Why Cryptosystems Fail

Reviewed by Yunkyu Sung
merius@kdb.snu.ac.kr
Contents

- Introduction
- ATM Fraud Examples
- The Wider Implications
- A New Security Paradigm
- Conclusion
Introduction

The purpose of this paper

- Presenting the results of a survey
- Wrong threat model
  - Implementation error
  - Management failure
- Paradigm shift
Limitation of Cryptosystem at that time

- No learning mechanism
  - Aircraft crashes → Professional Investigators rush to the scene
- Beginning as a military purpose
  - Limited network → integrating various areas

Banking

- After government, the next biggest application
- Various miss-operation
ATM Fraud Examples

- Simple attack
  - Inside attack
    - Stealing cards and PINs by Staff
    - Record customer’s PIN and account
  - Outside attack
    - Card with full account, shoulder surfing
    - Replay attack
      - Hijack a Response signal from Bank to ATM
    - Programming error
      - If telephone card was inserted after clean card, ATM recognize as clean card
ATM Fraud Example

- Simple attack
  - Limitation of PIN
    - Many card owner write their PINs on own cards
    - Simple PIN checking logic
    - Encrypt PIN, apart from account number
      - Not to exposure to programmer
    - VISA recommends that banks should combine the customer’s account number with the PIN before encryption
How ATM encryption works?

- The security of the system depends on keeping the PIN key absolutely secret.
How ATM encryption works? (cont’d)

- The standard approach is to use a security module (PC in a safe)
- All the bank’s key & PINs are in encrypted form, so that mainframe programmers only oversee an encrypted string
ATM Fraud Example

Problems with Encryption products

- Expensive, difficult to install. And it takes long time to install
  - Software level implementation
  - PIN key can be found without too much effort by system programmer
- Each IBM, DEC module can not talk to each other
  - emulation
  - emulator’s log file
Problems with Encryption products

- Not all security products are equally good. And Lack of expertise
  - Trapdoor
  - Different parameter between products
  - Physically accessibility
  - Back up in wrong place
- Sloppy operating procedure
  - Ignore a error messages
  - Kept in open files, rather than being locked up
The implications for equipment vendors

- Lack of expertise
- Failure of suppliers
  - Over-estimating of customer’s level of security design
  - Ignoring application level implementation of security function
  - Changing threat environment
- Solutions
  - System level approach
  - Certification process – hierarchy of license
The Wider Implications

Wrong threat model
- Lack of expertise, basic errors in system
  - What could possibly happen?
    → What was likely to happen?
- Reason of wrong assumptions
  - Military purpose
    - Limited network → integrating various areas
  - Human factor
    - No security team, just sales products
  - Consultants without expertise
The Wider Implications

Confirmation of analysis
- Poor implementation is the main security problem
- Designer just choose better components
  - Fostering complacency
- Quality control!
A New Security Paradigm

- Systematic study of “what is likely to happen?”
- From evaluated product to an engineering discipline concerned with quality control process
- Research mode from other discipline
  - Railway signaling system
  - Aviation paradigm
A New Security Paradigm

Safety critical system
- Failure results in loss of life, injury or damage to the environment
  - Aircraft, nuclear power station control system

Spec.
- List of all possible failure modes of the system
- Strategy has been adopted to prevent each of these failure modes
- Detailed explain of these strategies
  - Must be assessed by independent experts
A New Security Paradigm

Railway signaling system
- In control
- If the driver falls asleep, the train will stop automatically

Aviation paradigm
- The pilot remains firmly in command
- The progress has made his job ever more complex and demanding

But, we need an infrastructure which enables information owners to control and trade their own property, rather than trusting everything to a centralized administrative structure
The lack of information feedback has led to a false threat model being accepted.

- What could go wrong? → too complex to solve

Limitation of component-level certification

A paradigm shift is underway

- We need fusion of security with software engineering