ПО сервера реализует в отличие от ПО блока сбора данных сразу несколько функций: обмена пакетами с блоком сбора данных при помощи TCP/IP-сокета (прием данных и настройка датчиков), хранение данных в БД (в качестве СУБД была выбрана MySQL и технология доступа dbExpress), формирование HTML-страниц (технология WebSnap) и предоставление их удаленному клиенту (веб-браузер). Связь с веб-браузером организована через стандартный веб-сервер Apache.

Таким образом, в результате проведенной работы с целью проверки гипотезы о практической возможности создания распределенной системы мониторинга, была предложена структура системы мониторинга, разработана ее модель в среде Simulink(Matlab), выбраны средства ее разработки и разработан программный комплекс, реализующий проект рассмотренной архитектуры. Опытные результаты эксплуатации прототипа показали его работоспособность и эффективность.

Можно выделить несколько путей развития данного проекта: полнофункциональная реализация предложной архитектуры распределенной системы мониторинга или реализация данного подхода и прикладного интерфейса программирования для создания отдельных датчиков с веб-интрефейсом, каждое из которых является весьма перспективным.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Таненбаум Э., Ван Стеен М.* Распределенные системы. Принципы и парадигмы. – СПб.: Питер, 2003. – 877 с.
2. *Сигаев А.* Embedded Internet // Компоненты и технологии. – 2000. – № 2.
3. *Зубинский А.* МикроWeb // Компьютерное обозрение. – 2000. – № 20.

Статью рекомендовал к опубликованию д.т.н., профессор В.В. Тютиков.

Фролова Марина Владимировна
Научно-исследовательский институт физических измерений.
E-mail: niifi@sura.ru, fro-mi2@yandex.ru.
440026, г. Пенза, ул. Володарского, 8/10.
Тел.: 88412591932.

Frolova Marina Vladimirovna
Research Institute of Physical Measurements.
E-mail: niifi@sura.ru, fro-mi2@yandex.ru.
8/10, Volodarskogo Street, Penza, 440026, Russia.
Phone: +78412591932.

УДК 004.021

Р.Н. Селин, С.А. Чурилов

МОДЕЛЬ СЕТЕВЫХ ПРОЦЕССОВ И АЛГОРИТМ ОБНАРУЖЕНИЯ УГРОЗ В КОМПЬЮТЕРНОЙ СЕТИ

Представлена модель сетевых процессов и алгоритм обнаружения угроз в компьютерной сети, предназначенные для прогнозирования изменения уровня информационной безопасности в зависимости от происходящих сетевых событий. Авторы предлагают новый способ моделирования механизма угроз информационной безопасности, который позволяет предугадывать различные варианты развития компьютерных атак. С помощью приведенной модели решаются задачи прогнозирования компьютерных атак с целью их предотвращения.

Информационная безопасность; модель; сетевой процесс; уязвимость; обнаружение угроз.

R.N. Selin, S.A. Churilov

ANALYSIS OF INFORMATION SECURITY LEVEL FOR VIRTUAL SOCIETIES BASED ON TYPE AND NUMBER OF VULNERABILITIES FOUND

This article presents a model of network processes and the algorithm of detecting threats in computer networks, designed to predict changes in the level of information security in dependence on the network events. The authors propose a new way of modeling the mechanism of threats to information security, which allows you to anticipate the various options for the development of computer attacks. By means of the resulted model primal problems of computer attacks for the purpose of their preventing are solved.

Information security; security model; network event; system exploit; threat detection.

Существующие технологии распознавания подозрительной сетевой активности на практике показали, что для эффективной работы простых эвристических правил и наборов сигнатур недостаточно. Типовая структура компьютерной атаки имеет комплексную и достаточно сложную организацию, полностью выявить и распознать которую сигнатурным способом без дополнительных связей невозможно. С другой стороны, если говорить об анализе сетевой среды, каждый анализируемый сетевой пакет – атомарное событие – дает определенную порцию информации, которую аналитическая система обнаружения компьютерных атак может использовать для решения трех задач:

1. Оценки полноты контроля над текущей ситуацией в сетевой среде.

2. Прекращения злонамеренной деятельности по результатам обнаруженных следов или попыток совершения злонамеренной деятельности.

3. Прогнозирования компьютерных атак с целью их предотвращения.

Для создания математической модели, описывающей подобные процессы необходимы понятия "видимости", "доверия" и "контроля". Математическое представление некоторых из этих сущностей присутствует в формальном языке описания криптографических протоколов "BAN-logic", разработанном Борройс, Абади и Нидхэмом [1].

К сожалению, существующей семантики языка БАН-логики недостаточно для описания таких процессов, как контроль сетевого трафика, наличие или отсутствие угрозы информационной безопасности. В следствие этого, математический аппарат БАН-логики необходимо существенно дополнить требуемыми понятиями.

Введем основные определения, которые понадобятся для моделирования процесса мониторинга компьютерной сети:

- существуют субъекты сети, каждый из которых мы будем обозначать через P, которые могут получать доступ к различным объектам X компьютерных сетей (при этом P могут выполнять две функции – пользовательскую, т.е. организовывать прием и передачу информации, и наблюдательную, т.е. наблюдать за этим процессом и блокировать его);
- существует некоторый канал C передачи сообщений m, который обладает целым рядом свойств, а именно:
  а) данные, передающиеся в канале, могут видеть одновременно несколько наблюдателей;
  б) канал надежен, т.е. переданное абонентом A сообщение m абоненту B гарантированно доставляется;
  в) канал не имеет временных задержек (условимся считать, что данное допущение не влияет на качество моделирования);

- через $P \mid\equiv X$ будем обозначать то, что наблюдатель P верит в некоторую сущность X. На практике это означает, что P считает значение некоторого условия X истинным;
- операцией $P_x \overset{m}{\triangleleft} P_y$ обозначают то, что P_x видит (т.е., получает) сообщения m, посылаемые P_y (например, при передаче X по каналу связи C) при этом P не только знает о X, но и имеет возможность прочесть X (возможно даже после декодирования, расшифрования или даже дешифрования);
- использование $P \mid\sim C(m)$ означает, что P однажды передал в канал связи C сообщение, содержащее m – мы опять же не делаем никаких ограничений на время, в течение которого P осуществил передачу;
- применение $\#(m)$ необходимо для того чтобы указать, что значение m не было передано в канал связи C до текущего момента. Таким образом, можно утверждать, что о значении m не осведомлен никто другой, кроме его владельца.

Также в предлагаемой модели присутствуют сущности "событий безопасности", т.е. некоторых последействий того, что имеет место, происходит, наступает в произвольной точке компьютерной сети в произвольное время после совершения определенных действий в компьютерной сети и имеет природу, связанную с информационной безопасностью. События будем обозначать как $d^{mun}_{P_k \leftrightarrow P_q}$, где mun – это тип произошедшего события, поясняющего его смысл, а связь $P_k \leftrightarrow P_q$ демонстрирует между какими узлами сети произошло данное событие (соответственно связь $P_k \leftrightarrow P_q$ обозначает локальные события на уровне хоста). Также как и для сообщений будем использовать $\#(d^{mun}_{P_k \leftrightarrow P_q})$ для обозначения нового события в системе. Для удобства моделирования ограничим понятие "события" некоторым рядом типов:

- появление сигнатуры, распознаваемой системой как часть злонамеренного воздействия;
- отключение узла от контура охраны (влияет на "видимость" узлов);
- включение узла в контур охраны (влияет на "видимость" узлов);
- повышение вероятности реализации угрозы информационной безопасности (влияет на состояние всей системы);
- уменьшение вероятности реализации угрозы информационной безопасности (влияет на состояние всей системы);
- определение или переход в новую фазу атаки (см. предыдущий раздел для определения типовых фаз сетевой атаки) на систему.

Событие "уменьшение вероятности реализации угрозы информационной безопасности" возникает в случае, когда завершается логическое действие, которое привело к появлению события "повышения вероятности реализации угрозы", а также через некоторый достаточно долгий промежуток времени Θ – назовем его временем толерантности системы к атакам. Данное время изначально может быть задано экспертно и затем изменяться во время работы системы динамически.

Например, в случае, если суммарное количество атак на систему в единицу времени (за минуту, за час, за день) превышает некоторый порог, значение Θ рас-

тет пропорционально количеству атак, в противном же случае постепенно уменьшается до некоторого минимального порога Θ_{min}.

Решающий модуль системы представим в виде конечного автомата (для краткости будем называть его иногда главным автоматом системы защиты). Главный автомат системы защиты служит для определения состояний системы и переключения между ними под воздействием правила "переключения состояния главной системы".

Переход из одного состояния в другое в главном автомате системы происходит под влиянием событий, происходящих в системе, предполагаемых атак и общего уровня безопасности. Этот процесс управляется специальными моделирующими правилами, которые представлены ниже.

Также следует учесть то, что события информационной безопасности, происходящие в системе, имеют срок актуальности, например, рассмотрение факта отправки запроса по протоколу HTTP актуально только до момента получения ответа на него, аналогично любые другие запросы в интерактивных протоколах (SMTP, POP3, IMAP4, DNS, FTP и пр.). Кроме того, актуальность может быть утеряна в связи с большим количеством прошедшего времени. В связи с этим, список событий информационной безопасности можно представить в виде множества кортежей (*источник, получатель, тип события, тип закрывающего события, время жизни*).

При задании переходов между состояниями автомата существует несколько основных замечаний, которые следует обязательно учитывать:

- злоумышленник может не проводить определенные этапы в ходе осуществления атаки, поскольку может быть снабжен необходимой информацией из других источников (либо данная информация ему попросту не нужна для реализации попытки вторжения);
- обязательными этапами реализации вторжения являются только "попытка проникновения" и "удаленное управление", поскольку они определяют сам характер вторжения – получение несанкционированного (возможно, негласного) контроля или доступа к информации;
- вследствие того, что наблюдатель может "пропустить" или "не увидеть" начало атаки, некоторые наиболее характерные этапы атаки могут стать началом ее выполнения (с низкой вероятностью);
- после проведения сетевой разведки, злоумышленник может обнаружить следы предыдущего проникновения и оставленные программные закладки, а затем начать их использовать, минуя остальные этапы атаки – отсюда прямая связь между этапами сетевой разведки и удаленного управления;
- попытка проникновения может не привести злоумышленника к желаемому результату и в этом случае он может попытаться замаскировать следы даже попытки проникновения – связь между этапами проникновения и маскирования следов.

С помощью нескольких экземпляров автомата сетевой атаки, имеющих возможно различные состояния и описывающих действия с различными защищаемыми узлами, возможно осуществлять прогнозирование поведения злоумышленника:

- на техническом уровне с помощью предсказания наиболее вероятной следующей фазы атаки (для этого используется граф состояний автомата и вероятности перехода);
- на логическом уровне с помощью определения наиболее вероятной угрозы, которая может быть реализована вследствие действий злоумышленника, которые зафиксировала система защиты.

Таким образом, с помощью данной модели решаются задачи прогнозирования компьютерных атак с целью их предотвращения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Monniaux D.* Decision Procedures for the Analysis of Cryptographic Protocols by Logics of Belief // Proceedings of The 12th Computer Security Foundations Workshop, 1999.
2. *Чирилло Дж.* Обнаружение хакерских атак (Hack Attacks Revealed). – СПб.: Питер, 2002. – 864 с.
3. *Симонов С.В.* Методология анализа рисков в информационных системах // Конфидент. – 2000. – № 1. – С. 72-76.
4. *Милославская Н.Г., Толстой А.И.* Интрасети: доступ в Internet, защита: Учебное пособие для вузов. – М.: ЮНИТИ-ДАНА, 2000.
5. *Лукацкий А.* Адаптивное управление защитой // Сети. – 1999. – № 10.
6. *Польман Н., Кразерс Т.* Архитектура брандмауэров для сетей предприятия: Пер. с англ. Изд-во Вильямс, 2003. – 432 с.
7. *Онтаньон Р.Дж.* Создание эффективной системы выявления атак // LAN/Журнал сетевых решений. – 2000. – № 10.

Статью рекомендовал к опубликованию д.т.н., профессор Е.А. Башков.

Чурилов Сергей Анатольевич
Селин Роман Николаевич
ФГНУ НИИ "Спецвузавтоматика".
E-mail: sva@rsu.ru.
344007, г. Ростов-на-Дону, Газетный пер., 51.
Тел.: 88632975084.

Churilov Sergey Anatol'evich
Selin Roman Nikolaevich
FSRI "Spetsvuzautomatika".
E-mail: sva@rsu.ru.
51, Gazetny'j Lain, Rostov-on-Don, 344007, Russia.
Phone: +78632975084.

УДК 621.323.11

Е.С. Синютин

СИСТЕМА АВТОМАТИЧЕСКОЙ ПРОВЕРКИ РАБОТОСПОСОБНОСТИ МОБИЛЬНЫХ ПОЛИГРАФОВ С ПРИМЕНЕНИЕМ ИНСТРУМЕНТАРИЯ LABVIEW

Описываются основные задачи систем тестирования и поверки мобильных полиграфов, описаны основные отличия классического подхода к их построению и нового подхода с применением инструментария LabView. Разобраны особенности подходов к построению виртуальных приборов, и показано как с помощью нового инструментария можно сделать поверочную установку более гибкой и настраиваемой под различные типы приборов. Показан пример подобной системы, отмечены основные достоинства и недостатки данного подхода. В статье показано, что для применения новых методов отладки и поверки фирме-изготовителю продукции потребуется помимо инженер-метролога ввести должность разработчика виртуального оборудования.

Мобильные полиграфы; тестирование и отладка; автоматизация тестирующих аппаратных средств; LabView; виртуальные приборы.