Уязвимости и требования безопасности в MAC

Ляпустин Антон Евгеньевич
Аспирант Университета ИТМО,
Россия, г. Санкт-Петербург
E-mail: Lyapustinae@gmail.com

Хотя общепринятого определёния нет, большинство исследователей согласны с тем, что общие характеристики агента, как программного обеспечения (ПО), в отношении ситуативности, местоположения, автономии и гибкости (situatedness, autonomy, flexibility) [1, 4-6] отличают агентскую парадигму от других программных парадигм. Ситуативность означает, что агент знает о своих конкретных условиях на основе сенсорного ввода, получаемого от своей среды. Автономия означает, что агенты способны контролировать свои собственные действия и внутренние состояния без прямого вмешательства людей или других агентов. Автономия означает, что агенты могут контролировать свои собственные действия и внутренние состояния без прямого вмешательства людей или других агентов. Гибкость — способность адаптироваться к изменяющимся ситуациям и беспрепятственно выполнять действия, необходимые для достижения целей агента.

Гибкость обладает тремя свойствами (см. выше): способность реагировать, инициативность (проактивность) и социальная способность (responsiveness, proactiveness, social-ability). Способность реагировать означает, что агенты могут выполнять действия, которые изменяют среду, или давать обратную связь в качестве ответа, когда они знают об окружающей среде. Проактивность означает, что агенты не просто действуют в ответ на воздействие своей среды, скорее, они могут демонстрировать целенаправленное поведение [4]. Социальная способность означает, что агенты могут взаимодействовать с другими агентами и людьми, чтобы решать свои проблемы или помогать другим.

Кроме того, существуют дополнительные характеристики, такие как мобильность, рациональность, достоверность и доброжелательность (mobility, rationality, veracity, benevolence). Мобильный агент, как упоминалось ранее, является агентом, который также обладает характеристикой мобильности, то есть возможностью миграции по сетям и между различными узлами [2]. В то время как агентские системы могут значительно выигрывать от такой мобильности агентов, мобильность агентов также создает серьёзные проблемы с безопасностью. Несколько исследователей сосредоточились на проблемах безопасности мобильных агентов. В данной работе более подробное описание проблем и существующих решений будут приведены в следующих разделах.

Как уже отмечалось, парадигма агента является перспективным подходом к разработке интеллектуальных, гетерогенных и открытых систем, из-за особенностей агента, таких как автономность, гибкость и совместное поведение при решении проблем. Однако такие характеристики усложняют обеспечение безопасности MAC. В настоящее время многие приложения разрабатываются как MAC, в том числе в критически важных областях, таких как онлайн-бизнес, банковское дело и медицинское обслуживание. Многие исследователи обращают внимание на уязвимость безопасности MAC и выявление возможных атак.

В работах [7, 8], авторы представляют требования безопасности MAC на основе характеристик агентов. В отношении характеристики ситуативности считается, что проверка происхождения информации является критическим вопросом. Если информация об окружающей среде поступает от хостового агента, то требования безопасности могут быть минимальными.

Однако, если агенты получают информацию из Интернета, необходимо проверить, можно ли считать эту информацию достоверноой или нет. В принципе агент должен знать источник и достоверность информации, которую он использует. Эти проблемы связаны с аутентификацией и целостностью информации. Автономность агента может привести к серьёзным проблемам безопасности, поскольку вредоносные агенты могут распространяться без какого-либо запроса от других агентов или людей [8]. Следовательно, агенты должны быть в состоянии предотвратить или устранить ущерб, который может быть нанесён несанкционированным доступом, и MAC должна быть защищена от вредоносных вторжений, вызванных другими автономными агентами.

Что касается социальной способности, необходимо быть в состоянии обеспечить безопасную связь между агентами, а также между агентами и людьми. Для этого следует обеспечить гарантию нескольким целям безопасности в MAC, таким как конфиденциальность, целостность, доступность, подотчётность и отказоустойчивость. Кроме того, мобильность агента может вызвать серьёзные проблемы с безопасностью. Узел может быть повреждён злонамеренным мобильным агентом. С другой стороны, вредоносный хост может скомпрометировать безопасность мобильных агентов. Соответственно, необходимы защитные решения для защиты, как хостов, так и мобильных агентов. Чтобы обеспечить безопасность мобильного агента, следует обратить внимание на взаимодействие с другими вредоносными агентами и пользователями, а также с вредоносными хостами. Кроме того, сотрудничество между агентами может вызвать более серьёзные проблемы безопасности. Для достижения своих целей агентам иногда может потребоваться доступ к защищённым ресурсам, которые принадлежат другим владельцам или знания о внутреннем состоянии других агентов. Если межагентское сотрудничество разрешено без соответствующих механизмов аутентификации и авторизации, также могут возникнуть серьёзные проблемы безопасности.

В дополнение к выявлению конкретных уязвимостей, связанных с характеристиками агентов, различными исследователями были изучены другие возможные атаки против MAC. В статье Poslad и др. [9], обсуждались атаки на безопасность, связанные с абстрактной архитектурой MAC. Эта работа анализирует архитектуру FIPA (см. выше). Абстрактная архитектура FIPA [3] определяет, как агенты могут находить и связываться друг с другом, регистрируясь и обмениваясь сообщениями на абстрактном уровне. Для этого определён ряд архитектурных элементов и взаимосвязей между ними. Среди этих элементов, Poslad и др. фокусируют внимание на модели обнаружения сервисов, совместимости протоколов передачи данных, языка передачи сообщений между агентами (Agent Communication Language, ACL), языке контента и представлении нескольких служб каталогов. Они описывают несколько угроз, связанных с сервисом имён, службой каталогов и службой связи архитектуры FIPA MAC. Компонент службы имён может допускать ложную идентификацию агентов в обмене сообщениями или запросе обслуживания. При предоставлении службы каталогов возможны атаки типа отказа в обслуживании (DoS) или несанкционированные изменения. Во время связи между объектами в MAC ключевыми проблемами являются несанкционированное извлечение информации из канала связи или искажение передаваемых данных. Авторы анализируют возможные атаки в отношении абстрактной архитектуры FIPA, но не предоставляют решений для этих атак.

Помимо угроз безопасности, вызванных уязвимостями архитектуры, был проведен ряд исследований в отношении атак на безопасность, связанных с системами мобильных агентов. В [2] атаки на системы мобильные агентов были классифицированы по семи различным типам: искажение, DoS, нарушение конфиденциальности или кражи, преследование, психологические атаки, атаки, синхронизированные по событиям, и сложные атаки. Атака, синхронизированная по событиям, называемая логической «бомбой» (logic bomb), — это атака, инициированная внешним событием, таким как время, местоположение или приход конкретного человека. Сложная атака состоит из нескольких атак, возможно, с помощью сотрудничающих агентов или хостов. В работе

[10], описаны атаки, связанные с мобильностью агента. Авторы утверждают, что мобильный агент уязвим для таких атак, как нелегальное проникновение, DoS, несанкционированный доступ и копирования-ответ. С другой стороны, хост может быть уязвим для нелегального проникновения, DoS, несанкционированного доступа и копирования-ответа. Кроме того, авторы описывают атаки на сотрудничающих агентов, такие как нелегальное проникновение, DoS, несанкционированный доступ и отказ от прав.

Литература

1. Jung Y., et al. A Survey of Security for Multiagent Systems / Artificial Intelligence Review. — March 2012. — Vol. 37, Issue 3. — P. 239–260.
2. Greenberg M.S., et al. Mobile agents and security // IEEE Commun. Mag. — 1998. — Vol. 36(7). — P. 76–85.
3. FIPA Abstract Architecture Specification. — http://www.fipa.org.
4. Franklin S., Graesser A. Is it an agent, or just a program? A taxonomy for autonomous agents / In: Proceedings of the workshop on intelligent agents III, LNCS 1193. — Agent Theories, Architectures, and Languages. — London, 1996. — P. 21–35.
5. Jansen W.A. Countermeasure for mobile agent security // Comput. Commun. — 2000. — Vol. 23(17). — P. 1667–1676.
6. Jennings N.R., et al. A roadmap of agent research and development // Auton. Agents Multi Agent Syst. — 1998. — Vol. 1(1). — P. 7–38.
7. Borselius N. Mobile agent security // Electron Commun. Eng. J. — 2002. — Vol. 14(5). — P. 211–218.
8. Mouratidis H. Secure tropos: a security-oriented extension of the tropos methodology // Int. J. Softw. Eng. Knowl. Eng. (IJSEKE). — 2007. — Vol. 17(2). — P. 285–309.
9. Poslad S., et al. Specifying standard security mechanisms in multi-agent systems / In: Proceedings of autonomous agents and multi-agent systems (AAMAS 2002).
10. Wang Y, Singh M.P. Trust representation and aggregation in a distributed agent system / In: Proceedings of 21-st AAAI — 2006. — P. 1425–1430.