

Practices in Software Security

PhD dissertation
Yngve Espelid

University of Bergen



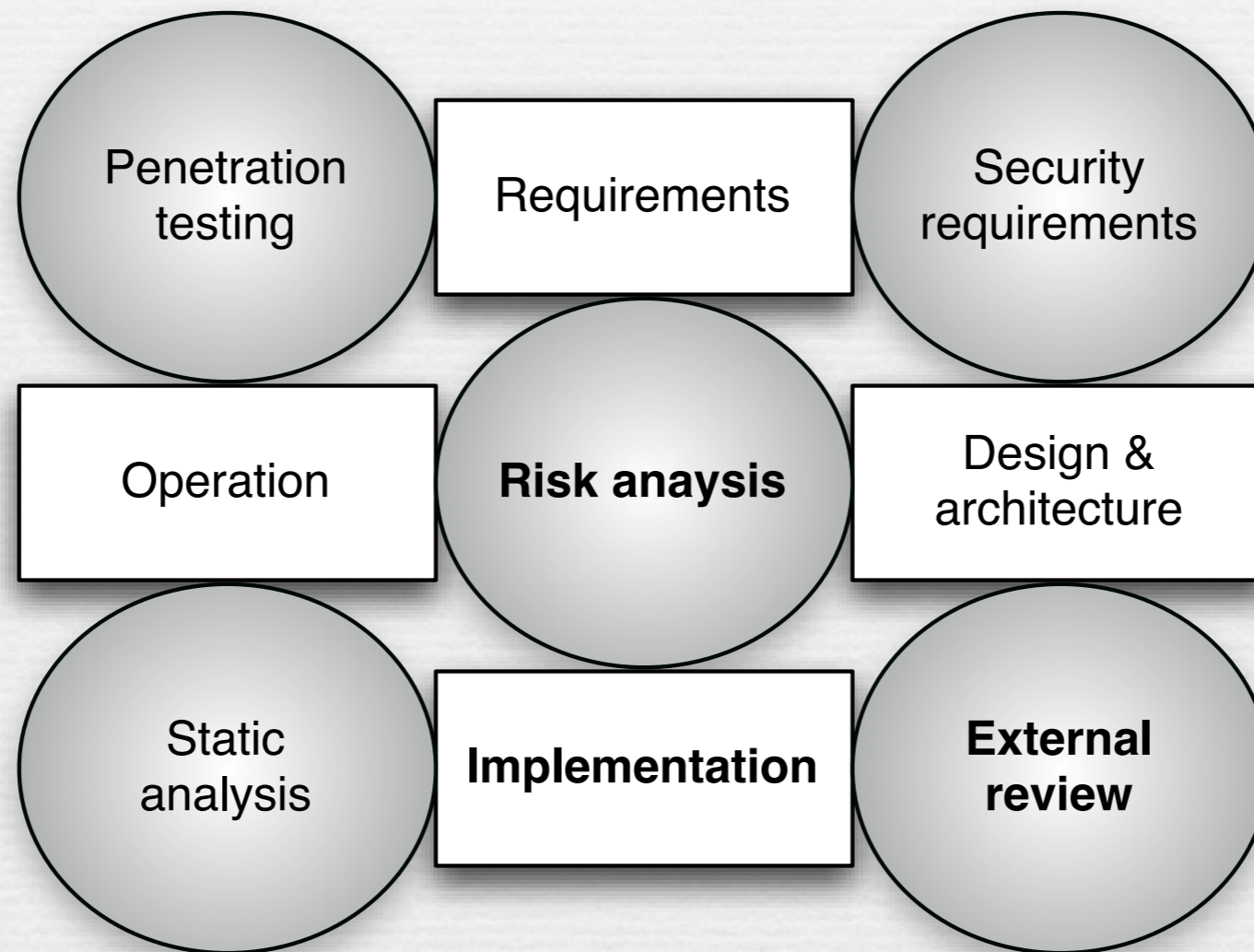
27th of March 2008

Software Security

- ◎ Main security goals
 - ◎ Confidentiality
 - ◎ Integrity
 - ◎ Availability
- ◎ ... the idea of engineering software so that it continues to function under malicious attack
G. McGraw, 2004 *

* "Software Security," *IEEE Security & Privacy*, vol. 2, no. 2, 2004

Software Development



Risk Analysis

- ◎ Secure enough
- ◎ A **risk** is a function of the level of threat, vulnerability, and the value of the information asset
- ◎ Continuous process

Paper I:
Next Generation Internet
Banking in Norway

K.J. Hole, T. Tjøstheim, V. Moen, L-H. Netland,
Y. Espelid, and A.N. Klingsheim

Submitted to *IEEE Security & Privacy*

Paper I: Next Generation Internet Banking in Norway

- ◎ **BankID:** a security infrastructure developed by the Norwegian banking industry
- ◎ Public-Key Infrastructure (PKI) with customers' keys stored on a central infrastructure
- ◎ 1 080 000 bank customers have BankIDs
- ◎ Aims to become a national ID infrastructure

Paper I: Next Generation Internet Banking in Norway

BankID entities

Infrastructure

Storage of customers' keys and certificates

OTP validation service
Signing service
Verification service

Customer

Birth number

OTP generator

Fixed password

Merchant

Locally stored keys and certificate

BankID server

Paper I: Next Generation Internet Banking in Norway

- ⊙ Main risks to **customers** using BankID
 - ⊙ Distributed denial-of-service attack at BankID's **application layer**
 - ⊙ **Interposition** (man-in-the-middle) attack exploiting vulnerabilities in the BankID authentication procedure
 - ⊙ No independent third party involved in the non-repudiation service

Paper II:
**Open Wireless University
Networks**

K.J. Hole, L-H. Netland, Y. Espelid, A.N. Klingsheim,
H. Helleseth, and J.B. Henriksen

Updated version to be published in
IEEE Security & Privacy, May/June 2008

Paper II: Open Wireless University Networks

- ⊙ Risk analysis for IT departments considering running open wireless university networks
- ⊙ Advantages
 - ⊙ Better learning environment, increased use of information resources, etc.
- ⊙ Risks
 - ⊙ Illegal downloads, attacks on local and remote networks, negative press coverage etc.

Risk Management

- ⊙ Understand business context
- ⊙ Identify risks
- ⊙ Rank risks
- ⊙ Define mitigation strategy
- ⊙ Follow strategy

External Review

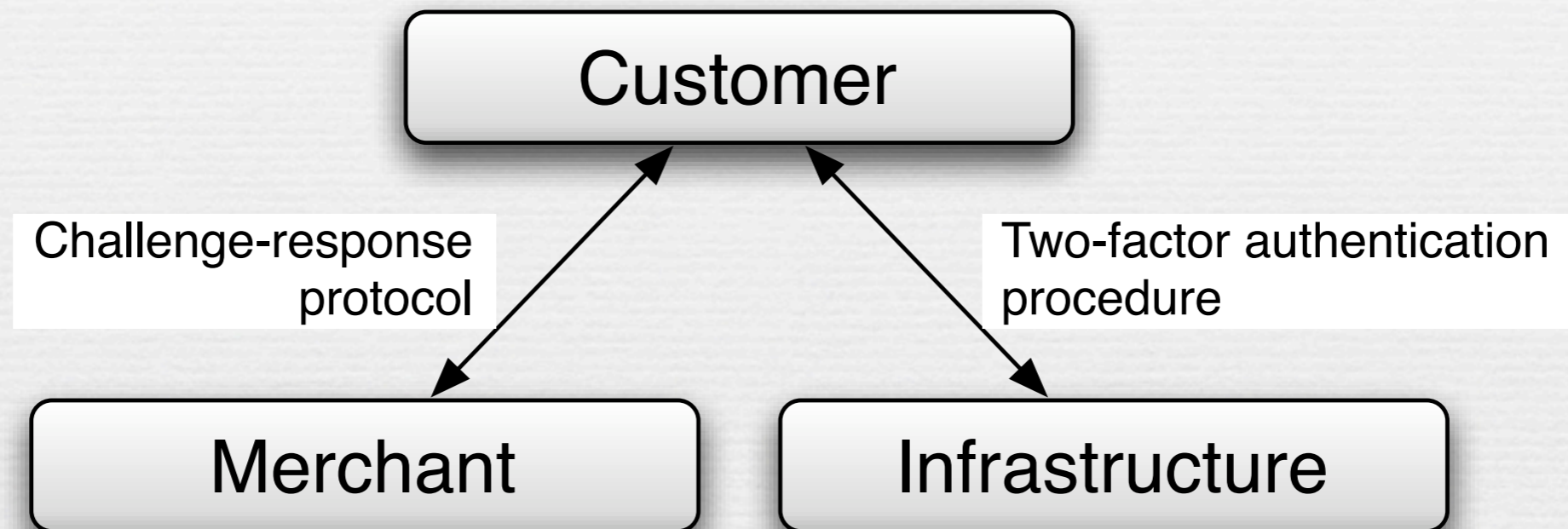
- ⊙ Having external experts review the system throughout its life cycle
- ⊙ Interposition attack:
BankID's authentication procedure
- ⊙ Red teaming
 - ⊙ from the attacker's viewpoint

Paper VI:
**A Proof of Concept Attack against
Norwegian Internet Banking
Systems**

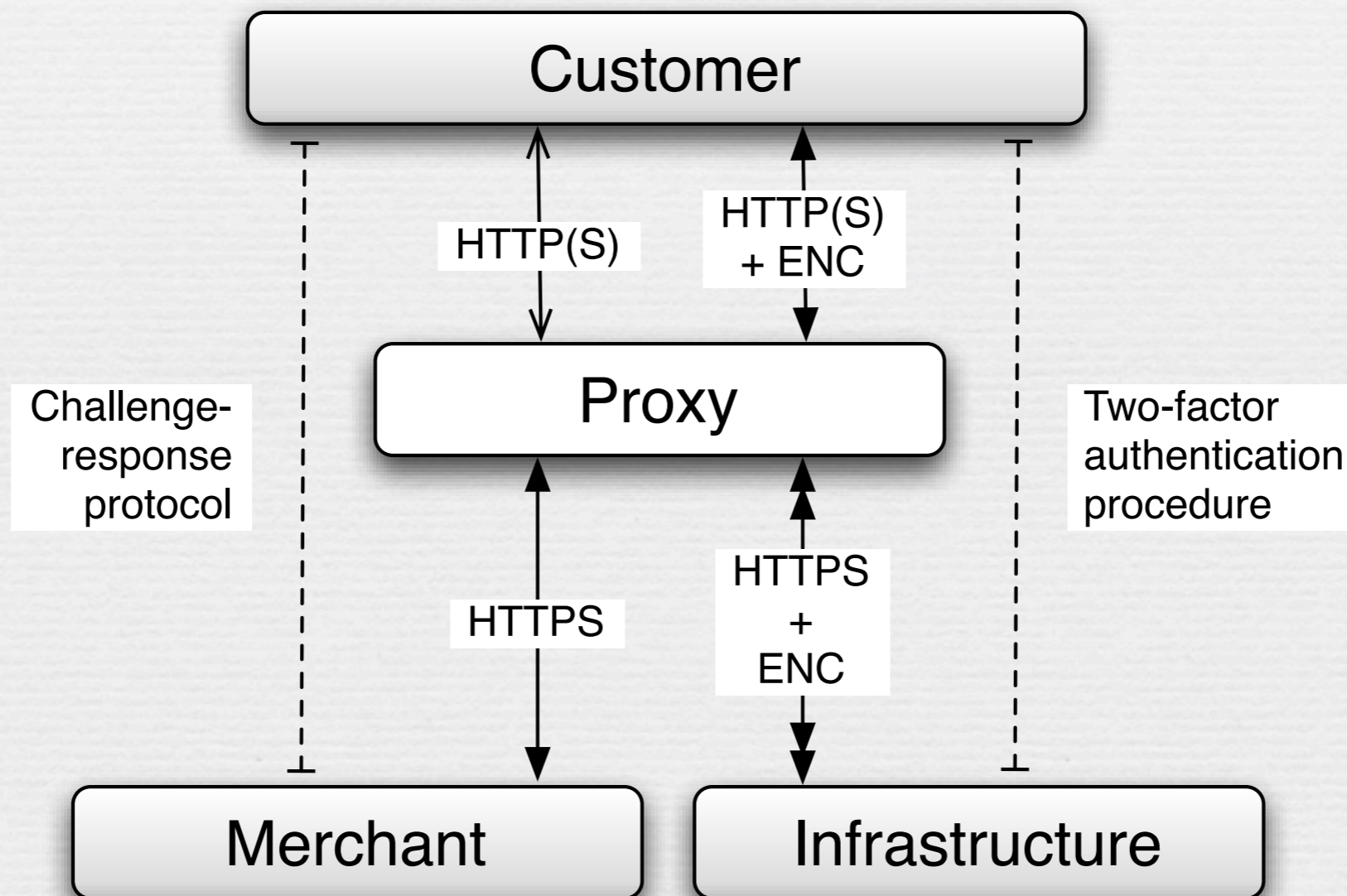
Y. Espelid, L-H. Netland, A.N. Klingsheim, and K.J. Hole

Published in *Proc. International Conference on Financial
Cryptography and Data Security (FC)*, January 2008

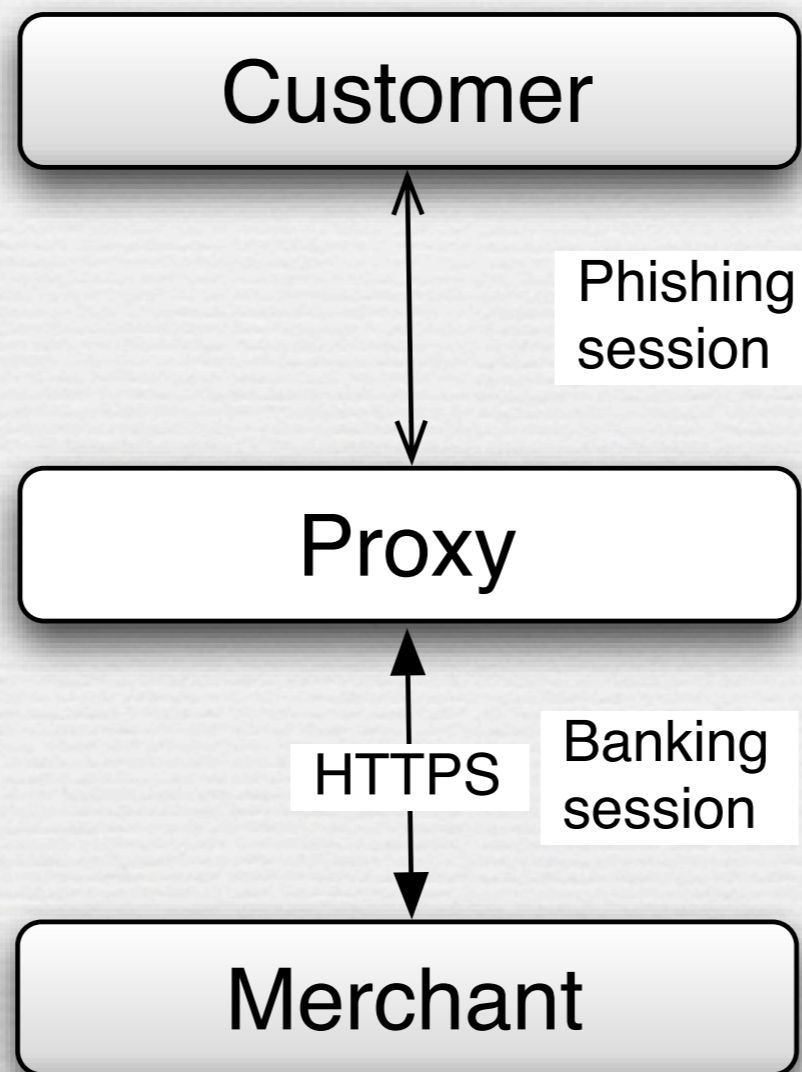
Paper VI: A Proof of Concept Attack against Norwegian Internet Banking Systems



Paper VI: A Proof of Concept Attack against Norwegian Internet Banking Systems



Paper VI: A Proof of Concept Attack against Norwegian Internet Banking Systems

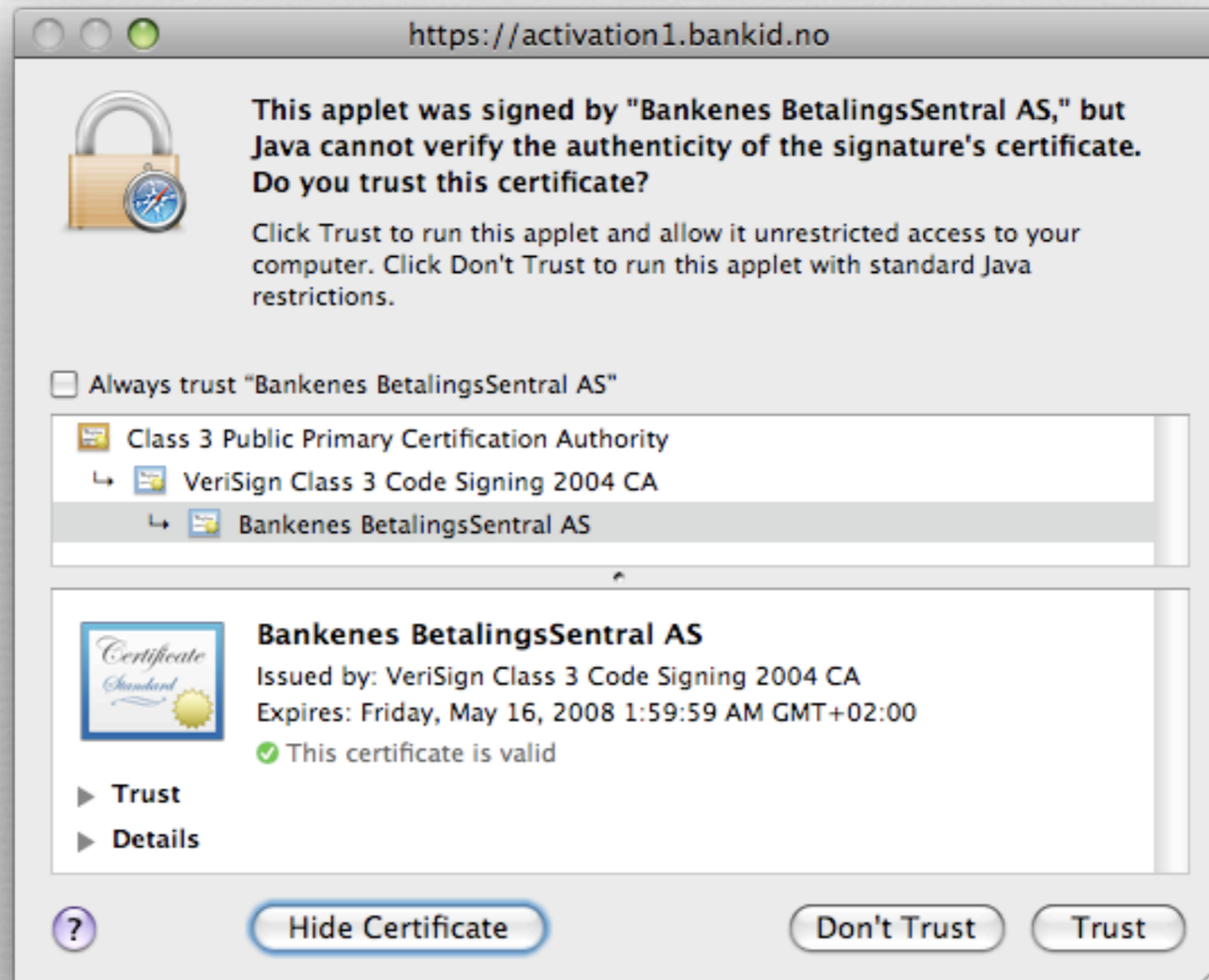


Paper VII:
**Robbing Banks with Their Own
Software—an Exploit against
Norwegian Online Banks**

Y. Espelid, L-H. Netland, A.N. Klingsheim, and K.J. Hole

To be presented at the *International Information Security Conference
(SEC 2008)*, September 2008

Paper VII: Robbing Banks with Their Own Software— an Exploit against Norwegian Online Bank



Paper VII: Robbing Banks with Their Own Software— an Exploit against Norwegian Online Bank

- ⊙ Building a detailed profile
 - ⊙ Using the system
 - ⊙ Reverse engineering the authentication protocol
 - ⊙ Reverse code engineering
- ⊙ Apply resources on the most rewarding places

Risk analysis of BankID

Our research results
discussed during a
Question Time session in the
Norwegian Parliament

Developed proof-of-concept attack

February
2007

Informed BSK, BSS, and FSAN

New countermeasures
introduced

March

Sent technical report to BSK

January
2008

May

Released interim report
(Paper I)

Disclosure Process

The attack was again
successfully run
using version rollback

December

Demonstration for FSAN

September

A November patch
on BankID addressed the
interposition attack

November

October

Demonstration for security
experts with influence on the
Norwegian banking industry

Told of the exploit in a
large Norwegian newspaper

Distributed early version of
papers (Paper VI and Paper VII)
to BSK, BBS, and the
BankID coordinator

Financial Supervisory Authority of Norway (FSAN)
Bankenes Standardiseringskontor (BSK)
The Norwegian Banks Payment and Clearing Centre (BBS)

Legality

- ◎ Responsible disclosure
(no “attack code” was published)
- ◎ The Data Inspectorate considers the research to be of importance for Norwegian citizens
5.12.2007, Computerworld, <http://www.idg.no/computerworld/article78059.ece>
- ◎ The Minister of Government Administration and Reform supports this type of research, and wants more...
7.12.2007, Computerworld, <http://www.idg.no/video/article78402.ece>

Implementation Challenges

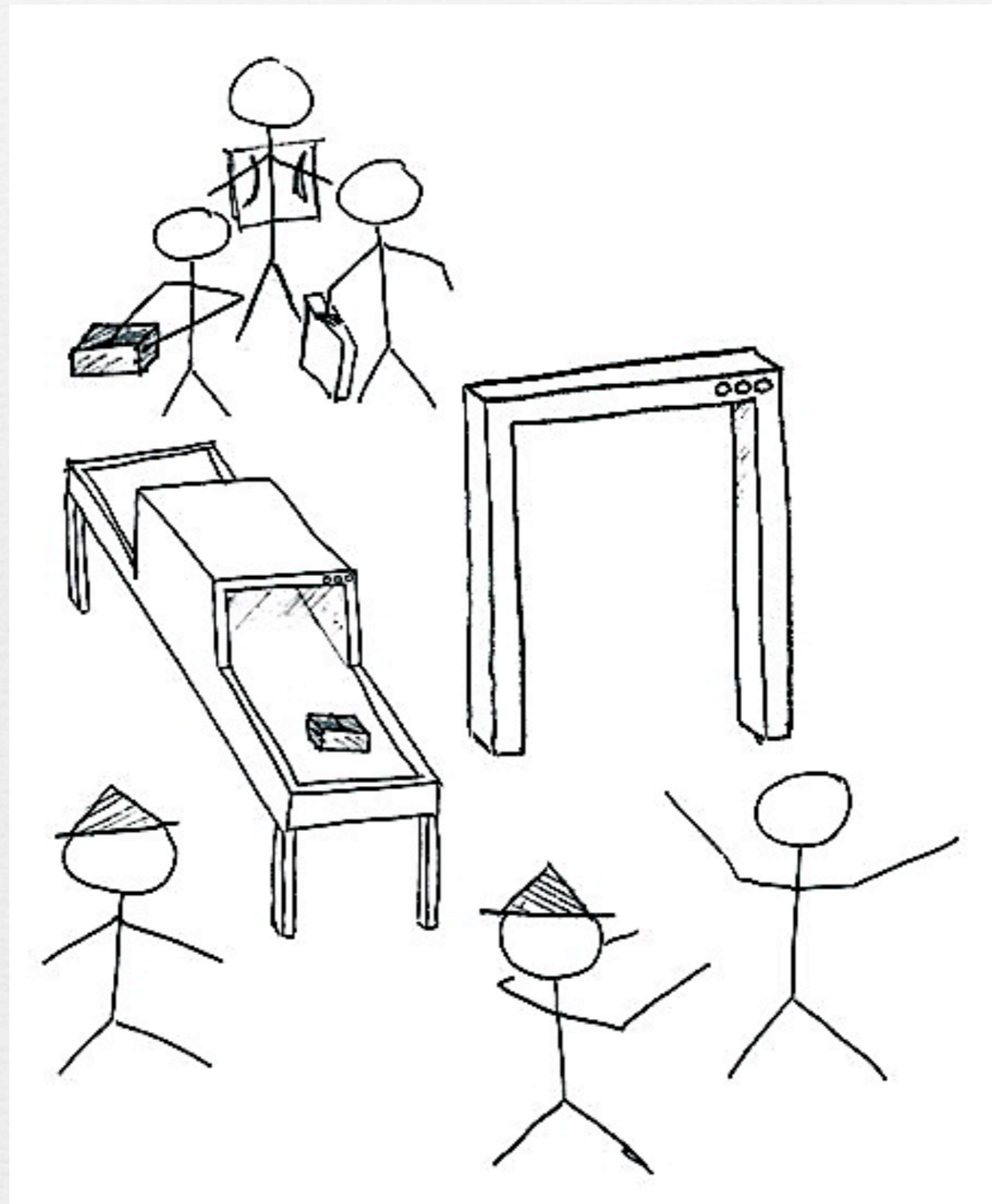
- ⊙ Trinity of trouble:
complexity, connectivity, and extensibility
- ⊙ Input validation
 - ⊙ Transfer of knowledge from security experts to developers using patterns (Paper III)
 - ⊙ Code reuse can reduce complexity (Paper IV)
 - ⊙ Developing solutions that can be quickly adjusted to meet change in requirements (Paper V)

Paper III:
Security Pattern for Input
Validation

L-H. Netland, Y. Espelid and K. Mughal

Published in *Proc. Nordic Pattern Languages of Program Conference
(VikingPLoP)*, Sept./Oct. 2006

Paper III: Security Pattern for Input Validation

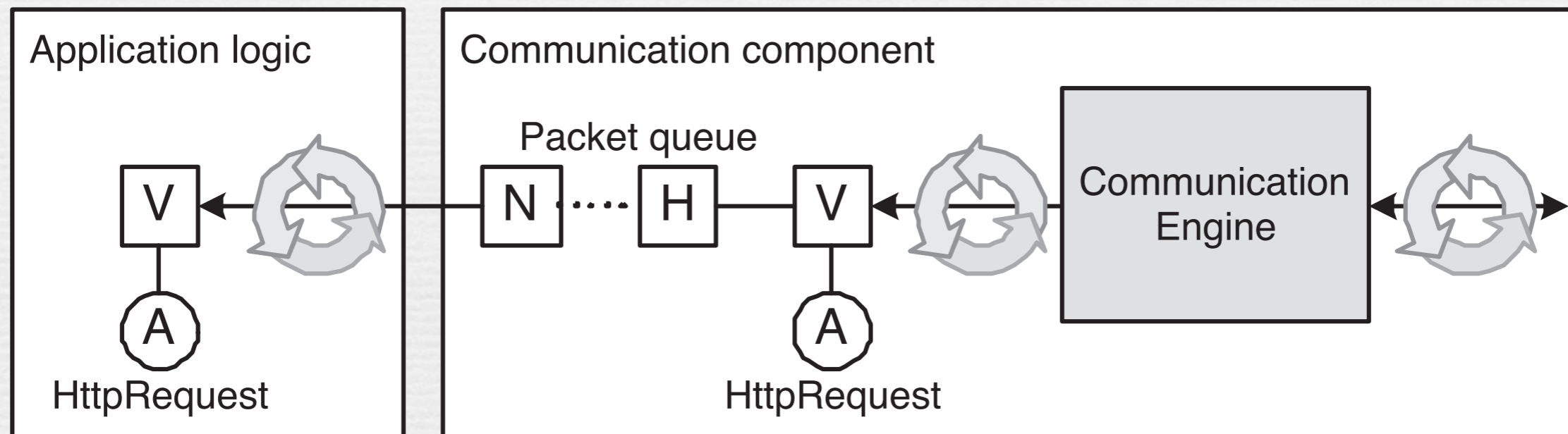


Paper IV:
Simplifying Client-Server
Application Development with
Secure Reusable Components

Y. Espelid, L-H. Netland, K. Mughal, and K.J. Hole

Published in *Proc. International Symposium on Secure Software
Engineering (ISSSE)*, March 2006

Paper IV: Simplifying Client-Server Application Development with Secure Reusable Components



H Handshake completed

N New client connection

V Valid client request

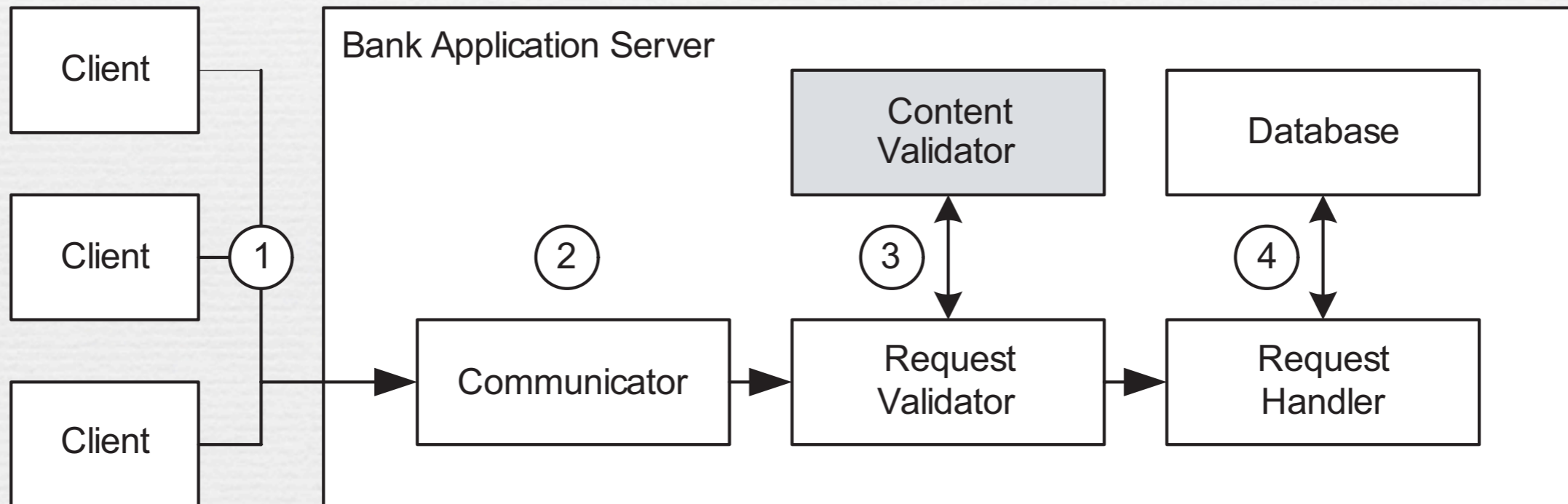
A Attachment

Paper V:
**A Reflection-Based Framework
for Content Validation**

L-H. Netland, Y. Espelid and K. Mughal

Published in *Proc. International Conference on Availability, Reliability,
and Security (ARES)*, March 2006

Paper V: A Reflection-Based Framework for Content Validation



Contributions

- ⊙ Risk analyses of
 - ⊙ BankID, and
 - ⊙ open wireless university networks
- ⊙ Two components/prototypes addressing implementation challenges
- ⊙ Proof-of-concept code demonstrating the seriousness of the interposition attack

Impacts

- ◎ Two patches inserted into BankID in Nov'07 and Jan'08
- ◎ Debate in media
- ◎ Increasing public awareness of software security
 - ◎ independent evaluation of candidates for a new national identity system

Dissertation and presentation available at



<http://www.nowires.org>