УДК 004.652.4

05.00.00 Технические науки

АДАПТИВНАЯ ПОДСИСТЕМА ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ АНОМАЛИЙ КАК СРЕДСТВО ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК

Симанков Владимир Сергеевич
д.т.н

Колодий Александр Сергеевич
аспирант

Кучер Виктор Алексеевич
к.т.н.

Трофимов Виктор Маратович
д.ф.-м.н.
Кубанский государственный технологический университет, Краснодар, Россия

Описаны результаты практической реализации системы обнаружения и предотвращения сетевых аномалий на базе модульного адаптивного подхода. Перечень конкретных модулей, используемых в ходе практической реализации СОА, их архитектуру, алгоритмическое, программное и организационно-техническое обеспечение предлагается определять на этапе техно-рабочего проектирования на основании результатов проведенного аудита, оценки и анализа рисков. В общий перечень таких модулей (подсистем) может входить: подсистема обнаружения и предотвращения вторжений (IPS/IDS); подсистема мониторинга, сбора, аналитики и корреляции событий; подсистема администрирования и управления и другие. Продемонстрирована на примерах специфика формирования требований к базовым механизмам подсистем с точки зрения разработки и реализации конкретной архитектуры СОА, а также структура практически реализованных модулей СОА. Рассмотрены вопросы организационно-технического обеспечения функционирования данной системы

Ключевые слова: МОДЕЛИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ, СЕТЕВЫЕ АТАКИ И АНОМАЛИИ, СЕТЕВАЯ БЕЗОПАСНОСТЬ, СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК, СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ, УПРАВЛЕНИЕ РАЗРАБОТКОЙ

UDC 004.652.4

Technical sciences

ADAPTIVE SUBSYSTEM FOR DETECTING AND PREVENTING ANOMALIES AS A PROTECTION MEANS AGAINST NETWORK ATTACKS

Simankov Vladimir Sergeevich
Dr.Sci.Tech.

Kolodiy Alexandr Sergeevich
postgraduate student

Kucher Victor Alekseevich
Cand.Tech.Sci.

Trofimov Victor Maratovich
Dr.Sci.Phys.-Math.
Kuban State Technological University, Krasnodar, Russia

This article describes the results of networks anomalies detection system based on modular adaptive approach practical implementation. The list of specific modules used in the practical implementation of IPS, their architecture, algorithms, software, organizational and technical support determined at technical working design based on the results of the audit, evaluation and risk analysis. In the general list of modules (subsystems) we may include: intrusion detection and prevention (IPS / IDS) subsystems; monitoring, data collection, and event correlation, administration and management subsystem and others. We have demonstrated the specificity of formation requirements for the basic mechanisms of the subsystems in terms of development and implementation of specific architecture with some examples, plus practically implemented structure of system modules, as well as organizational and technical support system functioning

Keywords: NETWORK ATTACKS, INTRUSION DETECTION SYSTEMS, INTRUSION DETECTION SYSTEM DESIGN, DESIGN MANAGEMENT, NETWORK SECURITY

Введение

Среди проблем практической реализации систем обнаружения и предотвращения аномалий можно выделить две главных: минимизация количества ложных сигналов при произвольном (в общем случае -

описываемом вероятностными соотношениями) поведении хостов, пользователей и сетевой активности, а также сокращение временных и ресурсных затрат на обучение модулей, т.е. на определение и формирование базы шаблонов "нормального" состояния сети [1, 2]. Целью работы является разработка мер по практической реализации защиты от сетевых атак на основе адаптивной подсистемы обнаружения и предотвращения аномалий.

На практике основной задачей при развертывании СОА является создание профилей, описывающих приемлемое состояние и поведение компонентов и функционирования сети. На современном этапе развития системы обнаружения аномалий методы обнаружения аномалий не находят практического применения в чистом виде, а используются как дополнения к методам обнаружения вторжений, расширяющие функциональность системы информационной безопасности в целом.

Перечень конкретных модулей, используемых в ходе практической реализации СОА, их архитектуру, алгоритмическое, программное и организационно-техническое обеспечение определяют на этапе техно-рабочего проектирования на основании результатов проведенного аудита, оценки и анализа рисков. В общий перечень таких модулей (подсистем) может входить: подсистема обнаружения и предотвращения вторжений (*IPS/IDS*); подсистема мониторинга, сбора, аналитики и корреляции событий; подсистема администрирования и управления и другие [2,5]. По результатам практического анализа модели угроз и нарушителя, сделан вывод о том, что для объекта защиты являются актуальными следующие угрозы:

1) неверные настройки ПО, изменение режимов работы ТС и ПО (случайное либо преднамеренное);
2) доступ в среду функционирования прикладных программ (локальная СУБД, например);

3) доступ непосредственно к информации пользователя, обусловленный возможностью нарушения ее конфиденциальности, целостности, условий доступности;

4) сканирование сети и анализ сетевого трафика для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены;

5) применение специальных программ для выявления пароля (сниффинг, *IP*-спуффинг, разные виды перебора);

6) подмена доверенного объекта сети с присвоением его прав доступа, внедрение ложного объекта сети;

7) реализация угрозы отказа в обслуживании;

8) сетевые атаки;

9) применение утилит администрирования сети;

10) внедрение программных закладок;

11) внедрение вредоносных программ (случайное или преднамеренное, по каналам связи и непосредственное).

Продемонстрируем на примерах специфику формирования требований к базовым механизмам подсистем с точки зрения разработки и реализации конкретной архитектуры СОА.

1. Модули мониторинга, сбора и анализа информации в режиме реального времени (на примере *XSpider*, рисунок 1).

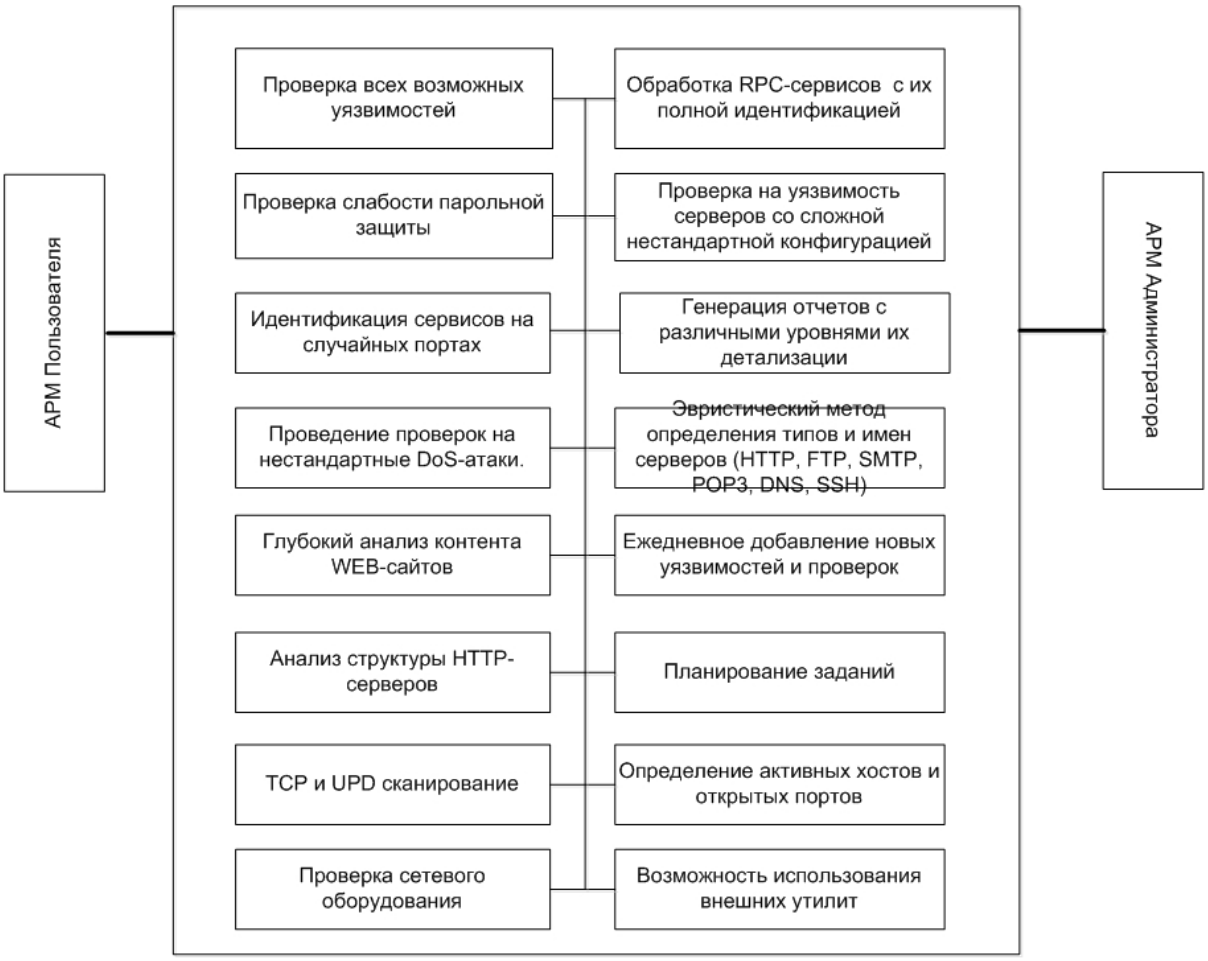

Рисунок 1 - Функциональная схема модуля мониторинга и анализа в СОА

Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.

Основные реализуемые механизмы [1,3]:

1) полная идентификация сервисов на случайных портах;
2) проверка на уязвимость серверов со сложной нестандартной конфигурацией;
3) эвристический метод определения типов и имен серверов;
4) определение настоящего имени сервера и корректной работы проверок;

5) определение *RPC*-сервисов и поиск уязвимостей в них, а также определение детальной конфигурации компьютера в целом;

6) проверка стойкости парольной защиты;

7) подбор паролей в сервисах, требующих аутентификации, для выявления нестойких паролей/не соответствующих разработанным политикам;

8) глубокий анализ контента *WEB*-сайтов;

9) анализ скриптов *HTTP*-серверов и поиск в них следующих уязвимостей;

10) анализатор структуры *HTTP*-серверов;

11) поиск и анализ директорий доступных для просмотра и записи;

12) проведение проверок на нестандартные *DoS*-аномалии;

13) осуществление проверок «на отказ в обслуживании»;

14) механизмы, уменьшающие вероятность ложных срабатываний при сканирования;

15) методы, уменьшающие вероятность ошибочного определения уязвимостей.

2. Модули централизованного управления (на примере управления комплексом *StoneGate IPS*) - централизованное управление с помощью специализированного компонента «*StoneGate SMC*»:

1) дистанционная установка дополнительного программного обеспечения;

2) формирование прав доступа пользователей;

3) внесение изменений в конфигурацию;

4) формирование, просмотр и анализ правил фильтрации;

5) запрос, получение, просмотр, анализ и обработка указанной по виду и времени регистрационной информации о событиях безопасности;

6) автоматический мониторинг состояния *StoneGate IPS*;

7) централизованный контроль состояния и управление комплексом;

8) проверка доступности рабочих станций сети или другого оборудования.

Таким образом, данный модуль целесообразно представить в виде схемы Система *StoneGate IPS*, состоящей из сенсора (*Sensors*), анализатора (*Analyzers*) и центра управления *StoneGate Management Center* (рисунок 2).

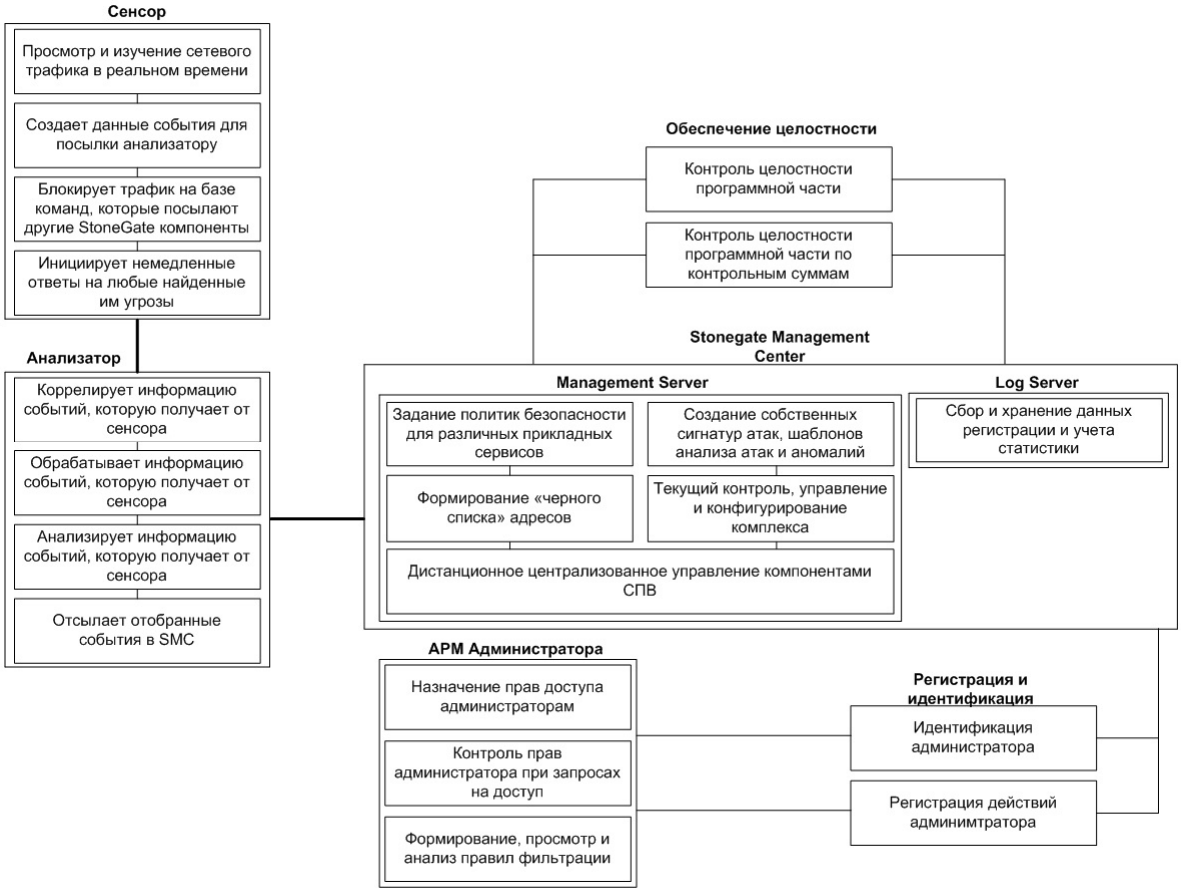

Рисунок 2 - Функциональная схема реализации подсистемы управления СОА на платформе *StoneGate*

Сенсор выполняет следующие функции: отвечает за просмотр и изучение сетевого трафика в реальном времени и создает данные события, которые он посылает анализатору для дальнейшей обработки. Далее сенсор инициирует немедленные ответы на любые найденные им угрозы и блокирует трафик на базе команд, которые посылают другие *StoneGate* компоненты [4].

Задачи анализатора - корреляция, обработка и анализ информации событий, которую он получает от сенсора. Один сенсор может видеть только часть возможной попытки вторжения, так что роль анализатора заключается и в том, чтобы собирать всю картину соединений сети и далее рассматривать более сложные виды угроз.

Управление сенсорами и анализаторами производится централизованно через центр управления *StoneGate Management Center* (*SMC*), который состоит из сервера управления *Management Server*, а также одного или нескольких серверов *Log Server*.

Для обеспечения взаимодействие компонентов СОА была реализована следующая архитектура. Сенсор инспектирует сетевой трафик на предмет любых аномалий и информирует анализатор о событиях, представляющих интерес. Анализатор далее обрабатывает эти события и находит интересующие его шаблоны при наблюдении за одним и более сенсорами. Анализатор добавляет, то, что он нашел в информационный поток, но комбинирует связанные события вместе и отбрасывает ненужные события. Далее результат пересылаются в *StoneGate Management Center* (*SMC*) для просмотра администратором (рисунок 3).

В данном процессе, известные аномалии, обнаруженные при помощи сравнения с сигнатурами аномалий, а также с пониманием состава протокола, чтобы сформировать мощные отпечатки, характеризующие аномалии (*attack fingerprints*). Понимание протокола

уменьшает количество ложных срабатываний, по сравнению с использованием отдельной сигнатуры. Каждый шаблон применяется только к корректному типу трафика; к примеру, аномалия, использующая *HTTP*, может быть обнаружена только, когда шаблон найден в *HTTP* трафике, но ошибочно не сравнивается с заголовком электронного письма, транспортируемого через *SMTP* [3,4].

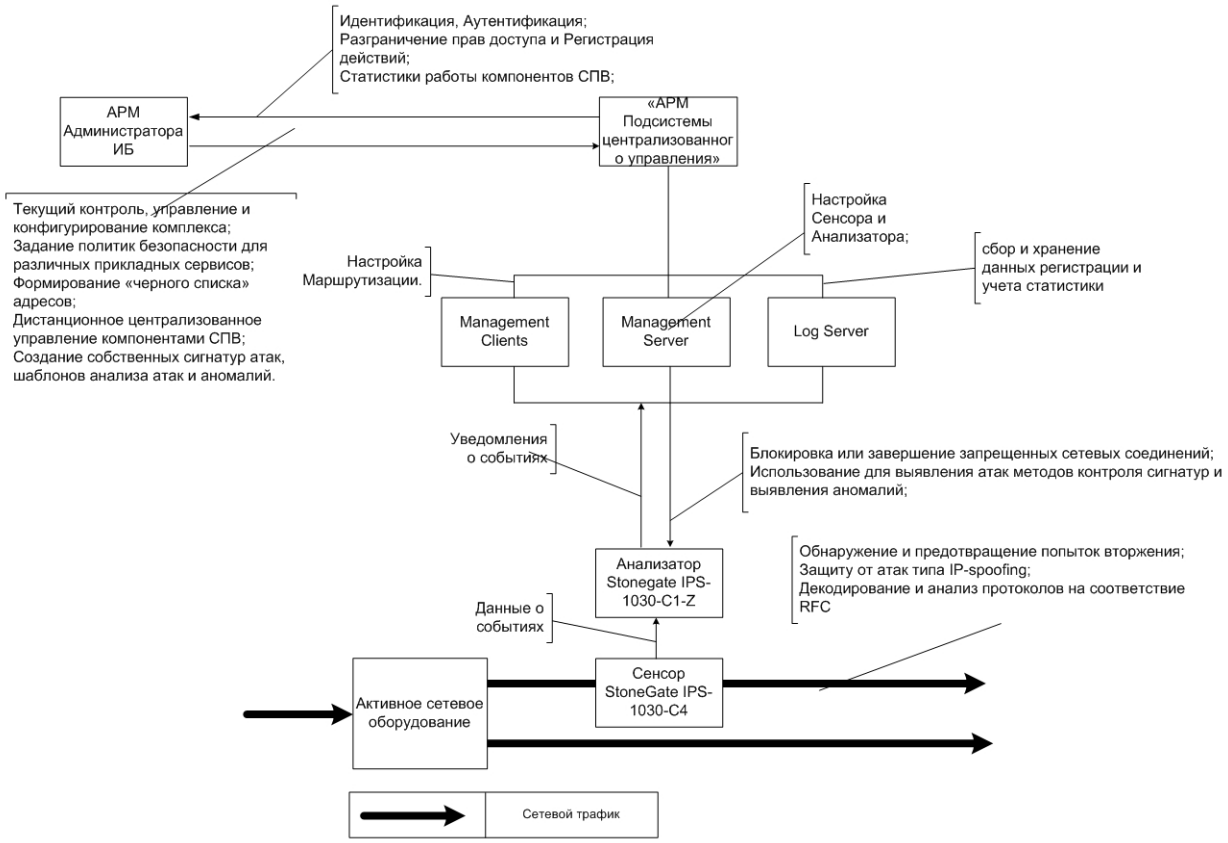

Рисунок 3 - Схема реализации взаимодействия компонентов СОА

В итоге, данная архитектура предоставляет два типа обнаружения аномалий в дополнение к сравнению с отпечатками (шаблонами): анализ протокола и статистическое обнаружение аномалий:

1) анализ протокола идентифицирует нарушения в сетевых соединениях;

2) статистическое обнаружение аномалий собирает статистику по трафику и обнаруживает события, такие как медленное сканирование, необычное число соединений и т.д.

Заключение

Таким образом, система обеспечивает выполнение следующих функциональных характеристик:

1) полный охват источников информации о состоянии сети;
2) наращивание количества источников информации;
3) масштабирование возможностей сбора, ведения и анализа неструктурированной информации;
4) разграничение доступа к информации для различных категорий пользователей;
5) межмодульное взаимодействие отдельных подсистем и ролей персонала в процессе функционирования, с возможным привлечением экспертов-аналитиков.

Предложенный подход к формированию архитектуры исключает ситуации, когда события, критичные для надежного и защищенного функционирования сети, окажутся вне поля зрения аналитиков, и в отношении них не будут приняты соответствующие превентивные меры.

Литература

1. Правиков Д. И., Закляков П. В. Использование виртуальных ловушек для обнаружения телекоммуникационных атак //Проблемы управления безопасностью сложных систем: Труды международной конференции. Москва, декабрь 2011 г./ Под ред. Архиповой Н. И. и Кульбы В. В. Часть 1. М.: РГГУ - Издательский дом МПА-Пресс. 342 с., с 310-314.

2. Отчёт фирмы Symantec по угрозам безопасности в Интернете. http://www.symantec.com/region/ru/ruresc/download/SymantecInternetSecuri...

3. Манн С., Крелл М. Linux. Администрирование сетей TCP/ IP. Пер. с англ. - М.: ООО «Бином-Пресс», 2003.

4. Kohlenberg, Toby (Ed.), Alder, Raven, Carter, Dr. Everett F. (Skip), Jr., Foster, James C., Jonkman Marty, Raffael, and Poor, Mike, "Snort IDS and IPS Toolkit", Syngress, 2007, ISBN 978-1-59749-099-3.

5. Сигнатурный метод анализа, 2010. http://www.ssl.stu.neva.ru/sam/IDS%20Methods.htm

6. Информационная безопасность. Обзор рисков. Телеком - LETA Group, 2012 - http://www.leta.ru/netcat_files/File/riski_telecom.pdf

References

1. Pravikov D. I., Zakljakov P. V. Ispol'zovanie virtual'nyh lovushek dlja obnaruzhenija telekommunikacionnyh atak //Problemy upravlenija bezopasnost'ju slozhnyh sistem: Trudy mezhdunarodnoj konferencii. Moskva, dekabr' 2011 g./ Pod red. Arhipovoj N. I. i Kul'by V. V. Chast' 1. M.: RGGU - Izdatel'skij dom MPA-Press. 342 s., s 310-314.

2. Otchjot firmy Symantec po ugrozam bezopasnosti v Internete. http://www.symantec.com/region/ru/ruresc/download/SymantecInternetSecuri...

3. Mann S., Krell M. Linux. Administrirovanie setej TCP/ IP. Per. s angl. - M.: OOO «Binom-Press», 2003.

4. Kohlenberg, Toby (Ed.), Alder, Raven, Carter, Dr. Everett F. (Skip), Jr., Foster, James C., Jonkman Marty, Raffael, and Poor, Mike, "Snort IDS and IPS Toolkit", Syngress, 2007, ISBN 978-1-59749-099-3.

5. Signaturnyj metod analiza, 2010. http://www.ssl.stu.neva.ru/sam/IDS%20Methods.htm

6. Informacionnaja bezopasnost'. Obzor riskov. Telekom - LETA Group, 2012 - http://www.leta.ru/netcat_files/File/riski_telecom.pdf