Application BASTRI

Fiches Equipes

PESTO (SR0729KR)

Proof techniques for security protocols

CASSIS (SR0055XR) PESTO PESTO (SR0758TR)

Statut: Terminée

Responsable : Steve Kremer

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2024" : *Aucun mot-clé.*

Mots-clés de "B - Autres sciences et domaines d'application - 2024" : *Aucun mot-clé.*

Domaine : Algorithmique, programmation, logiciels et architectures
Thème : Sécurité et confidentialité

Période : 01/01/2016 -> 31/10/2016
Dates d'évaluation :

Etablissement(s) de rattachement : <sans>
Laboratoire(s) partenaire(s) : <sans UMR>

CRI : Centre Inria de l'Université de Lorraine
Localisation : Bâtiment Ada Lovelace - Centre Inria de l'Université de Lorraine
Code structure Inria : 051105-0

Numéro RNSR : 201622052E
N° de structure Inria: SR0729KR

Présentation

L'objectif de l'équipe PESTO est de concevoir des modèles et technique pour l'analyse et la conception assistée par ordianteur de protocoles de sécurité. Alors qu'historiquement les protocoles de sécurité visaient à protéger la confidentialité et l'authentification, la situation a changé. Les protocoles de vote électronique doivent garantir l'anonymat du votant, tout en garantissant la transparence du scrutin; les données sont transmis en utilisant des services web; les protocoles implantés dans les puces RFID et les téléphones portables doivent garantir qu'on ne puisse pas tracer les utilisateurs. À cause des logiciels malveillants de plus en plus répandus, les protocoles de sécurité utilisent de nouveaux mécanismes, tels que du hardware de confiance ou des authentifications multi-facteurs, afin de garantir des propriétés de sécurité et ceci même si la plateforme sur laquelle ces protocoles s'exécutent est compromise. Les techniques et outils existants sont cependant incapables d'analyser les propriétés de sécurité requises par ces nouveaux protocoles et prendre en compte les nouveaux mécanismes déployés et modèles d'attaquants correspondants.

Axes de recherche

- Formal methods for Cryptographic protocols
- Automated reasoning
- Electronic voting
- Privacy in social networks

Relations industrielles et internationales

Contact

- **Responsable :** Steve Kremer
- **Tél :** 03.54.95.86.60
- **Secrétariat Tél :**

En savoir plus

- Site de l'équipe
- Site sur inria.fr
- Site du responsable
- Derniers Rapports d'Activité : 2016 , 2017 , 2018 , 2019 , 2020 , 2021 , 2022 , 2023 , 2024

Documents sur la structure

- Intranet
- Privés

Décisions

- 11361 (16/01/2016) : création

Localisation

- **Adresse postale :** Centre Inria de l'Université de Lorraine, Bâtiment Ada Lovelace, 615 rue du Jardin Botanique, 54600 Villers-lès-Nancy France
- **Coordonnées GPS :** 48.666, 6.157