

Vulnerabilities in Distributed Computer Systems

PhD dissertation
Vebjørn Moen
Universitetet i Bergen



Overview

- Introduction.
- Papers.
- Impact.
- Lessons learned.

Introduction

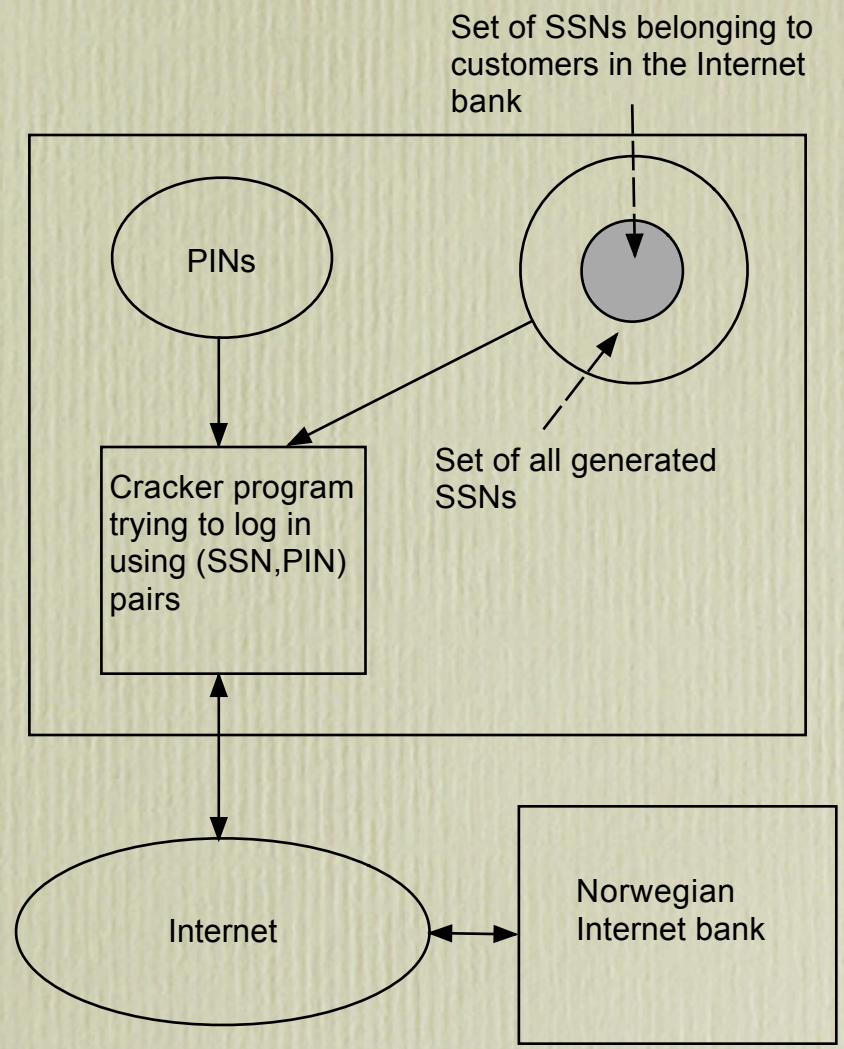
- Increased use of distributed computer systems.
- Engineering and security.
 - Consider the risks.
 - Create the system.
 - Reconsider the risks.

New risks

- What happens to a system when a serious new attack is found?
- Should new attacks be kept secret?
- Who should decide what to do about the risks?

Paper I: Vulnerabilities in Online Banks

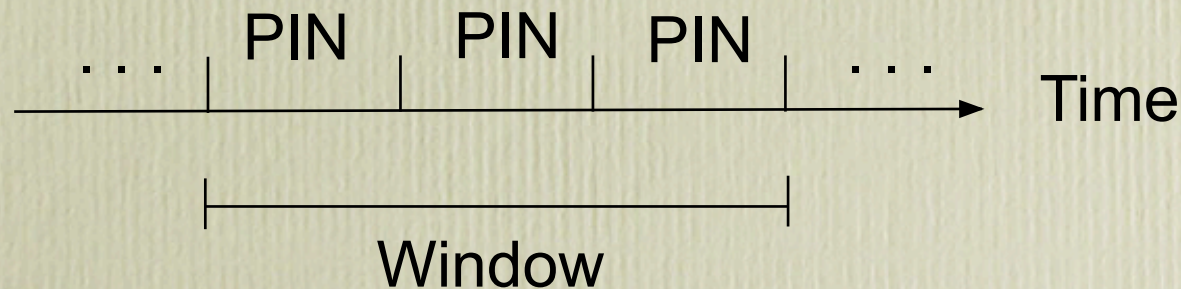
- Describes a simple brute-force attack on a Scandinavian bank.
 - Idea: try a few PINs for each customer.



Paper II:

Case Study: Online Banking Security

- Results from Paper I applied to different banks with slightly different solutions.
- PIN calculators more secure?
 - PIN window and synchronization problems.



Paper II:

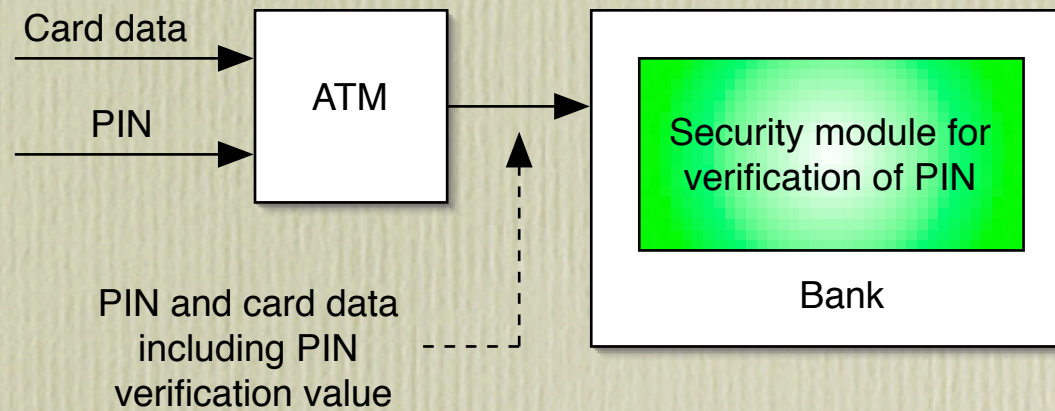
Case Study: Online Banking Security

- Making the attack practical:
 - Distributed attack using “bot net”.
 - Denial of Service.

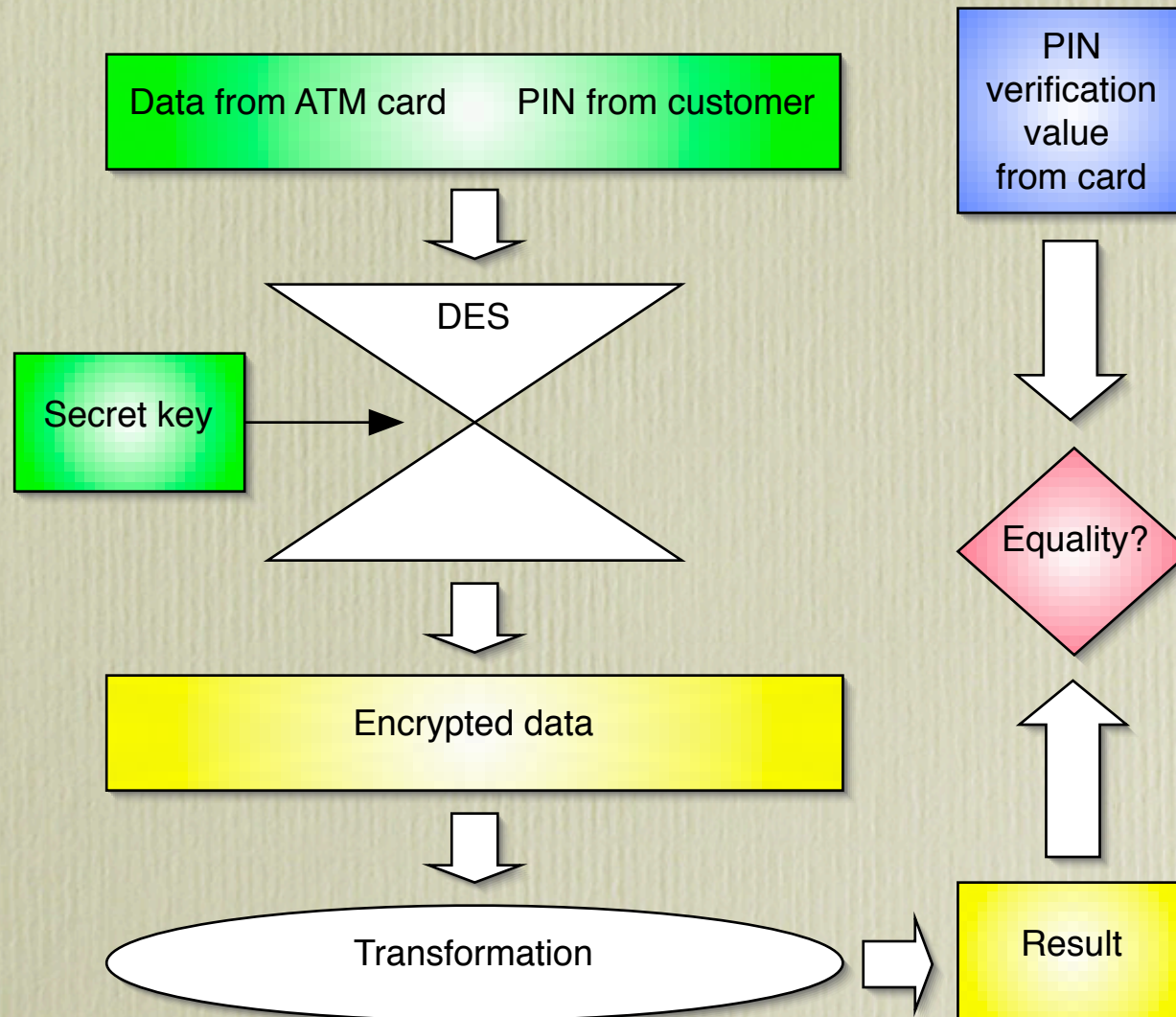
Paper III: Lessons from the Norwegian ATM System

- The true security of the Norwegian ATM system compared to the claimed security of the system.
 - How does this effect a court case between a customer and the bank.
 - Should the banks be allowed to keep the security solutions secret?

Paper III: Lessons from the Norwegian ATM System



Paper III: Lessons from the Norwegian ATM System

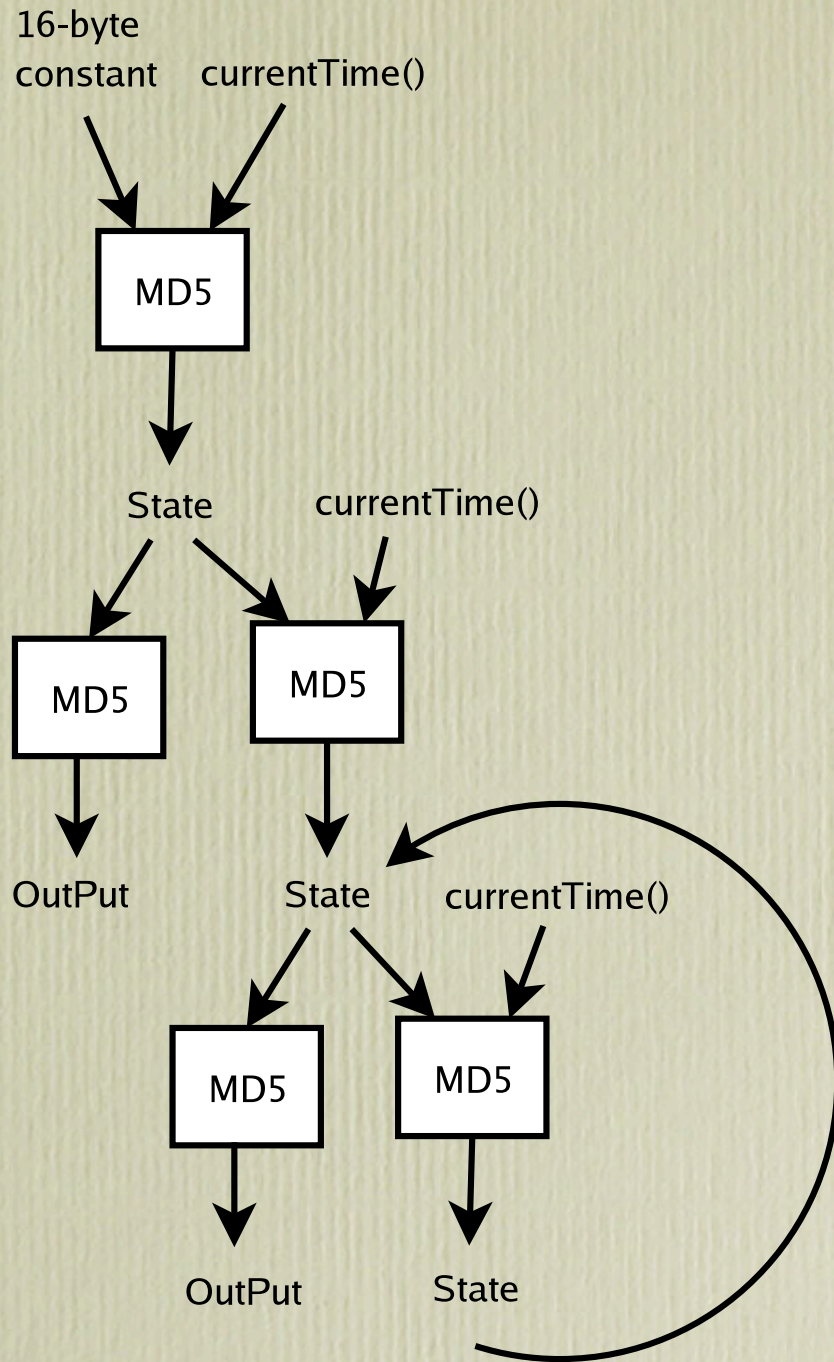


Paper IV: Weaknesses in the Temporal Key Hash of WPA

- Wired Equivalent Privacy (WEP).
 - Completely broken - WPA was suggested to fix the immediate threat.
- Given some WPA packet keys we find the the 128-bit master key.
- Possible to find the 128-bit master key in WPA with work equivalent to 2^{105} RC4 encryptions.

Paper V: Attack on Sun's MIDP Reference Implementation of SSL

- Seeding key-generation with time.
 - Old problem in a new wrapping.
- How is this solved in mobile phones?



Paper VI:

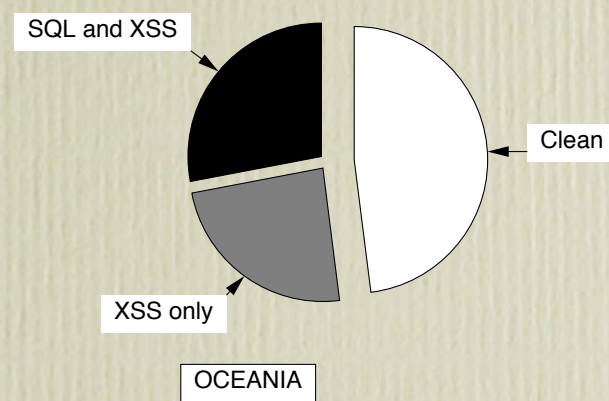
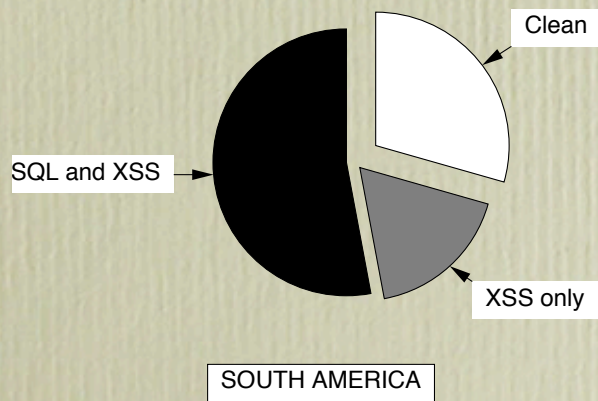
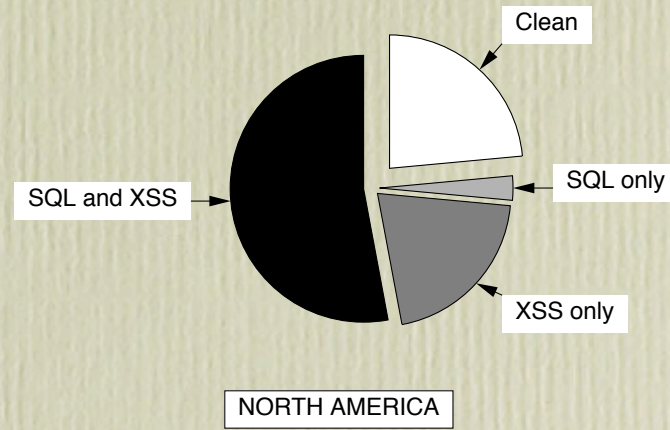
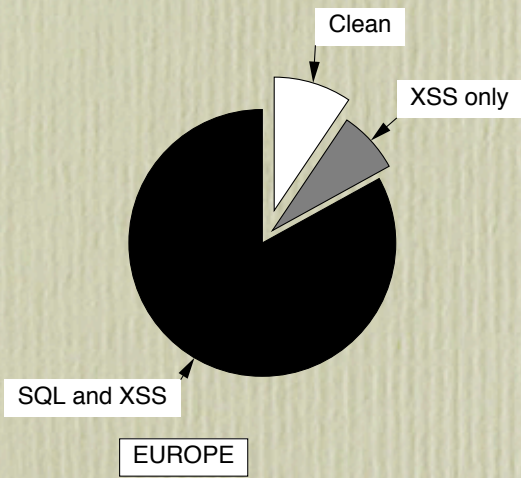
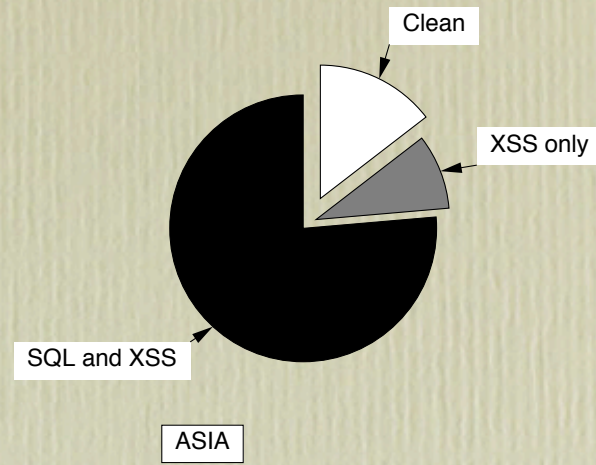
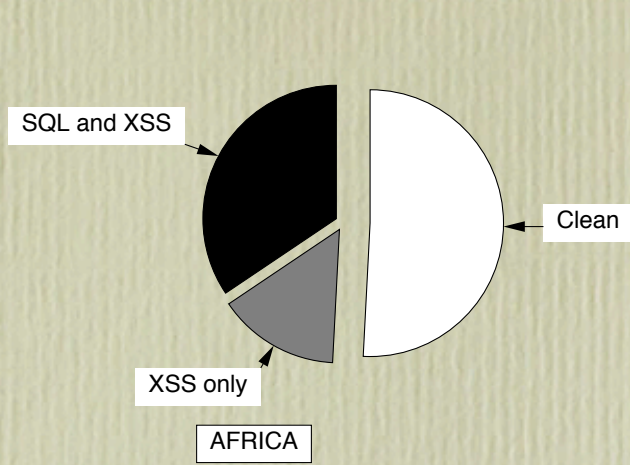
Secure Networked J2ME Applications: Problems and Challenges

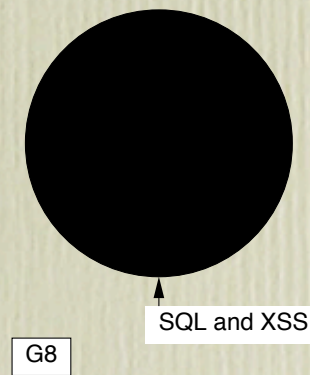
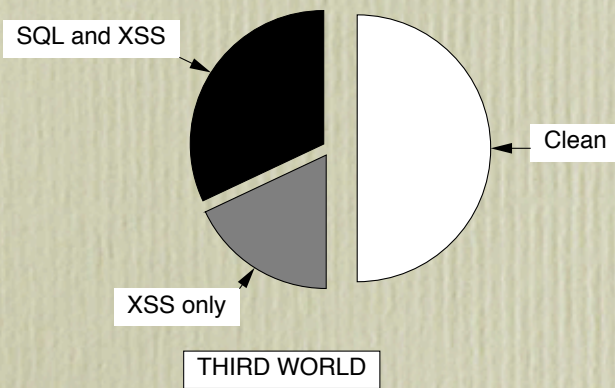
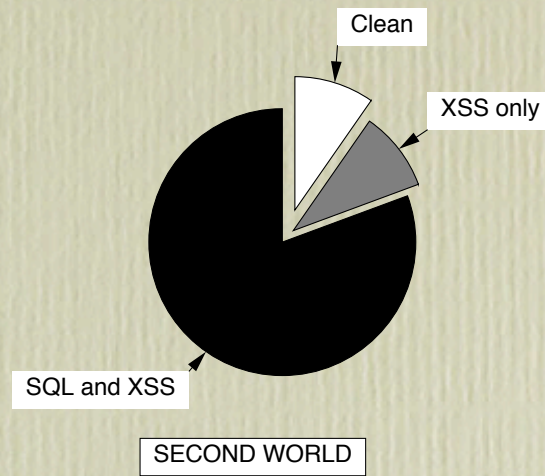
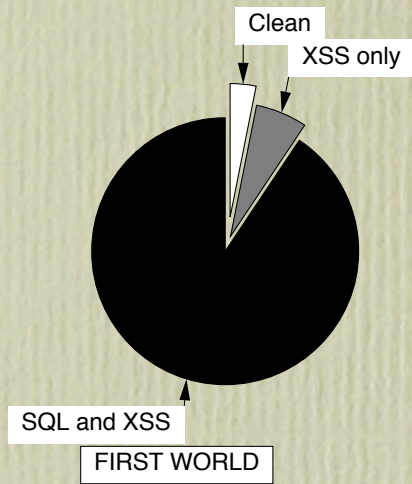
- Designing secure applications for smartphones.
- Immature technology with a lot of bugs and unimplemented features.
- Will SATSA give programmers the tools they need to create secure software on mobile phones?

Paper VII:

Vulnerabilities in E-Governments

- We tested the Web pages of governments around the world for simple Web applications attacks (Cross Site Scripting and SQL injection).
 - More than 80% of the e-governments in the world are vulnerable to one of these attacks.
 - Industrialized countries are more vulnerable than under-developed countries.





Paper VII: Vulnerabilities in E-Governments

- Collecting Social Security Numbers.
 - Pension fund.
 - Order services using only SSN.

Impact

- Seven published articles - three in conferences and four in journals.
- A large number of news articles (>30) written about the results in the papers in the thesis.
- Meetings with the The Financial Supervisory Authority of Norway and The Norwegian Consumer Council.
- At least one bank has changed their solution due to our work.

Lessons learned

- Security-by-obscurity.
- Independent security research.
- No such thing as perfect security.
- Calculated risks.