Modélisation de cérémonies de sécurité

Projet de recherche M1 SIF, encadré par **Barbara FILA**, équipe SPICY

Mots clés

Cérémonies de sécurité, protocoles, modélisation formelle

Contexte et motivation

Pour analyser la sécurité des systèmes distribués du XXI siècle, Ellison a proposé en 2007 d'élargir la notion d'un protocole cryptographique à celle d'une *cérémonie* [1]. Les protocoles focalisent uniquement sur les messages cryptographiques échangés entre les machines (ordinateurs, serveurs) et ne sont donc pas appropriés pour capturer les attaques reposant sur le comportement non-déterministe et souvent influençable des humaines, sur des failles matérielles, etc. Une cérémonie, en revanche, spécifie les interactions entre *tous* les composants d'un système — y compris ses utilisateurs et son infrastructure physique — et s'intéresse à tous les aspects qui peuvent potentiellement impacter son fonctionnement, par exemple l'ingénierie sociale. Au delà des messages cryptographiques, les cérémonies prennent en compte l'échange d'objets physiques ou des droits légaux, ainsi que des aspects comme les émotions (le stress, la fatigue, etc.) pouvant influencer le déroulé et le résultat du protocole. Effectuer un virement en ligne est un exemple typique d'une cérémonie. L'humain doit d'abord se connecter à son compte en ligne (en utilisant un protocole d'authentification spécifique), ensuite remplir des données nécessaires et enfin vérifier et valider le code reçu par sms pour finaliser la transaction.

Objectif

Plusieurs approches ont été proposées depuis 2007 pour spécifier et analyser les cérémonies de manière formelle [2, 3]. Souvent il s'agit des approches ad-hoc : certaines s'intéressent principalement à la modélisation du comportement humain [4, 5], d'autres focalisent sur les cérémonies spécifiques [6, 7], encore d'autres étudient le modèle de l'attaquant dans le contexte des cérémonies [8, 9]. Inspirés par ces différentes approches, Fila et Radomirović ont conçu en 2024 un formalisme abstrait et générique pour spécifier les cérémonies [10]. Ce formalisme repose sur deux éléments clés :

- une relation binaire de *possession* qui modélise ce que les différentes entités (humains, machines, documents, objets, etc.) impliquées dans une cérémonie possèdent (physiquement ou légalement), connaissent, contiennent, etc.,
- la notion de *transformation de possession* formalisée à l'aide des relations n-aires qui modélisent comment les possessions de différentes entités évoluent lors de l'exécution d'une cérémonie.

L'objectif du présent projet est de mettre en pratique le formalisme introduit dans [10] afin de développer des recommandations de modélisation sous-jacentes, telles que des heuristiques, ou des patrons de transformations. Il s'agit aussi de montrer que le formalisme de Fila et Radomirović généralise et unifie les différentes approches de modélisation des cérémonies, proposées de manière ad-hoc depuis 2007.

Déroulement du projet

Pour pouvoir mener à bien ce projet, nous l'avons découpé en trois phases principales dont les buts scientifiques et pédagogiques sont présentés ci-dessous. Certaines tâches seront itératives ou pourront être effectuées en parallèle.

Phase 1 : Étude bibliographique

Tâche 1 :
Lecture des articles scientifiques formalisant les cérémonies. Les premiers articles seront suggérés par l'encadrant.

Objectif pédagogique visé :
Apprendre à lire les articles scientifiques de manière méthodique.

Tâche 2 :
Rechercher d'autres articles pertinents pour ce projet.

Objectif pédagogique visé :
Apprendre à identifier des sources pertinentes et de qualité dans le déluge d'information disponible entre autre sur l'Internet.

Phase 2 : Modélisation formelle

Tâche 3 :
Extraire les éléments et les aspects saillants des modèles étudiés lors de l'étude bibliographique. Les modéliser en utilisant les transformations de Fila et Radomirović.

Objectif pédagogique visé :
Apprendre à décortiquer un modèle formel et à bien comprendre ses composants.

Tâche 4 :
Concevoir une cérémonie inspirée par la vie réelle qui permettra d'illustrer l'ensemble d'aspects identifiés dans la tâche précédente. La modéliser à l'aide du formalisme développé dans [10].

Objectif pédagogique visé :
Pratiquer la créativité et la modélisation formelle.

Phase 3 : Rédaction d'un article scientifique

Tâche 5 :
Contribuer à la rédaction d'un article de recherche de type *systematization of knowledge* (SOK), rédigé en anglais et portant sur l'état de l'art en modélisation formelle des cérémonies. L'article sera construit autour des recommandations de modélisation identifiées grâce à ce projet, notamment à la Tâche 3. La cérémonie définie lors de la Tâche 4 servira de comparaison entre les différents modèles existants étudiés.

Objectif pédagogique visé :
Apprendre à structurer et à rédiger un article de recherche.

Organisation et environnement

Le projet sera effectué au sein de l'équipe SPICY, sous l'encadrement de Barbara FILA. Si les résultats de la Phase 1 sont prometteurs, l'étudiant aura l'opportunité de collaborer lors des Phases 2 et 3 avec *University of Surrey* en Angleterre, notamment avec Saša RADOMIROVIĆ. Cette collaboration pourra porter sur la modélisation de la cérémonie de vote électronique actuellement développé en Suisse par Swiss Post [11].

Enfin, si le résultat définitif de ce projet est satisfaisant, la collaboration avec l'étudiant pourra être reconduite aux années suivantes, par exemple sous forme d'un séjour de recherche à *University of Surrey*, d'une thèse de master à l'IRISA ou d'une thèse doctorale.

Candidatures

Nous sommes à la recherche d'un candidat

- intéressé par la recherche,
- enthousiaste de la modélisation formelle (logique, vérification, théorie),
- curieux et ouvert d'esprit,
- ayant des bonnes compétences en anglais (écrit, oral).

N'hésitez pas à prendre contact avec Barbara Fila (par mail `barbara.fila@irisa.fr`) si vous avez des questions ou si vous souhaitez discuter de ce projet de manière informelle.

Références

[1] Carl M. Ellison. Ceremony design and analysis. *IACR Cryptol. ePrint Arch.*, page 399, 2007.

[2] Luca Viganò. Formal Methods for Socio-technical Security - (Formal and Automated Analysis of Security Ceremonies). In *COORDINATION*, volume 13271 of *LNCS*, pages 3–14. Springer, 2022.

[3] Kenneth Radke, Colin Boyd, Juan Manuel González Nieto, and Margot Brereton. Ceremony Analysis: Strengths and Weaknesses. In *SEC*, volume 354 of *IFIP Advances in Information and Communication Technology*, pages 104–115. Springer, 2011.

[4] Giampaolo Bella and Lizzie Coles-Kemp. Layered analysis of security ceremonies. In *SEC*, volume 376 of *IFIP Advances in Information and Communication Technology*, pages 273–286. Springer, 2012.

[5] Diego Sempreboni and Luca Viganò. A mutation-based approach for the formal and automated analysis of security ceremonies. *J. Comput. Secur.*, 31(4):293–364, 2023.

[6] Sebastian Gajek, Mark Manulis, Ahmad-Reza Sadeghi, and Jörg Schwenk. Provably secure browser-based user-aware mutual authentication over TLS. In *AsiaCCS*, pages 300–311. ACM, 2008.

[7] Giampaolo Bella, Rosario Giustolisi, and Carsten Schürmann. Modelling human threats in security ceremonies. *J. Comput. Secur.*, 30(3):411–433, 2022.

[8] Marcelo Carlomagno Carlos, Jean Everson Martina, Geraint Price, and Ricardo Felipe Custódio. An updated threat model for security ceremonies. In *SAC*, pages 1836–1843. ACM, 2013.

[9] Diego Sempreboni, Giampaolo Bella, Rosario Giustolisi, and Luca Viganò. What Are the Threats? (Charting the Threat Models of Security Ceremonies). In *ICETE (2)*, pages 161–172. SciTePress, 2019.

[10] Barbara Fila and Sasa Radomirovic. Nothing is out-of-band: formal modeling of ceremonies. In *CSF*. IEEE Computer Society, 2024.

[11] Swiss Post Voting System. Available at `https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/master/System?ref_type=heads`.