МЕТОДЫ ОБНАРУЖЕНИЯ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СЕРВИСАМ ТРАНСПОРТНОЙ СЕТИ NGN

Персиков А.В.
Харьковский Национальный Университет Радиоэлектроники
61166 Харьков, пр.Ленина,14, кафедра ТКС, т.702-13-20,
E-mail: white_seal@mail.ru

In this work the actual problem of malicity activity in high-speed transport network was investigated. Actuality of results conditioned on possibility of modified methods detects attacks with low rate of false positives in decisions. There are different methods based on classification procedures and network hosts state evolution model in autonomic systems are suppose. For control of heterogeneous network environment using of special coordination intrusion detection and prevention server supposed.

Введение

Многие атаки на транспортную сеть сети последующего поколения (Next Generation Network, NGN), которая строиться на основе технологии коммутации пакетов, направлены на получение несанкционированного доступа (НСД) к сервисам, реализующим управление потоками данных, и, в результате, компрометацию, как отдельных узлов сети, так и сети в целом. Основным типом атак, который осуществляется в данных сетях, является сканирование портов серверов, исполняющих сервисы, для реализации НСД к наименее защищенным приложениям.

Задачей работы видится разработка методов обнаружения попыток НСД в условиях высоких скоростей, которые присущи транспортной сети NGN. Актуальность работы заключается в том, что современные методы обнаружения атак показывают высокий уровень ложных тревог на высоких скоростях обмена пакетами в сети и производят неточную оценку количества хостов сети, занятых злоумышленником при интенсивных атаках, направленных на компрометацию системы в целом.

Целью работы было создание методов, адаптированных на использование в высокоскоростных сетях, и способных обнаруживать активность злоумышленника в режиме реального времени. В работе модифицировались существующие методы обнаружения попыток НСД к сервисам с использованием процедур классификации задач, выполняемых хостами, и оценок коэффициента скомпрометированности сети на основе моделей автономного развития сетей.

Метод оценки степени и характера компрометации сети

Для обнаружения скомпрометированных хостов, используемых для сканирования уязвимостей, возможно использовать метод, предложенный в [1], и используемый в большинстве сетевых сканеров. Исследуется отношение количества хостов, производящих попытку соединения к сервису с быстрым отказом от доступа n_a, к количеству хостов, которые произвели полноценные попытки n_s:

$$\phi = \frac{кол-во\ хостов,\ сделавших\ попытку\ соединения\ и\ быстро\ отказавшихся\ от\ сервиса}{кол-во\ хостов,\ которые\ произвели\ полноценные\ попытки\ доступа} = \frac{n_a}{n_s}.$$

Показатель ϕ стандартно вычисляется для всего множества хостов, вне зависимости от задачи, которые они выполняют. Это упрощает алгоритм обнаружения, но его точность высока лишь при использовании злоумышленником простейших алгоритмов последовательного сканирования доступных хостов по адресному пространству. Затем, используя этот показатель, система обнаружения вторжений вычисляет пороговое значение интенсивности активности отдельных хостов и, используя, например, метод последовательного анализа [1, 5], определяет, была ли попытка получить доступ к сервису в каждом конкретном случае.

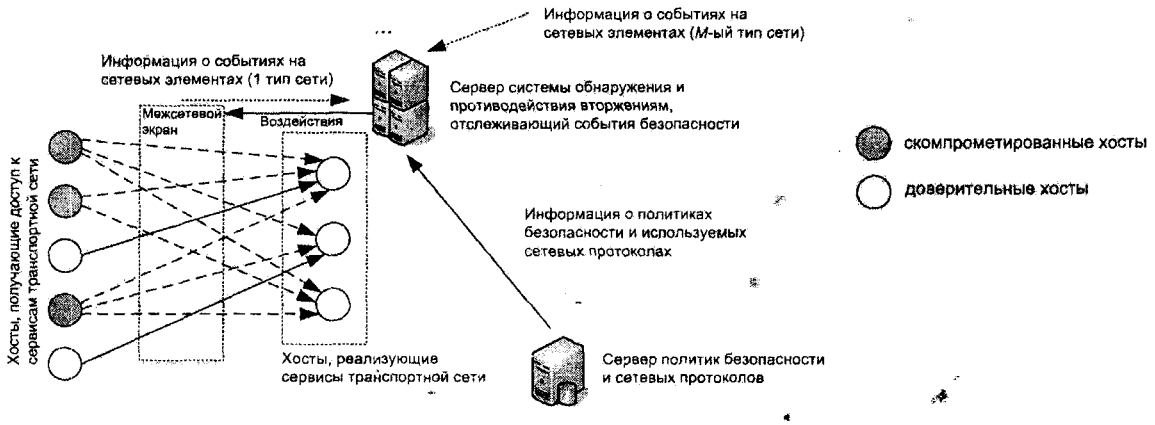

Рис. 1. Введение координирующих серверов

Метод может быть улучшен за счет классификации хостов в пределах отдельной сети (и формирования не интегрального показателя ϕ, а множества показателей), в соответствии с выполняемыми ими задачами при реализации сервисов NGN (определяются согласно используемым протоколам), а также введения дополнительного управляющего сервера, который взаимодействует с базой данных политик безопасности и сетевых протоколов. Это позволяет одновременно увеличить точность анализа, при неизменной его скорости: уменьшение временных затрат на анализ компенсируется увеличением затрат на обмен информацией между системой обнаружения и противодействия вторжениям и сервером (рисунок 1).

Классификация может быть использована для точного выборочного воздействия на хосты (фильтрация трафика от хостов, антивирусная проверка, перезагрузка, принудительное отключение от сети и др.) программно-аппаратной платформы системы защиты [4]. Такое воздействие особенно эффективно при условиях, что [2]:

- в сети одновременно происходит не одна распределенная атака, а несколько;
- для предотвращения атаки необходимо одновременное воздействие сразу на несколько хостов;
- ресурсов системы хватает лишь для воздействия на часть хостов в сети;
- есть жесткие временные ограничения, обусловленные спецификой динамики состояния сетевых элементов (переход в скомпрометированное состояние/восстановление доверительного состояния).

Классификацию можно производить на основе вовлеченности тех или иных служб и хостов в процесс транспортировки данных в сети NGN (данные протокола), поддерживаемых (управляемых) хостом ресурсов, а также специфических функций сервиса [2, 3]. Аналогичная схема может быть использована для противодействия распределенным атакам (атака исходит из нескольких сетей и направлена одновременно на сервисы, реализованные в нескольких сетях). Здесь можно использовать комбинацию процедур классификации хостов по критериям принадлежности к сети, скорости компрометации отдельных сетей, последовательного анализа и проверки гипотез.

Могут быть сформулированы несколько подзадач для решения задачи противодействия:

- блокирование скомпрометированных сетей на основе информации о скорости захвата злоумышленником хостов в отдельной сети;
- блокирование запросов от отдельных хостов межсетевым экраном с согласно гипотезам, проверяемых с применением метода последовательных оценок;
- блокирование группы хостов, принадлежащих различным сетям на основе информации о задаче сервиса NGN и характера распространения распределенной атаки (определяется топологией атаки и изменением топологии во времени).

В методе последовательных оценок может быть модифицирован характер воздействия на сервис и принято, например, экспоненциальное распределение интервалов между сканирующими запросами. Поскольку длины интервалов подчиняются экспоненциальному распределению, совокупное время сканирования подчиняется эрланговскому распределению $f_n(T_n) = \frac{\lambda(\lambda T_n)^{n-1}}{(n-1)!} e^{-\lambda T_n}$ (λ – средняя скорость следования запросов от хоста сервису, регулируемая межсетевым экраном, T_n – время соединения хоста с сервисом). Такой характер сканирования более подходит при распределенных атаках, когда скомпрометированный хост сканирует уязвимости множества доверительных хостов (сложная топология атаки), где поддерживается сетевой сервис [3].

Выводы

В работе предложено использование модели развития сети для оценки изменения количества скомпрометированных злоумышленником хостов для улучшения точности оценки количества доверительных хостов в сети, а также методы отслеживания скомпрометированных хостов в сети с использованием дополнительных сведений о их задачах в NGN и политике общесетевой безопасности.

Модифицирован метод противодействия распределенным атакам на основе оценок топологии сети и изменения топологии во времени. Такой подход позволяет сохранить режим реального времени обнаружения попыток компрометации сервисов для высокоскоростных сетей с использованием программно-аппаратных решений начального уровня. Для решения вышеобозначенных подзадач, необходимы процедуры унифицированного сбора информации в режиме реального времени. Основой для реализации процедур может служить программный пакет типа PCap, реализованный для операционных систем типа Windows, Linux, UNIX.

Литература

1. J. Jung, V. Paxson, A. Berger, H. Balakrishnan. Fast Portscan Detection Using Sequential Hypothesis Testing, IEEE Symposium on Security and Privacy 2004, May 2004.

2. H. Dreger, A. Feldmann, V. Paxson, R. Sommer. Operational experiences with high-volume network intrusion detection. In CCS '04: Proceedings of the 11th ACM conference on Computer and communications security, pp 2-11, ACM Press, New York, NY, USA, 2004.

3. Персиков А.В. Восстановление функции управления в телекоммуникационных системы после атак подмены кода программных агентов. // Восточно-Европейский журнал передовых технологий. – №.5 – Харьков. – 2007. – с.82-87.

4. Персиков А.В., Дорошенко Я.В. Некоторые вопросы реализации функций защиты телекоммуникационных систем, построенных на основе концепции Autonomic Computing. // Радиотехника. – №151 – Харьков. – 2007. – с.220-225.

5. Левин Б.Р. Теоретические основы статистической радиотехники. Книга вторая. М., «Сов. радио», 1975, 392 с.