Why Cryptosystems Fail

By Ahmed HajYasien CS755

Introduction and Motivation

- Cryptography was originally a preserve of governments; military and diplomatic organisations used it to keep messages secret.
- Later, cryptographic mechanisms have been incorporated in a wide range of commercial systems.
- Automatic teller machines (ATMs) were the pioneers, and much of commercial cryptology was developed after that.

Introduction and Motivation

- Cryptography was introduced to the commercial world from the military by designers of automatic teller machine (ATM) systems in the 1970s.
- The most Cryptosystems failure observations is due to automated fraud.
- This century has seen significant advances in the level of sophistication, as well as an increased awareness of the strategic significance of cryptography.

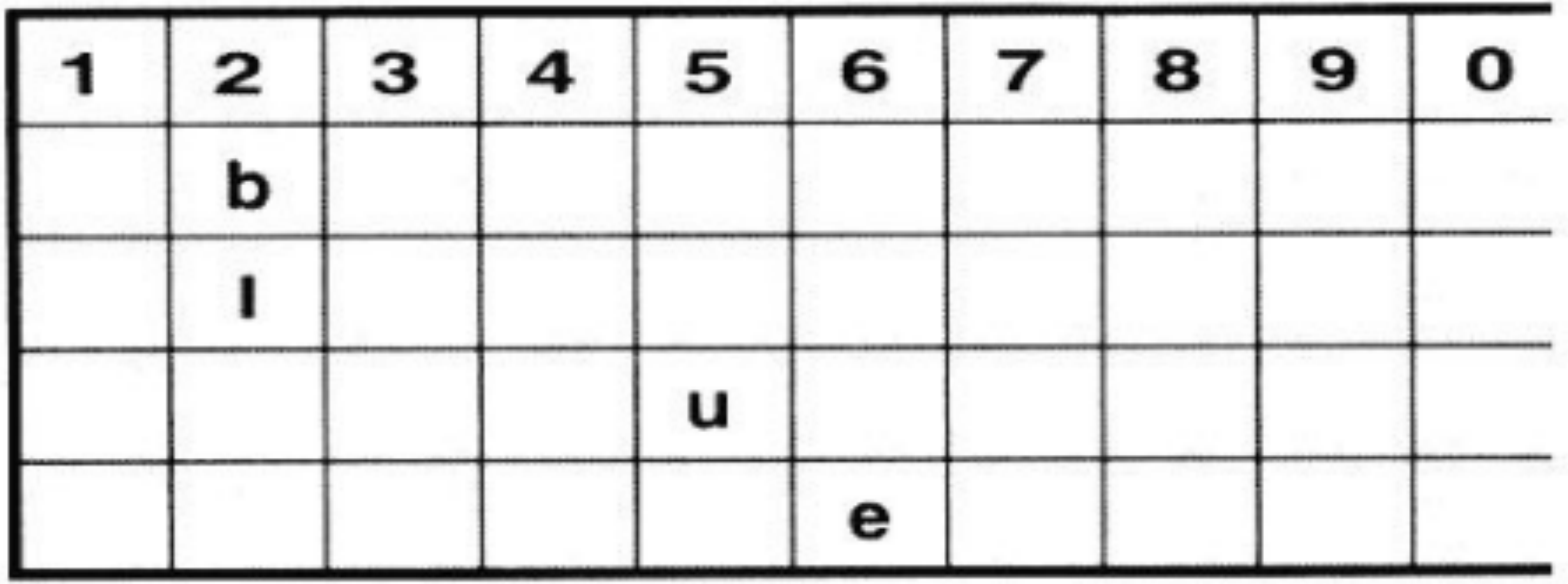
Introduction and Motivation

- Unfortunately, governments classified the use of cryptosystems.
- Only recently has information about the causes of crypto failure been available.
- The advent of ATMs has for the first time produced empirical data, in the form of court proceedings, allowing analysis of the reliability of cryptosystems.
- Ross Anderson published the first such study.

Introduction and Motivation (cont.)

- According to Ross, Of the hundreds of cases of ATM-related fraud, only two cases involved technical attacks.
- Since ATMs generally use cryptography to assure integrity, the resulting court cases (especially in the U.S., where the banks are obliged to prove fraud) provided interesting insight.
- Ross cited many amusing stories.
  - My favorites were one where the bank had issued ATM cards that all had the same PIN code.
  - Another where a programmer had deliberately introduced an error such that there were only 3 different PINs.

The squared cardboard



1	2	3	4	5	6	7	8	9	0
	b								
	l								
				u					
					e				

Figure 1. How not to encrypt PINs

More exotic attacks

- Customers of one British bank got a credit card PIN with digit one plus digit four equal to digit two plus digit three; and a debit card PIN with one plus three equals two plus four.
- Villains eventually discovered that they can use stolen cards in offline devices by entering a PIN such as 4455.

Problem of Store and forward processing

- Anyone can open an account, get a card and PIN, make several copies of the card and get accomplices to draw cash from a number of ATMs at the same time.
- This was a favorite modus operandi in England in the 1980’s.

Three common problems with ATM security

- First: Transactions that are wrongly processed.
  - ex: Deposit to or withdraw from the wrong account.
- Second: Postal services.
  - ex: In Cambridge 4000 people open accounts in oct.
- Third: Theft by bank staff.
  - ex: British banks dismiss 1% of its employees/year.

Early conclusions

- The conclusion that we can draw from these cases is that computer security in the most of it is an organizational problem, not a technical one.
- It is important that we keep this in mind when we listen to complaints.
- Also, we must make sure that our legal framework puts the burden of proof on the financial institution, not the customer.

The problem

- Cryptology is used in many disciplines like banking systems, military communication or diplomatic communication in a country.
- These areas (especially the last two) of application have high level of Confidentiality and Integrity requirements.
- Cryptosystem designers work is quite challenging here, as there is no failure feedback provided to them, which means that developers and researchers can not learn from common management and implementation errors which happen across the globe.
- The failures which occur are not disclosed to global audience by wrapping it up in the box of National Security.

Public interest issue

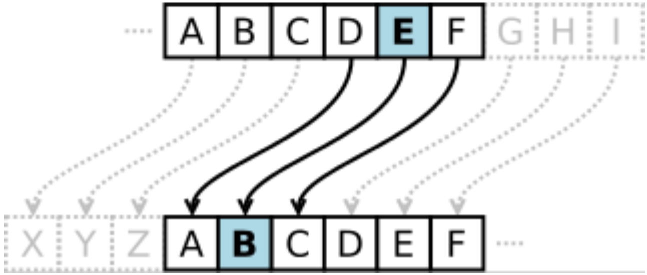
- Shall the burden of proof fall on the customer or on the bank system operator?
- Thousands of innocent victims of card fraud are routinely being deprived of payouts worth thousands of pounds by their banks.
- Banks claim it is impossible for a thief to make a chip-and-pin payment without a correct personal identification number (pin) - the four-digit security code personal to each cardholder.

Organizational aspects

- Unlike UK, in the US the financial organization carries the risk.
- Many organizations have no computer security team at all.
- These organizations get outside consultants to do their security policy-making.
  - 40 banks in Asia encrypted their PINs with Caesar Cipher.

Caesar Cipher

- The action of a Caesar cipher is to replace each plaintext letter with one fixed number of places down the alphabet.



- This example is with a left shift of three, so that a E in the plaintext becomes B in the ciphertext.

Problems with security products

- High tech attacks are rare??? Reference???
- The policy makers in the National Security Agency write security standards, “Orange Book”.
- This led public and private investments towards building security products and this might be misleading.
- Security products should only be certified if they are simple enough for ordinary staff to use.

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, the majority of security failures is a combination of careless insiders and opportunist attack.

The nature of robustness

- Robustness means that security system should be resilient against minor errors in design and operation, and provide redundancy against component failure.
- No silver bullet.
- Suggests that explicitness should be the organizing principle for security robustness.

cont.

- Explicitness means no implications; all objects and assumptions should be fully and clearly expressed.
- A typical problem is to identify which objects in a system have security significance.
- Evaluating the significance of all objects in an operating system is a Hereculean task.

Another difficult problem

- Verifying whether an authentication protocol is correct.
    - This problem can be tackled by **formal methods**; the best known technique involves tracing object’s dependencies on crypto keys and freshness information.
- **Formal methods** are a particular kind of mathematically based techniques for the specification, development and verification of software and hardware systems

Formal methods answer questions

- What does this protocol achieve?
- Does this protocol need more assumptions than another one?
- Does this protocol do anything unnecessary that could be left out without weakening it?
- Does this protocol encrypt something that could be sent in clear without weakening it?
- Formal methods answer all the above questions and this technique guides us in identifying mistakes and suggest corrections to the protocols.

Formal Methods

- Example: For shared keys, we suppose:

$$\frac{P \mid\equiv Q \overset{K}{\leftrightarrow} P, \quad P \triangleleft \{X\}_K}{P \mid\equiv Q \mid\sim X}$$

- That is, if P believes that the key K is shared with Q and sees a message X encrypted under K, then P believes that Q once said X.

Another example:

- For Private keys, we suppose:

$$\frac{P \models \xrightarrow{K} Q, \quad P \triangleleft \{X\}_{K^{-1}}}{P \models Q \mid\!\sim X}$$

- That is, if P believes that the key K belongs to Q and sees a message X encrypted under K^{-1}, then P believes that Q once said X.

Formal methods

- Although formal methods is a great solution to prove that authentication protocol is correct, it is still not a silver bullet.
- Many subtle difficult mistakes exist where assumptions about security properties fail at the interface between different levels.
- We have to be careful to ensure that all our assumptions are made explicit and considered carefully.

A good design practice

1. The specification should list all possible failure modes of the system.
2. It should explain what strategy has been adopted to prevent each of these failure modes or at least make them acceptably unlikely.
3. It should then spell out how these strategies are implemented, including the consequences when each single component fails.
4. The certification program must include a review by independent expert and test whether the system can be operated by people with the stated level of skills and experience.

Strengths of the paper

1. The paper is very interesting and informative as it gives insights into the working of banking systems.
2. Many real life examples have been incorporated so as to explain how frauds actually happen.
3. Although the study of the security systems was carried out 19 years ago and the results and conclusions are of that time only, yet the papers findings are still relevant in present.

Weaknesses of the paper

1. The paper addresses the problems with the security model but does not give specific methods to make this security model better and stronger.

2. Some statistics and impact details should have been mentioned depicting the monetary loss of the banks as well as the customers due to these problems.

3. Some of the points have been repeatedly written resulting in redundancy.

Conclusions

- ATM security involves many conflicting goals including controlling internal and external fraud.
- It could be helpful to compare secure critical systems and safety critical systems.
    - They are known to be related but the former must do at most x while the later must do at least x.

Conclusions

- Cryptographic systems suffered from the lack of feedback about how they fail as opposed to how they might fail in theory.
- Many CS products ended up so complex and tricky to use which led to security failures.
- A good research questions:

Are we building the right robust security systems?

and

Are we building the robust security systems right?

References

- Burrows, Michael, Martin Abadi, and Roger M. Needham. "A logic of authentication." *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 426, no. 1871 (1989): 233-271.
- Anderson, Ross J. "Liability and computer security: Nine principles." In*Computer Security—ESORICS 94*, pp. 231-245. Springer Berlin Heidelberg, 1994.
- Adida, Ben, Mike Bond, Jolyon Clulow, Amerson Lin, Steven Murdoch, Ross Anderson, and Ron Rivest. "Phish and Chips." In *Security Protocols*, pp. 40-48. Springer Berlin Heidelberg, 2009.

Discussion

- Do you think that all the problems mentioned in the paper still applicable till today?
- Shall the burden of proof fall on the customer or on the bank system operator?
- What is a phantom withdrawal?
- What is a silver bullet?
- Do you think that high tech attacks are rare?
- Secure critical systems must do at most X while safety critical systems must do at least x ???

Thank You

Appendix

- **phantom withdrawal**
  - is a cash withdrawal from an automatic teller machine where money has been withdrawn from an account, and neither the customer nor the bank admit liability.
- **A modus operandi**
  - the usual way that a particular criminal performs a crime.
- **Store and forward**
  - telecommunications technique in which information is sent to an intermediate station where it is kept and sent at a later time to the final destination or to another intermediate station.
- **Orange book**
  - Computer Security standards written by NSA.
- **Trusted Computer System Evaluation Criteria** (**TCSEC**)
  - is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system.