

Security Research Issues for Sentinels

`www.sentinels.nl`

Jaap-Henk Hoepman, Bart Jacobs

Dep. Computer Science, University of Nijmegen,
`www.cs.kun.nl/~{jhh,bart}`

January 29, 2003

The goal of this short note is to explore some known security research issues, and to identify possibly other relevant areas for further research. It does not try to be complete and exhaustive. It is intended as a basis for discussion, and should in the end result in a broadly supported and focused view on the type of research that should be conducted in the next few years by universities and companies in the Netherlands, in order to obtain an internationally competitive position (with both impact and profit) in a knowledge-driven economy.

More concretely, the ideal outcome of the discussion is a mapping of identified industrial needs to either existing research expertise, or to concrete research questions that can be addressed within the Sentinels programme.

1 Analysis of existing security research issues

To set the scene for the discussion, several known security research issues for Dutch industry are presented in brief. At first the focus is on an application-based classification, which can be extended and refined in the discussion later on.

- e-living (aka Ambient systems)
When more and more intelligent devices embedded in household equipment start surrounding us, and more and more services collect and depend on personal user profiles, the protection of the privacy of the user becomes ever more important.
Several privacy enhancing technologies are known (e.g. pseudonyms, mixmaster style anonymous routing networks, Digicash style (semi)anonymous electronic money systems), but their practical applicability - especially when combined, e.g. paying by anonymous money and receiving the digital goods through anonymous remailers - remains to be determined.
- e-media (aka DRM)
Under strong pressure from the content industry, consumer electronics industry needs to implement content protection mechanisms to prevent copyright infringements. On the other hand, to sell their equipment to consumers, these protection mechanisms should not excessively restrict the functionality of the equipment (compared to current possibilities) and should not incur a large increase in price either.
Current DRM methods are quite restrictive in theory, but easily circumvented in practice. For the next generation of DRM more research is necessary into

new, less restrictive, models of digital rights management, and how these can be implemented onto consumer electronics devices cheaply, securely and reliably.

- e-defence

To reduce cost and decrease product development time, the defence industry would like to use commercial of the shelf (COTS) components as much as possible in the development of new products. The problem is that such components are generally believed to be less reliable and less secure. So the question is how to safely use COTS components and open-standards networks to build and interconnect military and emergency-services equipment, especially for multi-level security.

The solution to this question can partly be found into the application of formal methods to model the behaviour of these components, and the development of special, small, wrappers that encapsulate a component. This wrapper shields a component from the other components in the system and the other way around.

- e-health

How can we achieve the right combination of availability and protection of privacy sensitive data?

- e-business

Is it possible to foster trust and confidence in deals that are negotiated electronically? Apart from the major players in this field, there are about 19 million small and medium enterprises (SMEs) in the European common market poised to benefit...

- e-commerce

In this area the use of a public key infrastructure (PKI) or biometry for identification, authentication & access control is important.

Also, the issue of payment over the Internet is not resolved, especially where small amounts are concerned (e.g. micropayments). A related point is dispute resolution, especially wrt. various national legal systems

- e-government

International standardisation of e-travel documents, trust and confidence in e-voting

- ...

2 Determining other relevant security research issues

Based on the examples of research issues discussed in the previous section, we now aim to explore other security research questions that are particularly relevant for Dutch industry. To stimulate discussion, we present two other classifications of the field.

2.1 Precedence-based classification

- Before attack
 - predict (an attack might happen; e.g. risk/threat analysis)
 - prevent (stop an attack happening; e.g. remove incentive, legal repercussions, unavailability of means (e.g. gun control))
- during attack
 - detect (an attack is happening: e.g. intrusion detection systems)
 - protect (make sure an attack cannot happen: e.g. firewall, cryptography)
 - respond (strike off an attack: e.g. counteract, disconnect)
- after attack
 - audit (detect an attack has happened: e.g. monitoring)
 - repair (restore to state before attack)

2.2 Means-based classification

- organisational
- legal
- technical (with associated certification)
 - cryptography
 - security hardware: smart-cards & tokens
 - biometry
 - software engineering (e.g. operating system & database security)
 - formal verification

3 Questions for discussion

1. Which topics are of strategic interest for the ICT industry in the Netherlands?
2. Which research questions related to these topics need to be answered (and by whom)?
3. Which expertise is already available within universities, research institutes and companies, and which expertise needs to be developed further?