Protocol Analysis: Combining Existing Tools

TECAP

Appel : Projets génériques

Année : 2017

Instrument : Recherche coopérative

Contact : vincent.cheval@inria.fr

COORDINATEUR : Inria Nancy

PARTENAIRES : LMF, Inria Paris, IRISA, Inria Sophia Antipolis, LIX

Résumé :

Les protocoles cryptographiques permettent de sécuriser nos communications en ligne. Au sein du projet TECAP, nous combinons et améliorons plusieurs « state-of-the-art » outils de vérification automatique que nous appliquons à des protocoles de télécommunication, de vote électronique et d'authentification.

CONTEXTE ET OBJECTIFS

Les transactions numériques sont protégées par des **protocoles cryptographiques** :

- des **programmes informatiques distribuées**
- qui utilisent des **primitives cryptographiques** (chiffrement, signature numérique, …)
- pour garantir des **propriétés de sécurité** (confidentialité, anonymat, authenticité, …)

Il existe de nombreux outils de vérification (semi)-automatiques de protocoles cryptographiques (CryptoVerif, EasyCript, ProVerif, Tamarin, AKiSs, APTE, AVANTSSAR) mais tous ont des forces et faiblesses différentes: Lequel choisir ?

MÉTHODOLOGIE ET RÉSULTATS

Le but de ce projet est de tirer le meilleur de ces outils:

- En améliorant la théorie et l'implémentation de chaque outil individuellement: GSVerif (un front-end de ProVerif), nouvelles versions de Tamarin, ProVerif, Sat-Equiv et CryptoVerif
- En explorant des techniques novatrices: Création d'un nouvel outil Squirrel.
- En construisant des ponts permettant la coopération entre les techniques employées et entre les outils: création de DeepSec (outil combinant des techniques de APTE et AKiSs); développement d'un compilateur d'hypothèses cryptographiques de CryptoVerif vers EasyCrypt.

ainsi que de rendre ces outils de vérification plus polyvalents:

- Uniformiser et intégrer les outils au sein d'une plateforme commune: Plateforme SAPIC+
- Rendre nos outils plus accessibles pour les secteurs industriels et éducatifs: DeepSec UI

EasyCrypt

ProVerif

DEEPSEC

Sat-Equiv

Tamarin Prover

AKiSs

Squirrel

CryptoVerif

VALIDATION

Validation de nos résultats par l'analyse de protocoles et primitives cryptographiques:

- WireGuard Virtual Private Network (VPN) Protocol
- 5G-AKA Authentication protocol
- Protocoles d'authentification Multi-facteurs
- TLS 1.3, HPKE Standard, SHA-3
- CanAuth, Yubikey

30+ Publications:

1. H. Comon, C. Jacomme, G. Scerri (2020). Oracle simulation: a technique for protocol composition with long term shared secrets. ACM Conference on Computer and Communications Security (CCS '20)
2. G. Barthe, B. Grégoire, C. Jacomme, S. Kremer, and P.-Y. Strub. Symbolic Methods in Computational Cryptography Proofs. IEEE Computer Security Foundations Symposium (CSF'19).
3. D. Baelde, S. Delaune, C. Jacomme, A. Koutsos, and S. Moreau. An Interactive Prover for Protocol Verification in the Computational Model. In Symposium on Security and Privacy (S&P'21).
4. V. Cortier, S. Delaune, and J. Dreier. Automatic generation of sources lemmas in Tamarin: towards automatic proofs of security protocols. European Symposium on Research in Computer Security (ESORICS'20) – Best paper award
5. B. Blanchet, V. Cheval, and V. Cortier. ProVerif with lemmas, induction, fast subsumption, and much more . In IEEE Symposium on Security and Privacy (S&P'22) .