UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

université PARIS-SACLAY

université PARIS-SACLAY

UE « Calcul sécurisé »

Louis Goubin – Professeur, UVSQ

M1 informatique - Site de Versailles

Contexte

- Traditionnellement, en cryptographie, on cherche à garantir la confidentialité, l'intégrité et l'authenticité de "messages", qui sont des objets "statiques" (stockés, ou transmis tels quels sur des canaux de communication non sécurisés).
- En revanche on ne considère pas la sécurité des algorithmes et protocoles cryptographiques eux-mêmes (qui sont en général des programmes, qui s'exécutent, et sont donc des objets "dynamiques").
- Par exemple on ne s'intéresse pas :
  - à la confidentialité des programmes (le principe de Kerckhoffs suppose qu'ils sont connus de tout le monde),
  - ni à leur intégrité (on suppose qu'Alice et Bob exécutent ces algorithmes/protocoles/programmes correctement, sans aucune modification/erreur/bug),
  - ni à leur authenticité (on suppose que les algorithmes/protocoles/programmes exécutés par Alice et Bob ont été installés par une autorité de confiance).

Objectif et contenu (1)

- Dans l'UE « Calcul sécurisé », on verra qu'en réalité il est très important de sécuriser également les calculs (au sens d'algorithmes/protocoles/programmes).
- Le cours :
  - couvrira des aspects pratiques de ces problèmes de sécurité (débordement de tampon, rétro-analyse de code, attaques par canaux auxiliaires, injection de fautes, …)
  - sera aussi l'occasion d'approfondir des questions plus théoriques (modélisation de la notion de calcul, machines de Turing, garbled circuits, programmes auto-modifiants, obfuscation de code, …)
  - en montrant comment ces notions peuvent être utilisées pour prévenir les vulnérabilités du logiciel.

Objectif et contenu (2)

- Le cours et les TDs seront illustrés par de nombreux exemples, notamment issus de la sécurité des cartes à puce, de la virologie informatique, et des applications émergentes dans le « calcul en nuage » (cloud computing).
- On abordera au passage les notions récentes de
  - chiffrement homomorphe (comment calculer sur des données chiffrées ?)
  - schéma de calcul vérifiable (qui permet à un client de déléguer un calcul à un serveur tout en ayant l'assurance que le calcul a été correctement effectué)
- Un autre exemple typique d'application récente est celui des techniques de « machine learning », où il s'agit d'analyser les informations stockées dans des bases de données tout en préservant la confidentialité des données.

Positionnement pédagogique dans le master informatique

- Prérequis pour suivre l'UE « Calcul sécurisé » : avoir suivi l'UE « Cryptographie » au 1er semestre
- L'UE « Calcul sécurisé » est obligatoire pour poursuivre dans le parcours (M2) SeCReTS
- Responsable de l'UE « Calcul sécurisé » : Louis Goubin – Professeur, UVSQ
- Volume horaire : 12h CM, 24h TD
- Calendrier : sur 6 semaines (de mars à mai 2017)