

PRIVATICS

Privacy Models, Architectures and Tools for the Information Society

INRIA

Grenoble-Lyon

PRIVATICS

- A New INRIA Group about Online PRIVACY
- With members from PLANETE, LICIT and SWING Groups.

Permanent Staff

- Planete Group
 - Claude Castelluccia: applied. crypto, security, networking
 - Dali Kaafar: networking, security
 - Cedric Lauradoux: crypto., embedded systems
 - Vincent Roca: networking, systems, standardisation
- Licit Group
 - Daniel Le Métayer: formal methods, legal aspects
- Swing Group
 - Marine Minier: symmetric cryptography, security

Objectives

- Understanding Privacy
- Privacy Foundations
- Privacy-Preserving Systems

Understanding Privacy

What is Privacy?

- Abstract and subjective concept, hard to define
- Dependent on cultural issues
- A couple of popular definitions:
 - “The right to be let alone”
 - Focus on freedom from intrusion
 - “Informational self-determination”
 - Focus on control
- How do we formalize privacy properties in computer systems?

Understanding Privacy

- Understanding economic and socio-economic aspects
- Understanding legal aspects
- Understanding privacy leakage and attacks in IT systems (in OSN, mobiles, smart grid, profiling, re-identification, etc.)

Privacy Foundations

- Privacy metrics :
 - privacy definitions
 - What does privacy mean in different applications?
 - In geolocalisation systems, location is one of the metrics!
 - Quantification
 - How do we measure this privacy violation?
 - In geo-systems, it could be the geographical granularity (street, city, region,...)
- Privacy models :
 - Attacker model
 - Privacy model
 - differential privacy, k-anonymity, ...?
- Risk analysis/Certification :
 - Can we define a methodology to assess privacy levels (as done in Security)?

Building Privacy-Preserving Systems

- Architecture of privacy : privacy by design (Ex. OCN, EphPub)
 - Principles / Methodology
 - Experimentations / Validation
- PETs / building blocks privacy preserving algorithms
 - applied crypto
 - Anonymization
 - Sanitization..