Таким образом, предложен новый метод обнаружения сетевых аномалий по временным рядам одного из показателей состояния сети, который не требует наличия данных для обучения системы обнаружения аномалий.

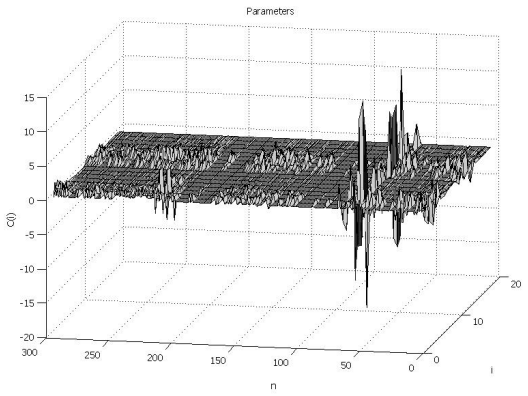

Рис. 1

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Гостев А.*, Современные информационные угрозы, I квартал 2007, http://www.viruslist.com/ru/analysis?pubid=204007545

2. *Thottan M. and Ji C.*, Anomaly Detection in IP Networks, IEEE transactions on signal processing, Vol. 51, No. 8, 2003

3. *Gautama T., Mandic D., Van Hulle M.*, A differential Entropy based method for determining the optimal embedding parameters of a signal, 2003

4. MIT Lincoln Library DARPA Intrusion Detection Evaluation, http://www.ll.mit.edu/IST/ideval/data/data_index.html

П.П. Кравченко, Н.Ш. Хусаинов, А.Н. Шкурко
Россия, г. Таганрог, Технологический институт ЮФУ

МЕТОДЫ ОГРАНИЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ПЕРЕДАВАЕМЫМ МЕДИАДАННЫМ В АРХИТЕКТУРЕ СИСТЕМЫ МНОГОСТОРОННЕЙ ВИДЕОКОНФЕРЕНЦСВЯЗИ «ДЕЛЬТА-КОНФЕРЕНЦИЯ»

В последнее время все большее распространение в задачах управления бизнесом получают системы многосторонней видеоконференцсвязи (ВКС). Это связано с тем, что эффект от аудиовизуального общения значительно выше, чем при общении по телефону, а тем более посредством электронной почты и т.п. Во время сеанса видеоконференцсвязи имеется возможность наблюдать реакцию собеседника, что может быть особенно важно в деловых переговорах. Но, несмотря на явные преимущества подобных систем, не многие компании активно используют их в своей работе. Это связано, прежде всего, с тем, что, во-первых, существующие на рынке системы отличаются дороговизной, и, следовательно, могут быть по карману только достаточно крупным компаниям, во-вторых, существующие системы зачастую отличаются низким соотношением цена/качество и, наконец, большинство известных программных систем ВКС предполагают взаимодействие между пользователями через централизованный сервер компании-производителя (через Интернет). Также этот выделенный сервер (аппаратно-программный комплекс) может быть приобретен отдельно, но его стоимость крайне высока. Следует также

отметить, что значительная часть существующих коммерческих систем ВКС являются аппаратными, а, следовательно, имеют более высокую стоимость закупки и внедрения по сравнению с программными решениями.

Поскольку система ВКС является, по сути, распределенным приложением, то выбор архитектуры соединения программных терминалов имеет принципиальное значение для ее функционирования и развития. Анализируя область применения и среду использования системы ВКС, можно выделить следующие требования к архитектуре соединения терминалов:

- архитектура должна обладать высокой отказоустойчивостью;
- должна присутствовать возможность масштабирования;
- архитектура должна учитывать конфигурацию сетевых инфраструктур.

В существующих системах ВКС чаще всего применяется архитектура типа "клиент-сервер". В роли клиентов здесь выступают терминалы участников конференции, а в роли сервера – выделенное устройство MCU (Multipoint Control Unit), состоящее из двух основных модулей: модуля централизованного управления MC (Multipoint Controller) и, опционально, модуля централизованного обмена данными MP (Multipoint Processor).

При этом функционирование конференции может происходить в двух режимах:

- централизованном – обмен данными и управляющей информацией между участниками сеанса конференции происходит через модуль MCU, управляющая информация распространяется посредством MC, а данные посредством MP;
- децентрализованном – обмен управляющей информацией происходит через MC, а данными участники (по возможности) обмениваются напрямую, модуль MP при этом не используется.

Данная архитектура в применении к задачам ВКС имеет ряд недостатков:

- функционирование всей системы в целом полностью зависит от MCU, таким образом, при выходе из строя (выключении) данного модуля сеанс конференции будет прерван;
- данная архитектура отличается ограниченными возможностями масштабирования, так как количество клиентов напрямую зависит от производительности устройства MCU.

В качестве архитектуры, преодолевающей указанные недостатки, предлагается использование одноранговой архитектуры соединения терминалов (рис.1).

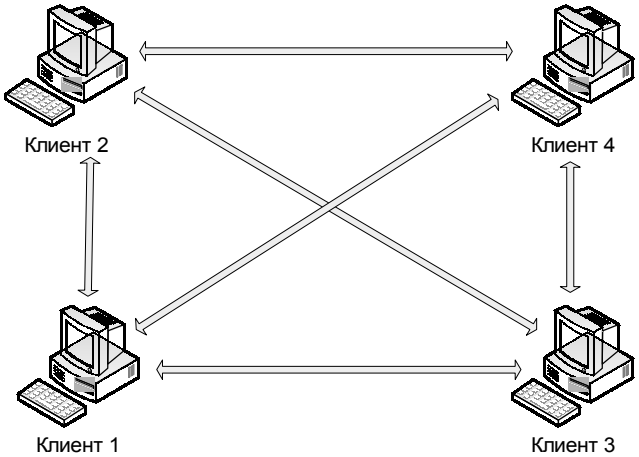

Рис. 1. Одноранговая архитектура соединения терминалов

При использовании данной архитектуры каждый терминал, участвующий в сеансе конференцсвязи, имеет одинаковый набор функциональных возможностей и может выступать либо как клиент (рабочее место участника сеанса), либо, как клиент и маршрутизатор одновременно. В случае, если между всеми участниками сеанса конференции можно установить прямые соединения, все терминалы работают в режиме клиента и взаимодействуют между собой напрямую. В противном случае один или несколько терминалов автоматически задействуют функции маршрутизации и перенаправляют потоки данных на терминалы, недоступные другим клиентам (рис.2).

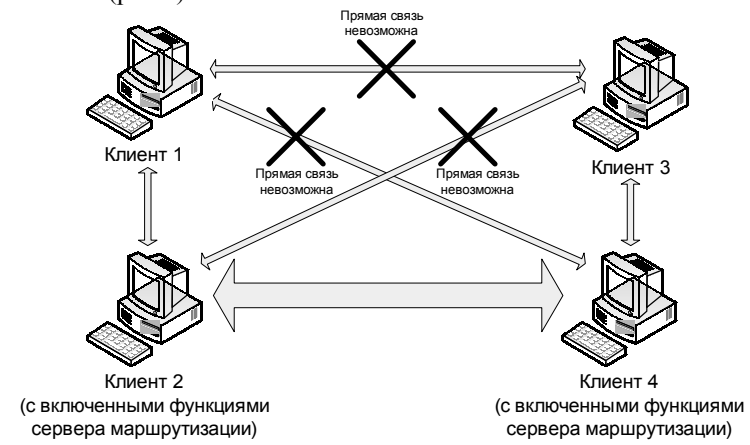

Рис. 2. Соединение терминалов в случае, если невозможно обеспечить прямое соединение всех участников взаимодействия

Необходимость включения в терминалы функций маршрутизации сетевых потоков продиктована тем, что для обеспечения качественного и оптимального функционирования системы необходимо оптимизировать сетевые потоки между терминалами. Так, например, для терминалов, находящихся в одной подсети, наиболее эффективным с точки зрения нагрузки на сетевые каналы является метод, при котором взаимодействие между ними выполняется при помощи широковещательных (broadcast) пакетов. Но такой метод неприменим для терминалов, находящихся в различных подсетях. В этом случае необходимо использовать направленные (unicast) рассылки пакетов.

Непосредственное использование направленных рассылок в случае, когда взаимодействие происходит между несколькими (более 2-х) терминалами в различных подсетях может привести к дублированию идентичных сетевых потоков. Такое использование каналов связи нельзя назвать эффективным. Использование автоматически настраиваемых межсетевых модулей маршрутизации в данной ситуации позволяет минимизировать количество дублирующихся сетевых потоков и, следовательно, использовать каналы связи более оптимально. Использование встроенных в терминалы функций автоматической маршрутизации позволяет также более гибко выполнить настройку безопасности, чтобы осуществлять взаимодействие между терминалами, которые принадлежат сетям, закрытым для непосредственного доступа.

Одноранговая архитектура соединения терминалов обладает практически неограниченными возможностями масштабирования.

Количество участников конференции и качество их обслуживания напрямую не зависят от производительности отдельных компьютеров, так как функции сервера маршрутизации могут быть задействованы на нескольких клиентских терми-

налах одновременно. Одноранговая архитектура может быть легко адаптирована под любую сетевую инфраструктуру без установки дополнительных серверов. Она обладает также повышенной отказоустойчивостью, так как при выходе из строя одного из терминалов (даже с включенным сервером маршрутизации) сеанс конференции не разрывается (за счет возможности использования нескольких серверов маршрутизации в рамках одного сеанса конференции и независимости остальных терминалов).

Несмотря на существенные преимущества данной архитектуры, ей присущ достаточно существенный недостаток, связанный с тем, что потоки данных системы передаются либо широковещательными пакетами, либо посредством других участников системы, что делает их доступными для перехвата. В данной ситуации особую важность приобретает проблема ограничения несанкционированного доступа к этим данным.

Кодирование медиаданных в современных системах обмена аудио- и видеоинформацией выполняется на основе стандартов компрессии (H.xxx, G.xxx). Механизмы ограничения несанкционированного доступа к медиапотокам, а также компенсации потерь при передаче пакетов не стандартизованы и пока не нашли широкого применения в современных системах конференцсвязи.

Решение данных проблем разработчики систем обмена медиаданными обычно ищут в применении крайне трудоемких стандартов шифрования типа AES (Rijndael) или DES (DEA). Совместное применение алгоритма шифрования такого класса в реальном масштабе времени "поверх" трудоемкого алгоритма видеокомпрессии на основе межкадрового кодирования (например, H.263, H.264) позволяет обеспечить высокую степень защищенности данных за счет высокой трудоемкости схем кодирования и декодирования.

С другой стороны, данные схемы ограничивают возможность использования более сложных алгоритмов компрессии и декомпрессии медиаданных с целью повышения качества сеанса связи, а также ограничивают набор используемых разрешений видеокадров.

При использовании алгоритмов компрессии медиаданных на основе оптимизированных дельта-преобразований второго порядка выходной поток кодера характеризуется следующими основными свойствами:

- близость распределения дельта-последовательности к равномерному, увеличивающая расстояние единственности для этого алфавита, что приводит к отсутствию альтернатив при выборе результатов криптоанализа и не позволяющая строить эффективные критерии на открытый текст;

- минимальная фиксированная длина кодового слова (1бит), приводящая к устранению статистических зависимостей входного потока;

- искажение сигнала при изменении бита, что позволяет использовать эту операцию в качестве составной части разрабатываемых алгоритмов защиты компрессированных данных.

Использованный в системе «Дельта-конференция» метод основан на использовании описанных выше свойств оптимизированных дельта-преобразований второго порядка, что позволяет обеспечить высокую степень защищенности дельта-последовательности (аудио- или видеокодера) от несанкционированного доступа путем применения к битовому потоку нескольких дополнительных битовых операций непосредственно в ходе кодирования/декодирования, что приводит к крайне низкой трудоемкости реализации схемы "компрессии-ограничения доступа" при высоком уровне защищенности данных.

Таким образом, описанная в данной работе схема позволяет обеспечить достаточный уровень защиты информации при минимальных накладных расходах на

операции криптографического преобразования потока медиаданных, что делает возможным повышение качества сеанса связи без задействования дополнительных вычислительных мощностей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Кравченко П.П.* Основы теории оптимизированных дельта-преобразований второго порядка. Цифровое управление, сжатие и параллельная обработка информации: Монография. – Таганрог: Изд-во ТРТУ, 1997.

5. *Кравченко П.П., Хусаинов Н.Ш., Погорелов К.В., Хаджинов А.А., Шкурко А.Н.* Программная система аудиовидеоконференцсвязи для локальных и корпоративных IP-сетей. Программные продукты и системы (Software & Systems). 2004. №1. – С.27–30.

В.С. Несов
Россия, г. Москва, ИСП РАН

ИСПОЛЬЗОВАНИЕ ПОБОЧНЫХ ЭФФЕКТОВ ФУНКЦИЙ ДЛЯ УСКОРЕНИЯ АВТОМАТИЧЕСКОГО ПОИСКА УЯЗВИМОСТЕЙ В ПРОГРАММАХ

Введение

В Институте системного программирования РАН разработана среда обнаружения уязвимостей [1][2] в исходном коде программ на языке C, позволяющая обнаруживать уязвимости и дефекты следующих типов:

- переполнение буфера (buffer overflow);
- неконтролируемая форматная строка (format string);
- разыменование нулевого указателя (null pointer) ;
- утечка памяти (memory leak).

Перед средой ставилась задача не пропускать уязвимости. Для этого предупреждения о возможных дефектах выводятся во всех местах анализируемой программы, в которых при помощи анализа не удалось доказать отсутствие дефектов.

Среда использует межпроцедурный итеративный анализ потока данных. Высокая точность выполняемого анализа требуется для снижения количества ложных предупреждений, число которых в данной постановке задачи непосредственно от нее зависит.

При межпроцедурном анализе информация о значениях переменных распространяется через точки вызовов функций. Для того, чтобы информация о значении некоторой переменной распространилась от одной функции к другой, она проходит через все промежуточные функции на графе вызовов.

Так как каждая функция программы может вызываться из нескольких мест, среднее количество информации, проходящей через каждый вызов в графе вызовов, увеличивается с увеличением размера анализируемой программы.

В статье описывается метод, позволяющий сократить количество распространяемой по графу вызовов информации о значениях переменных, тем самым сокращая время анализа и требуемое количество памяти. Метод основан на нахождении побочных эффектов функций одновременно с выполнением основного анализа, и ограничении распространяемых значений переменных с использованием этой информации.

Отавшаяся часть статьи организована следующим образом. В разделе 2 приводится обзор процесса анализа. В разделе 3 подробно описывается анализ инструкции вызова функции, передающей данные между процедурами. В разделе 4 описано использование побочных эффектов функции для ограничения распро-