Trusted Logic
5 rue du Bailliage
78000 Versailles
www.trusted-logic.fr

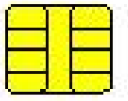
Spécification et Vérification
CNRS UMR 8643, ENS Cachan
61, avenue du président-Wilson
94235 Cachan Cedex
www.lsv.ens-cachan.fr

Verimag
CNRS UMR 5104,
Univ. Joseph Fourier, INPG
2 av. de Vignate, 38610 GIÈRES
www-verimag.imag.fr

EVA : Explication et Vérification Automatique de protocoles cryptographiques

Le contexte : besoins croissants en matière de sécurité informatique





Domaines en forte expansion : téléphonie mobile, télévision à péage, commerce électronique, transactions bancaires, domotique, etc.

Manque d'outils pour faciliter le développement de systèmes sécuritaires.

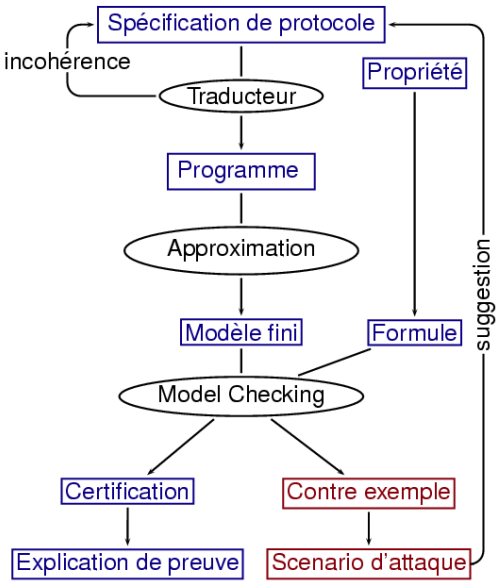
Un standard pour la certification : les Critères Communs de sécurité.

La démarche EVA : automatiser et expliquer

Automatiser la vérification dans un cadre ciblé crucial pour la sécurité : les protocoles cryptographiques.

Permettre l'explication de preuves et leur utilisation dans un contexte de certification Critères Communs.

Faciliter la mise au point des protocoles (processus itératif).



Résultats attendus

Langage de définition de protocoles et de propriétés : confidentialité, authenticité, responsabilité etc.

Base de test représentative : protocoles d'authentification, de distribution de clés, de paiement en ligne sécurisé, de commerce électronique, etc.

Environnement de conception et de vérification de protocoles :

- vérification automatique à base d'abstraction et de model checking;
- aide à la mise au point de protocoles;
- explication de preuves.

Contact : Daniel.Le_Metayer@trusted-logic.fr