Gestion Décentralisée de Clefs Cryptographiques dans un Système Multi-Agents Embarqués

Arthur Baudet, Annabelle Mercier, Oum-El-Kheir Aktouf, Philippe Elbaz-Vincent

▶ **To cite this version:**

Arthur Baudet, Annabelle Mercier, Oum-El-Kheir Aktouf, Philippe Elbaz-Vincent. Gestion Décentralisée de Clefs Cryptographiques dans un Système Multi-Agents Embarqués. 20èmes Rencontres des Jeunes Chercheurs en Intelligence Artificielle, Jun 2022, Saint-Etienne, France. hal-03765411

HAL Id: hal-03765411
https://hal.science/hal-03765411

Submitted on 31 Aug 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Gestion Décentralisée de Clefs Cryptographiques dans un Système Multi-Agents Embarqués

Arthur Baudet[1,2], Annabelle Mercier[1], Oum-El-Kheir Aktouf[1], Philippe Elbaz-Vincent[2]

[1] Univ. Grenoble Alpes, Grenoble INP, LCIS, Valence, France
[2] Univ. Grenoble Alpes, CNRS, Institut Fourrier, Grenoble, France

{arthur.baudet, oum-el-kheir.aktouf, annabelle.mercier}@lcis.grenoble-inp.fr
philippe.elbaz-vincent@univ-grenoble-alpes.fr

Résumé

Nous présentons les travaux réalisés et en cours dans le cadre d'une étude menant à la proposition d'une architecture de sécurité pour des systèmes multi-agents embarqués : des systèmes décentralisés et autonomes constitués d'agents coopérant pour réaliser la tâche qui leur est attribuée.

Mots-clés

Système multi-agents, système embarqué, infrastructure à clefs publiques

Abstract

We present an ongoing work on defining a security architecture for multi-agent systems of embedded agents, a kind of decentralized system of autonomous and embedded agents coordinating to fulfill their objectives.

Keywords

Multi-agent system, embedded system, public key infrastructure

1 Contexte et problématique

Nos travaux concernent ce que nous nommons les systèmes multi-agents embarqués (SMAe) ouverts, des systèmes où des agents, des systèmes embarqués autonomes coopérant pour atteindre leurs objectifs, ne venant pas forcément du même constructeur, peuvent se connecter ou se déconnecter du système durant son exécution. On retrouve, par exemple, ce genre de système dans les réseaux de véhicules autonomes connectés et communicants ou les réseaux de capteurs sans fil.

La sécurisation des communications et l'authentification des membres d'un système dépendent fortement de solutions cryptographiques ; notamment afin d'assurer la non-répudiation, la détection d'atteinte à l'intégrité et la confidentialité des échanges ainsi que l'authentification des parties communicantes. Tout cela pouvant être réalisé à l'aide d'une infrastructure à clefs publiques (PKI) telles que la PKIX [**?**]. Néanmoins, dans ce contexte, l'hypothèse de précharger et mettre à jour en temps réel des clefs ou certificats dans chaque agent ne peut pas être satisfaite. De plus, l'absence d'une autorité centrale rend tous les systèmes de gestion de clefs centralisés inapplicables.

Notre problématique est donc la suivante : dans le cas d'un attaquant possédant un contrôle total sur le réseau, pouvant donc intercepter, modifier ou forger des messages sans que nous ayons un a priori sur son comportement, comment élaborer un système de gestion de clefs cryptographiques pour un système multi-agents embarqués ouvert ?

2 Bibliographie

Nous avons réalisé une étude rigoureuse de la littérature récente concernant la problématique de sécurisation des SMAe [**?**]. Elle nous a permis de rendre compte d'une abondance de travaux proposant une protection contre des attaques venant de l'intérieur, notamment par l'usage de système de gestion de confiance ou de détection d'intrusion, mais peu de travaux concernant les attaques venant de l'extérieur, ce qui nécessite généralement l'usage de cryptographie. De plus, nous avons remarqué que ces systèmes de gestion de confiance nécessitent eux-mêmes une base cryptographique sûre pour garantir de l'authenticité et l'intégrité des communications entre agents.

La raison évoquée par les auteurs des différents travaux concernant le peu de travaux sur le sujet de l'usage de cryptographie dans les SMAe est la difficulté de mise en place d'une infrastructure cryptographique dans tels systèmes décentralisés. Nous avançons néanmoins que cela est nécessaire et cherchons à proposer une solution à ce problème.

3 Architecture de sécurité

L'objectif de ces travaux est de fournir la description d'une architecture de sécurité pour SMAe. Comme nous l'avons indiqué précédemment, nous trouvons qu'une solution cryptographique décentralisée est nécessaire à l'utilisation d'outils, tous aussi nécessaires, tels que les systèmes de gestion de confiance.

L'architecture que nous envisageons de proposer doit pouvoir assurer que chaque agent possède une identité et que ses communications soient sécurisées. Plus précisément, dans le cas d'un échange entre deux agents, la confidentialité de l'échange doit être maintenue, les atteintes à l'intégrité

de la communication détectées, l'identité de l'interlocuteur vérifiée et la répudiation des envois impossible.
Dans le cas d'une communication unidirectionnelle entre un agent et un ensemble d'agents, les atteintes à l'intégrité de sa transmission doivent être détectée, son identité liée à cette dernière et la répudiation de l'envoi impossible.

4 Infrastructure

Pour répondre à ces besoins, l'utilisation d'une PKI à certificats semble être le plus approprié.
Chaque agent génèrera une paire de clefs et les utilisera pour signer ses communications ainsi que pour engager des processus d'établissement des clefs de chiffrement éphémères. Son identité sera liée à sa clef publique qu'il devra faire certifier par une autorité afin de pouvoir se connecter au système.
Néanmoins, l'absence de serveurs centraux rend l'implémentation d'une PKI traditionnelle difficile puisqu'il n'y a pas de tierce partie de confiance candidate au rôle d'autorité de certification, d'autorité d'enregistrement et spécialement d'autorité de certification racine.
De plus, n'ayant pas de média de communication structuré, assurer une communication portant sur tout le système est difficile et coûteux.

4.1 Gestion des certificats

Certification et stockage Dans le cas où il n'est pas possible d'avoir une confiance absolue dans les autorités, il semble intéressant pour les agents de posséder plusieurs certificats. Si une autorité n'est plus jugée comme digne de confiance, ses certificats perdront leur valeur et de nouveaux seraient nécessaires pour les remplacer.
Par défaut, chaque autorité aura la responsabilité de stocker et partager (sur demande ou gratuitement) les certificats valides qu'elle aura signés, mais on pourrait imaginer donner cette tâche à certains autres agents du système.

Révocation La révocation d'un certificat, et donc l'exclusion d'un agent sera menée d'une part par l'ajout de l'identité de l'agent à une liste de révocation, et d'autre part, par l'utilisation de certificats à courte date d'expiration qui ne seraient pas renouvelés. La première méthode est rapide et directe mais seule la seconde est définitive.

Usurpation et conservation d'identité Dans un système hétérogène et ouvert, les agents n'ont pas forcément d'à priori sur leurs pairs, il est donc possible de réduire l'identité d'un agent à sa clef publique et ainsi prévenir toute tentative d'usurpation d'identité. Il reste néanmoins une nécessité de coopération entre autorités de certification pour assurer la conservation des identités afin de s'assurer que deux agents ne s'enregistrent pas avec la même clef en deux points différents du système, même si cela est très peu probable.

4.2 Intégration dans un système de gestion de confiance

Afin de proposer une architecture de sécurité plus transversale, le système de gestion de confiance pourrait être en partie intégré dans notre PKI. On peut notamment imaginer les autorités ajouter la valeur de confiance qu'elles ont en les agents certifiés dans leurs certificats. De même, une autorité dont la confiance baisserait pourrait perdre son statut. L'exclusion d'un agent par le système, de par sa réputation trop basse, pourrait aussi se concrétiser par la révocation de son certificat et le refus de lui en attribuer un nouveau.

5 Scénarios d'usage

Scénario A Lors de la mise en place du système, plusieurs agents sont déployés avec l'objectif de servir d'autorité de certification. Ce scénario est le plus simple à mettre en œuvre mais limite l'autonomie du SMAe et peut mener à un goulot d'étranglement ou de point de défaillance unique si le nombre d'autorités de certification n'est pas correctement calibré.
Une partie des agents se voit attribuer le rôle d'autorité de certification. Ces agents auront un rôle important d'un point de vue de sécurité et il serait préférable qu'ils soient les mieux équipés pour réaliser leurs tâches dans le système. Tout agent souhaitant entrer dans le système génèrera une paire de clefs et fera la demande de certificat à, au moins, une autorité. Une fois certifié, l'agent pourra prendre part aux communications du système.

Scénario B Lors de la mise en place du système, aucun agent n'est déployé avec l'objectif de servir d'autorité de certification. Ce scénario, plus « sauvage » ou « libertaire », offre des possibilités de résilience plus grande une fois le challenge du choix et du maintien de la confiance dans les autorités de certification résolu.
Tout comme dans le scénario A, il faut pouvoir s'assurer de la fiabilité de l'autorité délivrant un certificat. Il faut pouvoir motiver les agents à devenir autorité de certification. Cela peut être une obligation dans le comportement des agents dans un premier temps et être lié à un système de réputation dans un second.

6 Conclusion

Ces travaux se poursuivent actuellement et devraient permettre d'obtenir une approche de gestion décentralisée des clefs cryptographiques, adaptée aux SMAe. Une étude de cas sur une application de drones autonomes est prévue comme preuve de concept.

Remerciements

Ce travail a bénéficié d'une aide de l'État gérée par l'Agence Nationale de la Recherche au titre du programme « Investissements d'avenir » portant la référence ANR-15-IDEX-02.

Références

[1] Arthur Baudet, Oum-El-Kheir Aktouf, Annabelle Mercier, and Philippe Elbaz-Vincent. Systematic mapping study of security in multi-embedded-agent systems. *IEEE Access*, 9 :154902–154913, 2021.

[2] Jean-Guillaume Dumas, Pascal Lafourcade, and Patrick Redon. *Architectures de sécurité pour internet-2e éd. : Protocoles, standards et déploiement*. Dunod, 2020.