WHY CRYPTOSYSTEMS FAIL

Ross J. Anderson
Communications of the ACM (CACM) Vol. 37, No. 1, November 1994

Presented by Duc Huy Bui, Duc Anh Le
2016/11/22
Agenda

1. Introduction
2. Examples of Failures
3. ATM Security Issues
4. ATM Fraud
5. Organizational Aspects
6. Problems with Security Products
7. Nature of Robustness
8. Explicitness
9. Explicitness and Software Engineering
10. Conclusion
Introduction

• Originally, used by governments, military and other organizations to keep messages secret
• Later, incorporated in wide range of commercial systems
• Introduced to commercial world from military by designers of automatic teller machines (ATM) systems in 1970
• ATM security techniques inspired many other systems
Introduction (cont’d)

• Engineering of cryptosystems more difficult than traditional engineering like aeronautical engineering
  • No public feedback
  • Secrecy

• Further analysis from author on banking systems
  • Next biggest application of cryptography after government [2]
Examples of Failures

• In USA, regulations require banks to refund all disputed electronic transactions unless they can prove fraud by customer
  • ~15,000$ yearly loss for each bank [2]
  • Video camera installation

• In Britain, regulations not that strict
  • Bankers deny that system can ever have a fault
  • „Phantom Withdrawals“ are customer’s problem
  • Many court cases
    • At first: customer got fined or went to jail
    • At the end: someone else fault, security system error
ATM Security Issues

- ATM Encryption of PINs [2, 3]
  - Based on variants of a system developed by IBM
  - Example:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Number</td>
<td>8807012345691715</td>
</tr>
<tr>
<td>PIN key</td>
<td>FEFEFEEFEFEEFEEFEFEEFE</td>
</tr>
<tr>
<td>Result of DES</td>
<td>A2CE126C69AEC82D</td>
</tr>
<tr>
<td>Result decimalised</td>
<td>0224126269042823</td>
</tr>
<tr>
<td>Natural PIN</td>
<td>0224</td>
</tr>
<tr>
<td>Offset</td>
<td>6565</td>
</tr>
<tr>
<td>Customer PIN</td>
<td>6789</td>
</tr>
</tbody>
</table>

Encrypted with 'Terminal key' and sent to bank’s central computer.

No specific cryptographic use -> enables customer to choose their own PIN.
ATM Security Issues (cont’d)

• Threat model from military presumes technical sophisticated attacks
• Only two out of hundred cases of ATM-related fraud are skilled attacks
• Three common main causes were simpler
  1. Phantom Withdrawals
     • Caused by processing errors
  2. Postal service
     • E.g. in Cambridge, 4000 students open bank account yearly -> documents sent to pigeonholes
  3. Theft by bank staff
     • Banks dismiss 1% of their staff for disciplinary reasons yearly
ATM Fraud

• Internal Fraud (staff)
  • Issuing extra card
    • Complaints from customer about phantom withdrawals were generally ignored
    • Security hole: address changes unnoticed
  • Recording customer’s PIN and account number with handheld computer
    • Produce counterfeit cards
  • ATMs w/ test transaction mechanism
    • Typing in 14 digit number outputs 10 bank notes
    • Instructions written in some manual
    • Lead to series of crimes
    • Feature was patched later on
ATM Fraud (cont’d)

• External Fraud (external people)
  • Observing customer’s PIN and copy bank details to blank cards
    • Full account number on discarded ATM tickets
  • Telephone card trick
    • ATM believes previous card had been put in again
    • PIN observed
ATM Fraud (cont’d)

- External Fraud (bank policies)
  - Cardboard
    - Assume PIN is 2256
    - Choose a four letter word, say BLUE

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>W</td>
<td>B</td>
<td>T</td>
<td>J</td>
<td>K</td>
<td>L</td>
<td>P</td>
<td>A</td>
<td>H</td>
<td>E</td>
</tr>
<tr>
<td>S</td>
<td>L</td>
<td>U</td>
<td>G</td>
<td>U</td>
<td>F</td>
<td>G</td>
<td>J</td>
<td>I</td>
<td>D</td>
</tr>
<tr>
<td>D</td>
<td>F</td>
<td>I</td>
<td>I</td>
<td>U</td>
<td>K</td>
<td>N</td>
<td>G</td>
<td>O</td>
<td>U</td>
</tr>
<tr>
<td>T</td>
<td>O</td>
<td>Z</td>
<td>G</td>
<td>H</td>
<td>E</td>
<td>B</td>
<td>F</td>
<td>T</td>
<td>X</td>
</tr>
</tbody>
</table>

NOT safe at all! Higher probability of guessing right PIN
ATM Fraud (cont’d)

• External Fraud (bank policies)
  • PIN encrypted on magnetic stripe
    • Account number could be changed
    • Document about this technique circulated in British prison
  • Schemes
    • Example: PIN 4455 (or 4545)
    • Verification: digit one + digit four = digit two + digit three (similar for second example)
  • Store and Forward
    • Several card copies and draw money from different ATMs at the same time
    • Example: in Italy, ATMs were offline during weekend

• Early conclusions
  • Incentives for security improvements only when customer carries burden of proof
  • More an organizational problem rather than technical one
Organizational Aspects

• No computer security team or dedicated department
• Picking wrong external consultants
  • E.g. 40 banks in Asia used Caesar cipher to encrypt PINs for 5 years (very insecure)
• Management argues about centralizing security or not
  • Two philosophies
    • Railway system
      • Tight central control
    • Aircraft system
      • Remain in command
• Continuity matters
  • Difficult to maintain effective security control -> constantly changing structure
The Problems with Security Products

• High-tech attacks were rare, but most exercising for the crypto industry
• Security standards are written in the Orange Book
• Misguided focus towards building cryptosecurity products without knowing how to use them in real systems
• Security products should only be certified if they are simple enough for ordinary stuff to use
The Problems with Security Products

• Security researchers tend to use threat and risk models in which only one thing goes wrong at a time
• In reality: combination of careless insiders and opportunistic attacks
The Nature of Robustness

• Essence: Solution that is slightly less than optimal but provides benefits such as:
  • Reducing design or operational complexity
  • Resilience against minor errors
  • Redundancy against component failure (doesn’t work for computational systems)
• Example: many aircraft accidents are caused by the failure of critical components → Extensive use of redundancy
• BUT: Doing more rounds of a bad encryption algorithm doesn’t make it better!
The Nature of Robustness

• Unthinking use of redundancy in computer systems can lead to resilience

• ATM systems therefore inspired us to look for an organizing principle for robustness properties

• No Silver Bullet

• Cryptographic algorithms fail, if designers do not specify the required properties explicitly
Explicitness

• Importance of explicitness is confirmed in field of computer systems security

• Approaches:
  • Formal methods
    • Check desirable properties, verify correctness of protocols
  • Integrate security with software engineering
    • Problem: identifying which objects have a security significance
    • Solution: dependency analysis
Explicitness and Software Engineering

• Explicitness fits well in the general principles of SE
• Elementary problem: establishment of security goals
• Many SE methodologies require a concept of operations before any detailed specifications are defined
• Conflicting goals for ATM security:
  • Controlling internal and external fraud
  • Arbitrating disputes fairly
• Security systems were built without any clear ideas
Explicitness and Software Engineering

• Compare secure systems with safety critical systems

• Four principles of software safety:
  1. Specification should list all possible failure modes
  2. Explain what strategy has been adopted to prevent each of these failure modes, or at least make them acceptably unlikely
  3. Should tell, how these strategies are implemented, including consequences when each component fails
  4. Certification program must include a review by independant experts
Conclusion

• Designers for cryptosystems have suffered from a lack of feedback
• This has led to a false threat model:
  • Focused on what could possibly go wrong instead of what was likely to
  • Products ended up being too complex to use
• Almost all security failures were in fact due to implementation and management errors
• Component level certification (TCSEC) is unlikely to achieve its goals
  → Security standards should take more account of environment in which components are used
Conclusion

• Fact: most research budget went into activities of marginal relevance
• Robust security systems can be achieved by explicitness
• Examine assumptions in a systematic and careful manner → central for cryptography and secure operating systems
• Above all: determine security goals → concerns how a system performs
QUESTIONS?
References


BACKUP
Threat Model

• Threat Modeling
  • Planned activity for identifying and assessing application threats and vulnerabilities
  • Defining countermeasures to prevent, or mitigate the effects of threats to the system

• Threat
  • is a potential or actual undesirable event that may be malicious (such as DoS attack) or incidental (failure of a Storage Device)

Caesar Cipher

• One of the simplest and most widely known encryption techniques

Plain:      ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:     XYZABCDEFGHIJKLMNOPQRSTUVWXYZ

Plaintext:  THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Ciphertext: QEB NRFZH YOLT K CLU GRJMP LSBO QEB IXWV ALD

Silver Bullet

• Action, which cuts through complexity and provides an immediate solution to a problem