This work is based on initial discussion carried out between S. Chaumette (LaBRI) , K. Markantonakis, K. Mayes (RHU) and D. Sauveron (XLIM).

Roadmap and challenges for a Multilevel Java Card Grid

Serge Chaumette and Jonathan Ouoba

LaBRI,
Equipe Systèmes et Objets Distribués

wistp'07
Workshop in Information Security Theory and Practices Smart Cards, Mobile and Ubiquitous Computing Systems

ABSTRACT

"The goal of the Multilevel Java Card Grid project is to explore new application domains, by extending to a mobile context based on mobile phones the possibilities offered by the original JavaCard Grid developed at LaBRI [...]"

S.Chaumette, K. Markantonakis, K. Mayes et D. Sauveron.

This project is therefore an extension of the Java Card Grid, defining a multilevel framework which could bring security and robustness in communications in a mobile environment."

PROBLEM

"How can we use the possibilities offered by Java Cards in terms of security in a ad hoc context integrating different wireless technologies (WIFI, Bluetooth, GSM, 3G). "

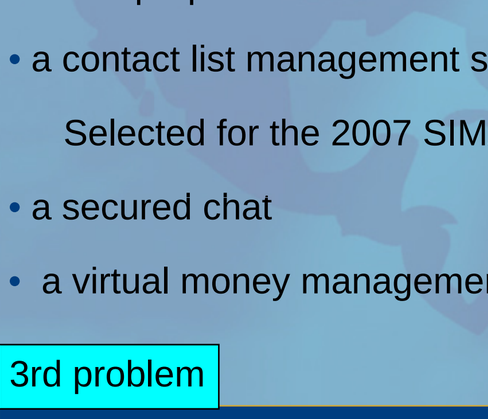
SOLUTION

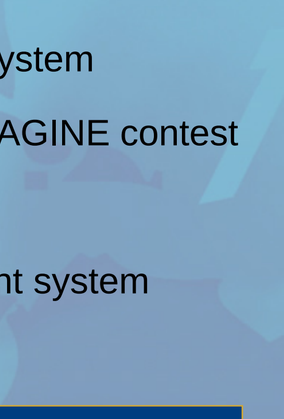
"A new framework, the Multilevel Java Card Grid, is proposed, that extends the existing Java Card Grid."

The Java Card Grid

The goal of the Java Card Grid project developed at LaBRI is to provide a secure hardware and software environment to experiment and thereafter propose innovative high level security solutions for distributed and mobile applications.

The Java Card Grid is a grid-like hardware platform composed of a number of Java Cards (readers) connected together through USB hubs.

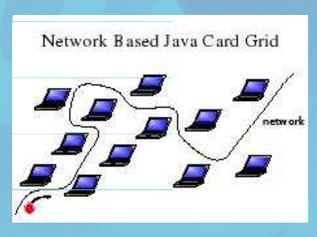




It received the "e-smart 2005 Isabelle Attali Award for the best innovative technology".

Variations of the Java Card Grid Platform

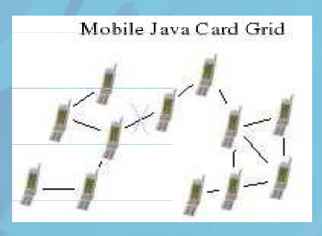
- Network based Java Card Grid
  Java cards over the network



University of Bordeaux
LaBRI Laboratory

Using INBRIA Proactive framework

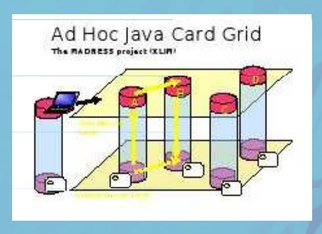
- Mobile Java Card Grid
  Java cards over mobile terminals with no infrastructure



University of Bordeaux
LaBRI Laboratory

(partly supported by the French Army DGA)

- Ad Hoc Java Card Grid

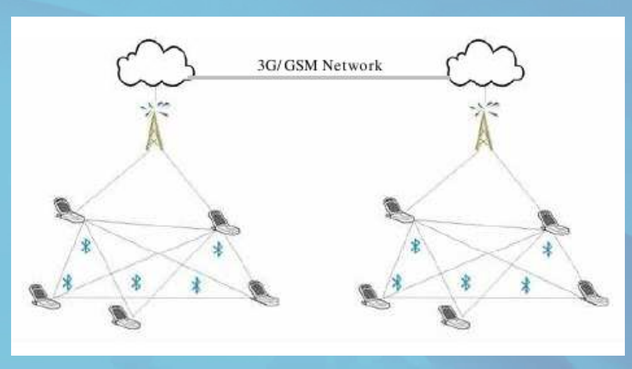


University of Limoges
XLIM Laboratory
MADNESS project

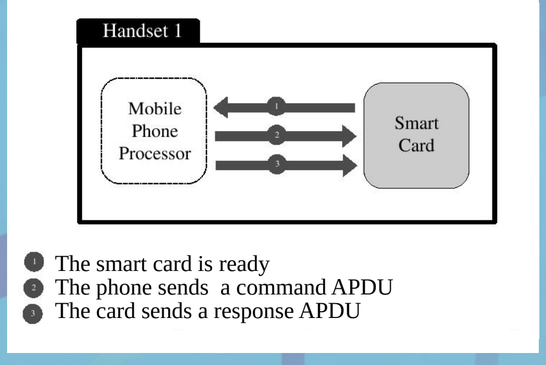
The Multilevel Java Card Grid

The multilevel grid will be composed of mobile phones embedding (U)SIM cards.

➔ phones support Bluetooth and/or Wi-Fi
➔ SIM cards support GSM/3G



Mobile phone / SIM communication



Target Applications

The following applications are being designed for the purpose of illustration

- a contact list management system
  Selected for the 2007 SIMAGINE contest
- a secured chat
- a virtual money management system

3rd problem

Application deployment

It has to be:

- Safe
- Global Platform compliant
- Bandwidth efficient or at least aware

solution — W.G. Sirett. *Temporally Aware Behavior-Based Security in Smart Cards.* Thesis, Royal Holloway University of London,septembre 2006.

1st problem

Communication Security

message confidentiality and authenticity must be guaranteed

solution — Experience of the original java card grid

Conclusion and future work

It is an innovative project that proposes effective applications that take advantage of the currently available communication technologies.

- The problems/solutions are identified
- The roadmap is almost defined

Next step is a proof of concept prototype.

2nd problem

Management of identities

It is important to ensure:

- the uniqueness of identities in the grid.
- the permanency of identities so that a device cannot deny its own identity.
- the mono-identity (one single identity per node)

solution — Eve Atallah, Serge Chaumette. *A Smart Card Based Distributed Identity Management Infrastructure for Mobile Ad hoc Networks.* WISTP 2007, Greece.

Additional References

E. Atallah, S. Chaumette, F. Darrigade, A. Karray et D. Sauveron. A Grid of Java Cards to Deal with Security Demanding Application Domains.

S. Chaumette, K. Markantonakis, K. Mayes et D. Sauveron. The Mobile Java Card Grid Project. e-Smart 2006. 20-22 septembre 2006, Nice, France.