Smart Card Attack Tree

Yaochuan Chen, Manasa Veeragandham
Email: {yaoch809, manve201}@student.liu.se
Supervisor: Anna Vapen, {x07annva@ida.liu.se}
Project Report for Information Security, Second Course
Linköpings universitet, Sweden

Abstract

This paper describes the actual state of smart card security. We firstly introduce that we want to utilize attack trees to list most attacks aimed at smart cards. Next we look at the methods of creating attack trees. We then list a forest composed of attack trees, which display the attack goal and attack methods. Afterwards, the method of attack will be evaluated and some countermeasure of the attacks will be discussed. We hope that our attack trees can list the majority of threats aimed at smart card and give a whole image on the state of smart card security.

1. Introduction

This part will introduce the threats and that are encountered when smart cards are used and shall describe why and how attack trees are used to mitigate threats. Furthermore, the introduction will also include a map of the paper.

”Smart cards, credit-card sized devices with a single embedded chip, processor and memory play a vital role in computer security. Despite their wide acceptance as key devices in the security world, they have threats associated with them. Access control, electronic commerce, authentication, privacy protection, etc are the various set of application areas for smart cards. But the stress laid on the analysis of the security risks specific to smart cards and the unique threat environments that they face, is a little low”.

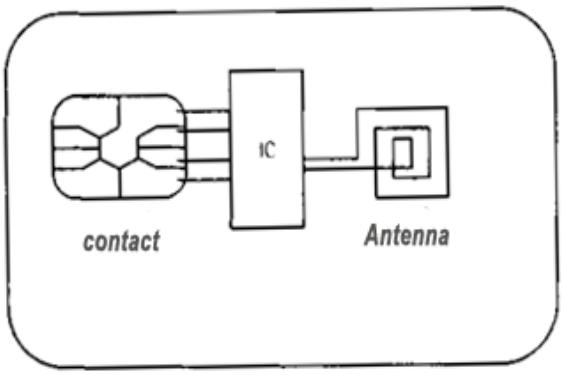
In the further part of the paper, the threats to smart cards will be discussed and an attack tree will be created and explained with an example. Attack trees are used for analyzing all the possible attacks by creating a tree of attacks that a smart card is susceptible to. With these attacks it is possible to narrow down the scope and focus on the attacks that are most harmful and then mitigate them.

A threat is something or someone that can be harmful to a system, for example an attacker.”There are two types of attackers involved in smart card attacks, one is the internal attacker, and for example a card issuer trying to cheat a cardholder and the other is the intruder who tries to steal the card from the card holder or tries to change the terminal software or hardware”. As we know there are attacks on protocols in general computers where the attackers take the advantage of various properties of the system which handle several tasks because it is easier for the attackers to break the security of the system. This is an unusual situation for a typical computer, but common when it comes to smart cards. For many applications, using a smart card is not completely the most secure way to accomplish the task, but it is used with limited computational abilities with limited data storage. “There are various classes of attacks against smart cards. They can be divided into the following groups: attacks by the terminal against the cardholder or data owner, attacks by the cardholder against the terminal, attacks by the cardholder against the data owner, attacks by the cardholder against the issuer, attacks by the cardholder against the software manufacturer, attacks by the terminal owner against the issuer, attacks by the issuer against the cardholder and attacks by the manufacturer against the data owner”. [1]

2. Smart Cards

“Smart card has the size of credit card with an integrated circuit built in it. Smart card includes a RAM, ROM and CPU in case of memory. Smart

card includes a microchip as the CPU, RAM and storage of data around 10MB. Smart cards can store and process information. A smart card is like a mini computer embedded with computer chip. Smart cards store thousands of bytes of electronic data and transact data between user and card reader. This data is stored and processed within the cards chip, in a microprocessor with internal memory". The data from the card is transacted via a card reader. The host computer and card reader communicate to the microprocessor and the microprocessor enforces access to the data on the card. [3]



.

Fig: 1 Double interface smart card

"Smart cards can confirm identities in three ways

- Something you have (a secure Id card)
- Something you know(a password)
- Something you are (a palm print or eye retinal scan)". [4]

Fig: 2 Example of Smart Card

The fig.2 is a student id card which is accessed with a password. This card is used to borrow books in library, access for the doors in the university where there is a restricted access for the user. The working of this card is, when the user swipe the card in a card reader the data on the card is read and asks for the relevant authentication like for a password to give access to the user.

2.1 History of Smart Cards

"The first smart card was introduced in Europe. To reduce thefts smart cards were used as a stored value tool. Later on smart cards were used as storing of data instead on a paper and credit purchasing. Where in U.S people were using this chips for everything like for purchasing groceries, for libraries etc in their everyday life. Later on industries have implemented the smart cards into their products such as GSM digital cellular phone to satellite TV decoders". [3]

2.2 Security of Smart cards

Smart cards give the security of any data transaction. It provides security to user's account identity. Smart cards also provide system security for exchanging of data in any network. Smart cards provide physical security. They give access only to the authorized user. For example, e-mail and PCs can be locked by smart cards. Digital videos broadcast are accepted by smart cards as electronic key for protection. All over the world people are using smart cards in their daily life. [3]

2.3 Applications

"Smart cards have a wide variety of applications ranging from phone cards to digital identification cards for the individuals. In daily life some smart card application are identity of the student ID card, electronic-wallet, access to doors of organization for security, etc. For all such applications one card can be issued to an end-entity. Smart cards hold these data within different files, and, as you will read, these data is only visible to its program depending on the operating system of the card". The most common smart card applications are: [3]

- Credit cards
- Electronic cash
- Computer security systems
- Wireless communication
- Loyalty systems
- Banking
- Satellite TV
- Government identification
- ID Verification and Access Control

2.4 Types of Smart cards

Smart card is of two categories: Contact and contact-less:

"Contact smart cards must be inserted into a smart card reader to make direct connection for the transfer of data. Contact smart cards have more memory and processing power than contact-less smart cards".

"Contact-les smart cards require proximity to a reader to achieve data transmission. Both card and reader have internal antennas and wireless circuitry for secure communication. Contact-less smart cards are every bit secure. Contact-less smart cards are safe for access control, mass transit, vending and cafeteria payment, and dozens of other applications". [4]

2.5 Process of Card Communication

Normally, the card reader read the data through the metal connections; the only connections supply the function of power, reset, a clock, and a serial port (This connection are specified in ISO7816). Most of the time, the communication between card reader and card will be encrypted and the two sides should identify each other through a type of peer entity authentication, such as RSA, and the data transmitted are encrypted by DES(most of time is, but there are also other encryption algorithm we can use like RC5, AES). If it is possible, the data can be verified through a digital signature. For a credit card, the communication with POS and bank gateway is based on a standard of EMV, and there is a CA to certificate each side, during a transaction. [13]

3 Attack Tree

"An attack tree is a way of describing the security of system by analyzing various attacks. It is a technique for knowing various risks. Attack trees are represented in a graphical view by constructing all the possible attacks and then by differentiating the most effective attacks with the attacks which are beyond the capability of attacker. The remaining attacks are the ones which may cause damage to the system". The construction of an attack tree is simple. We start by placing the goal of an attack on top of the tree where the system may subject to multiple attacks with different motivations. From where you can see the possible and impossible attacks. [5]The advantage of an attack tree is that in the future a new attack type can be inserted or existing node values can be modified and the attack ways can be recounted. There is also possible to connect different attack trees. The attack tree analysis allows us to see the attacker's behavior. [6]

Advantages and Disadvantages of Attack tree: [7]

Advantages

- Identifies key security
- Documenting plans of attacks and likelihood
- Knowing the system

Disadvantages

- Amount of documentation
- Can only ameliorate foreseen circumstances
- Difficult to prioritize

4. Methods

Firstly, by identifying some threats that the smart card are facing with. Secondly, attacks as nodes which can implement the goals and repeat the step describe more attacks that we can mention more. During this process, we insert some values into the nodes to show the cost of the attacks or the need of special equipments. Because smart cards are used in many aspects, So we couldn't include all attacks or attack goals in forest or trees, but we had try our best to makeup the attacks and renew the nodes step by step. We have chosen the example as Bruce uses here, is that of opening a safe. Placing "Open Safe" at the top of this simplified tree, he branches out under it "Pick Lock," "Learn Combo," "Cut Open Safe," "Install Improperly.". The "Learn Combo" sub-goal can be accomplished in several ways and so under *it* branch off nodes for "Find Written Combo" and "Get Combo from Target." In fact, the "Get Combo from Target" sub-sub-node branches too, since there are many methods. When we have completed the tree we have made some possible (P) and impossible (I) nodes for the attacks by analyzing some example. It means the possible attacks and impossible attacks in a tree as shown in the fig 3. We have just analyzed some attacks and studied the possible attacks. In fact our project is a literature study and we did not perform any actual attacks ourselves. [5]

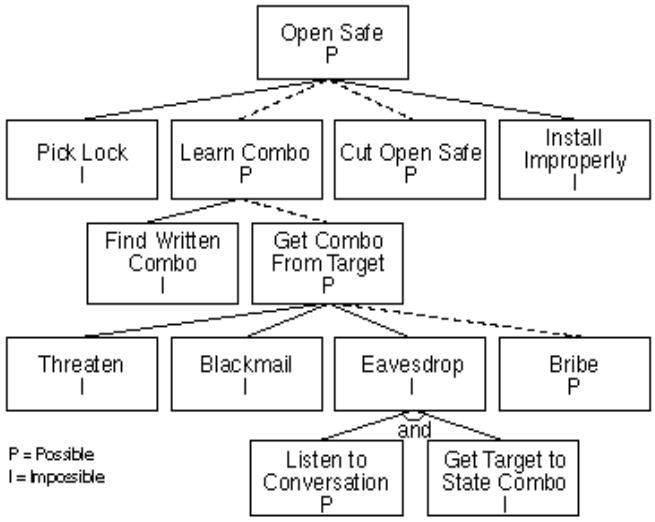


Fig: 3 Example of an Attack Tree

5. Smart Card Attack Tree

Smart card attack tree

1 <OR> Get sensitive data
  1.1 <OR> Get the pin code
    1.1.1 <OR> Eavesdropping
      1.1.1.1 Use a camera to monitor the entering of PIN-code
      1.1.1.2 Hacked terminal
      1.1.1.3 Counterfeit terminal
      1.1.1.4 Terminal skimmer
      1.1.1.5 Write down PIN
      1.1.1.6 Smartcard Relay Attacks
    1.1.2 <OR> spoofing card holder
      1.1.2.1 Phishing
      1.1.2.2 Cheat through mail or phone
  1.2 <OR> Dump communication get encryption keys
    1.2.1 <OR> Analyze data
      1.2.1.1 <OR> Break symmetric key
        1.2.1.1.1 Brute-force attack
        1.2.1.1.2 <OR> Break symmetric encryption mathematically
          1.2.1.1.2.1 Square attack
          1.2.1.1.2.2 Differential attack
          1.2.1.1.2.3 Interpolation attack
          1.2.1.1.2.4 Linear cryptanalysis
      1.2.1.2 <OR> Break asymmetric encryption
        1.2.1.2.1 Brute-force attack
        1.2.1.2.2 <OR> Break asymmetric encryption mathematically
          1.2.1.2.2.1 Factoring by computing
          1.2.1.2.2.2 Differential attack
          1.2.1.2.2.3 Common modulus attack
          1.2.1.2.2.4 Chosen-ciphertext attack
    1.2.2 Man-in-the-middle attack
    1.2.3 Protocol failure
    1.2.4 API attack
2 <OR> Get unauthorized access
  2.1 <OR> Chip rewrite
    2.1.1 ROM overwrite attacks
    2.1.2 EEPROM modification attacks
    2.1.3 Gate destruction attacks
    2.1.4 Memory Remanence Attack
  2.2 <OR> Non-invasive attacks
    2.2.1 Voltages and temperatures change
    2.2.2 Power and clock transients change
  2.3 <OR> Physical attack
    2.3.1 Fuming nitric acid
    2.3.2 Electron beam tester
    2.3.3 Use commercial machine
  2.4 <OR> Break encryption
    2.4.1 Differential Power Analysis
    2.4.2 Simple Power Analysis
    2.4.3 Differential Fault Analysis
  2.5 Bad ACL settings
  2.6 <AND> Use card without permission
    2.6.1 Bad authentication rule
    2.6.2 Card lost or stolen
  2.7 Internal attack
    2.7.1 Mechanical detection
    2.7.2 Microscopic analysis
    2.7.3 Application of test mode
3 <OR> Block service and damage card
  3.1 <AND> Block access
    3.1.1 Block PIN
    3.1.2 Block PIN2/PUK
  3.2 Denial of Service
  3.3 <OR> Card damage
    3.3.1 Card reader damage

(The graphic of attack tree will be shown on our presentation.)

5.1 Evaluation of attacks

(The table of detail evaluation is listed in the appendix)

We can find that there are lots of attacks against smart card listed above, but the major of technical attacks are expensive, uneconomical, and unfeasible. What's more, some attacks seem to be easy to perform, but they should be used with other attacks and need some special equipment to get the access to the card.

6 Solution and Analysis

Most of the attacks need special knowledge or equipment, some attacks even require laboratory support. However, these attacks are not always feasible. With the rapid development of card security measures, now, the smart card manufacturers have several methods to face the challenges from different attacks. To prevent microscopic analysis, the usage of random mapping prevents reconstruction of data. Furthermore, more advanced manufacturing technology and special protection layer (add an additional Si layer as safe layer) will help smart card to avoid reverse engineering and mechanical detection. Through the special design, such as the parallel coprocessor, the smart card can reduce the risk of DPA and non-invasive attacks. Lots of researches have showed that a key that is long enough will raise the difficulty of cryptanalysis. Moreover, the signing of data with private key should be cautious to prevent chosen-ciphertext attack. [9] It suggests that we use different private key to encrypt or sign for different applications. [10]

On the other hand, the eavesdropping attacks have a surprising possible rate. The advantage of cost and easy performance lead it to be one of the most popular attacks. However, if the attackers are well-prepared, they can use the access to the customer's card and PIN in real-time: this is called a relay attack.

An example mentioned by Ross Anderson display a scenario attack, when you pay for a meal in a restaurant using your smart card, the waiter take advantage a counterfeit terminal to simply forward all the traffic from your card wirelessly to an accomplice at a jeweler on the other side of town. The smartcard data stream would go maybe via GPRS to a PDA in the crooks pocket, then to his fake card, and the captured PIN read out via a headphone in his ear. You think you're paying for lunch, but in fact you're buying the crooks a diamond! And unluckily, this type of fraud is difficult to find if the amount of stolen money is small. Although it was found, the bank also rejected being responsible for the loss. [11]

This sort of attack is not expensive and easy to perform, if the merchants are complicity with crooks.

Browsing the entire smart card attack tree, we can also find that the attacks focusing on negligence of human beings and the problem of authentication occupy a part of proportion. It's easy to solve the problem of authentication through biometrics, such as fingerprint identification, voice recognition and handwriting recognition. These measures can really offer the highest security, but think of the expensive equipments and trouble of operation, is this the type of security what we need? [8]

7 Conclusion

We have used the attack tree to list the majority of attacks against smart card. We have also discussed some mitigation to attacks. Through the paper, we understand the state of smart card attack tree. Through our understanding of attacks, we believe that the smart card is not easily hacked and a lot of countermeasures have been used to protect smart cards. There are many advantages we can find, such as the strong encryption, the availability of structure and so on. But it is not satisfying enough. The prevention of phishing and eavesdropping attacks are sometimes shouldered by the card holder. According the last example we give, it shows that the protocol (especially, the protocol "EMV" widely used by VISA and MASTER) need to be improved.

References

[1] Bruce Schneier, Adam Shostack Breaking "*Up Is Hard To Do: Modeling Threats for Smart Cards"* October 19, 1999

[2] Smart Card Basics" *Smart Card Overview"*

[3] Howstuffworks.com *"What is a "smart card?"*

[4] Fargo.com *"Applications- working with smart card"*

[5] Bruce Schneier *"Attack tree"* December 1999

[7] Natalie Podrazik *"Threat Analysis"* February 27, 2006

[8]Smart Card Alliance, "*Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems*" , May 2002

[9].Mike Hendry. "*Smart card security and applications*", 2001

[10].Ross Anderson "*Security Engineering: A Guide to Building Dependable Distributed Systems*", 2001
[11].Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Steven Murdoch, Ross Anderson, and Ron Rivest "*Phish and Chips*" 9th Feb 1998
[12] Zoli Kinceses "*Attack tree of smartcards*", 29th July 2005
[13].Dinoj Surendran"*An overview of Smart Card Security*", 2000
[14].Ken Warren, "*Access Control: Smart Cards under Attack*" March 17, 2006"

Appendix

P: Possible
IM: Impossible

Name of Attack	Equipment needed	Cost	Possibility	Comments
Use a camera to monitor the entering of PIN-code	Camera	Less than $25 low cost	P (if the attacker cooperates with the merchant, it is possible)	Easy, but not always successful. Sometimes, it should be used in combination with other attacks
Hacked terminal	Probes and special knowledge	Medium cost	P	Not a good attack, complicated, and not practical
Counterfeit terminal		More than $200	P	Corrupt merchant would be a good cooperator
Terminal skimmer	Skimming device	$100-2500	P	Capture devices decide the cost of attack, collusion with the merchant would be a good idea
Write down PINs	Mistake made by card holder	No cost	P	Just PINs are not enough.
Phishing	Low technique demand	Low cost	P	Popular attack, but more and more countermeasures are used to prevent it
Cheat through mail or phone	No special demand	Low cost	P	Low vigilance of card holder
Brute-force attack	High speed of computation		IM	Maybe possible in the future, because of the rapid development of computers
Chosen-cipher text attack	Special knowledge		IM	A good cryptanalysis method, but it need some known ciphertext most of time it's impossible
Differential attack	Special knowledge		IM	Just useful on low-round DES
Interpolation attack	Special knowledge		IM	It can be used together with chosen-cipher text attack to improve the rate of success
Linear cryptanalysis	Special knowledge		IM	Old method of cryptanalysis
Common modulus attack	Special knowledge		IM	A large prime can prevent this attack
Chosen-ciphertext attack/RSA	Special knowledge		IM	protect private key carefully

Man-in-the-middle attack	Special knowledge and equipments	Medium cost	P	High risk on RF card/contactless card
Protocol failure	Special knowledge	Low cost	P	Most found and used by staff. It is simple to use and easy to find
Back-end API attack	Special knowledge	Low cost	IM	The flexibility and extensibility requirements of the protocol have made it difficult to implement
ROM overwrite attacks	Special knowledge and laser cutter microscope	Expensive	P	
EEPROM modification attacks	Micro probing needles and special knowledge	Expensive	P	Expert and special equipments
Gate destruction attacks	Laser cutter and special knowledge	Expensive	P	
Memory Remanence Attack	Special knowledge	Medium	P	Result from the ROM to store a value too long
Voltages and temperatures change	Special equipments	Medium	IM	It is particularly effective in the early smart card
Fuming nitric acid		Low cost	P	Sometimes, clear protection layer is useless.
Electron beam tester	Special equipments	Expensive	P	
Use commercial machine	Special equipments	Expensive	P	
Reverse engineering chips	Special equipments	Expensive	P	
Bad ACL settings	Special knowledge	Medium	P	Bad design of OS
Differential Power Analysis	Special knowledge	Medium	P	Effective but special design can prevent from this attack
Simple Power Analysis	Special knowledge	Medium	P	
Differential Fault Analysis	Special knowledge	medium	IM	Complex and not always successful
Mechanical detection l	Special knowledge and needles	Expensive	P	Card can protect by passivation layer
Application of test mode	Special knowledge and equipments	Medium	IM	Use the existing test contact or test mode to restore data. Good safe layer can prevent form this attack
Bad authentication rule			P	No sign check or other negligence on authentication
Card lose or stealing		Low cost	P	Ex. fraudulent use of other people's credit card
Block PIN		Low	P	Utilize the system’s built-in protection measures to reject usage
Block PIN2/PUK		Low	P	Same as above
Denial of Service	Special knowledge	Low	P	Particularly on certification, such as Kerberos
Card reader damage			P	Physical or logic damage result from card reader