окремо, а для цілої групи. Це, в свою чергу, зменшує як часові, так і матеріальні витрати на адміністрування КС. Слабким місцем рольової ПБ є наявність надзвичайних повноважень адміністратора безпеки, що, відповідно, збільшує ймовірність реалізації загроз, спричинених людським фактором. Запобіжними заходами можуть слугувати запровадження протоколювання та аудиту, надання контролюючих функцій іншим користувачам, захист файлів протоколу тощо.

Література: ***1.*** *Бондаренко М, Потій О., Лавріненко В., Горбенко. Ю. Визначення політики безпеки інформаційно-телекомунікаційних систем. – Тези доповідей VI Міжнародної науково-практичної конференції "Безпека інформації в інформаційно-телекомунікаційних системах", 13-16 травня 2003.* ***2.*** *Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-002-98, ДСТСЗІ СБ України, Київ, 1998.* ***3.*** *Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. М.: "Яхтсмен", 1996.* ***4.*** *Bell D. E., La Padula L. J. Secure Computer Systems: Mathematical foundations and model // Report ESD-TR-73-278, Mitre Corp., Bedford, MA, March 1976.* ***5.****Ferraiolo, D. and Kuhn, R. 1992. Role-based access control. In Proceedings of the NIST–NSA National (USA) Computer Security Conference, 554–563.* ***6.*** *David F. Ferraiolo, Ravi Sandhu, Serban Gavrila and D. Richard Kuhn and Ramaswamy Chandramouli. Proposed NIST Standard for Role-Based Access Control. - ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001.* ***7.*** *Антонюк А. О., Жора В. В. Моделювання доступу та каналів витоку в інформаційних системах. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Вип. 3 – К.: 2001, с. 156-160.* ***8.*** *Антонюк А О., Жора В. В. Загрози інформації і канали витоку. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Вип. 2 – К.: 2001, с. 42-46.*

УДК 681.3.067

РЕШЕНИЕ НЕКОТОРЫХ ПРОБЛЕМ ЗАЩИТЫ МУЛЬТИАГЕНТНЫХ СИСТЕМ

Александр Хошаба, Наталья Месюра
Винницкий национальный технический университет

Аннотация: **Проводится анализ категорий распределенных систем и характерных для них угроз. Основное внимание уделяется разработке методов защиты мультиагентных систем. Рассмотрена реализация платформенных методов защиты мультиагентных систем.**
Summary: **In article the analysis of categories of the distributed systems and characteristic threats for them is carried out. The basic attention is given development of methods of protection in multiagent systems. Realization of platform methods of protection in multiagent systems is considered.**
Ключевые слова: **Защита информационных ресурсов компьютерных сетей, интеллектуальные технологии, мультиагентные системы, распределенные системы.**

I Введение

Работа распределенных систем базируется на функционировании корпоративных и глобальных компьютерных сетей, которые, в свою очередь, требуют использования современных средств защиты информации. В период создания распределенных систем для решения этой задачи главным образом использовались методы, направленные на защиту информационных ресурсов и средств передачи данных. Однако в настоящее время все большую актуальность приобретает решение вопросов политики безопасности распределенных систем, которая должна быть гибкой и прогрессивной.

К одному из важных способов решения задач политики безопасности специалисты относят создание концепции агента для описания современных программных компонент [1 – 5]. Решение задач гибкости и универсальности функционирования программных компонент приводит к созданию мультиагентных систем (МАС).

Для изучения проблем защиты МАС необходимо провести анализ категорий распределенных систем, определить их отличительные характеристики функционирования в смысле использования системных компонент, рассмотреть реализацию платформенных методов защиты МАС.

II Классификация архитектурных стилей распределенных систем

Классификация архитектурных стилей распределенных систем позволяет определить взаимосвязь между

структурой системы и конкретными средствами защиты. В общем случае специалистами [2] предлагается выполнять деление на три категории, которые в свою очередь могут иметь свои шаблоны или архитектурные стили [1].

Рассмотрим три архитектурных стиля, внося в список компоненты, которые характеризуют каждый стиль. Первый называется "распределенные объекты". Такие объекты связаны через отдаленный вызов процедуры. Этот стиль характеризуется тем, что данные скрыты в пределах объектов, и ими можно управлять только через отдаленные интерфейсы. Подключенные через отдаленные обращения методы должны выполнять ограничения на действия пользователя или системы. Объекты используются как компоненты, отдаленные обращения метода – как соединители, – чтобы координировать данные и управление [5]. К важным представителям данного стиля относят технологии CORBA [6] и DCOM [7].

Второй стиль называется "мобильные агенты". Мобильные агенты имеют два вида компонентов: первый состоит из активных объектов с кодом и состоянием, которое может быть передано по сети. Ко второму виду принадлежат компоненты мобильных агентов со средой их выполнения. Соединитель перемещения, доступный в этом стиле, позволяет компоненту агента динамически изменять свое место, передавая его код и данные. Этот соединитель – один из возможных интерфейсов системы, основанных на подвижном коде, который может быть получен из описания [8]. По описанию эти данные взаимодействуют в распределенном регистре объектов, где имеется дополнительный соединитель перемещения, который позволяет изменить местоположение агента при сохранении состояния вычисления. К представителям этого стиля относят Mole [9] и Aglets [10].

Третий архитектурный стиль называется "мультиагентными системами". Единственный соединитель этого стиля представлен интерфейсом связи. К главной особенности компонента агента относится его автономия – агент может инициализировать взаимодействия без внешнего стимула. Эта основная особенность автономии может также поддерживаться компонентами стиля мобильных агентов. К главной особенности стиля мультиагентных систем относят также специфическое взаимодействие данных управления. Соединитель связи позволяет агентам обмениваться сообщениями, принадлежащими к языку связей агентов (ACL). Такие языки основаны на речевой теории [11, 12] и обладают логической структурой, которая выражает их семантику. В этом случае для связи между компонентами может быть использован один из ACL. К представителям этого стиля относят FIPA стандарт [13] и dMARS систему [14].

Разработка данной классификации, основанной на архитектурных стилях распределенных систем [1], позволяет моделировать угрозы. Это дает возможность определить вид угрозы, который является наиболее нежелательным при использовании разных информационных технологий. Существует и другой подход, позволяющий выполнить моделирование состояний угроз, исходя из неблагоприятных факторов. К примеру, несанкционированному доступу наиболее подвержены стили мобильных агентов, которые связаны с их спецификой взаимодействия со средой окружения [15, 16].

Такой прогрессивный класс распределенных структур, как МАС, наиболее подвержен неавторизованному доступу к информации и получению данных из каналов связи. Поэтому, к основным методам решения проблемы защиты информационных ресурсов МАС следует отнести анализ таких важных вопросов, как агентная платформа, обобщенная модель защиты, полномочие свидетельства, идентификация пользователей и объектов, разрешение выполнения операций, делегация полномочий, политика защиты и безопасная связь.

III Реализация платформенных методов защиты мультиагентных систем

При реализации платформенных методов защиты МАС необходимо иметь ввиду следующие требования:

- модель защиты должна быть адаптирована к архитектурному стилю МАС;
- модель защиты должна быть главным образом направлена на механизмы безопасной работы при делегировании полномочий между агентами.

На наш взгляд [3, 4, 17] наиболее полно вышеперечисленным критериям отвечает программная платформа JADE [18].

Агентная платформа. JADE является программной структурой для разработки МАС в соответствии со спецификациями FIPA [19]. Она поддерживает большинство структур, связанных со спецификациями FIPA, таких как транспортные протоколы, кодирование сообщений, механизм белых и желтых страниц. Кроме того, она имеет различные инструментальные средства, которые облегчают отладку и управление агентами. В разработанной стандартной реализации JADE имеются недостатки, которые связаны с отсутствием развитой системы прав и разрешений на выполнение отдельных операций, со слабой защитой при передаче трафика агентам. Однако, данные недостатки устранены в экспериментальной версии JADE.

Обобщенная модель защиты. Агентная система JADE использует язык Java. Модель защиты JADE обеспечивает концепции, представляющие взаимодействия администраторов, ресурсов и разрешения доступа для идентификации пользователей и агентов, для предоставления необходимых разрешений на

выполнение операций. Кроме того, она должна обеспечить конструкции, облегчающие системную администрацию и иерархию функций. Платформа JADE способна принимать от администратора политику защиты с перестройкой конфигурации для разрешения или запрета доступа к выполняющемуся коду. MAC, как и любая другая многопользовательская среда, требует инфраструктуры и программных интерфейсов для подтверждения пользователей и назначения им привилегий. В модели защиты JADE администратор системы представляет любой объект, тождество которого может быть заверено. Кроме того, в JADE пользователь составляет группу членств, что делает возможным предоставить всем агентам специфические разрешения, которые выполняются объектами. Ресурсы для модели защиты JADE включают уже обеспеченные моделью Java локальные элементы файловой системы, сетевые интерфейсы, системные переменные, подключения базы данных. Однако существуют ресурсы, типичные для MAC, которые должны быть защищены от неправомерного доступа. В данном случае разрешение представляет собой объект, предоставляющий возможность выполнять действия. Разрешения JADE, унаследованные от модели защиты Java, представляют системные ресурсы. У каждого разрешения есть имя и список разрешенных действий. При попытке обратиться к ресурсу, функции управления доступа сравнивают разрешение, предоставленное администратором, с разрешением, необходимым для выполнения операций. Доступ разрешается, если все требуемые параметры находятся в соответствии с правилами.

Полномочие свидетельства. Защита JADE в большой части основана на доступности некоторых удостоверений (специальных программ или прав пользователей), которые могут засвидетельствовать объект. Для подтверждения подлинности удостоверений необходимо, чтобы они были подписаны публично признанным владельцем. Владелец процесса JADE имеет пару ключей, один из которых частный, а другой известный всем (публичный). Этот простой подход позволяет использовать агентную платформу JADE в существующей ключевой инфраструктуре, использованной для идентификации пользователей или процессов.

Идентификация пользователей и объектов. В агентной системе JADE пользователь подтверждает себя именем и паролем, и получает разрешение на выполнение операций и доступ к информационным ресурсам. Такие разрешения также могут быть делегированы агентам, поддерживая таким образом контроль над действиями, которые можно исполнять. Агенты должны быть заверены системой, когда они требуют доступа к защищенным ресурсам. Идентификация включает в себя представление свидетельства тождества. Элементы свидетельства тождества включают тождество темы, тождество объекта. Эти элементы могут использоваться, чтобы установить законность свидетельства и связь между свидетельством и агентом.

Разрешение на выполнение операций. Модель защиты Java – это набор классов, которым предоставляют привилегии. Однако эта форма разрешения недостаточна в среде JADE, где агенты могут принадлежать различным пользователям. Имея свидетельства тождества, каждый агент может распорядиться различными удостоверениями разрешения и специальными разрешениями. Агент может получить эти удостоверения при его создании непосредственно от его владельца или при делегации от других агентов системы. В каждом случае система проверяет, действительно ли объект делегирования имеет эти разрешения и право далее делегировать их другим информационным структурам.

Делегация полномочий. Для реализации безопасной делегации необходимо иметь возможность проверить, что объект, объявляя действия от имени других, имеет действительно необходимые разрешения. Кроме того, в случае MAC механизм делегации должен быть достаточно гибок, чтобы использоваться как основание для безопасной обработки данных и протоколов взаимодействия, позволяя, например, отменить делегацию или запретить дальнейшую делегацию данной задачи. Для предоставления этих характеристик модель защиты JADE использует подход, который поддерживает различные стили и протоколы. Модель, принятая для безопасной делегации в JADE, основана на наработках авторов [20], адаптированных ко многим системам агента с различным выполнением и различной структурой разрешений. Ряд агентов может быть включен в механизм взаимодействия. По результатам исследования некоторых авторов [21], механизм делегации также может быть возможной альтернативой наследования. Примером этого является язык Self [22]. В [23] авторы анализируют делегацию в MAC, использующих структуру, основанную на действиях и состояниях. В этой работе также предлагается семантика для передачи данных. Например, агент А выполняет передачу сообщения на выполнение задачи другому агенту Б, который соглашается принять эти данные. Агент Б может выполнить задачу самостоятельно или сформировать и направить подзадачу другому агенту С. Это формирует цепочку делегаций, где инициатор – агент А, С является заключительным адресатом и агент В – промежуточным звеном. Поэтому существуют три подхода, которые могут применяться к таким цепочкам:

1) без делегации; промежуточное звено только осуществляет собственные права для дальнейших запросов;

2) простая делегация, которая может быть ограничена или не ограничена;

3) каскадная делегация, при которой права, исходящие от процесса-инициатора, объединены с правами делегированного объекта.

Современные версии агентной платформы JADE также используют удостоверения для осуществления безопасной делегации. Агент, который начинает процесс делегации, устанавливает содержание свидетельства для того, чтобы управлять использованием ресурсов вычисления и механизмами защиты агентов. Можно даже идентифицировать группу пользователей или агентов, которым предоставлена делегация.

Политика защиты и безопасная связь. Модель политики защиты агентной платформы JADE определяет ресурсы, которые доступны для администратора. Это расширенная политика, принятая в Java. В результате формируется политика доступа для мультиагентной среды, основанной на Java.

Контейнеры JADE могут быть связаны с главной платформой через отдаленные ссылки, которыми могут быть корпоративные компьютерные сети. Для защищенной передачи в JADE имеется возможность использовать протокол SSL, который появился как стандарт безопасной связи компьютерной сети Internet. Протокол SSL также позволяет взаимную идентификацию обеих сторон сетевого подключения. Данная особенность позволяет платформе JADE защищать информационные ресурсы от несанкционированного доступа.

IV Выводы

1. Выполнен анализ классификации распределенных систем; определены наиболее характерные виды угроз.
2. Определены требования платформенных методов защиты мультиагентных систем.
3. Показано, что наиболее полно критериям реализации платформенных методов защиты отвечает программное средство JADE.
4. К основным методам решения проблемы защиты информационных ресурсов МАС следует отнести такие, как агентная платформа, обобщенная модель защиты, полномочие свидетельства, идентификация пользователей и объектов, разрешение на выполнение операций, делегация полномочий, политика защиты и безопасная связь.

*Литература: **1.** D. Garlan, M. Shaw. “An Introduction to Software Architecture”. In Advances in Software Engineering & Knowledge Engineering, Vol. II, World Scientific Pub Co., 1993, pp. 1-39. **2**. F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad, S. Stal. “Pattern Oriented Software Architecture: A System of Patterns”. John Wiley & Sons, 1998. **3**. Хошаба О. М., Месюра Н. В., Войцех О. А. Використання інтелектуальних технологій при побудові засобів захисту інформації в комп'ютерних м9ережах //Вісник Технологічного університету Поділля №3, 2003.-Хмельницький.-С.138-142. **4**. Хошаба А. М., Месюра Н. В. Использование мультиагентных систем в области защиты информационных ресурсов компьютерных сетей //Труды 4 международной научно-практической конференции "Современные информационные и электронные технологии", 2003.-Одесса.-С.134. **5**. B. Meyer. “Object-Oriented Software Construction, 2nd Ed.”. Prentice Hall, 1997. **6**. Object Management Group. “CORBA 2.4 specification”. http://www.omg.org. **7**. D. Box. “Essential COM”. Addison-Wesley, 1998. **8**. A. Fuggetta, G. P. Picco, G. Vigna. “Understanding Code Mobility”. IEEE Transactions on Software Engineering, 24(5): 342-360, 1998. **9**. J. Baumann, F. Hohl, K. Rothermel and M. Strasser. “Mole – Concepts of a Mobile Agent System”. World Wide Web, 1(3):123-137, 1998. **10**. D. B. Lange, M. Oshima. “Programming and Deploying Java Mobile Agents with Aglets”. Addison Wesley, 1998. **11**. J. L. Austin. “How to do things with words”. Oxford University Press, 1962. **12**. B. Schneier. “Secrets and Lies”. J. Wiley and Sons, 2000. **13**. FIPA 2000 Specifications. Available at http://www.fipa.org. **14**. A. S. Rao, M. P. Georgeff. “BDI Agents: From Theory to Practice”. Proc. of ICMAS ’95, 1st International Conference on Multi-Agent Systems, San Francisco, CA, 1995; 312-319. **15.** H. Peine. “Security Concepts and Implementation in the Ara Mobile Agent System”. In Proc. of 7th IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, Stanford University, USA, 1998. **16.** V. Roth, M. Jalali. “Concepts and Architecture of a Security-centric Mobile Agent Server”. Proc. of ISADS’01, 5th International Symposium on Autonomous and Decentralized Systems, Dallas, TX, 2001. **17.** Хошаба А. М., Месюра Н. В. Использование интеллектуальных систем для создания средств защиты информационных ресурсов компьютерных сетей //Міжнародна науково-практична конференція студентів, аспірантів та молодих вчених: Мат. допов.-Київ, 2003.-С. 129. **18**. F. Bellifemine, A. Poggi, G. Rimassa. “Developing Multi-Agent Systems with a FIPA-compliant Agent Framework”. Software: Practice & Experience, 31:103- 128, 2001. **19.** The JADE Project Home Page. http://jade.cselt.it. **20**. N. Nagaratnam, D. Lea. “Role-based Protection and Delegation for Mobile Object Environments”. Proc. of COOTS ’98, 1998 USENIX Conference on Object- Oriented Technology and Systems, Santa Fe, NM, 1998. **21**. G. Agha. “Actors, A Model of Concurrent Computation in Distributed Systems”. MIT Press, 1986. **22**. R. B. Smith, D. Ungar. “Programming as an*

Experience: The Inspiration for Self". Proc. ECOOP '95, Aarhus, Denmark, 1995. ***23****. T. J. Norman, C. Reed. "Delegation and Responsibility". In Proc. of ATAL '00, 7th International Workshop on Agent Theories, Architectures and Languages, Boston, MA, 2000.*

УДК 681.511.3

ТЕХНОЛОГИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ ПРИ ОСНОВНЫХ ПОКРЫВАЮЩИХ СООБЩЕНИЯХ В ВИДЕ БИНАРНЫХ ИЗОБРАЖЕНИЙ

Ирина Маракова
Одесский национальный политехнический университет

Анотація: **Виконано оцінку ефективності систем з прихованими цифровими мітками. Розглянуто систему з прихованими цифровими мітками з використанням бінарних зображень у вигляді головного повідомлення та в умовах адитивної атаки шумом. Одержані формули для P_m та P_{fa} як функцій від числа елементів водяних знаків (ВЗ), постійної перекручень, порогу. Це дозволяє оцінити кількість потрібних біт ВЗ для забезпечення надійності системи в певних умовах.**
Summary: **Watermarking (WM) technology at use as the cover massage of binary images. We consider private (WM) system at use as the cover message of binary images with additive noise attack. The formulas for P_m and P_{fa} are derived as a dependence on the number of WM elements, distortion constraints, chosen threshold. It allows to find out how many bits of WM is necessary to use in order to embed reliable WM for different conditions.**
Ключевые слова: **Водяные знаки, основное покрывающее сообщение, идентификатор.**

I Введение

Цифровые системы с водяными знаками (ВЗ) являются одним из основных приложений сокрытия информации и отличаются от классических стеганографических систем тем, что скрывают не секретное сообщение, а некоторый идентификатор. Параметры систем с ВЗ и требования к ним существенно зависят от их практического применения (защита авторских прав, мониторинг вещания, контроль копирования, сохранение целостности и т. д.). С другой стороны, для идентификации цифровых сообщений используется цифровая подпись (ЦП), которая в итоге является последовательностью цифр, сформированных в зависимости от сообщения в соответствии со специальными стандартными преобразованиями и добавляемых к сообщению. ЦП без труда может быть отделена от сообщения. Погружение же ВЗ в основное покрывающее сообщение (ОПС), которое может быть изображением, аудио, видео подразумевает не только сокрытие ВЗ, но и неотделимость от ОПС, а также одинаковое восприятие ОПС и стегасообщения (ОПС и ВЗ) [1].

Частный случай, когда ОПС является бинарным изображением, весьма важен на практике, например, в электронной диагностике, факсимильной связи и т. д. Кроме того, любое ОПС после квантования можно представить в бинарном виде. Погружение ВЗ при этом представляет собой сложение по модулю 2 содержимого пикселей изображения (0 или 1) и в общем случае кодированного двоичного ВЗ. В качестве критерия верности используется количество ошибочных двоичных пикселей изображения. Другими словами, метрикой верности является вес Хэмминга.

Оценка эффективности бинарных систем с ВЗ осуществляется посредством оценки вероятностей ошибок, а именно, вероятности ложного обнаружения ВЗ P_{fa} и вероятности пропуска ВЗ P_m [2]. Рассмотрены следующие структуры систем с ВЗ: информированный кодер и декодер (используется информация об ОПС как кодером, так и декодером); не информированные кодер и декодер (информация об ОПС не используется ни в декодере, ни при формировании стегасообщения в кодере); информированный кодер и не информированный декодер (информация об ОПС не используется декодером, но учитывается при погружении ВЗ в ОПС) [3]. Не умаляя общности исследований, рассматриваются системы с нулевым битом, когда декодер принимает решение о наличии или отсутствии ВЗ, т. е. по сути является детектором или обнаружителем ВЗ. На выходе такого декодера может быть только два вида сигнала, свидетельствующего либо об отсутствии ВЗ (0), либо о присутствии его в принятом сигнале (1).

В канале атакующего, целью которого является удаление или искажение ВЗ при сохранении неизменным ОПС, рассматривается только аддитивная помеха. Несомненно, современные алгоритмы канала атакующего значительно сложнее (сжатие, геометрические преобразования, фильтрация и т. д.). С другой стороны, исследование системы с ВЗ в условиях воздействия только аддитивного шума атаки позволит получить