Scientist who joined IRISA

2016
Education
• 2006: PhD at ENS Cachan
  Award for « outstanding thesis » given by France Télécom (now Orange Labs)
• 2011: Habilitation thesis at ENS Cachan

Employment
• 2006-2007: Post-doctoral stays at Birmingham University (UK) and University of Lorraine (FR)
• Since 2007: CNRS Research Scientist hosted at:
  • ENS Cachan (2007-2016)
  • IRISA (Rennes) from September 2016
Research project

Verifying security protocols: a difficult task

▶ testing their resilience against well-known attacks is not sufficient;
▶ manual security analysis is error-prone.

→ Caution: Do not underestimate your opponents!
Verifying security protocols: a difficult task

- testing their resilience against well-known attacks is not sufficient;
- manual security analysis is error-prone.

→ Caution: Do not underestimate your opponents!

Security

Defects in e-passports allow real-time tracking
This threat brought to you by RFID

The register - Jan. 2010

Privacy issue

Contactless card theft: Users warned to watch out for 'digital pickpockets'


Authentication issue
A successful approach: formal symbolic verification

→ provides a rigorous framework and automatic tools to analyse security protocols and find their flaws.

Main limitations of existing verification tools:

1. do not allow to take physical properties into account
   → transmission delay, location of participants, network topology

2. are not suitable to analyse privacy-type properties.
   → untraceability, anonymity, ...

→ two important features for analysing contactless systems!
A successful approach: formal symbolic verification

→ provides a rigorous framework and automatic tools to analyse security protocols and find their flaws.

Main limitations of existing verification tools:

1. do not allow to take physical properties into account
   → transmission delay, location of participants, network topology

2. are not suitable to analyse privacy-type properties.
   → untraceability, anonymity, . . .

→ two important features for analysing contactless systems!
Reasoning about **Physical properties** Of **security Protocols** with an Application To **contactless Systems**

Main issues:
- specificities of contactless systems are not well understood;
- a lack of **formal model** to reason about these systems.

Main outcomes:
- solid **foundations** to reason about **physical properties**;
- new **algorithms** and **tools** to analyse the security and **privacy** of modern protocols;
- make the upcoming generation of **nomadic contactless devices** more secure.