HARDWARE SIDE-CHANNELS AND PROTECTED ENCLAVES

Nature	UE

RESPONSABLES

Benoît Gerard

OBJECTIFS

La cryptographie est un élément clef de la sécurité numérique. Son utilisation permet la mise en oeuvre de systèmes complexes dont les propriétés de sécurité reposent de façon prouvée sur des problèmes reconus comme difficiles.

Néanmoins, ces garanties obtenues dans des modèles théoriques se retrouvent rapidement mises à mal lors de la mise en œuvre concrète de ces systèmes. Les mauvaises configurations, les erreurs d'implémentation ou la présence de canaux auxiliaires non pris en compte dans le modèle de la preuve rendent la grande majorité des systèmes sécurisés vulnérables bien que cryptographiquement surs d'un point de vue théorique.

Ce cours a pour objectif de mettre en lumière la complexité de la mise en œuvre de la cryptographie dans un cas d'usage réel. Il aborde différentes vulnérabilités pouvant être induites par une mauvaise implémentation de la cryptographie et apporte des principes et bonnes pratiques permettant de limiter ces erreurs. Pour cela, tous les aspects de la réalisation d'un système sécurisé sont balayés en partant d'un point de vue système et en descendant jusqu'aux détails d'implémentation des primitives cryptographiques sur un composant.

MOTS-CLÉS

cryptographie, implémentation, vulnérabilités, canaux-auxiliaires

PRÉREQUIS

Bases de cryptographie, connaissance du langage C

CONTENU

Dans un premier temps, il est question de la spécification de systèmes et de produits (gestion des secrets, déploiement, API de sécurité, ...). L'on se concentre ensuite sur les implantations à proprement parler en débutant par les vulnérabilités classiques non liées à la cryptographie mais pouvant être désastreuses dans du code manipulant des secrets (e.g. Heartbleed). Pour ce qui est des vulnérabilités liées à la cryptographie, la dynamique est de commencer par les vulnérabilités pouvant être exploitées par un attaquant distant (e.g. timing attacks) puis local non-invasif (e.g. DPA) puis finalement local (semi-)invasif (e.g. attaques en fautes). Des séances de TP permettent de mettre en pratique certaines attaques vues en cours sur un exemple de code mal conçu.

COMPÉTENCES ACQUISES

Vision plus globale de la mise en pratique de la cryptographie, connaissance des différentes menaces existantes, acquisition de bons réflexes méthodologiques.

APPARTIENT À

Master 2 informatique parcours Science Informatique

Mise à jour le 17 juillet 2017

CONTACT(S)

Département Informatique et télécommunications
École normale supérieure de RennesCampus de Ker LannAvenue Robert Schuman
35170 BRUZ
Tél. : 02 99 05 52 43
E-mail
Site Internet