

Security Research Issues for Sentinels

Bart Jacobs

bart@cs.kun.nl
www.cs.kun.nl/~bart.

Dep. Computer Science, Univ. Nijmegen, NL

Contents

- I. Overview (with Jaap-Henk Hoepman)
 - E-areas
 - Sentinels projects: focus & coordination
- II. Example: Java for mobile phones
 - MIDP
 - Certification project

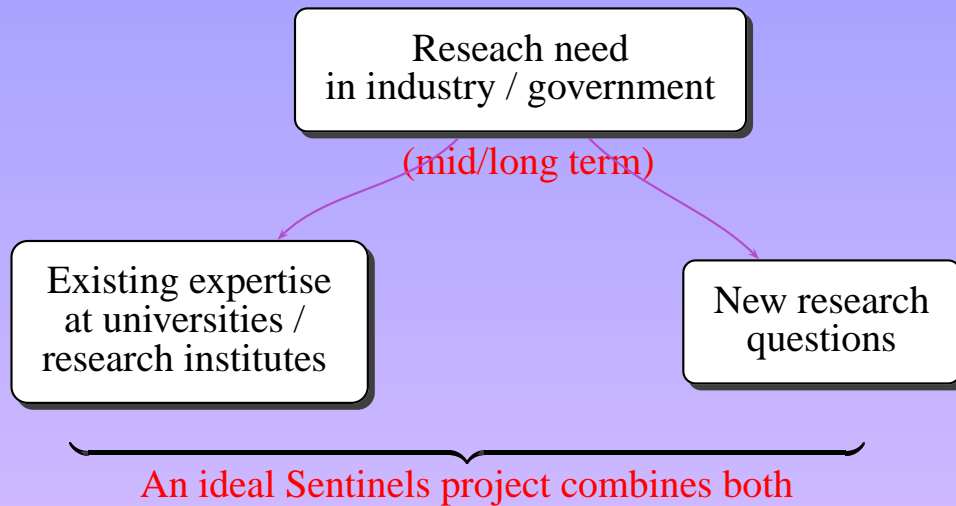
I. Research Issues & Projects

Your favourite e-area & security

- *e-living*: privacy protection by ambient devices
- *e-media*: content protection in consumer electronics
- *e-defence*: multi-level security & COTS components
- *e-health*: esp. privacy in multi-lateral security
- *e-business*: security of digital contracts
- *e-commerce*: authentication & payments
- *e-government*: authentication, voting, . . .

What can Sentinels do?

Focus & coordination



Security Research Issues for Sentinels (p.5 of 10)

Bleuprint for project (“Kiemkaart”)

1. Title of the project: ●●●
2. Explanation / background of the research questions: ●●●
3. Relevance for companies / government branches: ●●●
4. Which research institutes want to solve the problem: ●●●
5. What will be agreed: ●●●

Let's do it!

Security Research Issues for Sentinels (p.6 of 10)

II. Example: Java for mobile phones

Background

- Newest mobile phones support Java (J2ME), and Java applications may be downloaded.
(Note: they run in the phone, not in the SIM)
- Example applications:
 - single-player games: only I/O
 - multi-player games: network access
 - E-commerce: authentication, non-repudiation, ...
- Applications require different protection domains, as defined in open MIDP framework, see

<http://java.sun.com/products/midp>

- Demo ...

Security Research Issues for Sentinels (p.7 of 10)

Security Research Issues for Sentinels (p.8 of 10)

MIDP protection domains

- A protection domain is a set of *permissions*, regulating access to specific API functions (eg. for calling)
- A permission is either *Allowed* or *User*
- A “User” permission is either *blanket*, *session* or *one-shot*
- A downloaded application is bound to a protection domain, via authentication and signing based on a X.509 PKI.
- **Big question:** when is an application “safe enough” so that it can signed?

Sentinels project?

- **Title:** Certification of MIDP applications
- **Explanation:** see before
- **Companies:** Telco’s, TNO, . . .
- **Research institutes:** only Nijmegen can do this ;-)
- **Agreement:**
 - Nijmegen will adapt its program verification techniques to MIDP (involves research on . . .)
 - Telco’s will provide realistic examples, and offer consultancy support for . . . days, and feedback
 - TNO intends to incorporate the new techniques into its certification process, and will steer the development process (days + €’s).
 - Sentinels pays most of the bill!