Sécurité des implémentations pour la cryptographie

Introduction

Benoît Gérard

28 novembre 2017

Présentations

Benoît Gérard
benoit.gerard@irisa.fr

- Thèse
  cryptographie symétrique
- Post-doctorat
  attaques par canaux auxiliaires
- Ingénieur (DGA)
  codage et vérification d'implémentations cryptographiques
  évaluation des composants contre (canaux auxiliaires)

Objectifs du cours

La voiture c'est un outil formidable mais qui peu se révéler très dangereux si on l'utilise mal.

Idem pour la cryptographie :

- au niveau de l'implémentation,
- au niveau de la configuration/utilisation.

But

- Sensibilisation aux erreurs classiques.
- Apprentissage des bons réflexes.

Conception d'un système de sécurité

Focus sur l'implémentation et l'utilisation de la cryptographie du plus haut au plus bas niveau.

Trame du cours

1. Spécifications (architecture, APIs de sécurité).
2. Développement de code de sécurité (focus sur le C).
3. Implém. de la cryptographie : attaques distantes.
4. Implém. de la cryptographie : attaques locales non-invasives.
5. Implém. de la cryptographie : attaques locales invasives.

Organisation

Séances

- 6 séances de cours + 5 de TP

Support

- Planches, énoncés (et corrections) disponibles sur

http ://people.irisa.fr/Benoit.Gerard/teaching_fr.html

Évaluation

1/2 TP noté

1/2 Contrôle écrit de 2 heures