ARTIST 2

Network of Excellence

IST-004527 ARTIST2:
Embedded Systems Design

Activity Progress Report for Year 1

JPRA-Cluster Integration:

Verification of Security Properties

Activity Leader:

Yassine Lakhnech (Verimag)

Focus and align research in the area, with an emphasis on security for smart cards, e-commerce, and cell phones. Establish coherent links between research and industry.

Develop the basic technology needed to certify security applications at levels EAL6, and EAL7, from the Common Criteria.

Create the necessary critical mass for moving the state security technologies forward for embedded systems in Europe. This implies taking the next steps towards a ubiquitous, tight, and fluid security infrastructure for the area.

Table of Contents

1. Introduction

1.1 Activity Leader

Team Leader: Yassine Lakhnech (Verimag)
Areas of his team's expertise: semantics and models for security protocols.

1.2 Policy Objective

Focus and align research in the area, with an emphasis on security for smart cards, e-commerce, and cell phones. Establish coherent links between research and industry.

Develop the basic technology needed to certify security applications at levels EAL6, and EAL7, from the Common Criteria.

Create the necessary critical mass for moving the state security technologies forward for embedded systems in Europe. This implies taking the next steps towards a ubiquitous, tight, and fluid security infrastructure for the area.

1.3 Industrial Sectors

These include Smart cards, telecommunications, e-commerce, e-voting, consumer electronics.

As embedded systems within consumer electronics and communication tend to be more and more complex, integrating an increasing number of functionality, there is a trend towards increasing functionality on Smart Cards (eg: multi-function cards carrying health, insurance, identity, retailer fidelity, telecommunications, driver’s license, and banking information). In this context, confidentiality and integrity issues concerning the data on these cards becomes a critical issue for consumers.

E-voting and more generally e-democracy issues are related to the voting infrastructure, and to the need to provide guarentees for voters concerning preserving privacy, and accuracy of the vote count.

Concerning consumer electronics, there is a need for ensuring security properties, such as digital rights management and copy protection schemes.

The impact of the research performed will provide validation methods and tools that support the design of secure systems. Information security is a key issue for these industrial sectors.

2. Overview of the Activity

2.1 Artist2 Participants and roles

Team Leader: Hans Hüttel (BRICS/Aalborg)
Areas of his team's expertise: process algebra and security, mobile code, modelling and verification.

Team Leader: Pieter Hartel (Twente)
Areas of his team's expertise: java card, modelling and verification.

Team Leader: Jean-François Raskin (Centre Fédéré de Verification)
Areas of his team's expertise: e-commerce, protocols, modelling and analysis.

Team Leader: Hubert Comon (LSV)
Areas of his team's expertise: security protocols, logics.

Team Leader: F. Klay (FTR&D)
Areas of his team's expertise: Formal methods applied to security protocols.

2.2 Affiliated partners and Roles

2.2.1 Academic

Team Leader: Andrea Bondavalli (University of Firenze)
Areas of his team's expertise: competency.

Team Leader: Michael Rusinowitch (INRIA)
Areas of his team's expertise: proofs, and protocols.

2.2.2 Industrial

Boutheina Chetali (SchlumbergerSema: smart cards)

Daniel LeMetayer (Trusted Logics: secure components, smart cards)

2.3 Starting date, and expected ending date

September 1st, 2004 to September 1st 2005

2.4 Baseline

Ensuring data integrity, confidentiality and other security related properties is a key issue in many embedded systems with smart cards perhaps being the most prominent example. Security requires dedicated algorithms, methods and tools. For embedded systems -- having limited resources and being costly to patch -- efficiency and correctness are key issues that must be addressed. Today there is a lack of well-established methodologies, languages and tools for verifying embedded security protocols. The situation is even worse when it comes to certification (due to the huge costs).

The teams involved are conducting substantial research in this field as witnessed by their participation in many important national and international projects in the field. The consortium brings complementary expertise ranging from development of smart cards technology to mathematical formalisms for modelling and analyzing security issues.

Collaboration exists between France Telecom, INRIA, SchlumbergerSema, and the University of Twente in the framework of the FP5 Roadmap project RESET.

Verimag, France Telecom, LSV, LIM, Trusted Logic, and LORIA/CASSIS already cooperate in several national-level projects (EVA, PROUVE, ROSSIGNOL). All three revolve around modelling and analysis of security protocols.

Verimag, Trusted Logic and Schlumberger cooperate in a French national project (EDEN), for developing certification technology for smart card applications.

2.5 Technical Description

The technical objective is to develop dedicated, rigorous specification languages for security protocols and their properties. Development of automated for analyzing security protocols. Transfer and share results and know-how between academia and industry. In particular, we develop a common language and semantic framewrok fro describing security protocols. This common language will be used as a common platform for combining different validation tools each having specific, complementary strengths.

3. Activity Progress Report

3.1 *Work achieved in the first 6 months*

Over the first 6 months:

- We have developed a classification and studied the relation between different existing specification methods (multiset rewriting and process algebra) for security protocols.
- We used standard model-checkers for analysing various security protocols (e.g. use of muCRL, SPIN and CADP) and for addressing security treats based on real-time issues (using UPPAAL).
- We studied the expressive power of a process calculus that allows one to express arbitrarily many runs of ping-pong protocol thanks to the presence of recursive definitions. We have established a number of decidability results that indicate the limitations of automatic verification even in this simple setting. Most prominently, we show that our process calculus is Turing-powerful.
- We developed a common language for describing security protocols and their porperties.
- A publicly available database of security protocols and their analysis (attacks, proofs, assumptions/properties,...) has been developed http://www.lsv.ens-cachan.fr/spore/ .

3.2 *Work achieved in months 6-12*

During the first year the following results has been obtained:

- a general verification method for security protocols that can handle unbounded sessions, unbounded message size and unbounded fresh nonce creations;
- a sound and complete inference system for bounded-sessions cryptographic protocols (the messages size is still unbounded), method that has been extended to take into account protocols that can use timestamps;
- a proof that the Dolev-Yao model is a sound abstraction of the complexity theoretic model for protocols that combine several cryptographic primitives.
- We consider the problem of access control for the Calculus of Mobile Resources due to Godskesen, Hildebrandt, and Sassone. We establish a type system that lets us establish security policies for processes and show that our type system satisfies the usual requirements of type preservation under reduction and safety (i.e. that well-typed processes cannot misbehave.) Moreover, we present a sound type inference algorithm that will let us extract minimal security policies.
- We have worked on a protocol for an electronic purse provided by France Telecom. We specified the protocol and the common language as well as its properties and conducted a first set of validation experiments showing a potential attack.

3.3 Recommendations

It would be most beneficial to include other teams working on security, but not from a perspective of verification. For instance, additional partners could include teams working on cryptographic processors and architectures for security, but also teams working on physical attacks on secure infrastructures.

As action leader, I would like to strengthen ties with the other partners in the future. In particular, encourage PhD student exchange.

3.4 Milestones

- A toolset for the verification of security protocols, available via the internet.
- The thorough study of the electronic purse case example.
- A prototype tool for certification that targets the highest level of the CommonCriteria.
- Integration of the certification methodology in TrustedLgic's tool suite.
- A common semantic framework for Trust management.

3.5 Main Funding

Main sources of funding are

FP5 Roadmap project RESET

French National Programmes

IST-2000-26410 AVISS (Automated Verification of Infinite State Systems)

French national projects PROUVE, ROSSIGNOL

Various national funds and centres, such as:

- ❖ the Centre for Embedded Systems,
- ❖ CISS (http://ciss.auc.dk/),
- ❖ BRICS (http://www.brics.dk/),

Ongoing EU projects, in particular SECURE: Secure Environments for Collaboration among Ubiquitous Roaming Entities IST Project: IST-2001-32486

(http://www.dsg.cs.tcd.ie/dynamic/?category_id=-30)

3.6 Indicators for Integration

A critical issue concerning the development of verification tools and their acceptance by non-expert users is the choice of the specification language. This issue is even more delicate for cryptographic protocols because of the semantic subtleties of these programs. Indeed, these are not only concurrent but they are run in presence of an active adversary that tries to break the protocol and they use cryptographic primitives whose semantics is defined by means of probabilistic Turing machines and probabilistic games. For instance, the behaviour of a protocol critically depends on the power that is given to the adversary. This for instance determines whether a static corruption model is considered or a dynamic one, what is the effect of a cooruption: does it leak only long-lived keys or also the whole state , etc.…

It is well-known (see for instance the proceeding of AsiaCrypt 2005) that protocol proved correct in one model are not correct in an other model. Thus, we consider that an important out come of the integration work could be an agreed on common specification language for describing security protocols and their properties including notions of "trust".

3.7 Evolution

Security Protocols:: After one year, we expect to have a reference model for security protocols.

After two years, we expect to have developed prototypes capable of performing automatic analysis of security protocols.

The long-term perspective is the development of standards for security protocols.

SamrtCard Certification:

We developed a certification methodology that targets the highest level of evaluation according to the CoomonCriteria, namely the level EAL7. We also implemented prototype tools and used them on toy case studies. Our objective for the next period is to integrate the methodology within the tools of TustedLogic and validate it on an industrial case study.

Trust Management:: In ubiquitous computing systems (aka smart surroundings), embedded devices are forced to work together. However, working together is only possible if the group members have a way of trusting each other and of sharing their resources in a way that complies e.g., to regulations and user's wishes. Trust is essential, not only for the working of the devices but also for the human acceptance of smart surroundings.

The technical objective is to develop a rigorous and enforceable model for the specification of security and trust policies of embedded systems. Long term target include the design and implementation of tools for the specification, the prototyping and the verification of distributed trust management policies for embedded systems.

During the first 12 months, we will focus on the definition of a common rigorous model for the specification of trust management policies for embedded system. Then, we will focus on the development of a high-level architecture for the implementation of the model previously defined. Finally, we will address the problem of the verification of distributed trust management policies.

4. Detailed Technical View

4.1 Brief State of the Art

Security engineering is about building systems to remain reliable despite the presence of malice errors. As a discipline, it studies and develops the tools and methods to design, implement and validate systems that guarantee security properties. Many security systems and in particular embedded systems have critical requirements. Their failure may cause serious economic damages (cash machines, electronic purse and other bank systems), endanger personal privacy (medical record systems), endanger the viability of whole business sectors (pay-tv), etc….

Within Artist2, the focus is on tools and methods needed to design embedded systems that guarantee security protocols. More specifically, the focus is on security protocols.

Security protocols are components used to guarantee reliability of communication between a system and its environment on one hand and between different parts of the system on the other hand. In fact, security protocols are at the heart of any information security systems. To quote Ross Anderson: “”If security engineering has a unifying theme, it is the study of security protocols.”” To better understand this statement, notice that a typical security system involves a number of principals such as people, companies, computers or as in the case of embedded systems cellular phones, PDAs, Automatic Teller Machines (ATMs), smartcards, magnetic card readers, embedded crypto-processors, etc…. These principals communicate using a variety of channels in order to exchange messages, and authenticate other principals. Security protocols are the rules that govern these communications. If you consider, for instance, cash machines then you will find plenty of protocols that specify how a cash machine interacts with customers, with the bank, with the network operator, how keys are distributed, etc… These protocols together with other security primitives should ensure complex global properties.

Security protocols should be designed to resist against malicious attackers that may alter data, impersonate identities, and even perform physical intrusive attacks. Altough, the description of such protocols is usually short, it involves subtile semantics issues. Indeed, they can be seen as concurrent systems with dynamic process and fresh name creation that moreover use cryptographic primitives. Many pusblished protocols and standards have been shown to be flawed. Therefore, there is a need for developing methods and tools that help engineers design correct secutity protocols.

There are by now a number of efficient validation tools for authentication protocols, e.g., Hermes (Verimag), H1 (LSV), CASRUL (LORIA) mention tools developed by Artist2 partners.

Such validation tools have, however, not yet reached the level of maturity to be autonomously used by protocol designers. What is missing? A major obstacle is that these tools are based on a semantic model that is commonly called symbolic or Dolev-Yao model. This essentially means that cryptographic primitives are idealized and their behaviour is, hence, simplified.

This implies two problems: first we need to convince protocol designers that this idealization is justified, secondly we need to extend the semantic model to include more sophisticated cryptographic primitives such as blind signature, shared secret keys etc…, other properties such as non-repudation, fait signature etc.. and more generally we need to be able to handle protocols that go beyond authentication protocols.

Some of the partners have been intensively working on the first problem during the first year and have obtained interesting results . These results state that under reasonable cryptographic assumptions the symbolic semantic model is not an idealization but an abstraction in a rigorous sense such that validations performed in this model hold for the nore realictic cryptographic model. We have organized a workshop in june, entitled Workhsop on the link between formal and computational models with 70 participants and very prominent speakers around the world.

Many presentations were given by Artist2 partners.

Concerning the second problem, some Artist2 partners started considering :

- Protocols for e-voting (Verimag, LSV)
- Protocols for contract signing (LSV, Twente)
- Protocols and access control for mobile resources (Aalborg)

4.2 Industrial Needs and Experience

Ensuring security properties in general and developing methods for the design of security protocols has a deep impact on a large number of industrial sectors and societal concerns. We could mention consumer electronics, e-commerce and e-decmocracy such as e-voting.

To mention one example:

- **Consumer electronics**: The rapid transition from analogue to digital television is being driven by consumer demand for the very high-resolution, high-quality video that digital technology makes possible, as well as the promise of customized, interactive content and services. A major challenge is how to limit access to new content and services so that only paying subscribers can enjoy them. In the analogue broadcasting model, pay-TV content is most often protected by the use of proprietary set-top boxes, which connect to a television set to receive and descramble broadcast signals using encryption/decryption technology known as Conditional Access. A current trend using digital TV is to use removable security components. A smart card inserted into the module authenticates the subscriber and authorizes the module to decrypt broadcast content. Removable security modules can be easily removed or exchanged to upgrade services or to switch to a different operator using a different Conditional Access system.

4.3 Ongoing Work in the Partner Institutions

Twente: The team at Twente is currently working on the security of web services, trust management. Web services security (WS-Security) provides basic means to secure SOAP traffic, one envelope at a time. For typical web services, however, using WS-Security independently for each message is rather inefficient; besides, it is often important to secure the integrity of a whole session, as well as each message. To this end, recent specifications provide further SOAP-level mechanisms: WS-SecureConversation introduces security contexts, which can be used to secure sessions between two parties. WS-Trust specifies how security contexts are issued and obtained. The group develops a semantics for the main mechanisms of WS-Trust and WS-SecureConversation, expressed as a library for TulaFale, a formal scripting language for security protocols. Then, typical protocols are modelled relying on these mechanisms. Moreover, their main security propertie are automatically proved.

LSV Cachan: The security team at LSV is working on elevating the perfect cryptography hypothesis for validating security protocols. This is done by considering sets of equations that model the behaviour of an encryption primitive. If for instance the xor operation is used in the considered protocol then equations formalising the properties are introduced to model the properties of this operation. In general, developing validation methods for protocols while taking into account such equations is a hard and challenging problem. It is on the other hand necessary to gain confidence in the obtained results.

Verimag: The security team at Verimag is further working on the validation of security protocols extending their methods and tool to cover e-voting and other protocols. It is also working on certification methodlogy compatible with the Common Criteria. This is an international standard for certified security applications. It defines requirements on the development as well as evaluation of the product under certification. In the United States, the NIST, the National Institute of Standards and Technology together with the NSA, the National Security Agency, are undertaking effort to define a national program for the evaluation of information technology products for conformance to the International Common Criteria. There are seven Evaluation Assurance Levels from EAL1 to EAL7 with increasing demand of formal specifications and proofs. At the highest, level formal proofs of refinement steps are required from the developer. Verimag is interested in what is called the ADV-class in the Common Criteria that defines requirements for the stepwise refinement of the application from the security policy specification. It has developed a methodology with tool support that allows efficient certification of applications at the EAL7.

FT R&D: Francis Klay is collaborating with protocol designers within FT R&D on two important case studies: a n electronic purse protocol and e-vote protocol. He is acting as an intermediate between the protocol designers and some of the other partners in Artist in the sense that he is spending a great anount of effort explaining the validation tools and methods developed by these partners.

4.4 Interaction, Building Excellence Between Partners

There is a strong collaboration between LSV, VERIMAG, LORIA and FT R&D on developing a tool set for the design of correct security protocols. An feature of in this tool set is that it is based on the same langage for describing security protocols and their properties. Moreover, the tools included in the tool set are based on different verification techniques such as approximated fixpoint computation, constraint solving with rewriting, logic programming and tree-automata. Each of these verification techniques has its own strong and weak points. While the tool based on constraint solving is very efficient when it comes to findinf attacks, this is less the case for proving absence of attacks and does not easily handle general protocols. On the other hand, the tool based on fixpoint computation allows to efficiently verify general protocols but as it has hard-wired abstract domains, it is more difficult to add new features such as taking into account eqautional theories. The tool based on logic programming on the other hand can handle observational equivalence based properties as well as reachability based properties. For putting together these tools, it was necessary to develop a common programming language for security protocols whose semantics is rigorously formulated and studied.

This interaction should be enlarged to other partners essentially Twente and Aalborg.

4.5 Spreading Excellence

The partners are very active on dessimation of their results to other research teams as well as to the industry at conferences and industrial seminars. They also organized a very successful internation workshop entitled Workhsop on the link between formal and computational models (http://www.loria.fr/~cortier/workshop.html) with 70 participants and very prominent speakers around the world. This workshop should in the future take place regularly.