времени $t_з = 700$ с осуществляется переключение микропроцессорной системы на режим терминального регулятора и далее отрабатывается перевод профилемера на глубину 100 м за оставшиеся 300 с.

Заключение. Применение комбинированного управления (адаптивного и терминального) позволяет повысить репрезентативность термохалинных измерений для осуществления которых используются автономные глубоководные дрифтеры. Предложенный подход позволяет расширить спектр задач, которые могут быть решены с помощью данных устройств, в частности становится возможным выполнение синхронных маневров дрифтерами, объединенными в группировку. Полученные регуляторы обладают адаптивными свойствами, которые позволяют устранить влияние возмущающих сил, вызванных неоднородностями морской среды, на параметры движения, которое можно формировать при помощи программного устройства в соответствии с выбранной методикой измерений.

Библиографический список использованной литературы

1. Краснодубец Л.А. Управление морскими буями-профилемерами как метод повышения репрезентативности термохалинных измерений. Модели движения / Л.А. Краснодубец, В.И. Забурдаев, В.В. Альчаков // Морской гидрофизический журнал. – 2012. – №4. – С.69 – 79.

2. Краснодубец Л.А. Управление морскими буями-профилемерами как метод повышения репрезентативности термохалинных измерений. Синтез и моделирование системы управления / Л.А. Краснодубец, В.И. Забурдаев, В.В. Альчаков // Морской гидрофизический журнал. – 2012. – №5. – С.70 – 82.

3. Альчаков В.В. Применение управляемых ныряющих дрифтеров как средство повышения репрезентативности профильных измерений морской среды // Вестник СевНТУ. Серия Механика, энергетика, экология. – 2014. №2. – С. 133 – 138.

4. Краснодубец Л.А. Терминальное управление в морских наблюдательных системах с подвижными платформами сбора данных // Изв. РАН. Серия ТиСУ. – 2008. №2. – С. 141 – 153.

Alchakov V.V.Control system depth and sink rate dive Autonomous drifters

Two types of control dynamics dive diving autonomous drifters. The first type of control - control of adaptive type, used to stabilize the sink rate drifter in a heterogeneity of the marine environment. The second type - the type of control terminal is used to achieve the desired depth of penetration for a given period of time with zero final velocity drifter. Modeling process managed dive performed in Matlab.

Keywords: management diving drifters, adaptive control, terminal control.

УДК 004.056

Брюховецкий А.А., канд. техн. наук, доцент
Севастопольский национальный технический университет
ул. Университетская 33, г. Севастополь, Россия, 299053
Сосновский Ю.В., канд. техн. наук, доцент
Милюков В.В., канд. техн. наук, доцент
ТНУ им. В.И. Вернадского, Республика Крым, г. Симферополь, пр. Вернадского, 4.
mailsender256@mail.ru

ФУНДАМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ В ОБЛАСТИ МЕТОДОВ ПОСТРОЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ[9]

Выполнен фундаментальный анализ методы и алгоритмы построения систем идентификации и предотвращения сетевых вторжений. Осуществляется поиск критериев оценки эффективности подобных систем и результатов объективного тестирования.

Ключевые слова: *обнаружение и предотвращение сетевых вторжений, поддержка принятия решения, информационная безопасность*

Вместе с совершенствованием систем обнаружения и предотвращения сетевых вторжений, которые защищают информационные системы отвредоносных действий и утечек информации, растет число и разнообразие методов сетевых атак. На текущий момент наблюдается очередной этап развития систем обнаружения (IDS – IntrusionDetectionsystems), предотвращения вторжений (IPS – Intrusionpreventionsystems) и перехода их на качественно новый уровень – универсальные шлюзы безопасности. Такие устройства получили название UTM (UnifiedThreatManagement, объединенный контроль угроз). Под UTM-системами (универсальными шлюзами безопасности) будем подразумевать

[9] Работа выполнена при финансовой поддержке РФФИ (грант № 14-41-01564).

класс многофункциональных сетевых устройств, преимущественно фаерволов, которые содержат в себе множество функций, таких как антиспам, антивирус, защиту от вторжений (IDS/IPS) и контентную фильтрацию. Примером UTM может служить TrendMicroDeepSecurity (ru.trendmicro.com), KerioControl (kerio.ru), SonicwallNetworkSecurity (sonicwall.com), FortiGateNetworkSecurityPlatformsandAppliances (fortinet.com) или большинство специализированных дистрибутивов Linux — UntangleGateway, IPCopFirewall, pfSense и др.

Целью работы является выполнение сравнительного обзора систем обнаружения и предотвращения сетевых вторжений, учитывая их внутреннюю структуру, поиск критериев для оценки их эффективности и формирование вывода о возможных дальнейших путях решения задачи повышения эффективности подобных систем в ситуации большого потока данных, гетерогенного трафика.

Значительная часть IDS/IPS систем используют методы RBID-технологий, основанные на правилах (RBID, Rule-BasedIntrusionDetection). Обычно RBID системы для выявления потенциальной атаки используют сигнатуру атаки с последующий анализом входящего трафика. Сигнатуры весьма разнообразны и могут определять конкретные параметры от номера порта в пакете до последовательности байт в серии пакетов. После того, как сигнатура разработана, её использование обычно довольно эффективно предотвращает нежелательную сетевую активность.

Главный недостаток такого подхода состоит в том, что сигнатуры предварительно должны быть разработаны и внедрены в систему защиты. Самым оперативным поставщикам требуются часы, чаще – дни для выпуска сигнатуры. И, несмотря на оперативность этих действий, фундаментальная проблема остается: RBID-система не идентифицирует аномальную сетевую активность без сигнатуры новой атаки. Поэтому такие черви, как, например, W32.SQLExp, поражающие сеть в течение нескольких секунд, администратору не оставляют никаких шансов, несмотря на регулярно обновляемые RBID системы.

Решением этой проблемы может быть использование альтернативного метода обнаружения вторжений и аномалий поведении. Системы, использующие статистический подход (Statistic-BasedIntrusionDetection, SBID), как правило, реализуют следующую концепцию: система определяет нормальную сетевую активность и затем весь трафик, не подпадающий под определение «нормального» помечается как аномальный [1].

Для анализа сетевого трафика применяются разнообразные методы, толчком к широкому применению статистического анализа послужило установление наличия т.н. «тяжелого хвоста» распределения интервалов времени между пакетами и «взрывного» характера поведения интенсивности поступления сетевых пакетов протоколаTCP/IP. На сегодняшний день есть сведения о применении циклического анализа [2], параметрических и непараметрических статистических критериев согласия [3].

Сравнительная оценка существующих, разрабатываемых систем обнаружения и предотвращения вторжений представляет собой нетривиальную задачу, т.к. нет общепринятых методов проверки, верификации подобных систем, как нет единых стандартов оценки их эффективности. Анализ имеющихся данных по программным решениям, доступным на рынке приведен ниже.

Suricata. Система изначально работает в многопоточном режиме, что актуально для современных многопроцессорных конфигураций, имеется возможность аппаратной акселерации на стороне GPU за счет задействования CUDA и OpenCL. Изначально поддерживается IPv6, для перехвата трафика используются стандартные интерфейсы: LibPcap, NFQueue, IPFRing, IPFW. Блокировка нежелательного трафика производится средствами штатного пакетного фильтра ОС. Автоматически определяет и сканирует протоколы IP, TCP, UDP, ICMP, HTTP, TLS, FTP, SMB, SMTP и SCTP.

Основу механизма детектирования в Suricata составляют правила (rules). Есть возможность подключать рулесеты, созданные другими проектами (Sourcefire VRT, OpenSourceEmergingThreats (hemergingthreats.net) и EmergingThreatsPro. В настройках используются переменные (механизм flowint), позволяющие, например, создавать счетчики. Причем информацию можно сохранить из потока и в дальнейшем использовать. Такой подход применен для детектирования попыток подбора пароля и более эффективен, чем в Snort, который базируется на пороговом значении срабатывания. Планируется появление механизма IP Reputation. Существует готовый дистрибутив Smooth-sec (bailey.st/blog/smooth-sec), построенный на базе Suricata.

Samhain. Выпускаемый под OpenSource лицензией Samhain относится к хостовымIDS, защищающим отдельный компьютер. Используется несколько методов анализа, позволяющих полностью охватить все события, происходящие в системе:

- база данных сигнатур важных файлов, которая создается при первом запуске и в дальнейшем сравнивается с живой системой;
- мониторинг и анализ записей в журналах;
- контроль входа/выхода в систему;
- мониторинг подключений к открытым сетевым портам;
- контроль файлов с установленным SUID и скрытых процессов.

StoneGateIntrusionPreventionSystem. Реализованы функции: IPS, защита от DDoS и 0day атак, веб-фильтрация, поддержка зашифрованного трафика и т.д. Используя StoneGate IPS, системный администратор в ручном режиме имеет возможность заблокировать вирус, spyware, работу определенных приложений (P2P, IM и прочее).

Для веб-фильтрации используется постоянно обновляемая база сайтов, разделенных на несколько категорий. Особое внимание уделяется защите от обхода систем безопасности, разделяя корпоративную сеть на несколько виртуальных сегментов и для каждого устанавливая индивидуальные политики безопасности. Настройка политик проверки трафика производится при помощи шаблонов, содержащих типовые правила. Процесс создания политик происходит в оффлайн-режиме, по окончании администратор их проверяет и загружает на удаленные узлы IPS. Сходные события в StoneGate IPS обрабатываются по принципу, используемому в SIM/SIEM-системах.

Поставляется StoneGate IPS как в виде аппаратного комплекса, так и образа VMware. Последний предназначен для установки на собственном оборудовании или в виртуальной инфраструктуре.

IBM Security Network Intrusion Prevention System.Система использует запатентованную технологию анализа протоколов, которая обеспечивает превентивную защиту, в том числе и от 0day угроз. Как и во всех продуктах серии IBMSecurity, его основой является модуль анализа протоколов — PAM (ProtocolAnalysisModule), сочетающий в себе традиционный сигнатурный метод обнаружения атак и поведенческий анализатор. При этом PAM различает 218 протоколов уровня приложений (атаки через VoIP, RPC, HTTP и т.д.) и такие форматы данных, как DOC, XLS, PDF, ANI, JPG, чтобы предугадывать место, куда может быть внедрен вредоносный код. Для анализа трафика используется более 3000 алгоритмов, около 200 из них ориентированы на идентификациюDoS-атак. Функции межсетевого экрана позволяют разрешить доступ только по определенным портам и IP, без необходимости привлечения дополнительного устройства.

McAfeeNetworkSecurityPlatform 7.В дополнение ко всем функциями классического NIPS, новый продукт получил инструменты для анализа пакетов, передаваемых по внутренней корпоративной сети, что помогает обнаруживать вторжение в начальной стадии. В McAfee использована технология GlobalThreatIntelligence, которая собирает информацию с сотен тысяч датчиков, установленных по всему миру, и дает оценку репутации всем проходящим уникальным файлам, IP- и URL-адресам, протоколам. В результате NSP может обнаруживать трафик ботнета, 0day угрозы и DDoS атаки, а такой широкий охват позволяет свести к нулю вероятность ложного срабатывания.

В отличии от многих других IDS/IPS, NSP позволяет анализировать трафик между виртуальными машинами (VM), а также VM и физическим хостом. Для наблюдения за узлами используется агентский модуль от компании ReflexSystems, который собирает информацию о трафике в VM и передает их в физическую среду для анализа.

Ядро системы различает более 1100 приложений, работающих на 7-ом уровне OSI, просматривая трафик при помощи механизма контент-анализа и предоставляя простые инструменты управления [http://wpconfig.ru/?p=961].

Сведения об оценки эффективности IDS/IPS систем. Не существует единых общепринятых показателей эффективности систем обнаружения и предотвращения вторжений. Ввиду того, что большинство подобных систем имеют закрытый код, производитель указывает различные названия собственных технологий с не всегда ясными алгоритмами работы. Один из немногих доступных документов [4] от лаборатории nsslabs, предоставляет возможность перечислить оцениваемые технические показатели при тестировании IPS/IDS систем указанной лабораторией:

- число пакетов в секунду, обрабатываемое системой;
- число байт в секунду или средний размер пакета;
- количество уникальных хостов;
- скорость установления новых соединений;
- количество одновременных соединений;
- число предупреждений в секунду, генерируемое системой;
- пропускная способности при передаче трафика TCP, HTTP и реалистичной смеси трафика различных протоколов прикладного уровня.

Также, имеются сведения, что при тестировании аппаратного обеспечение BreakingPoint [http://www.ixiacom.com/solutions/ips-test/] компании Ixia оценивались времена задержки передачи пакета. Доступные данные чрезвычайно бедны. Указывается, что задержки лежат в окрестности 30 мкспри аппаратной обработке потока данных и 150-200 мкс при программной обработке.

Показатель, который оценивается nsslabs, Ixia и несколькими другими лабораториями, которые предоставляют соответствующие сведения – процент обнаруженных атак. В тоже время методика тестирования является закрытой, что не позволяет полноценно использовать результаты. При тестах систем IPS/IDS различными компаниями данный показатель колеблется от 70% до 10% у компании Ixia,

в тоже время при тестировании продуктов семейства IPS/IDS лабораторией «nsslabs» в 2013 году средний процент обнаруженных атак составляет 96,5%.

В связи с проведенным анализом, можно сделать следующие выводы:

1. В современном информационном пространстве предлагается значительное число аппаратных и программных средств обнаружения, блокирования вторжений, многие из которых на данный момент трансформируются в системы объединенного контроля угроз (UTM-системы);

2. Практически все значимые представители рынка IPS/IDS, UTM-систем работают по сигнатурному принципу анализа трафика;

3. Развитие подобных систем идет по направлениям:

– Повышение уровней анализа сетевого трафика модели OSI (многие системы анализируют данные на 7-м уровне – уровне приложения)

– Расширение базы правил (сигнатур), возможность импорта баз конкурирующих систем, возможность создания собственных правил системным администратором

– Внедрение в глобальной сети своих собственных сканеров (McAfee), собирающих информацию с датчиков, установленных по всему миру, и дающих оценку репутации всем проходящим уникальным файлам, IP- и URL-адресам, протоколам.

– Объединение в одной системе множества функций, таких как антиспам, антивирус, защиту от вторжений (IDS/IPS) и контентную фильтрацию (UTM-системы:TrendMicroDeepSecurity (ru.trendmicro.com), KerioControl (kerio.ru), SonicwallNetworkSecurity (sonicwall.com), FortiGateNetworkSecurityPlatformsandAppliances (fortinet.com) или большинство специализированных дистрибутивов Linux — UntangleGateway, IPCopFirewall, pfSense);

4. Таким образом, на современном этапе путь развития систем IPS/IDS ->UTM можно признать экстенсивным. Принципиально новые технологии не находят массового применения или являются засекреченными компаниями-разработчиками;

5. Подавляющее большинство компаний-производителей систем IPS/IDS описывает их возможности, но не предоставляет информацию о тестировании программного или аппаратного продуктов. Найти подобную информацию крайне сложно. Отдельные значимые исследования систем IPS/IDS, проводимые, к примеру, лабораторией nsslabs [https://www.nsslabs.com/reports/categories/test-reports] предоставляются только на коммерческой основе, диапазон стоимости материалов исследований колеблется от 1,450 до 3,500 долл. США.

Перспективами дальнейших исследований, несмотря на большую популярность данного направления, является разработка информационной технологии, позволяющего повысить объективность сравнения и тестирования систем обнаружения и предотвращения вторжений, а также математического аппарата, позволяющего обрабатывать значительные объемы сетевого трафика, выполнять его кластеризацию и идентификацию в условиях гетерогенных потоков данных.

Библиографический список использованной литературы

1. Карпук Н. М. Статистический анализ сетевого трафика / Н.М. Карпук // БГУ.– 2008. Электронный ресурс. Режим доступа: [http://elib.bsu.by/handle/123456789/7401]

2. Ажмухамедов И.М., Марьенков А.Н. Поиск и оценка аномалий сетевого трафика на основе циклического анализа / И.М. Ажмухамедов, А.Н. Марьенков // Электронный научный журнал «Инженерный вестник Дона». – №2. – 2012г. Электронный ресурс. Режим доступа [http://ivdon.ru/magazine/archive/n2y2012/742]

3. Ловягин В.С. Статистический мониторинг вирусных атак на основе параметрических критериев / В.С. Ловягин // ВісникСевНТУ: зб. наук.пр. Вип. 114/2011. Серія: Інформатика, електроніка, зв'язок. — Севастополь. – 2011 с. 31-35.

4. The Fifth International Conference on Digital Society ICDS 2011 / David J. Day Benjamin M. Burns // A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines. – 2011. – pp.187-192.

Bryukhovetskiy A.A., Sosnovskij Y.V., Milukov V.V. Fundamental research in the field of methods of construction of systems for detecting and preventing network intrusions

Fundamental analysis of methods and algorithms for constructing of intrusion detection and prevention systems is identification and prevent network intrusions carried out. The criteria for evaluating the effectiveness of such systems and the results of objective testing are proposed.

Key words: detecting and preventing network intrusions, decision support, information security