УДК 004.42

СТЕГАНОГРАФИЧЕСКАЯ СИСТЕМА “МЫШЬ”

Асташев В. Б., Данилевский А. В., Шипулин П. М.,
научный руководитель канд. техн. наук Шниперов А. Н.
Сибирский федеральный университет

Обширная слежка за людьми по всему является, наверное, одной из самых нерешаемых проблем. Ведь обычным людям не хочется знать, что их разговоры, переписка, местоположение и прочая конфиденциальная информация вовсе не являются закрытыми. А правительствам особо развитых стран, наоборот, предпочтительнее знать все о своих и не только гражданах. Так становится проще пресекать правонарушения на начальных стадиях.

Мы изучили лучшие мировые практики решения проблемы конфиденциальности. В качестве приоритетной области поиска решения нами была выбрана активно развивающаяся наука стеганография. В результате была разработана сетевая стеганографическая система.

Стеганографическая система “Мышь” не имеет открытых аналогов. Факт ее использования достаточно сложно выявить, а использованные средства защиты передаваемой информации позволяют надежно защитить передаваемые сообщения. Единственное средство ограничить использование нашей системы - отключить канал связи, по которому она работает.

В легальном канале передается информация о состоянии подконтрольной системы (загрузка процессора, размер свободной памяти, температура, и т.д.), контейнером для передачи сообщения являются задержки в передаче пакетов. Система состоит из двух элементов: клиента и сервера. Сервер передает информацию, клиент - получает.

За основу алгоритма передачи взят материал из диссертации Сердара Кабука, которая содержит теоретическую информацию об основах создания подобных стеганосистем.

Секретное сообщение разбивается на задержки (от 1 до 2 единиц), помехоустойчиво кодируется. От сервера к клиенту постоянно ведется передача информации в легальном канале по протоколу UDP. В каждый момент передачи генерируется случайная задержка (от 1 до 2 единиц), во время передачи секретной информации (вычисленное заранее) задержка имеет неслучайный характер (передается одна единица информации). Клиент собирает части сообщения, проверяет их на повреждения и, в случае необходимости, запрашивает испорченный кусок заново.

В определенное время производится тестирование скорости передачи данных. Опционально доступно шифрование секретного сообщения по алгоритму AES.

Стеганографическая система работает только в локальной сети. Для ее работы требуются два компьютера под управлением любых современных операционных систем из семейств Windows/Mac OS/Linux с установленным Python 3.

Стеганографическая система «Мышь» передает сообщения со скоростью до 30 байт/мин, при этом для передачи 1 бита секретной информации необходимо передать 128 бит информации в легальном канале (2 информационных пакета).

Программный комплекс (клиент, сервер) тестировался на двух компьютерах, каждый из которых поочередно являлся сервером и клиентом. Разницы во времени передачи от перестановки программ на компьютерах не замечено. Полная информация о компьютерах, на которых производилось тестирование представлена в таблице 1.

	Компьютер 1	Компьютер 2
Процессор	Intel Core i7 2.7 GHz	AMD A6 2.1 GHz
Количество ядер	2	2
Объем оперативной памяти	8 ГБ	4 ГБ
Операционная система	Mac OS X 10.9.1	Fedora 19
Разрядность операционной системы	64 бит	64 бит

Таблица 1. Технические характеристики компьютеров, на которых производилось тестирование комплекса.

Была проверена возможность передачи данных при полностью загруженном процессоре и оперативной памяти сервера. Как оказалось, полная загрузка не оказывает влияния на возможность передачи секретного сообщения.

Была проверена возможность передачи данных при трех видах организации локальной сети. Настройки программ для стабильной передачи подбирались опытным путем. Результаты тестирования, настройки программ и тип подключения представлены в таблицах 2, 3 и 4.

Длина сообщения (байты)	Время передачи (секунды)
10	18
20	29
40	57
80	116

Таблица 2. Тестирование системы при подключении через Ethernet.

Длина сообщения (байты)	Время передачи (секунды)
10	17
20	30
40	55
80	116

Таблица 3. Тестирование системы при подключении точка-точка через Wifi.

Длина сообщения (байты)	Время передачи (секунды)
10	39
20	77
40	149
80	293

Таблица 4. Тестирование системы при подключении через Wifi-маршрутизатор.

Стеганографическая система “Мышь” получилась точно такой, какой она была задумана. Ее основные преимущества - это скрытность факта передачи сообщения, а также возможности его дополнительного шифрования и тонкой настройки.

Все недостатки системы решаются путем продолжения разработки.

Разработка стеганографической системы “Мышь” может быть продолжена в следующих направлениях:

- внедрение сертифицированных алгоритмов шифрования,
- внедрение помехоустойчивого кодирования с возможностью исправления ошибок,
- разбитие сообщения на пакеты,
- внедрение “бесконечной” передачи со стороны сервера.