Langage et infrastructure d'architecture dynamique orientée données

Mots clés: sécurité, chiffrement basé attribut, architecture dynamique, système de systèmes
Lieu: Laboratoire IRISA (Vannes)
Équipe d'accueil: ArchWare (http://www.irisa.fr/casa)
Directeur de thèse: Nicolas Belloir, Jérémy Buisson
Co-encadrant: Lionel Touseau, Jamal El-Hachem
Financement: Industriel (Chaire Saint-Cyr THALES)

1 Description du projet

Ce sujet de thèse s'attache à concevoir une architecture dynamique sécurisée, décentralisée capable de contrôler l'accès aux données du système par des acteurs, qu'ils soient techniques (composants logiciels) ou humains, que nous qualifierons de sous-systèmes. Pour cela il est envisagé de faire porter ce contrôle par la donnée en utilisant des mécanismes de chiffrement basé attribut. Un des défis de cette thèse sera de gérer le caractère dynamique des participants au système: de nouveaux acteurs doivent pouvoir intégrer le système de manière opportuniste, et ceci sans garantie d'une infrastructure centralisée accessible en permanence. Un second défi consistera à prendre en compte le contexte opérationnel des sous-systèmes souhaitant accéder aux ressources du système, qui lui aussi est dynamique.

2 Hypothèses, questions posées, identification des points de blocage

Dans ce projet, nous faisons les hypothèses suivantes :

1) L'architecture est composée de plusieurs systèmes. À chacun de ces systèmes sont affectées des missions propres. Il existe un niveau de coordination ayant un objectif global, chargé d'affecter les missions à chaque système individuel. Nous faisons donc l'hypothèse que les systèmes ont un "sentiment d'appartenance", c'est-à-dire qu'ils sont prédisposés à collaborer dans le système de systèmes.

2) Malgré ce niveau de coordination global, dans notre principal cas d'étude, il n'est pas possible d'anticiper avant le déploiement toutes les interactions entre les systèmes participants. La complexité, mais également les imprévus dans l'exécution des missions de chaque système ne permettent pas de planifier ces interactions. Il s'agit également d'être capable de saisir des opportunités de collaboration qui se présenteraient au moment de l'exécution de la mission.

3) Malgré l'existence d'une coordination globale, il n'existe pas d'infrastructure centralisée accessible en permanence. Les collaborations entre les systèmes se font donc de point à point, en utilisant les technologies de communication disponibles, incluant des réseaux avec infrastructure, des DTN, des liaisons sans fil point à point, chacune avec des performances propres.

4) Malgré les hypothèses précédentes, l'architecture du système de systèmes n'est pas ouverte, dans le sens où seuls les systèmes autorisés peuvent accéder et fournir des ressources dans le cadre des collaborations au sein du système de systèmes. La notion d'autorisation reprend et généralise le couple droit et besoin d'en connaître habituel, pour l'étendre au contexte opérationnel, vu comme dynamique.

Dans un tel contexte, se posent les questions :

- Comment décrire l'architecture d'un tel système ?
- Comment concevoir l'infrastructure requise pour opérer un tel système ?

L'état de l'art mené en amont sur les langages de description d'architectures dynamiques sécurisés laisse plusieurs problèmes ouverts. D'une part, à notre connaissance, aucune approche ne répond à l'ensemble des questions comme un tout. D'autre part, les précédents travaux adoptent majoritairement une vision structurelle du système (en sous-systèmes ou en flots de données), mettant donc l'accent sur la sécurisation des canaux de communication plutôt que sur la sécurisation des objets.

Enfin, conformément à la vision de l'architecture zero trust, les décisions de contrôle d'accès devraient prendre en compte le contexte opérationnel, c'est-à-dire des attributs nécessairement dynamiques.

3 Objectifs et résultats attendus

Après avoir dressé un état de l'art sur la sécurisation d'architectures dynamiques, la thèse aura donc pour objectif de proposer un nouveau langage de description d'architecture, dans lequel l'architecture décrira les systèmes et les objets échangés par ces systèmes (par opposition aux flots). Les flots entre les systèmes seront déduits de cette description d'une part statiquement de cette description et de la description de l'opération, d'autre part dynamiquement selon les opportunités de collaboration.

Les résultats attendus sont donc :

1) Le langage de description, permettant de modéliser les objets et les systèmes, incluant les labels de sécurité des objets et le contexte opérationnel des systèmes.

2) Une infrastructure distribuée, représentative du système de systèmes que nous considérons, permettant les échanges de données tel que modélisés grâce au langage défini. Cette infrastructure dérivera donc les flots de communications en fonction de la description centrée données et en fonction des canaux effectivement déployés. Cette infrastructure supposera l'existence des mécanismes d'identification du contexte opérationnel et des mécanismes de chiffrement idoines.

3) L'identification des problèmes demeurant ouverts, tant pour l'identification du contexte opérationnel que pour les mécanismes de chiffrement.

4 Contexte

La thèse sera conduite dans le cadre d'un partenariat industriel avec THALES et le Centre de Recherche de Coëtquidan (CReC) sur la sécurisation d'une architecture composée de plusieurs systèmes, techniques comme humains. Le doctorant sera rattaché à l'équipe ArchWare de l'IRISA (site de Vannes, UBS) et au CReC (site de l'Académie Militaire de Saint-Cyr Coëtquidan).

References

[1] Humberto Cervantes, Didier Donsez, and Lionel Touseau. An Architecture Description Language for Dynamic Sensor-Based Applications. In *2008 5th IEEE Consumer Communications and Networking Conference*, pages 147–151, January 2008.

[2] Flavio Oquendo. Coping with Uncertainty in Systems-of-Systems Architecture Modeling on the IoT with SosADL. In *2019 14th Annual Conference System of Systems Engineering (SoSE)*, pages 131–136, May 2019.

[3] Flavio Oquendo. Fuzzy Architecture Description for Handling Uncertainty in IoT Systems-of-Systems. In *2020 IEEE 15th International Conference of System of Systems Engineering (SoSE)*, pages 000555–000562, June 2020.

[4] Jérémy Buisson, Fabien Dagnat, Elena Leroux, and Sébastien Martinez. Safe reconfiguration of Coqcots and Pycots components. *Journal of Systems and Software*, 122:430–444, December 2016.

[5] Phu H. Nguyen, Shaukat Ali, and Tao Yue. Model-based security engineering for cyber-physical systems: A systematic mapping study. *Information and Software Technology*, 83:116–135, March 2017.

[6] Stephan Seifermann, Robert Heinrich, and Ralf Reussner. Data-Driven Software Architecture for Analyzing Confidentiality. In *2019 IEEE International Conference on Software Architecture (ICSA)*, pages 1–10, March 2019.

[7] Stephan Seifermann, Robert Heinrich, Dominik Werle, and Ralf Reussner. Detecting violations of access control and information flow policies in data flow diagrams. *Journal of Systems and Software*, 184:111138, February 2022.

[8] Katja Tuma, Laurens Sion, Riccardo Scandariato, and Koen Yskout. Automating the early detection of security design flaws. In *Proceedings of the 23rd ACM/IEEE International Conference on Model Driven Engineering Languages and Systems*, MODELS '20, pages 332–342, New York, NY, USA, October 2020. Association for Computing Machinery.

[9] Scott W. Rose, Oliver Borchert, Stuart Mitchell, and Sean Connelly. Zero Trust Architecture. Technical Report SP800-207, NIST, August 2020.