ARTIST2 – Year 1 Review

Grenoble, October 3rd-4th, 2005

Activity *NoE Integration*

Verification of Security Properties

Activity leader : Yassine Lakhnech (Verimag)

Outline of the Presentation

Industrial Needs and Experience

Year 1 Activities

- Achievements & Ongoing Work
- Interaction and Building Excellence Between Partners
- Management Perspective

18 Month Perspective

- Work planned for the next 18 months
- Significant events or achievements expected

Activity Partners

- Core members:
  - LSV ENS Cachan
  - Twente University
  - Aalborg University
  - Verimag
  - France Telecom R&D
- Affiliated members:
  - LORIA-Nancy
  - Trusted Logic
  - SchlumbergerCP8 (Axalto)

Industrial Needs and Experience

- The design of secure embedded systems is difficult:
  - Complex behavior: Concurrency, Cryptography (pseudo-random number generators, public cryptography, signature,…)
  - Complex properties: not safety properties, e.g. information flow
  - Active malicious attackers: Cover channels, Logical attacks, DPA attacks, Physical attacks

Some spectacular attacks:

- Visa Security Module, Ross Anderson 2000
- IBM 4758 Common Cryptographic Architecture, Mike Bond 2001, 2005
- RSA PKCS#11: Cryptographic Token Interface standard, Jolyon Clulow 2003

Industrial Needs and Experience

❑Scalable Testing & Verification methods and tools.

❑Practical integrating of T&V methods and tools into existing practice.

❑Development of design and specification formalisms suitable for security systems.

❑Certification of secure applications according to the Common Criteria.

- During the first year, we focus on:
  - Security protocols: The main component in any embedded security system-France Telecom R&D
  - Common Criteria compliant Certification: a strong argument for product differentiation- Trusted Logic, SchlumbergerCP8

Year 1 activities

Achievements & Ongoing Work-Verification of security Protocols

- A common language for security protocols and their properties
- A set of complement tools for the validation of security protocols: some are efficient in finding attacks, some are efficient in proving absence of attacks, different cryptographic primitives considered
  - More realistic cryptographic assumptions: Security protocols with time stamps, Algebraic properties of cryptographic primitives, The link between the formal and computational models
  - SPORe: A Security Protocols Open Repository (link)
- On going work:
  - Integration of verification tools: common language for attacks
  - Security for mobile code and systems
  - Trust management
  - Industrial case studies: electronic purse protocol

Year 1 activities

Achievements & Ongoing Work-Certification Methodology

- A methodology for certification at the EAL6 and EAL7
  - A refinement based development - formal models and proofs
  - UML-notation model, Tools for model extraction, refinement proofs using model-checking tools
  - Collaboration with an evaluation body (CEA-LETI), with an industrial tool editor (Trusted Logic) and a Smart Card Applications editor (Axalto)
- Ongoing Work
  - Setting-up a project for:
    - Certifying an application at the EAL7
    - Integrating the methodology into Trusted Logic's tool suite
  - A patent is under study

Year 1 activities

Interaction & Building Excellence

- Interaction Between Partners
  - A close collaboration between LSV, Verimag, FT R&D and LORIA on the security protocols – in the near future Aalborg and Twente
  - A close collaboration between Verimag, Trusted Logic and Axalto on certification-Should include other partners
- Building Excellence
  - A substantial effort has been spent in bringing together the cryptography and formal methods.
  - International Workshop on the Link between the Formal and Computational Model for Security Protocols (70 participants), June 2005
    - Organized with Microsoft Research (Cambridge), Univ. of Santa Curz (M. Abadi)
  - A spring school on Security, April 2005
  - A master on Cryptology, Coding and Information Security

18 Month Perspective

Work Planned for the next 18 months

- An integrated tool set for the validation of security protocols
- Industrial case studies – electronic purse, e-voting
- A tool set for EAL7 certification with proof of concept
- First results on the validation of APIs of cryptographic processors and libraries
- Access control validation for mobile code

18 Month Perspective

Significant Events or Achievements Expected

- International Workshop on the link between the formal and complexity-theoretic models of security protocols
  - June 2005: 70 participants, 22 speakers
- A school on Testing, Verification and Security of Embedded Systems