A. A. Chechulin, I. V. Kotenko

Attack Graph Construction for Security Events Analysis

Keywords: *attack modeling, intrusion detection, security events processing, attack graphs*

The paper is devoted to investigation of the attack graphs construction and analysis task for a network security evaluation and real-time security event processing. Main object of this research is the attack modeling process. The paper contains the description of attack graphs building, modifying and analysis technique as well as overview of implemented prototype for network security analysis based on attack graph approach.

А. А. Чечулин, И. В. Котенко

ПОСТРОЕНИЕ ГРАФОВ АТАК ДЛЯ АНАЛИЗА СОБЫТИЙ БЕЗОПАСНОСТИ[1]

Введение

Основными задачами систем управления информацией и событиями безопасности (Security Information and Event Management, SIEM) являются сбор, обработка и анализ событий безопасности, обнаружение в режиме реального времени атак и нарушений политик безопасности, оценка защищенности ресурсов, выработка и принятие решений по защите информации [1, 2].

В SIEM-системах нового поколения анализ событий, инцидентов и их последствий включает процедуры моделирования событий и атак, анализа уязвимостей и защищенности системы, определения характеристик нарушителей, оценки риска, прогнозирования событий и инцидентов.

Предполагается, что моделирование инцидентов и событий безопасности, основанное на автоматических механизмах, которые используют информацию об истории анализируемых сетевых событий и прогнозе будущих событий, а также реализующее автоматическую подстройку параметров мониторинга событий к текущему состоянию защищаемой системы, позволит повысить уровень защищенности сети [3–5].

Поскольку результаты работы подсистемы моделирования атак часто не могут быть вычислены в режиме реального времени, их использование в процессах, проходящих в режиме реального времени, затруднено. Однако построенные графы атак сохраняют актуальность достаточно долгое время (до значительных изменений в политике безопасности или физической топологии сети). Благодаря этому в рамках общей системы анализа событий предлагается использовать построенные заранее графы атак [6]. Эти графы атак могут применяться для решения двух основных типов задач: для предсказания последующих действий нарушителя и для анализа и выявления его прошлых действий, приведших систему к текущему состоянию.

[1] Работа выполнена при финансовой поддержке РФФИ (проекты 13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), программы фундаментальных исследований ОНИТ РАН (контракт №2.2), проекта ENGENSEC программы Европейского Сообщества TEMPUS и государственного контракта №14.604.21.0033.

Основной целью данной работы является создание методики построения и анализа графов атак, позволяющей, с одной стороны, оценить защищенность компьютерной сети от атак, а с другой — участвовать в анализе событий безопасности для выявления наиболее вероятных трасс атак и, как следствие, наиболее вероятных нарушителей. Основной особенностью, отличающей предложенную методику от существующих, является способ использования графов атак и учета текущих событий безопасности для идентификации фрагмента графа атак.

1. Методика построения графов атак

Графы атак применяются в системах аналитического моделирования атак для оценки уровня защищенности системы от потенциально возможных атак и улучшения точности определения атакующих действий, осуществленных нарушителем. При этом главной проблемой моделирования атак в существующих системах управления информацией и событиями безопасности является невозможность выполнения моделирования в режиме реального времени. Для решения этой проблемы предлагается разделить процесс построения графов на подготовительный (не real-time) и рабочий (near real-time) этапы. В данной работе представлен подход к построению графов атак на подготовительном этапе.

На этапе подготовки к построению деревьев атак для каждого хоста строится трехмерная матрица по следующим данным: 1) класс атак (сбор данных, подготовительные действия, повышение привилегий, выполнение цели атаки); 2) необходимый тип доступа (удаленный источник без прав доступа, удаленный пользователь системы, локальный пользователь системы, администратор); 3) уровень знаний нарушителя (типы уязвимостей, которые нарушитель может реализовывать).

В результате, для каждого хоста формируется список возможных атакующих действий, разбитых на группы по следующим параметрам: класс атаки, необходимый тип доступа и необходимый уровень знаний нарушителя, а для каждой группы, в свою очередь, формируется список конкретных атак и уязвимостей, которые эти атаки используют. Общий список уязвимостей формируется на основе описания программно-аппаратного обеспечения хоста на языке CPE [7] и таких открытых баз уязвимостей, как NVD (National Vulnerability Database). Источниками данных об открытых уязвимостях также могут служить отчеты сканеров безопасности, таких как Nessus, MaxPatrol и др. Уязвимости в системе хранятся в формате CVE [8].

Кроме отдельных уязвимостей при построении графа атак используются шаблоны атак в формате CAPEC [9], которые могут выступать не только в качестве входной информации для построения графов атак, но и как результат анализа безопасности — они могут описывать наиболее часто встречающиеся последовательности эксплуатации уязвимостей и других действий атакующего. Также шаблоны содержат описания атак, которые не используют уязвимостей: например, первая стадия проведения атаки — это сбор информации о доступных хостах. Для этого используется шаблон CAPEC-292 (Host Discovery), описывающий группу различных способов проведения сканирования хостов и портов. В эту группу, например, входят: CAPEC-285 (ICMP Echo Request Ping), CAPEC-296 (ICMP Information Request), CAPEC-299 (TCP SYN Ping) и др.

Следующая стадия атаки — поиск уязвимого программного обеспечения. Для этого используются следующие шаблоны: CAPEC-310 (Scanning for Vulnerable Software), CAPEC-311 (Fingerprinting Remote Operating Systems), CAPEC-300 (Port Scanning) и т. д. На третьей стадии проведения атаки используются как отдельные уязвимости из словаря CVE, так и шаблоны, например CAPEC-233 (Privilege Escalation) и т. д.

После формирования матрицы потенциальных атак для каждого хоста, для анализируемой сети выбираются возможные типы нарушителей и точки доступа, в которых они могут получить доступ к сети. Примерами нарушителей могут являться: внешний хакер — пользователь, обладающий значительными знаниями в области информационной безопасности, но не имеющий никаких прямых возможностей подключится к внутренней сети, кроме как через компьютеры, к которым открыт

доступ из сети Интернет; внутренний пользователь — пользователь, обладающий начальными знаниями в области информационной безопасности и имеющий возможность зайти на некоторые компьютеры внутренней сети с правами локального пользователя или администратора; и т. д.

Далее для каждой выбранной модели нарушителя составляется список возможных целей. Так, для внутреннего пользователя это может быть месть (то есть причинение максимального ущерба компании), для внешнего хакера это может быть доступ к некоторой конфиденциальной информации, расположенной на определенном сервере внутри сети, а для червя целью может быть распространение инфекции по сети.

Соответственно, моделью нарушителя для конкретной сети является множество пар (тип нарушителя, цель), которые определяют ограничения по использованию атакующих действий и возможные начальные точки доступа в сеть. После этого на основе собранной информации формируются графы атак для всех выбранных моделей нарушителя.

2. Обработка событий безопасности

После того как графы атак будут сформированы для всех потенциальных нарушителей, система переходит в режим обработки событий безопасности. В этом режиме основная функция системы защиты информации — выявление конкретных нарушителей и формирование направленной защиты. Рассмотрим пример. Если нарушитель проводит атаку на некоторый хост в сети, то у него могут быть следующие цели: 1) захватить контроль над хостом для проведения дальнейших атак; 2) захватить данные на атакуемом хосте. Для того чтобы правильно построить защиту, необходимо определить цель нарушителя и предсказать его последующие действия. Рассмотрим варианты более подробно.

Первый вариант подразумевает, что нарушитель будет использовать атакуемый хост как промежуточный и конечной целью он не является. Таким образом, мы можем предсказать следующие действия нарушителя: он будет параллельно искать другие промежуточные хосты, а если захватит атакуемый, то атака продолжится уже и с атакуемого хоста. В качестве защитных мер в данном случае имеет смысл повысить чувствительность правил обнаружения атак, источником которых будет являться атакуемый хост, чтобы обнаружить захват этого хоста. Это позволит собрать дополнительную информацию о нарушителе и его методах.

Второй вариант подразумевает, что атакуемый хост является конечной целью нарушителя и содержит некоторую ценную информацию. Скорее всего, все хосты в сети, подконтрольные нарушителю, будут принимать участие в атаке. В данном случае имеет смысл временно заблокировать сомнительные или все соединения с данным хостом, а все хосты, обращающиеся к атакуемому хосту, считать потенциально захваченными.

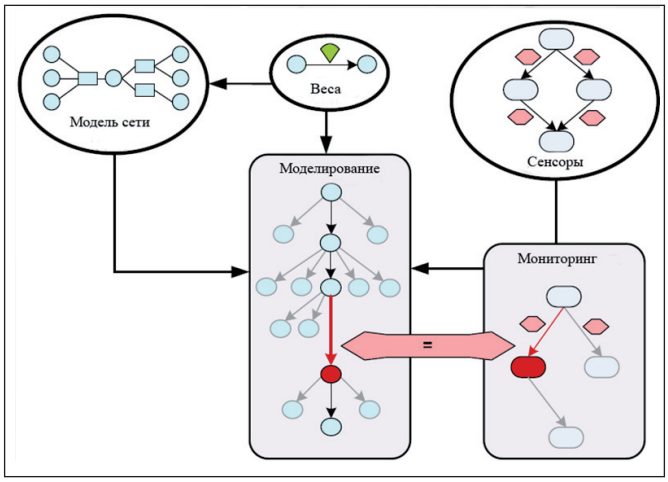

Рис. 1. Архитектура системы анализа событий

Таким образом, при одном и том же обнаруженном событии в сети (атаке) реакция системы защиты будет разной. Второй вариант реакции при первой цели фактически позволит выполнить нарушителю DoS-атаку, которая может привести к успешной реализации другой атаки, например IP spoofing. И наоборот, первый вариант реакции при второй цели может привести к утечке информации через соединения с другими хостами.

На рис. 1 представлена общая архитектура использования графов атак для обнаружения атак, проводимых в реальной сети.

Предлагаемый подход содержит три основных этапа:

1) на основе модели сети и вероятных нарушителей формируется граф атак;

2) в реальной сети формируется сеть связанных сенсоров, которые позволяют обнаруживать отдельные атакующие действия. Система мониторинга позволяет построить общую картину событий, происходящих в сети, на основе собранной от сенсоров информации;

3) далее общая система управления ищет соответствия между графами атак и событиями в реальной сети.

Таким образом, на основе анализа инцидентов с учетом деревьев атак становится возможным делать выводы о том, что существует большая вероятность того, что инциденту «производится сканирование хоста C хостом B» предшествовал необнаруженный инцидент «хост B был атакован хостом A» и что последующим действием нарушителя будет «хост C подвергается атаке со стороны хоста B».

3. Описание прототипа

Приведем пример применения предлагаемого подхода для оценки уровня защищенности критически важной инфраструктуры — компьютерной сети дамбы. На рис. 2 изображены основные зоны защищаемой сети: территория дамбы, подсеть управления дамбой и подсеть, обеспечивающая визуализацию состояния дамбы для внешних пользователей. В качестве исходного месторасположения атакующего выбран хост, находящийся вне защищаемой сети (Visualization Users). В качестве цели для атакующего выбран сервер, через который осуществляется управление дамбой (Application Server 1).

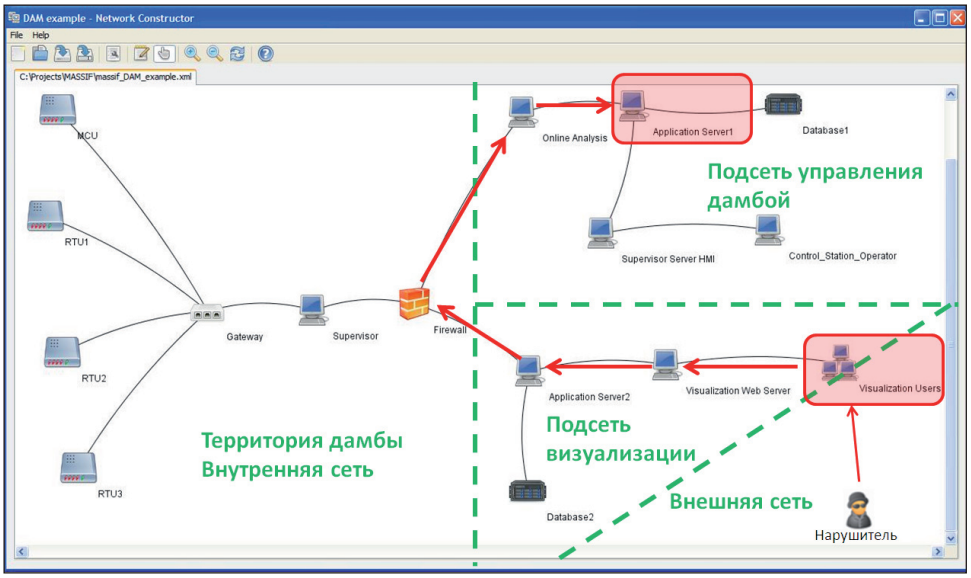

Рис. 2. Архитектура сети

На рис. 3 приведено дерево атак, ведущее от начального положения атакующего до его цели. В процессе построения графа моделировались три основные стадии проведения атак: сбор информации, выявление уязвимостей и их эксплуатация.

Этап сбора информации представлен на дереве атак (рис. 3) элементами, помеченными символом «V» и шагами, 3, 6, 9 и 12 трассы атаки. Опишем несколько шагов трассы, относящихся к этому этапу, более подробно. Шаг 1 — поиск узлов, связанных с начальным месторасположением нарушителя (хостом Visualization Users). Результатом выполнения шага 1 является обнаружение хоста Visualization Web Server. Шаг 4 — поиск узлов, связанных с хостом Visualization Web Server. Результатом выполнения шага 4 является обнаружение хоста Application Server.

Примерами выполнения этапа выявления уязвимостей являются элементы, помеченные символом «S» на рис. 3, и шаги 2, 5, 8, 11 и 14 трассы атаки. Приведем пример: шаг 2 — поиск уязвимостей хоста Visualization Web Server. Результат — обнаружены несколько уязвимостей операционной системы, установленной на данном хосте (Microsoft Windows Server 2003).

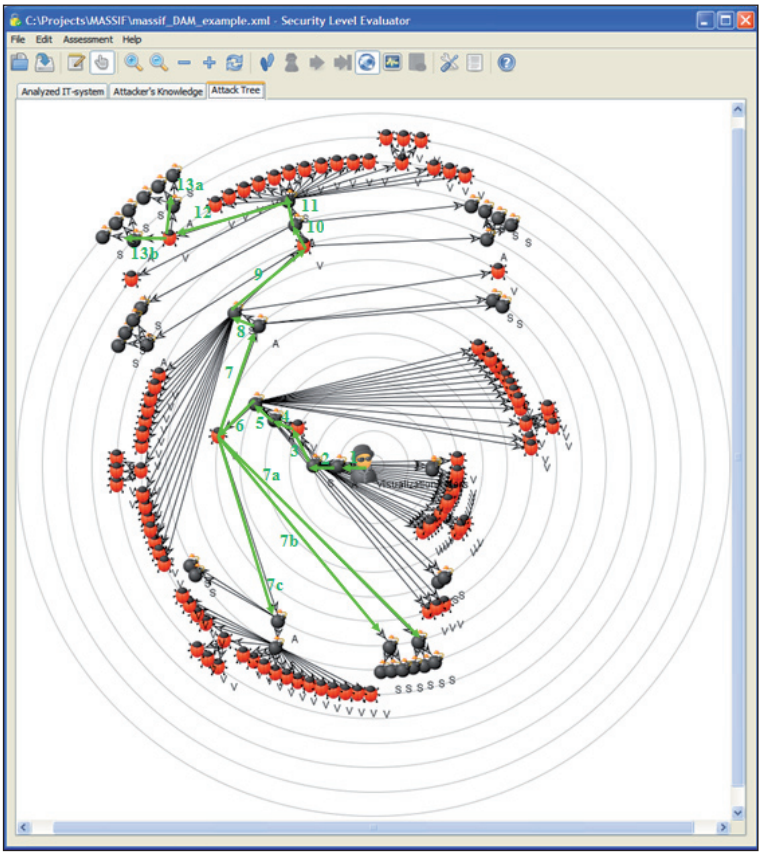

Рис. 3. Граф атак

Третий этап — эксплуатация уязвимостей. Он отображается на рис. 3 элементами, помеченными символом «A», и шагами 1, 4, 7, 7a, 7b, 7c, 10, 13a и 13b трассы атаки. Каждый из вышеперечисленных элементов содержит эксплуатацию как минимум одной уязвимости, продвигающей нарушителя к намеченной цели. Так, например, шаг 3 — эксплуатация уязвимости CVE-2007-0214, которая позволяет провести удаленную атаку и получить права администратора на хосте Visualization Web Server.

Общие результаты анализа защищаемой сети выглядят следующим образом: всего в графе атак задействовано 7 хостов, для этих хостов было построено около 150 различных трасс атак (трассы отличаются друг от друга набором использованных уязвимостей). Для каждого действия атакующего и для каждой трассы были рассчитаны параметры сложности (Access Complexity (AC)) и возможного ущерба (Mortality (M)). В результате была выбрана трасса, имеющая минимальные значения сложности и максимальные значения ущерба для каждого хоста. На основе

данных об этом маршруте был рассчитан уровень защищенности сети в целом. Значение уровня защищенности для анализируемой сети составило 3 из 4, где уровень 1 — это максимальная защищенность, что значит, что сеть требует срочного внимания специалиста по информационной безопасности. Наиболее слабым местом сети (то есть хостом, через который проходит максимальное количество трасс атак) оказался хост Web Server. Через него прошли все трассы атак. Таким образом, общая рекомендация системы моделирования — повысить уровень защищенности этого хоста. Более детальные рекомендации касаются исправления конкретных уязвимостей и формируются на основе данных, полученных из CVE.

На следующей стадии эксперимента в систему моделирования был загружен журнал сетевых событий. Данный журнал содержит 2 типа сетевых событий — изменения в сетевой топологии и обнаруженные сетевые атаки. Рассмотрим пример журнала событий:

1) 192.168.0.107 192.168.0.2 SCAN nmap TCP {tcp}
2) 192.168.0.2 installed cpe:/a:mysql:mysql:5.1.33

Запись под номером 1 содержит информацию об обнаружении процесса сканирования. Хост Database2 (192.168.0.2) был просканирован хостом Application server2 (192.168.0.108) с помощью сканера Nmap. Если другие атакующие действия в журнале отсутствуют, то система моделирования примет решение о том, что в сети действует внутренний нарушитель, так как внешние нарушители осуществили, прежде всего, атаку на Visualization Web Server.

Запись 2 говорит о том, что на хосте Database2 было установлено новое ПО. Данная запись содержит CPE-описание MySQL server (СУБД MySQL 5.1.33 был установлен вместо MySQL 5.0). Это событие приводит к тому, что некоторые уязвимости, существовавшие до изменения в сети, могли исчезнуть. Так, например, после обновления версии БД становится невозможным нарушить конфиденциальность и целостность данных, хранящихся на хосте Database2.

Заключение

В настоящей работе предложен подход к использованию системы моделирования атак для повышения точности и оперативности обнаружения атак в общем потоке событий. Рассмотренные в статье задачи являются составными элементами общей системы управления инцидентами и событиями. Кроме того, предложенный подход позволяет после обнаружения атаки вычислить вероятные характеристики нарушителя (такие, как уровень знаний, технические возможности, цели и т. д.), предсказать возможные направления развития атаки и возможные действия нарушителя, которые предшествовали проведению основной атаки (захват управления над сетевым оборудованием, кража паролей и т. д.). Результатом работы системы моделирования атак также могут быть следующие характеристики: 1) слабые места в топологии сети (хосты, через которые проходит наибольшее число графов атак); 2) выбранные контрмеры, позволяющие снизить вероятность максимального количества графов атак; 3) возможные последствия реализации контрмер, учитывающие зависимости сервисов.

В настоящее время продолжаются теоретические исследования способов построения графов атак, учитывающих существующие уязвимости и уязвимости нулевого дня, политики безопасности, зависимости сервисов и т. д., и осуществляется разработка программного прототипа системы построения и анализа графов атак. В дальнейшей работе планируется: 1) расширить функциональность системы, добавив в систему анализ атак нулевого дня и связей сервисов; 2) расширить список метрик безопасности для уточнения оценки уровня защищенности сети; 3) уточнить модель нарушителя; 4) ускорить работу системы за счет оптимизации процесса построения графов атак.

СПИСОК ЛИТЕРАТУРЫ:

1. *Котенко И. В., Дойникова Е. В., Чечулин А. А.* Общее перечисление и классификация шаблонов атак (CAPEC): описание и примеры применения // Защита информации. Инсайд. № 4. 2012. С. 54–66.
2. *Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. СПб.: Наука, 2012. Вып. 1 (20). С. 27–56.
3. *Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А.* Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. 2012. № 2. С. 57–68.
4. *Kotenko I., Chechulin A., Novikova E.* Attack Modelling and Security Evaluation for Security Information and Event Management // SECRYPT 2012. International Conference on Security and Cryptography. Proceedings. Rome. Italy. 24–27 July 2012. P. 391–394.
5. *Kotenko I., Chechulin A.* Attack Modeling and Security Evaluation in SIEM Systems // International Transactions on Systems Science and Applications. SIWN Press. Vol. 8. Dec. 2012. P. 129–147.
6. *Котенко И. В., Чечулин А. А.* Аналитическое моделирование атак для управления информацией и событиями безопасности // Труды конгресса по интеллектуальным системам и информационным технологиям «IS&IT». Россия, Краснодарский край, пос. Дивноморское. 2–9 сентября 2012 г. М.: Физматлит, 2012. С. 385–391.
7. Common Platform Enumeration (CPE). URL: http://cpe.mitre.org/ (дата обращения: 29.01.2013).
8. Common Vulnerabilities and Exposures (CVE). URL: http://cve.mitre.org/ (дата обращения: 29.01.2013).
9. Common Attack Pattern Enumeration and Classification (CAPEC). URL: http://capec.mitre.org/ (дата обращения: 29.01.2013).

REFERENCES:

1. *Kotenko I. V., Doiynikova E. V., Chechulin A. A.* Obshee perechislenie I klassifikatsiay shablonov atak (CAPEC):opisanie I primeri primeri primeneniay// Zashita inforvatsii. Isayd, № 4, 2012. P. 54–66.
2. *Kotenko I. V., Saenko I. B., Polubelova O. V., Chechulin A. A.* Primenenie tekhnologii upravleniay informatsieiy i sobitiaymi bezopasnosti dlay zashiti informatsii v kriticheskikh vagnikh infrastrukturakh // Trudi SPIIRAN. Vip. 1 (20) SPb.: Nauka, 2012.
3. *Kotenko I. V., Saenko I. B., Polubelova O. V., Chechulin A. A* Tekhnologii upravleniay informatsieiy i sobitiaymi bezopasnosti dlay zashiti komruternikh setey // Problemi informatsionnoiy bezopasnosti. Komputernie sistemi. 2012. № 2.
4. *Kotenko I., Chechulin A., Novikova E.* Attack Modelling and Security Evaluation for Security Information and Event Management // SECRYPT 2012. International Conference on Security and Cryptography. Proceedings. Rome, Italy. 24–27 July 2012.
5. *Kotenko I. V., Chechulin A. A.* Attack Modeling and Security Evaluation in SIEM Systems. International Transactions on Systems Science and Applications, SIWN Press. Vol. 8, Dec, 2012. ISSN 1751–1461.
6. *Kotenko I. V., Chechulin A. A.* Analiticheskoe modelirovanie atak dlay upravleniay informatsiey b sobitiaymi bezopasnosni // Trudi kongressa po intellektualnim sistemam I informatsionnim tekhnologiaym. "IS&IT". Rossiay, Krasnodarskiy kray, pos. Divnomorskoe. 2-9 sentaybray 2012. M.: Fizmatlit, 2012. P. 385–391.
7. Common Platform Enumeration (CPE). http://cpe.mitre.org/, 29.01.2013.
8. Common Vulnerabilities and Exposures (CVE). http://cve.mitre.org/, 29.01.2013.
9. Common Attack Pattern Enumeration and Classification (CAPEC). http://capec.mitre.org/, 29.01.2013.