Многоагентные технологии анализа уязвимостей

и обнаружения вторжений в компьютерных сетях*

И. В. Котенко, *д. т. н., профессор*
СПИИРАН
ivkote@spiiras.nw.ru

Окончание. Начало см. в № 2'2004.

Компоненты многоагентной системы обнаружения вторжений (МСОВ) – это взаимодействующие между собой агенты, совместно решающие общую задачу обнаружения вторжений в компьютерную сеть [11, 12]. Архитектура МСОВ включает один или несколько экземпляров агентов разных типов, специализированных для решения подзадачи обнаружения вторжений. Агенты распределены по хостам защищаемой сети, специализированы по типам решаемых задач и взаимодействуют друг с другом с целью обмена информацией и принятия согласованных решений. В принятой архитектуре исследуемого прототипа МСОВ в явном виде отсутствует «центр управления» семейством агентов – в зависимости от сложившейся ситуации ведущим может становиться любой из агентов, инициирующий и (или) реализующий функции кооперации и управления. В случае необходимости агенты могут как клонироваться (образовывать новые сущности), так и прекращать свое функционирование. В зависимости от ситуации (вида и количества атак на компьютерные сети, наличия вычислительных ресурсов для выполнения функций защиты) может потребоваться генерация нескольких экземпляров агентов каждого класса. Предполагается, что архитектура МСОВ может адаптироваться к реконфигурации сети, изменению трафика и новым видам атак, используя накопленный опыт.

Рассмотрим базовые типы компонентов разработанной модели МСОВ и ее программной реализации, размещаемые на каждом из хостов защищаемой компьютерной сети (рис. 5).

Агент-демон AD-E (AD-Events) осуществляет предварительную обработку поступающих на хост сообщений, фиксируя значимые для защиты информации события, и переадресует выделенные сообщения соответствующим специализированным агентам.

Агент-демон идентификации и аутентификации AIA ответственен за идентификацию источников сообщений и подтверждение их подлинности. **Агент-демон разграничения доступа ACA** регламентирует доступ пользователей к ресурсам сети в соответствии с их правами и метками конфиденциальности объектов защиты. Агенты AIA и ACA обнаруживают несанкционированные действия, направленные на получение доступа к информационным ресурсам хоста, прерывают соединения и процессы обработки событий, отнесенные к числу несанкционированных, а также посылают сообщения агентам обнаружения вторжений.

Агенты-демоны AD-P1 и AD-P2 (AD-Patterns) отвечают за обнаружение отдельных «подозритель-

* *Работа выполнена при поддержке РФФИ (проект № 01-01-00108).*

ных» событий или очевидных фактов вторжения и принятие решений (как предварительного, так и заключительного) относительно реакции на данные события (факты). В разработанном прототипе агент AD-P1 ответственен за обнаружение сканирования портов на прикладном уровне, использования утилиты finger и атак на переполнение буфера (buffer overflow). Агент AD-P2 отвечает за обнаружение сканирования портов SYN scanning класса Port scanning и атак SYN flood класса Denial of service. Обнаруженные агентами AD-P1 и AD-P2 факты сообщаются агентам IDA1 и (или) IDA2.

Интеллектуальные агенты обнаружения вторжений IDA1 и IDA2 реализуют более высокий уровень обработки и обобщения обнаруженных фактов. Они принимают решения на основе сообщений об обнаруженном подозрительном поведении и явных атаках как от агентов-демонов своего хоста, так и от агентов других хостов. IDA1 обрабатывает сообщения, возникающие в процессе реализации комбинированной спуфинг (spoofing)-атаки, отслеживает ее развитие и принимает решение о реакции на данную атаку. IDA2 выполняет высокоуровневую обработку фактов, направленную на обнаружение распределенных многофазных атак. IDA2 осуществляет выявление общего сценария вторжения и прогнозирование дальнейших действий злоумышленника по его развитию.

Возможными высокоуровневыми сценариями, обнаруживаемыми IDA2, являются: (1) разведка (reconnaissance) – разведывательные действия атакующего (действия по определению конфигурации сети, обнаружению хостов, функционирующих на хосте сервисов, определению операционной системы, приложений и т. п.), (2) внедрение в систему (host_penetration) – действия злоумышленника по взлому хоста и внедрению в систему, (3) повышение прав (escalating_privileges) – попытки атакующего, направленные на получение повышенных прав по доступу к объектам хоста, (4) распространение поражения на хосте (deepening_penetration_on_host) – нелигитимное распространение злоумышленника по объектам хоста (каталогам, файлам, программам), (5) распространение поражения по сети (deepening_penetration_through_net) – распространение атакующего по защищаемой компьютерной сети и др.

Модель функционирования и взаимодействия агентов МСОВ и ее программная реализация при обнаружении вторжений работает в соответствии со сценарием, состоящим из трех уровней обработки (рис. 5): (1) агенты-демоны AD-E выполняют первичную обработку

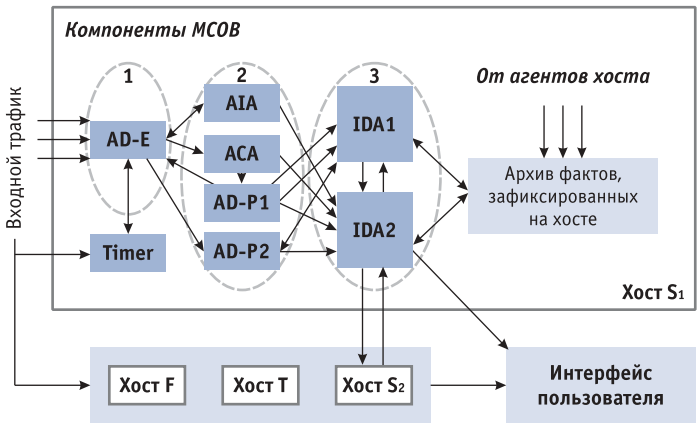

Рис. 5. ***Архитектура компонентов МСОВ на хосте*** *(1, 2, 3 – уровни обработки)*

сообщений входного трафика, результатом которой является представление трафика сообщений в виде потока значимых событий; (2) агенты-демоны AIA, ACA, AD-P1 и AD-P2 в реальном времени осуществляют предварительный анализ значимых событий, выявляя очевидные атаки; (3) агенты IDA1 и IDA2 обнаруживают многофазные атаки. Эти агенты также реализуют прогнозирование последующих действий пользователей, используя известные сценарии атак. Предполагаемые события в качестве возможных решений сообщаются остальным агентам хоста, а также агентам других хостов.

Рассмотрим пример сценария комбинированной атаки, реализованного в экспериментах с прототипом МСОВ (рис. 6). Сценарий атаки затрагивает хост злоумышленника X и хосты защищаемой многосегментной сети: хост S_1, являющийся промежуточной целью атаки, доверительный хост T, пользователи которого имеют расширенный доступ к хосту S_1, и хост S_2 – цель атаки. Цель злоумышленника – получить доступ к информации, находящейся на хосте S_2. Злоумышленник действует не напрямую, а «по цепочке»: сначала он осуществляет доступ к хосту S_1, затрагивая хост T, а затем к хосту S_2.

Можно выделить семь фаз сценария атаки: (1) сканирование портов хоста S_1 с целью определения открытых портов и функционирующих служб; (2) попытки подключения к хосту S_1 по telnet и ftp с разных адресов и подбора пароля; (3) реализация комбинированной spoofing-атаки; (4) попытки несанкционированного доступа к файлам хоста S_1; (5) реализация атаки на переполнение буфера для повышения прав на хосте S_1; (6) повторные попытки несанкционированного доступа к файлам хоста S_1; (7) попытки подключения к хосту S_2 по telnet или ftp.

Сценарий функционирования программного прототипа МСОВ по обнаружению описанной комбинированной атаки состоит в следующем. Первичную обработку получаемых на хостах сообщений осуществляют агенты-демоны AD-E, которые переадресуют соответствующие сообщения специализированным агентам. На первой фазе атаки основную роль выполняет

агент AD-P2 хоста S_1, на второй – агент AIA того же хоста, на третьей – агенты AD-P2 и IDA1 хоста S_1 и AD-P2 хоста T, на четвертой – агенты AIA и ACA хоста S_1, на пятой – агент AD-P1 хоста S_1, на шестой – агент ACA хоста S_1, на седьмой – агенты AIA и ACA. На всех фазах задействуется агент IDA2 хоста S_2. Он распознает высокоуровневые фазы комбинированной атаки и прогнозирует последующие действия атакующего, принимая решения о соответствующей реакции на действия злоумышленника.

Для обеспечения контроля работы МСОВ в рамках экспериментов по обнаружению атак используется управляемая модель реального времени Time Model и средства визуализации работы МСОВ.

Оценка возможностей многоагентной технологии защиты информации

Исследование возможностей агентских технологий и проведенные эксперименты с разработанными программными прототипами показали несомненные преимущества многоагентного подхода к построению систем обнаружения вторжений, в частности и систем защиты информации (СЗИ), в целом, по сравнению с традиционным подходом. В пользу этого тезиса можно выдвинуть следующие доводы.

1. Распределение объектов и средств защиты как в границах хоста, так и в рамках компьютерной сети диктует необходимость использовать распределенные интегрированные системы защиты, к классу которых относятся многоагентные СЗИ.
2. Большинство атак реализуется по предварительно заданным сценариям. Каждый сценарий состоит из последовательных стадий, предназначенных для преодоления различных уровней защиты. Сложные атаки на компьютерные сети могут затрагивать сразу несколько хостов сети и иметь целью поражение множества хостов. Они могут реализовываться посредством кооперации большой группы злоумышленников и использования множества хостов для инициирования отдельных фаз атаки из нескольких источников в сети. Реализованная в АСМА агентно-ориентированная технология позволяет адекватно моделировать распределенные скоординированные атаки. Кооперация распределенных агентов обнаружения вторжений может обеспечивать обнаружение атак, реализующих такие сложные сценарии.
3. Многоагентный подход обеспечивает повышение оперативности выполнения задач защиты в силу распараллеливания и автоматического выполнения решаемых задач. В разработанном прототипе МСОВ агенты IDA1 и IDA2 осуществляют обобщенный анализ обнаруженных фактов вторжения в рамках всей защищаемой сети. Это позволяет использовать режим автоматического обнаружения сложных координированных атак и минимизировать количество ложных срабатываний и пропусков атак.
4. Для больших распределенных систем крайне важна способность продолжать функционирование, когда ее компоненты разрушены или изолированы. СЗИ, имеющие централизованную архитектуру, могут легко поражаться злоумышленником, например, путем атаки «отказ в обслуживании» на хосты управления СЗИ. Как в АСМА, так и в МСОВ совокупность агентов, соответственно выполняющих атаку или реализующих задачу обнаружения, на каждом из хостов может взять на себя необходимые функции генерации или обнаружения распределенной атаки. Таким образом, агенты защиты хостов могут скоординированно выполнять операции сбора, агрегирования и управления. Кроме того, координация поведения агентов и взаимный обмен сообщениями позволяют вести единую виртуальную базу данных о вторжениях, что также существенно повышает надежность и безопасность функционирования СЗИ.
5. Исключительно важной является способность компонентов СЗИ отслеживать состояние среды функционирования и приспосабливаться к ее изменениям. В разрабо-

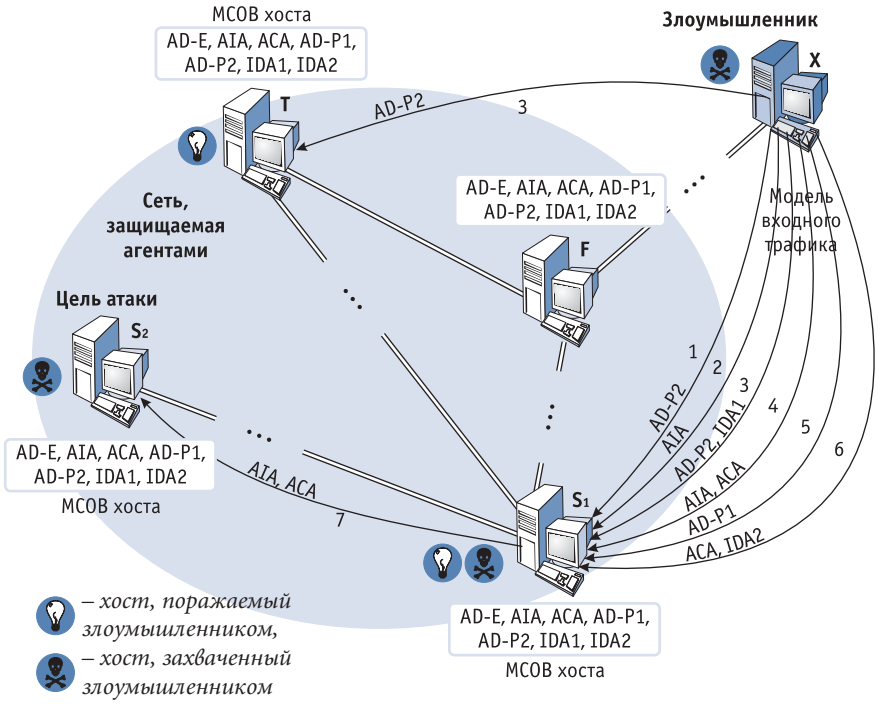

Рис. 6. ***Пример схемы функционирования агентов при обнаружении атаки***

танных прототипах агенты могут клонироваться для охвата всех необходимых в текущей ситуации задач защиты, обеспечения требуемой избыточности и параллелизма, а также обращаться к агентам других хостов для оказания помощи. Агенты, обладающие указанными характеристиками, автономно и асинхронно выполняющие свои функции, позволяют сформировать робастную и отказоустойчивую систему защиты.

6. Для повышения эффективности защиты различные подсистемы СЗИ должны взаимодействовать друг с другом на разных уровнях абстракции решений, сформированных каждой из них. Такой стиль функционирования и взаимодействия подсистем СЗИ, как показало исследование реализованных прототипов, определяет требуемый способ декомпозиции функций защиты и необходимые средства взаимодействия между подсистемами СЗИ. Данный подход естественным образом реализуется с использованием парадигмы многоагентной системы и позволяет препятствовать, обнаруживать и подавлять атаки на более ранних стадиях их развития.
7. Многоагентная система может составлять многокомпонентную вычислительную среду, независимую от аппаратных и программных средств, на которых она базируется. Это позволяет реализовать среду для задач обнаружения вторжений и защиты информации.
8. Разработка программных прототипов подсистем СЗИ была выполнена с помощью специально разработанной инструментальной системы создания многоагентных приложений MASDK. Эта система обеспечивает итеративный процесс наращивания и тестирования функциональных возможностей разрабатываемых агентов. С учетом этого, эксперименты в данной работе следует рассматривать не только как оценку функционирования программных прототипов, но и в более широком смысле – как проверку предлагаемой технологии создания многоагентных приложений. Кроме того, так как для построения СЗИ требуется формирование большого числа правил, необходима специальная технология поддержания и развития баз знаний о вторжениях, особенно с учетом того, что появление новых сетевых атак требует постоянного добавления новых и модификации старых правил базы знаний. Предлагаемый подход к формированию многоагентных СЗИ обеспечивает технологию модификации и наращивания знаний, адекватную потребностям защиты информации в компьютерных сетях.

Заключение

В статье представлены созданные в Лаборатории интеллектуальных систем СПИИРАН многоагентные системы, служащие для анализа уязвимостей и обнаружения вторжений в компьютерных сетях – агентно-ориентированная система моделирования атак (АСМА) и многоагентная система обнаружения вторжений (МСОВ). Эти системы являются исследовательскими прототипами и разработаны с использованием программного инструментария создания многоагентных систем MASDK. Проведенные с данными системами эксперименты позволили исследовать преимущества применения многоагентной технологии в области защиты информации в компьютерных сетях.

АСМА построена на основе предложенной формальной модели реализации атак. Отличительные черты реализованного в АСМА подхода к моделированию атак:

- моделирование атак базируется на спецификации задач хакеров и иерархии их намерений;
- многоуровневое описание атаки представляется в последовательности «общий сценарий распределенной атаки → намерения хакеров → простые атаки → входной трафик или данные аудита»;
- разработка планов действий хакеров и моделей отдельных атак основывается на задании онтологии предметной области «Атаки на компьютерные сети»;
- формальное описание сценариев взаимодействия агентов и реализации распределенных атак выполнено на базе семейства контекстно-свободных стохастических атрибутных грамматик, связанных операциями подстановки;
- в алгоритмической интерпретации процедур генерации атак каждой из грамматик ставится в соответствие автомат;
- генерация действий (атак) хакеров происходит в зависимости от реакции атакуемой сети в реальном масштабе времени.

Представляется, что наиболее действенный путь обнаружения распределенных многофазных атак, направленных на компьютерные сети, состоит в кооперации множества агентов защиты, распределенных по хостам сети. Поэтому основное достоинство МСОВ заключается в возможности относительно «легких» компонентов системы сотрудничать и совместно решать сложную задачу обнаружения таких атак. Базовые черты подхода, реализованного в МСОВ, таковы:

- расширяемая и адаптивная многоагентная архитектура;
- централизация внимания на обнаружении многофазных распределенных атак;
- обеспечение безопасности и робастности (обработка сетевых событий, важных с точки зрения защиты информации, и функции управления распределены среди множества агентов различных хостов).

Основные направления будущих исследований связаны с рас-

ширением функциональных возможностей рассмотренных систем, полной реализацией в них концепции командной работы, моделированием более широкого диапазона атак, проведением экспериментальной оценки свойств систем. ■

ЛИТЕРАТУРА

1. *Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей. Учебное пособие / Под редакцией И. В. Котенко. СПб.: ВУС, 2000, 190 с.*
2. *Gorodetski V., Kotenko I. The Multi-agent Systems for Computer Network Security Assurance: frameworks and case studies // IEEE ICAIS-02. IEEE International Conference «Artificial Intelligence Systems». Proceedings. IEEE Computer Society. 2002. P. 297–302.*
3. *Городецкий В. И., Грушинский М. С., Хабалов А. В. Многоагентные системы (обзор) // Новости искусственного интеллекта, № 2, 1998. С. 64–116.*
4. *Городецкий В. И., Карсаев О. В., Котенко И. В., Хабалов А. В. MAS DK: инструментарий для разработки многоагентных систем и примеры приложений // ICAI'2001. Международный конгресс «Искусственный интеллект в XXI веке». Труды конгресса. Том 1. М.: Физматлит, 2001. С. 249–262.*
5. *Gorodetski V., Karsaev O., Kotenko I., Khabalov A. Software Development Kit for Multi-agent Systems Design and Implementation // B. Dunin-Keplicz, E. Navareski (Eds.), From Theory to Practice in Multi-agent Systems. Lecture Notes in Artificial Intelligence, Vol. № 2296, 2002. P. 121–130.*
6. *Котенко И.В., Маньков Е. В. Моделирование атак на информационно-телекоммуникационные системы // Восьмая Международная конференция по информационным сетям, системам и технологиям. ICIN-SAT-2002. Труды. СПб.: СПбГУТ им. Бонч-Бруевича, 2002. С. 190–198.*
7. *Городецкий В. И., Котенко И. В. Командная работа агентов в антагонистической среде // Международная конференция по мягким вычислениям и измерениям. SMC'2002. Сборник докладов. Том 1. СПб: СПбГЭТУ, 2002. С. 259–262.*
8. *Городецкий В. И., Котенко И. В. Командная работа агентов-хакеров: применение многоагентной технологии для моделирования распределенных атак на компьютерные сети // КИИ-2002. VIII Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. М.: Физматлит, 2002. С. 711–720.*
9. *Gorodetski V., Kotenko I. Attacks against Computer Network: Formal Grammar-based Framework and Simulation Tool // Proceedings of the 5 International Conference «Recent Advances in Intrusion Detection», Lecture Notes in Computer Science, vol. 2516, Springer Verlag, 2002. P. 219–238.*
10. *Gorodetski V., Kotenko I., Karsaev O. Framework for Ontology-based Representation of Distributed Knowledge in Multiagent Network Security System // Proceedings of the 4th World Multiconference on Systems, Cybernetics and Informatics (SCI-2000), Vol. III: «Virtual Engineering and Emergent Computing». Orlando, USA, July 2000. P. 52–58.*
11. *Котенко И. В., Карсаев О. И. Использование многоагентных технологий для комплексной защиты информации в компьютерных сетях // Известия ТРТУ, № 4, 2001. С. 38–50.*
12. *Городецкий В. И., Котенко И. В., Карсаев О. В. Интеллектуальные агенты для обнаружения атак в компьютерных сетях // КИИ-2000. VII Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. М.: Изд-во физико-математической литературы, 2000. С. 771–779.*