Why Cryptosystems Fail

Ross Anderson

Proceeding of the 1st ACM Conference on Computer and Communications Security, 1993

2010-20784 김학봉
Introduction

- Information on how cryptosystems fail hard to get due to secrecy
- This paper surveys the failure modes of ATM in order to discover out the information
  - After government, the next biggest application is in banking
- It turns out that the threat model was wrong
  - Most frauds were not caused by cryptanalysis or other technical attacks
  - But by implementation errors and management failures
- Alternative models are analyzed which we might usefully import into the security domain
  - Safety critical systems
Limitation of Cryptology

- No public feedback about how cryptographic systems fail
  - Their major user have traditionally been government agencies, which are very secretive about their mistakes
  - Difference with most other engineering
    - The flying community has a strong and institutional learning mechanism
    - If an aircraft crashes..

- A typical example – phantom withdrawals
  - Nonetheless customers did not withdraw money from an account, there is the withdrawal record on the account
Outline

- Introduction
- How ATM fraud takes place
  - Simple attacks
  - Complex attacks
  - Discussion
- The wider implications
  - Why the threat model was wrong
  - Confirmation of our analysis
- A new security paradigm
- Conclusion
Simple Attacks (1)

- From inside (by bank staff)
  - Issuing extra cards
  - Recording customer’s PIN and account number, counterfeited cards
  - Using cards which can withdraw money from any customer accounts

- From outside
  - Observing customers’ PINs standing in ATM queues
    - It can be done because the full account number is printed on the ATM ticket
  - Recording a ‘pay’ response from the bank and keeping on replaying it until the machine is empty
Simple Attacks (2)

- From outside
  - Postal interception
    - 30% of all UK payment card losses
  - Test transaction
    - Outputting 10 banknotes when a 14 digit sequence is entered
  - False terminal
    - Collecting customer card and PIN data

- Using flaws on PIN
  - Offline ATMs used simple PIN checking logic
  - Encrypted PINs are written to a file or the card strip
Outline

- Introduction
- How ATM fraud takes place
  - Simple attacks
  - Complex attacks
  - Discussion
- The wider implications
  - Why the threat model was wrong
  - Confirmation of our analysis
- A new security paradigm
- Conclusion
How ATM Encryption Works

- Keys used to encrypt
  - PIN key: derive the PIN from the account number

<table>
<thead>
<tr>
<th>Account number:</th>
<th>8807012345691715</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN key:</td>
<td>FEFEFEFEFEFEFEFEF</td>
</tr>
<tr>
<td>Result of DES:</td>
<td>A2CE126C69AEC82D</td>
</tr>
</tbody>
</table>

- The security of the system depends on keeping the PIN key absolutely secret

<table>
<thead>
<tr>
<th>Customer PIN:</th>
<th>6789</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM terminal key</td>
<td></td>
</tr>
<tr>
<td>working key</td>
<td></td>
</tr>
</tbody>
</table>

- Working key encrypts the sensitive data between two servers
- Zone key encrypts working key
- Terminal key encrypts the sensitive data to a terminal (ATM)
Problems from Not Using a Hardware of Encryption Products

- Reasons for not using the hardware
  - Expensive
  - Difficult and time-consuming to install
  - ‘buy-IBM-or-else’ policy

- Solutions
  - Software level implementation

- Caused problems
  - PIN key can be found without too much effort by system programmer
Problems with Encryption Products (1)

- Bad security products
  - Trapdoor
    - A software-based hidden entrance to a computer system
  - Weak parameter used to make keys
  - Physically accessibility
  - Back up in wrong place

- Sloppy operating procedures even good products is purchased
  - Ignoring error messages
  - Loose key management
    - Giving keys to outside firms or maintenance engineers
    - Kept in open files
Problems with Encryption Products (2)

- Cryptanalysis
  (one of the less likely threats to banking systems)
  - Some banks are still using home-grown encryption algorithms
  - Someone tried to entice a university student to break a bank’s proprietary algorithm
  - Even a good algorithm is used, there are weak parameters
  - Implementation or protocol error
  - It is possible to find a DES key by trying all the possible keys
Outline

- Introduction
- How ATM fraud takes place
  - Simple attacks
  - Complex attacks
  - Discussion
- The wider implications
  - Why the threat model was wrong
  - Confirmation of our analysis
- A new security paradigm
- Conclusion
The Consequence for Banks

- In the UK, one ATM transaction with an error occurs out of 34,000 transactions according to an article.
  - This paper guesses that the probability is about 1 in 10,000.
- This is not news to large banks which employ staff to reconcile their bank accounts.
- When ATM customers complained without evidence, most bankers said that their systems are infallible.
  - This policy carries a number of risks.
- Their failure to face up to the problem may contribute to public pressure and ultimately legislation.
The Implication for Equipment Vendors

- The suppliers’ main failure is that they **overestimate** their customers’ level of design sophistication
  - They provide a fairly raw encryption capability
  - However, they leave the application designers to integrate the cryptographic facilities with application and system software

- Tackling this problem will require:
  - A system level approach
    - Not a component level
  - A certification process
    - A hierarchy of licences
Outline

- Introduction
- How ATM fraud takes place
  - Simple attacks
  - Complex attacks
  - Discussion
- The wider implications
  - Why the threat model was wrong
  - Confirmation of our analysis
- A new security paradigm
- Conclusion
Why the Threat Model was Wrong

- Uncritical acceptance of the conventional military wisdom of the 1970's
  - The military model stressed secrecy
  - The early systems had only limited network
  - Nowadays, however, ATM security involves a number of goals which including controlling internal & external fraud

- Human factors
  - It is hard to organize computer security team
    - The company’s managers is the only group with the motive to insist on good security

- Many of well known consulting firms pretend to have expertise which they do not possess
Confirmation of Our Analysis

- The vast majority of security failures occur at the level of implementation detail
  - The result above came from a workshop
- Survey of US Department of Defense organization has found that poor implementation is the main security problem
- The need for more emphasis on quality control is now gaining gradual acceptance in the military sector
  - The US Air Force is implementing ‘total quality management’ in its information security systems
Outline

- Introduction
- How ATM fraud takes place
  - Simple attacks
  - Complex attacks
  - Discussion
- The wider implications
  - Why the threat model was wrong
  - Confirmation of our analysis
- A new security paradigm
- Conclusion
A New Security Paradigm?

- We need to make a systematic study of what is likely to happen.
  - Instead of worrying about what might possibly go wrong.

- Core business will be an engineering discipline concerned with quality control processes.
  - Not just building and selling ‘evaluated’ products.

- There are alternative models which we usefully import into security domain, safety critical system.

- Safety critical system is that failure could result in loss of life, injury or damage to the environment.
  - Ex) aircraft, nuclear power station controller system.
Safety Critical Systems & Cryptosystems

- **Very basic points of safety critical systems**
  1. List all possible failure modes
  2. Make clear what strategy has been adopted to prevent each of these failure modes
  3. Explain in detail how each of these strategies is implemented
  4. Test whether the equipment in fact can be operated according to the specification

- **Comparison with cryptosystems**
  - No one has attempted even the first stage
  - As for the other three stages, it is clear that ITSEC (and TCSEC) will have to change radically
    - Because the standards are component-oriented, ignore the two most important factors, the system aspect and the human element

※ ITSEC : Information Technology Security Evaluation Criteria
TCSEC : Trusted Computer System Evaluation Criteria
Two Competing Approach within Safety Critical Systems

- **Railway signalling systems**
  - Based on the safety features on the integrity of a kernel of hardware and software
  - The system is in control
    - If the train driver falls asleep or goes through a red light, the train will stop automatically
  - The train driver has been progressively deskilled

- **Aviation system**
  - Based on constant top level feedback and incremental improvement
  - The pilot remains firmly in command
  - Progress has made his job ever more complex and demanding
The Computer Security Implications

- Both the railway and airline models find reflections in current security practice and research
- The railway model is dominant, due to TCSEC / ITSEC emphasis on kernelization and formal methods
- Nonetheless, we must consider whether this is the right paradigm to adopt
- If our parallel with signalling systems is accurate, it is probably a blind alley, we should follow the aviation paradigm instead
Conclusion

- A lack of feedback on cryptosystems’ failure has led to a false threat model
  - Designers should have focused on what was likely to go wrong
  - Their products are too complex and tricky to use
- As a result, most security failures are due to implementation and management errors
  - One specific consequence has been ATM frauds
- Next version of standards must take much more account of the environment
- A paradigm shift is underway
  - We need a fusion of security with software engineering