

Java Security

-an Infrastructure for Secure Client-Server
Communication



Lars-Helge Netland

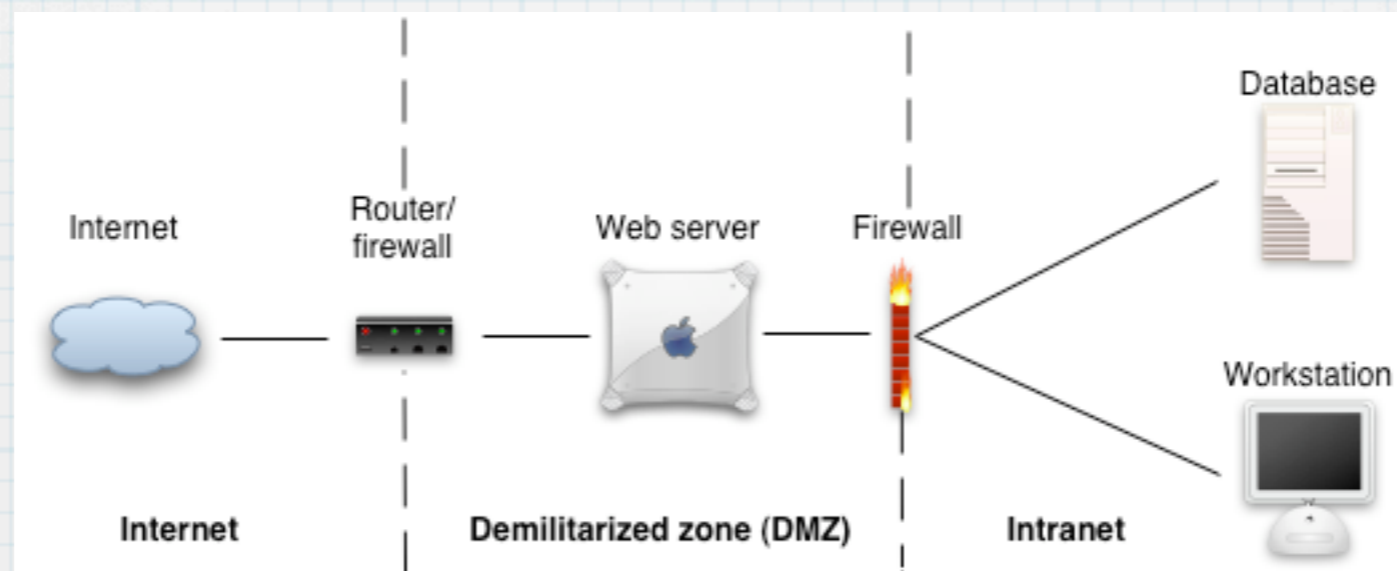
16th June 2005

Outline

- Introduction
- Security defined
- Internet banking
- Theoretical background
- Current deployments
- Implementations
- Summary and conclusions

Introduction

- Emphasis on functionality
 - Service oriented architectures
- Computer security = Network security
- Badly designed and implemented software



Cybercrime

- The bad guys are winning: total damage 2004 was a record \$17.5 billion (Computer Economics Inc.)
- HangUp team
 - “In Fraud We Trust”
- ShadowCrew
 - 4000 members worldwide
 - 19 people indicted

Security defined

- Holistic approach
- A set of non-functional goals
 - Prevention, traceability and auditing, monitoring, privacy and confidentiality, anonymity, authentication, and integrity
- The design and implementation of a foundation to build upon
 - Authentication, integrity, and confidentiality

Internet banking

- 2 million Norwegian users
- Interesting for both attackers and researchers
- Current initiative
 - BankID

The image displays two screenshots of a Norwegian internet banking login interface, presented as if on a clipboard. The top screenshot shows a standard login form with the title 'Pålogging'. It includes a 'Brukernavn' (Username) field with the text 'Username' and a 'Passord' (Password) field with seven asterisks. Below the fields are three buttons: 'Utfør', 'Avbryt', and 'Hjelp'. The bottom screenshot also has the title 'Pålogging' and includes a 'Tast inn sikkerhetskode 10:' field with four asterisks. Below this are fields for 'Serienummer' (00003717597) and 'Versjonsnummer' (1). It also features the same three buttons: 'Utfør', 'Avbryt', and 'Hjelp'.

Selmersenteret's research

- Weak authentication of clients
- Vulnerable to distributed DoS attacks joined with a brute-force PIN cracking scheme
- More information
 - "Security in Norwegian Internet banks," Kjell J. Hole et. al.

Current situation

- G. Sørensen on BankID in an interview with Dagbladet
- <http://www.dagbladet.no/dinside/2005/02/27/424662.html>
- BankID
 - Reluctant to disclose system details
 - Use Public Key Infrastructure (PKI) to provide services for society at large

Theoretical background

- Java
 - New Input/Output (NIO)
 - Cryptographic libraries
- PKI
- SSL

Java

- ◆ Java security fundamentals
- ◆ Crypto APIs
 - ◆ Java Cryptography Extension (JCE)
 - ◆ Java Authentication and Authorization Service (JAAS)
 - ◆ Java Secure Socket Extension (JSSE)

Java security fundamentals (1)

- ◆ Sandbox
 - ◆ Sensitive operations
 - ◆ Operations \leftrightarrow segments of code
 - ◆ A control center

Java security fundamentals (2)

- ◆ Example:

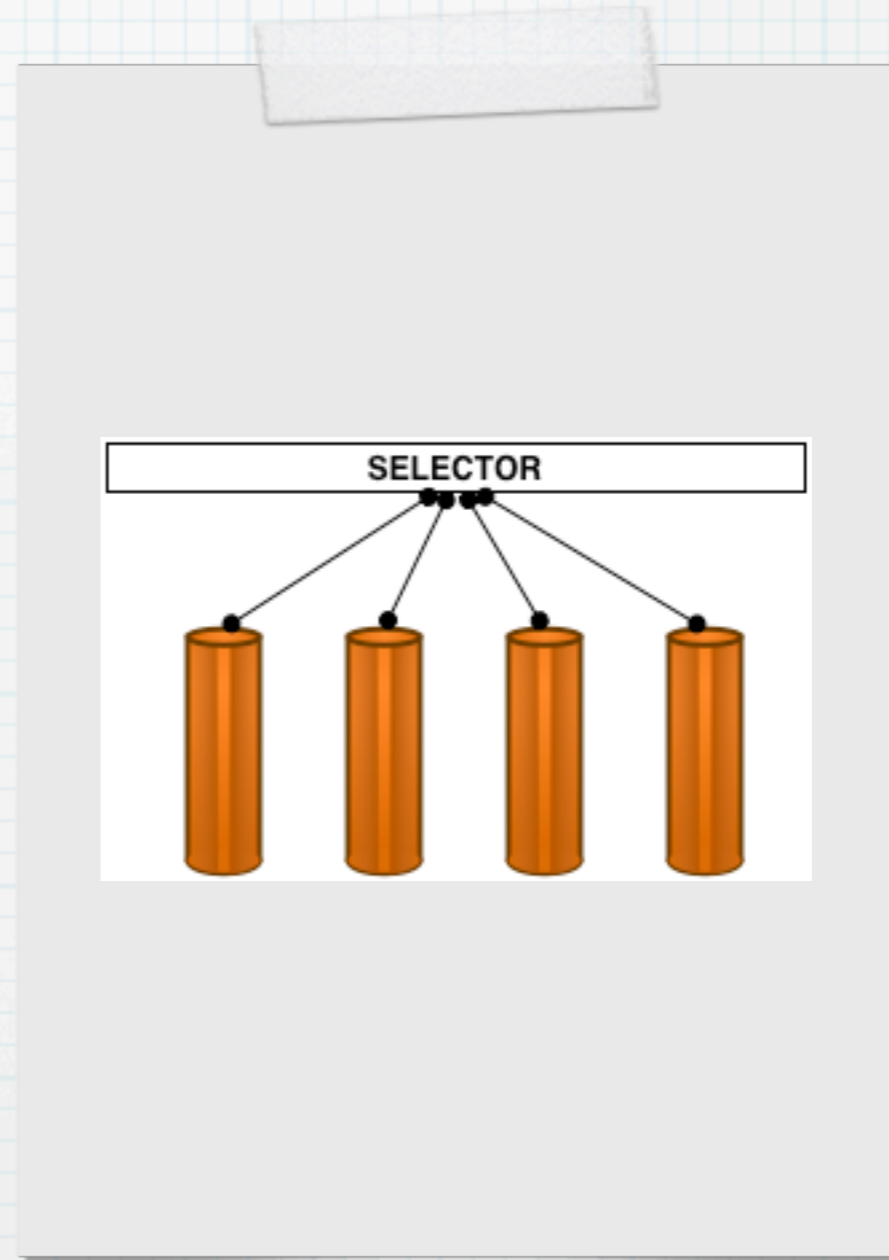
- ◆

```
grant codeBase "file:/safe/*" {  
    permission java.security.AllPermission;  
};
```

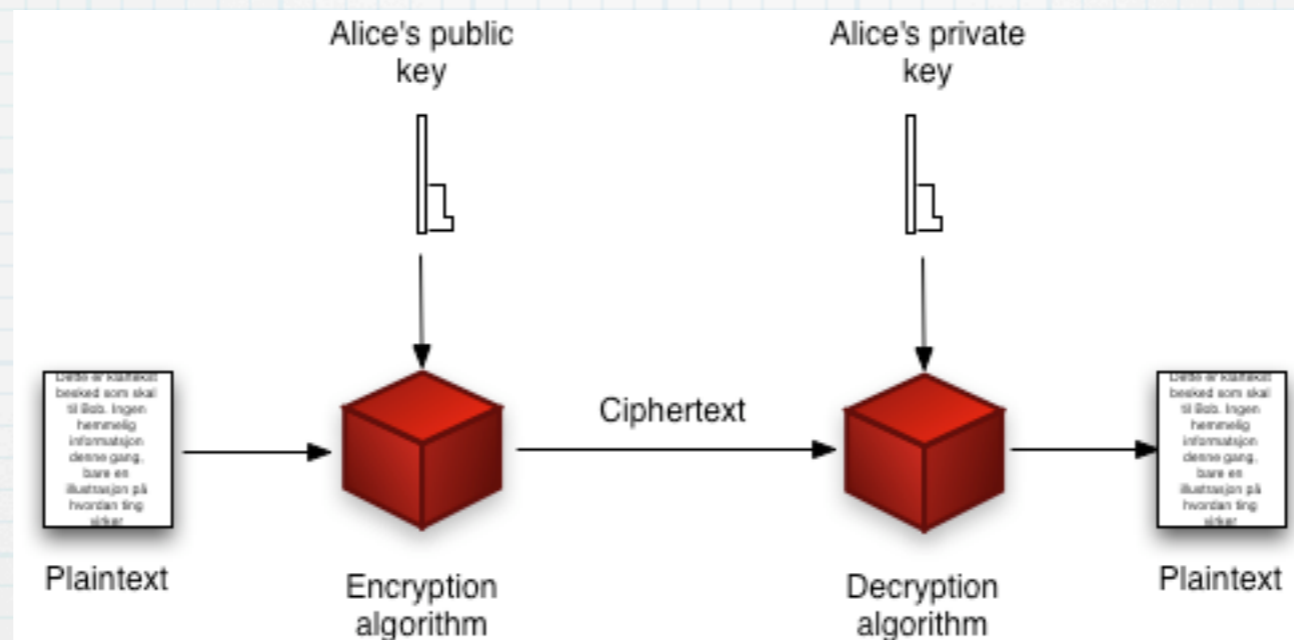
- ◆ Security checks performed by the access controller

NIO

- ◆ Enhanced I/O
- ◆ Readiness selection
- ◆ Selectors and channels



Public key cryptosystems



X509 certificate (1)

Subject

Issuer

Validity

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN) www.amazon.com
Organization (O) Amazon.com Inc.
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 0E:A5:09:3E:35:7E:74:DB:8A:D3:7D:44:83:20:F9:DD

Issued By

Common Name (CN) <Not Part Of Certificate>
Organization (O) RSA Data Security, Inc.
Organizational Unit (OU) Secure Server Certification Authority

Validity

Issued On 1/6/05
Expires On 1/7/06

Fingerprints

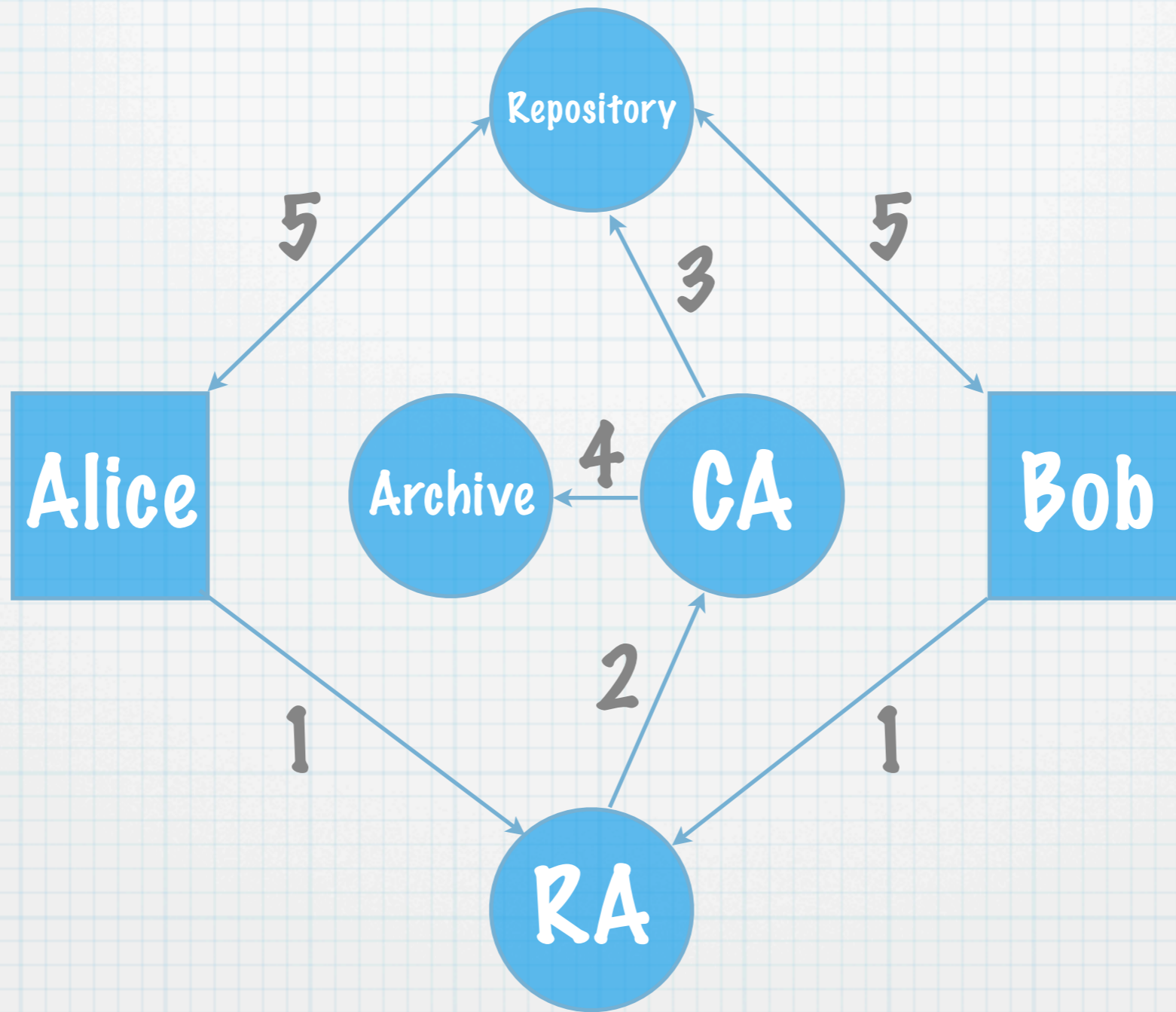
SHA1 Fingerprint 1E:52:BF:E8:3D:B2:7E:A2:B5:C2:A2:C7:B5:24:3B:5E:42:57:F9:81
MD5 Fingerprint B9:C1:B9:A3:40:3A:4A:93:A8:03:E8:78:1D:E3:9F:20

X509 certificate (2)

- ◆ **Public Key**
- ◆ **Serial number**
- ◆ **Digital signature**

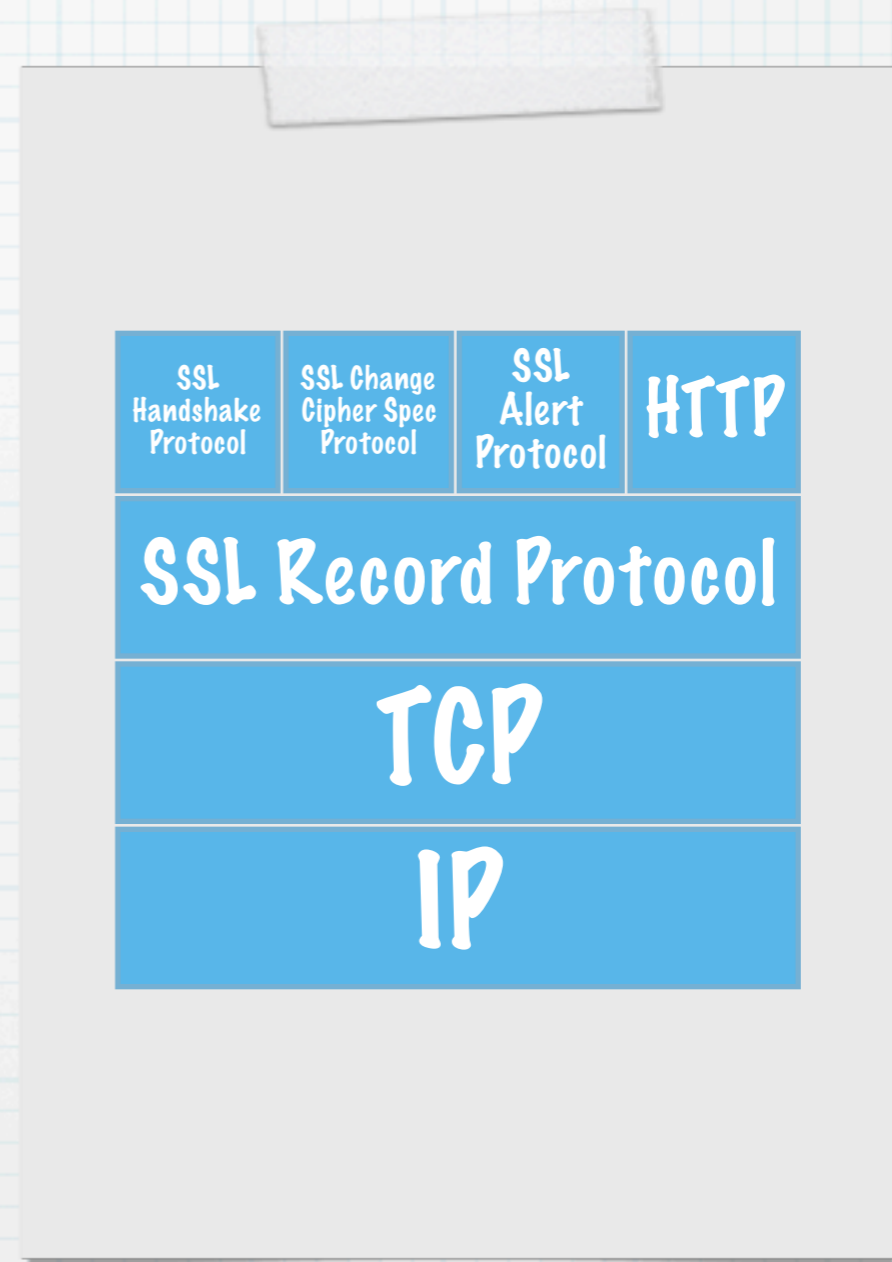
PKI components

- Certification Authority (CA)
- Registration Authority (RA)
- End users
- Repository
- Archive

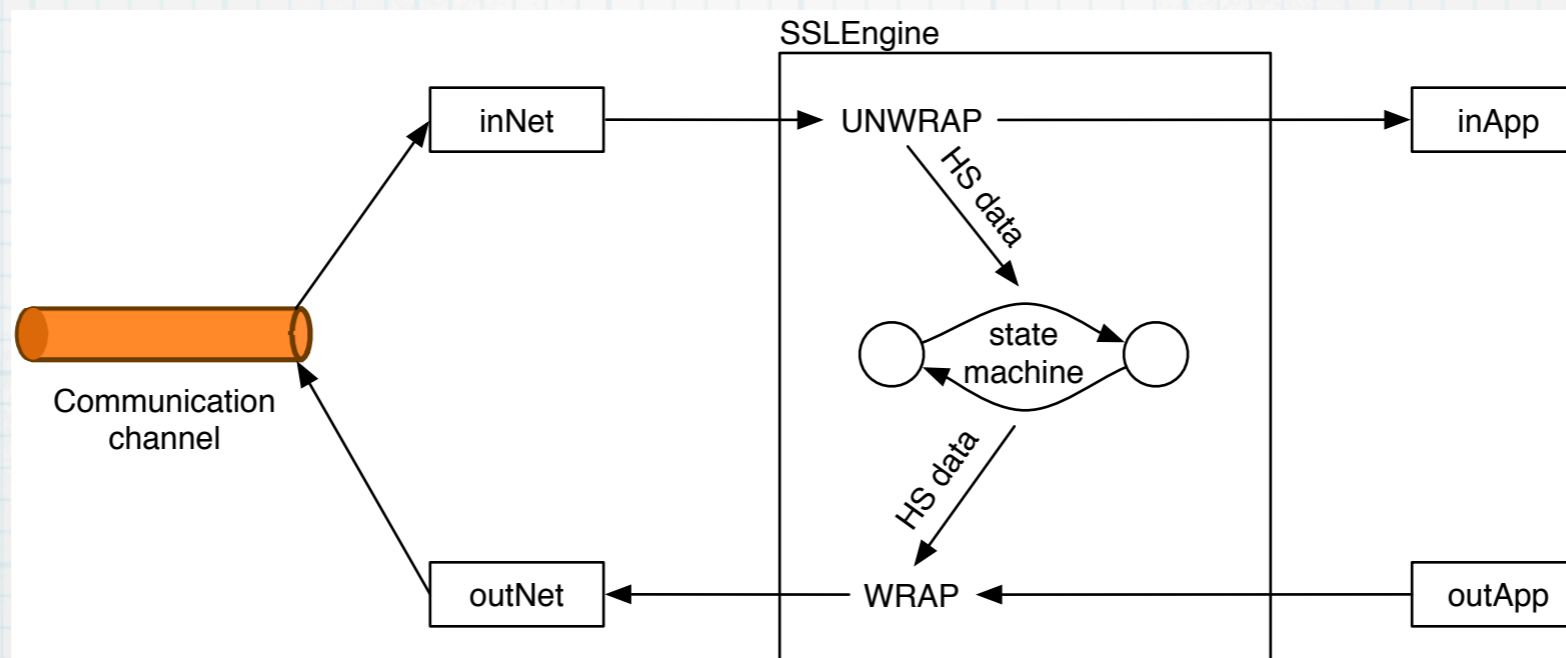


SSL

- **Motivation: bringing e-commerce to the Internet**
- **Created by Netscape in 1994**



JSSE



SPV server certificate

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	netbank.edb.com
Organization (O)	EDB IT Drift
Organizational Unit (OU)	Network Services
Serial Number	17:88:37:EB:67:BE:25:53:08:4A:9A:29:29:1C:76:E1

Issued By

Common Name (CN)	<Not Part Of Certificate>
Organization (O)	VeriSign Trust Network
Organizational Unit (OU)	VeriSign, Inc.

Validity

Issued On	8/3/04
Expires On	8/4/05

Fingerprints

SHA1 Fingerprint	AC:3E:BA:04:18:59:AA:3B:72:50:74:52:76:E2:F5:39:B6:3B:CC:CE
MD5 Fingerprint	14:66:91:49:40:AE:E0:A3:D1:45:1B:F0:56:6F:80:D2

Implementations

- NIO implementation of SPV's login procedure
- Basic operations in a PKI
 - Key generation
 - X509 certificate generation
 - CRL generation and revocation
 - Mutual authentication

NIO/PKI/SSL prototype

- ◆ Combination of NIO, PKI and SSL to provide a framework for secure client-server communication
- ◆ Implementation assuming same issuer of both client and server certificates
- ◆ More information
 - ◆ <http://www.i.uib.no/~yngvee/?sslnio>

Summary

- Internet security
- Java
- PKI
- SSL
- Implementations

Conclusions

- Network security approach insufficient
- Current Internet banking systems are flawed
- Java contains crypto and PKI capabilities
- A combination of NIO, PKI and SSL can provide an infrastructure to enhance security in client-server communication

Further work

- NIO/PKI/SSL prototype
 - Scalability
 - Evaluation
 - Paper
- SWAP
 - PKI with constrained devices
- Privacy

More information

- <http://www.nowires.org>
- <http://www.ii.uib.no/~larshn>