ضمان حماية الأنظمة المعتمدة على الوكيل البرمجي

بندر راضي اللهيبي

الملخص

في الآونة الأخيرة، تلقت تقنية البرمجيات المعتمدة على الوكيل البرمجي قدرًا كبيرًا من الاهتمام من مجتمع البحث نظرًا لفوائدها القيمة التي يمكن توفيرها لبناء أنظمة موزعة. ومع ذلك، يمثل الأمان تحديًا بارزًا في هذه التقنية، خاصةً عندما ينتقل الوكيل المتحرك من الجهاز المصدر إلى الجهاز الوجهة لأداء مهام حساسة. في هذا السياق، تم طرح ستة أسئلة بحثية، وهي (١) كيفية حماية الوكيل المتحرك الزائر من الجهاز الوجهة الخبيث وحماية الجهاز الوجهة من الوكيل المتحرك الخبيث ؟؛ (٢) كيف يمكن ضمان سلامة كل من كود الوكيل ونتائج المهمة التي ينفذها الوكيل ؟؛ (٣) كيف يمكن ضمان المقاومة العالية ضد الهجمات المتقدمة مثل (انكار الخدمة، والتعديل، والهجمات المتواطئة)؟ (٤) كيف يمكن ضمان متطلبات الأمان الشاملة في الأنظمة القائمة على الوكيل (السرية، النزاهة، المصادقة، التفويض، المحاسبة، التوفر، عدم التنصل، التحقق، إخفاء الهوية، المساءلة) ؟؛ (٥) كيفية تمكين ميزات الحماية الذاتية والاتصال الذاتي للوكيل المتنقل الزائر داخل فضاء الجهاز الوجهة؛ و (٦) كيف يمكن تكميم مستوى الأمان الذي تم تحقيقه؟. للرد على أسئلة البحث، تم اقتراح نظام أمان مرفق بمدير الوكيل. يحتوي نظام الأمان

على سبع موديلات، حيث يتعاونون لتنفيذ ثلاث نُهُج مقترحة، وهي نهج اختيار المهام الوهمية ونهج اختيار المهام الوهمية المحسّن، ونهج الاتصال الذاتي للحماية الذاتي .يختار نهج اختيار المهام الوهمية المهام الوهمية بشكل عشوائي من قاعدة البيانات التاريخية لإرباك المهاجم (آلة الوجهة). يستخدم اختيار المهام الوهمية المحسّن كلاً من الانتروبيا ونوع المهمة (المُراد تنفيذها في الجهاز الوجهة) كعوامل في عملية اختيار المهام الوهمية. يعتمد نهج الاتصال الذاتي للحماية الذاتي على مفتاح وسيط لعزل الوكيل البرمجي المتحرك الزائر عن فضاء الجهاز الوجهة، مُقدماً حماية للوكيل من الجهاز الوجهة وللجهاز الوجهة من الوكيل البرمجي الزائر. اعتمادًا على مقاييس أمان مقترحة، وهي مستوى الانتهاك ونقاط الأمان، تتفوق المنهجيات المقترحة على المنهجيات المماثلة من حيث المقاومة ضد الهجمات ودرجة الأمان ووقت الاستجابة.

ضمان حماية الأنظمة المعتمدة على الوكيل البرمجي

بندر راضي اللهيبي

المستخلص

إن الهدف الرئيسي لهذا البحث هو ضمان حماية الوكيل البرمجي المتحرك من الآلة الوجهة الخبيثة وحماية الآلة الوجهة من الوكيل البرمجي المتحرك الخبيث عندما يتم تنفيذ مهمة ما ضمن فضائها.
للإجابة على الأسئلة البحثية الثلاثة الأولى، تم اقتراح نهج اختيار المهام الوهمية ونهج اختيار المهام الوهمية المحسّن في هذه الأطروحة. يتم تنفيذها بواسطة موديل توليد المهام الوهمية المرتبطة بمدير الوكيل. تتعلق المشكلة بميزة التحرك، حيث يمكن للوكيل البرمجي الانتقال من الجهاز المصدر إلى الجهاز الوجهة لأداء المهام، حيث تعتبر مشكلات الأمان بالغة الأهمية في هذه التقنية. تصبح مشكلة الأمان في التقنية المعتمدة على الوكيل البرمجي المتحرك حرجة عندما تكون الآلة الوجهة هي المهاجم، حيث يكون لها سيطرة كاملة على الوكيل البرمجي الزائر. قد تفقد نتائج المهام المنفذة سلامتها، وقد يتغير سلوك الوكيل، وقد يطبق المهاجم هجمات نشطة متقدمة، مثل هجمات التعديل والتواطؤ وهجمات انكار الخدمة.

- من قاعدة بيانات تاريخية للمهام، تقوم منهجية اختيار المهام الوهمية بشكل عشوائي بإنشاء مهام وهمية لحماية المهمة الحقيقية، بهدف إرباك المهاجم عند تحديد المهمة الحقيقية بين المهام الوهمية والحد من قدرته على أداء الأعمال الضارة.
- تهدف منهجية اختيار المهام الوهمية المحسّن إلى إنشاء مهام وهمية تستند إلى ثلاثة عوامل: (١) المهام الوهمية لها نفس احتمالية التنفيذ مثل المهمة الحقيقية، والتي بدورها تضمن أعلى إنتروبيا؛ (٢) المهام الوهمية من نفس نوع المهمة الحقيقية (مهمة عادية أو حساسة للوقت)؛ و (٣) المواعيد النهائية للمهام الوهمية هي نفس المواعيد النهائية للمهمة الحقيقية.

للإجابة على الأسئلة البحثية الرابعة والخامسة، يتم تقديم ست وحدات وربطها مع مدير الوكيل لتلبية متطلبات الأمان المختلفة .تتعاون هذه الوحدات مع بعضها البعض لتنفيذ نهج الحماية الذاتية والاتصال الذاتي، والذي يتيح ميزات الحماية الذاتية والاتصال الذاتي للوكيل البرمجي المتحرك الزائر لعزله عن فضاء الالة الوجهة. بالتالي، يمكن لـ الالة الوجهة نفسها حماية من الوكيل البرمجي الزائر الخبيث.

- الوحدات الست هي: المصادقة والترخيص والتدقيق واكتشاف السلوك والتشفير وفك التشفير.
- يتم إجراء الاتصال بين الوحدات داخل مدير الوكيل (البرامج الوسيطة المثبتة على الجهاز الوجهة)
- بالإضافة إلى ذلك، يتم تنفيذ عملية فك التشفير باستخدام مفتاح وسيط، مما يضمن عدم التحكم في عملية إنشاء مفتاح تشفير الجلسة بواسطة الجهاز الوجهة.

بالنسبة للإجابة عن سؤال البحث الأخير، تم اقتراح مقياسين أمنيين جديدين في هذا العمل .يتم استخدام مقياس الأمان الأول لتقييم كل من نهج اختيار المهام الوهمية ونهج اختيار المهام الوهمية المحسّن، بينما يتم استخدام المقياس الثاني لتقييم نهج الحماية الذاتية والاتصال الذاتي.

- يعتمد مقياس الأمان الأول بشكل أساسي على الانتروبيا لتحديد مقدار الحماية، مع مراعاة مقدار الانتهاك الناجم عن جانب المهاجم .
- يعتمد مقياس الأمان الثاني على عدد متطلبات الأمان التي يتم تحقيقها .يستخدم هذا المقياس لأغراض التقييم ويتضمن ١٣ متطلبًا أمنيًا في نطاقه.

من أجل التقييم في سياق المقارنة، تتم مقارنة كل من نهج اختيار المهام الوهمية ونهج اختيار المهام الوهمية المحسّن بآليات الحماية المشابهة، وهي رمز التشويش والتشفير القائم على التجزئة . تتم مقارنة نهج الحماية الذاتية والاتصال الذاتي بثلاث طرق، وهي التوقيع المشترك والتوقيع الرقمي وتوقيع الرمز .

- أظهر نهجا اختيار المهام الوهمية ونهج اختيار المهام الوهمية المحسّن مقاومة عالية للهجمات المتقدمة وأداء أفضل.
- فيما يتعلق بمقاومة المناوبة والتواطؤ وهجمات انكار الخدمة، أظهر نهج اختيار المهام الوهمية المحسّن أعلى مقاومة وفقًا لمقياس الأمان (مستوى الانتهاك)، حيث كانت النسبة المئوية للحدود المحددة مسبقًا للانتهاك ٠ و٠,١ في التجارب الخمس الأولى والتجربة السادسة، على التوالي.
- فيما يتعلق بالأداء، احتل نهج اختيار المهام الوهمية المرتبة الأولى لأنها أداؤها أفضل من نهج اختيار المهام الوهمية المحسّن .السبب الرئيسي هو أن نهج اختيار المهام الوهمية المحسّن يعالج المزيد من الشروط لتحسين مستوى الأمان .بالإضافة إلى ذلك، وبالنظر إلى المشكلات الأمنية في سياق الوقت، فإن مناهجنا المقترحة تقضي الحد الأدنى من الوقت في جانب المهاجم.
- استنادًا إلى ١٣ من متطلبات الأمان - السرية، والنزاهة، والتوافر، وإخفاء الهوية، والمساءلة، والتفويض، والمحاسبة، وعدم التنصل، والضمان، والتحقق، وفك التشفير الذاتي، والتواصل الذاتي - يتفوق نهج المركز السعودي لسلامة المرضى على المنهجيات المماثلة، حيث حقق درجة ١٣.
- من حيث وقت الأداء، فإن نهج الحماية الذاتية والتواصل الذاتي يعطي نتائجاً أفضل من الأنظمة المماثلة عندما يزداد حجم الوكيل البرمجي.

بحث مقدم لنيل درجة دكتوراه الفلسفة
في علوم الحاسب

إشراف
أ.د فيجي ثايانانثان , أ.د احمد الزهراني

كلية الحاسبات وتقنية المعلومات
جامعة الملك عبد العزيز
جدة – المملكة العربية السعودية
ربيع الثاني ١٤٤٢هـ – ديسمبر ٢٠٢٠ م

Conclusion and Future Work

In this chapter, we conclude our work, highlighting the features of the proposed approaches. In addition, the limitation of the work is listed to be considered in future work.

Conclusion

In this technological age, agent based systems have received a wide attention from research community. This is due to the valuable features provided by the agent based software technology used for building agent based systems. Compared to other software technologies, agent-based software technology presents itself as an effective solution for many problems in distributed systems, such as network overhead and transmission challenge. However, the security issue is a main factor that contributes to limitations of the benefits of agent-based software technology as well as its applications. The main reason behind this issue, is that the agents can be attacked by the destination machines where they perform the missions, or the visiting agents can perform malicious activities on the host machine. Moreover, advanced attacks such as DoS, modification, and multiple colluded attacks can exacerbate the security problem. Based on the attacker (the visiting mobile agent and the destination or host machine):

- we review different techniques used to ensure the security in agent-based systems, critique them, and compare them according to well-defined cyber security requirements.

Based on protection goals (code and data, state, and itinerary of the mobile agent):

- A maturity model is employed to analyze the security techniques as well as rank the strength of the attacks.
- Seven research questions are provided in the research field of agent security that should be answered to ensure comprehensive security in agent-based systems. They are as follows:

1. How to protect visiting mobile agent against malicious DM and the DM against malicious mobile agents?
2. How to ensure integrity of both the code of the agent and the results of the task executed by the agent?
3. How to ensure high resistance against advanced attacks (DoS, alternation, and colluded) attacks?
4. How to ensure comprehensive security requirements in agent based systems (Confidentiality, Integrity, Authentication, Authorization, Accounting, Availability, Non-Repudiation, Verification, Anonymity, Accountability)?
5. How to enable self-protection and self-communication features for the visiting mobile agent within the space of the DM?
6. How to quantify the security level that is achieved?

For answering the first three research questions, both the DTS and Improved-DTS approaches are proposed in this thesis. They are executed by the dummy generation module that is linked with the agent manager. The problem is related to the mobility feature, where an agent can migrate from the home machine to the destination machine to perform tasks, security issues are critical in this technology. The security issue in ABST becomes critical when the destination machine is the attacker, where it has full control over the visiting agent. The results of executed tasks may lose their integrity, the behavior of the agent may be changed, and advanced active attacks, such as alternation, collusion, and DoS attacks, may be applied by the attacker.

- From a historical database of tasks, the DTS randomly generates dummy tasks to protect the real task, aiming at confusing the attacker when determining the real task among the dummy tasks and limiting their ability to perform malicious actions.
- The improved DTS aims at generating strong dummy tasks based on three factors: (1) dummy tasks have the same execution probability as the real task, which in turn guarantees the highest entropy; (2) dummy tasks are of the same type as the real task (normal or time-sensitive task); and (3) the deadlines of the dummy tasks are the same as that of the real task.

For answering the fourth and fifth research questions, six modules are presented and linked with the agent manager to satisfy various security requirements. These modules collaborate with each other's to perform the SPSC approach, which enables self-protection and self-communication features for the visiting mobile agent to isolate it from the space of the DM. Thus, the DM itself can protect itself from the malicious visiting mobile agents.

- The six modules are: authentication, authorization, auditing, behaviour detection, encryption, and decryption.
- The communication among the modules is conducted within the manager of the agent (middleware installed on the destination machine).
- In addition, the decryption process is performed using a mediator key, which ensures that the process of generating the encryption key of the session is not controlled by the destination machine.

As for answering the last research question, two novel security metrics are proposed in this work. The first security metric is used to evaluate both the DTS and the improved-DTS, while the second one is used to evaluate the SPSC approach.

- The first security metric mainly depends on the entropy to quantify the amount of protection, therein considering the amount of violation caused by the attacker side.
- The second security metric depends on the number of security requirements that are achieved. This metric is used for evaluation purpose and involves 13 security requirements in its scale.

For evaluation in the context of comparison, both the DTS and the improved-DTS are compared to well-known protection mechanisms, which are the obfuscation code (OC) and fragmentation-based encryption (FBE). The SPSC approach is compared to three approaches, which are Co-signing (CoG), Digital Signature (DS), and Code signing (CodG).

- The proposed DTS and improved-DTS approaches showed high resistance to advanced attacks and better performance.
- In regards to the resistance against alternation, collusion, and DoS attacks, the improved DTS showed the highest resistance according to the LoV security metric, where the percentage of the violation predefined thresholds was 0 and 0.1 for the first five trials and the sixth trial, respectively.
- In regard to performance, the DTS was ranked 1st because it performed better than the improved DTS. The root reason is that the improved DTS handles more conditions to improve the security level.
- In addition, considering the security issues in the context of time, our proposed approaches spend the minimum amount of time at the attacker's side.
- Based on 13 security requirements—confidentiality, integrity, availability, anonymity, accountability, authorization, accounting, non-repudiation, assurance, verification, self-

decryption, and self-communication—SPSC approach outperforms similar approaches, achieving a score of 13.

- In terms of performance time, the SPSC approach also performs better than similar systems when the size of the agent increases.

Limitations

Of course, as any given new approach or technique, our work has some limitations that can be listed as follows:

1. Ensuring privacy of agents is not considered in this work.
2. Resistance against other advanced threats, such as tailgating and blocking attacks, is not considered.
3. Attacking agent by another agent is not considered.

Future Work

The limitations listed above will be considered in future work, where we intend to ensure the privacy of agents, other advanced attacks will be taken into account, and ensuring security of agents against malicious agents will be also manipulated in future works.