передовых математических методов и мощных компьютеров, невозможен за обозримое человеком время.

Однако, в условиях удаленных сеансов связи с использованием открытых электронных каналов с учетом территориальной рассредоточенности и высокой мобильности абонентов возникает задача конфиденциальной доставки ключевой информации.

Криптостойкость используемых алгоритмов, протоколов и процедур существенно зависит от свойств ключевой информации. Под ключевой информацией понимают всю совокупность ключей, используемых в рассматриваемой криптосистеме. Часто нарушителю проще осуществить атаку на ключевую систему, чем непосредственно на сам алгоритм, лежащий в основе криптосистемы.

Важнейшим свойством ключевой информации для симметричных криптосистем является ее конфиденциальность (секретность). Поэтому процесс распределения ключевой информации должен обеспечивать ее максимальную конфиденциальность. По сложившейся в криптографии терминологии под распределением понимается доставка готовой ключевой информации или ее формирование у абонентов системы.

Распределение ключей в симметричных криптосистемах основано на использовании защищенных каналов и криптографических протоколов. В двухключевых и гибридных криптосистемах распространение (передача, распределение) ключей основано на предварительной аутентификации открытых ключей, которая осуществляется некриптографическими методами, и последующем использовании криптографических протоколов. Различают два типа протоколов распределения ключей:

– протоколы передачи (пересылки, доставки) ключей, которые предварительно уже сгенерированы.

– протоколы совместного формирования (выработки) ключей.

Основное отличие второго типа от первого состоит в том, что вырабатываемый ключ зависит от произвольного выбора двух и более сторон и каждая из взаимодействующих сторон получает этот ключ в результате проведенных вычислений. Различают протоколы и схемы распределения ключей между двумя пользователями (протоколы типа «точка — точка»), в которых передача (или выработка) ключей осуществляется в результате непосредственного взаимодействия двух сторон, и между многими пользователями. При распределении ключей между многими пользователями выделяют схемы централизованного распределения ключей.

ПРОГРАММНЫЙ КОМПЛЕКС АУДИТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ПРОТИВОДЕЙСТВИЯ АТАКАМ

А.И. Понамарчук, Вахаб Алаа, Т.В. Борботько, Юнис Али Аюб Юнис

Современные информационные системы используются для обработки различных сведений, в том числе в банковском секторе. Атаки на подобные системы приносят существенный ущерб банкам и влияют на их репутацию. Одним из способов противодействия таким угрозам является обнаружение уязвимостей в информационной системе и их своевременное устранение. Для практической реализации указанного способа созданы программные средства, которые позволяют обнаруживать уязвимости, а так же проверять возможность их использования при реализации тех или иных атак. Однако существенной проблемой применения таких средств является решение задачи снижения вероятности ложных тревог. Такая задача может быть решена за счет повышения достоверности получаемых сведений, когда события безопасности регистрируются несколькими датчиками и решение о наличии угрозы принимается на основе корреляции таких событий.

Разработанный комплекс основан на использовании программного обеспечения VMware Workstation и включает в себя: виртуальные машины с IDS/IPS, HoneyPot и с программным обеспечением для имитации атак; интерфейсы настройки HoneyPot, просмотра сообщений о событиях безопасности, управления атаками.

Первая виртуальная машина содержит следующие сервисы: системы IDS/IPS и HoneyPot; HTTP-сервер и PHP-интерпретатор для интерфейса конфигурирования HoneyPot; систему просмотра сообщений безопасности IDS/IPS.

В качестве системы IDS/IPS использовалось программное обеспечение Snort. Система HoneyPot включает в себя подсистемы: honeyd, arpd и набор скриптов. Интерфейс настройки HoneyPot позволяет упростить конфигурирование подсистемы honeyd, за счет исключения необходимости редактирования файла настроек в ручном режиме. Базовая настройка HoneyPot заключается в создании шаблона HoneyPot и его применение.

Интерфейс просмотра сообщений о событиях безопасности реализует процедуры аутентификации пользователей программного комплекса, разграничения прав их доступа к системному журналу, отображения событий с учетом их корреляции по различным критериям в виде графиков и отчетов.

Вторая виртуальная машина обеспечивает функционирование программного комплекса моделирования атак, который выполнен по модульному принципу. Основными компонентами данного комплекса являются: консоль управления; модуль эксплоитов; модуль, реализующий атаку «отказ в обслуживании» (DoS); модуль, реализующий атаку «подмены» (Spoofing); модуль фаззинга (Fuzzing); модули нагрузки и кодирования.

Разработанный программный комплекс позволяет оценить защищенность моделируемых информационных систем, выявить уязвимости их различных сервисов, проследить возможные сценарии атак, за счет использования систем-ловушек, проверить корректность работы системы обнаружения атак, за счет реализованной в нем методике, основанной на сравнении информации об атаках получаемых от различных источников.

АНАЛИЗ МЕТОДОВ И СРЕДСТВ УПРАВЛЕНИЯ ТОПОЛОГИЕЙ СЕТИ MANET

Д.Д. Альхимович

Рассматриваются сети MANET (Mobile Ad-Hoc Networks) — мобильные самоорганизующиеся сети с динамической архитектурой, предполагающие отсутствие фиксированной сетевой инфраструктуры (базовых станций) и централизованного управления. Одной из основных задач оперативного управления сетью MANET является управление ее топологией. Топология определяет потенциальные возможности сети по доставке данных между взаимодействующими узлами. Мобильность (отказы, уничтожение) узлов приводит к разнообразным сетевым топологиям. Тем не менее, сеть должна поддерживать необходимый уровень пропускной способности, который во многих ситуациях не удается достичь только за счет маршрутизации. Изменение топологии сети может иметь более значительный эффект, в отличие от использования адаптивной маршрутизации. Разработан алгоритм оперативного управления топологией MANET. Алгоритм предполагает оценку параметров функционирования MANET и при их уменьшении ниже допустимых значений — выработку управляющих воздействий (изменение мощностей передач узлов), позволяющих осуществить пользовательскую или системную оптимизацию. Применение алгоритма позволяет увеличить пропускную способность сети 1,5–2 раза. Таким образом, для повышения эффективности функционирования MANET, необходимо осуществлять оперативное управление топологией сети и осуществлять управление построением и поддержанием маршрутов при полученной топологии.

Литература

1. *Миночкин А.И., Романюк В.А.* Методика оценки методов управления в мобильных радиосетях // 15-я международная Крымская конференция «СВЧ-техника и телекоммуникационные технологии» (КрыМиКо), Севастополь, 2005. С. 43–44.