передачи скрытой информации, аналогичен методам анализа систем MIMO и методов пространственно-временного кодирования. Определяя возможных получателей информации в СУ ТС производит корреляционный анализ как параметров канала, так и передаваемых по ним данных. Информационное противодействие З и ЗС и здесь может моделироваться с помощью аппарата теории игр с участием множества З и ЗС.

Выводы

В работе рассматривался вариант организации системы противодействия обмену информации в скрытых подканалах, организованных на основе стеганографических методов. Был предложен метод противодействия, в котором совмещены классические способы противодействия с применением шумоподобных сигналов для воздействия на канал, а также способ анализа многоканальных систем передачи сигналов и метод противодействия коррекции параметров множества подканалов с использованем аппарата теории игр.