



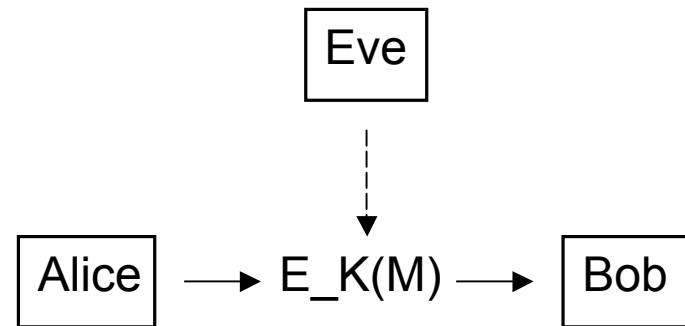
Security Analysis of Electronic Voting and Online Banking Systems

PhD Dissertation
Thomas Tjøstheim
University of Bergen

Introduction

- What is security?

- Confidentiality
- Integrity
- Availability



- Security analysis

- System-based analysis



Electronic Voting

- Electronics to cast or tally votes
- Improve speed, accuracy and accessibility for disabled voters
- Verifiable voting systems
 - Punchscan, ThreeBallots, and Prêt à Voter



What Makes Voting So Hard

- No neutral third parties
 - Voters cheating
 - System cheating
 - Coercers and vote buyers
- Conflicting requirements
 - Verifiability vs secrecy



Electronic Voting Study

- Developed model for system-based analysis of voting systems
- Case study of three voting schemes
- Proposed a new remote electronic voting scheme



Online Banking

- Widely used in Norway and in other countries
- Customer authentication
- Online banking fraud
 - Six Norwegian online banks victims of online fraud in 2006



Online Banking Study

- Norwegian online banks 2003-2006
 - Customers' perspective
 - Customer authentication in 2003-2004 had serious flaws
 - Vulnerabilities in new online banking system



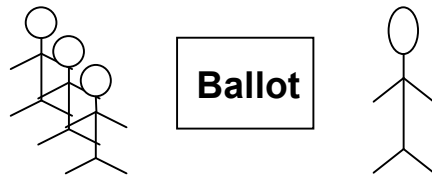
Paper I

A Model for System-Based Analysis of Voting Systems

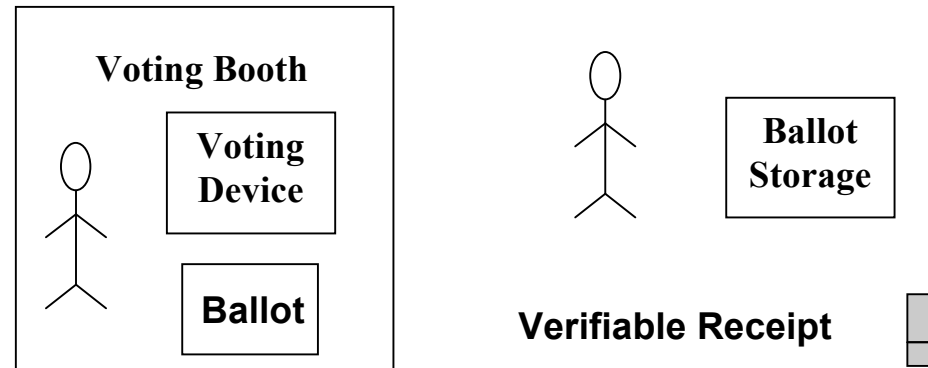
- Generic model for threat analysis
- Defines set of components and associated threat categories
- More systematic approach to high level analysis than previous work

Voting System

1. Registration

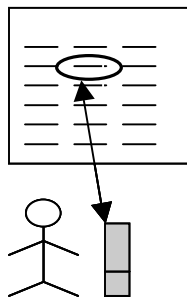


2. Voting



3. Verification

Web Bulletin Board (WBB)



4. Tallying

Election Results





Paper I

A Model for System-Based Analysis of Voting Systems

- Threats to ballot form component:
 - Identifiable information added
 - Authority knowledge
 - Voter's choice incorrectly represented
 - Ballot form spoiled
 - Ballot form faked



Paper II

A Case Study in System-Based Analysis: ThreeBallots and Prêt à Voter

- Applying the model:
 - Identify the main components of the scheme
 - Consider each threat category and whether or not it applies:
 - Interactions with component in the different phases of the protocol
 - Purpose and security requirements of component



Paper II

A Case Study in System-Based Analysis: ThreeBallots and Prêt à Voter

■ ThreeBallots

- Threats: methods for vote selling and methods for adding or subtracting votes

■ Prêt à Voter

- Threats: only minor threats identified, e.g. randomisation attacks

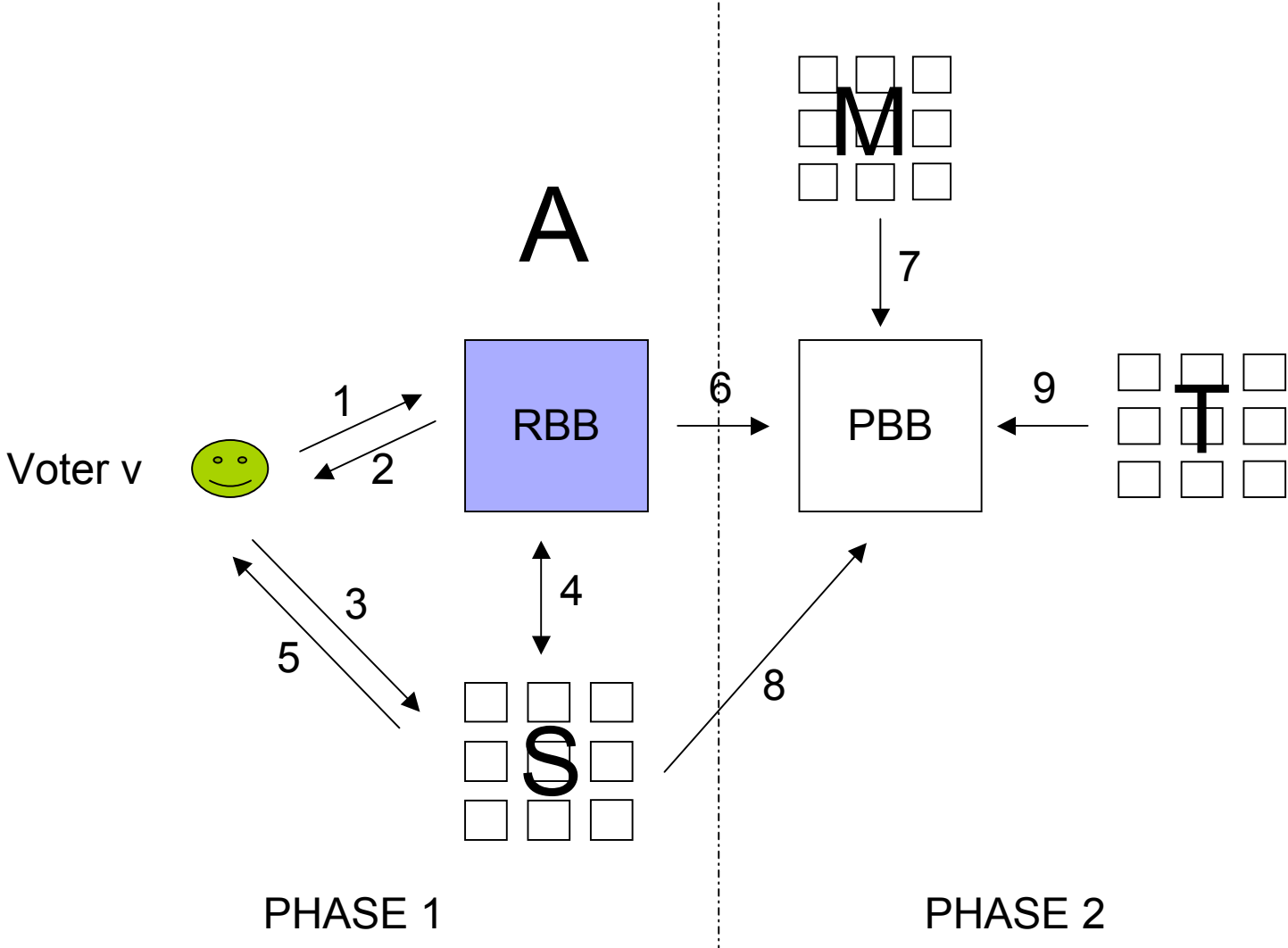


Paper III

Remote Electronic Voting Using Verifiable Chain Encryption

- Remote voting
- Practical and verifiable scheme
 - Receipt free
 - Scalable
- Main protection against coercion
 - Re-voting
 - Possibility of overwriting online vote in traditional poll place voting

Protocol overview





Paper IV

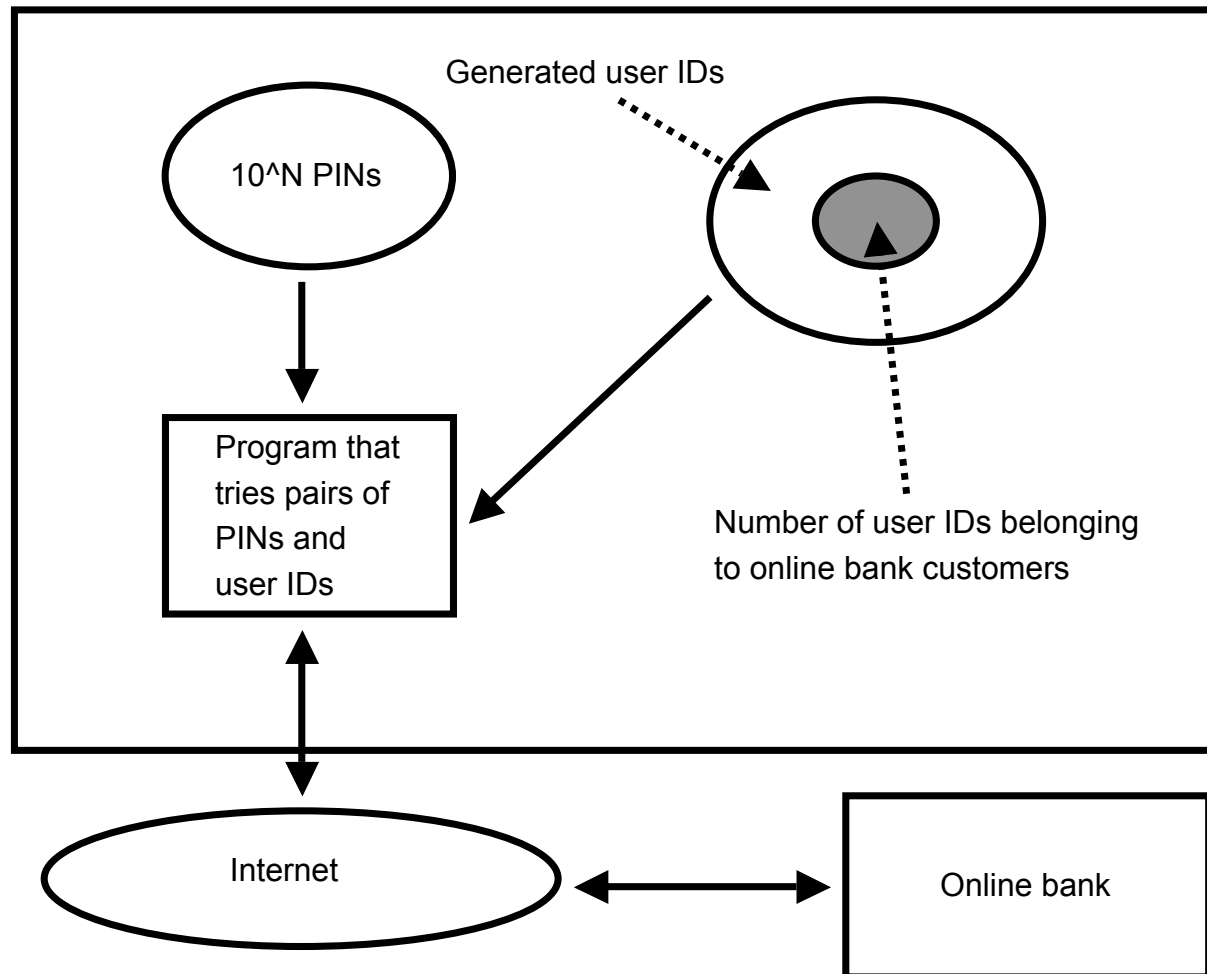
Vulnerabilities in Online Banks

- Vulnerable solutions
 - Structured user ID and PIN code
 - User ID examples: Social Security Number (SSN), account number
- Opens up possibilities for
 - Brute-force attacks
 - Denial of Service (DoS) attacks



Paper IV

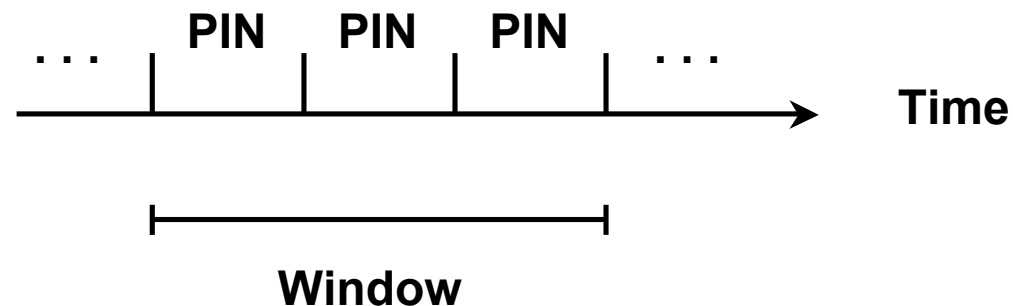
Vulnerabilities in Online Banks



Paper V

Case Study: Online Banking Security

- Broader case study of Norwegian online banks
- PIN calculators
 - Clock drift problems





Paper V

Case Study: Online Banking Security

- Link SSNs and names
 - Norwegian public service pension fund vulnerability
- Bad security
 - Security by obscurity
 - ATM influence



Paper VI

Next Generation Internet Banking in Norway

- BankID

- PKI-based infrastructure
- 700,000 customers

- Customer authentication

- SSN
- One time PIN
- Static password



Paper VI

Next Generation Internet Banking in Norway

■ Result of analysis

- 10 “Observations” that highlights weaknesses in BankID
- Examples of vulnerabilities:
 - DDoS attack
 - Level of non-repudiation
 - Man-in-the-middle attack



Impact

- Five published articles – two in conferences and three in journals
- BankID paper not submitted yet
- A large number of news articles (>60)
- At least one bank has changed their solution due to our work



Lessons Learned

- Openness and verifiability
 - Enable independent security analysis
 - Help people understand how systems work
- Perfect security does not exist
- Analysis at different levels and by different people



Thank You!