An Estimated Model of Risk Analysis of Attacks on Smart Card Authentication Schemes

Deepak Kumar
Research Scholar
Department of Computer Science
Faculty of Technology
Gurukul Kangri
Vishwavidyalaya, Haridwar,
Uttarakhand,India.

Vinod Kumar
Professor and Head
Department of Computer Science.
Faculty of Technology
Gurukul Kangri
Vishwavidyalaya,Haridwar,
Uttarakhand, India

ABSTRACT
With the rapid growth of computer networks, more and more users access the remote server's service in a distributed computing environment. Due to the fast development of the Internet and wireless communications, many activities like online-shopping, online banking, online voting are conducted over it. Authentication is one of the essential security features of network communication. The authentication process ascertains the legitimacy of the communicating partners in communication. In the authentication procedure, the promoter of the communication and the defendant derives some identification codes of each other prior to start of the message transaction. Sundry methods have been introduced regarding the authentication process from time to time. The static approach authentication schemes are vulnerable to different types of attacks. The growth of smart card systems faces security threats to both the card and its environment. Issues related to readers, protocol implementations, the smart card's hardware security features or a combination of logical and physical attacks is of legitimate concern. All the elements of a smart card system have their own specific behavior. They could be attacked in various ways. In this paper we analyze the smart card attacks through a noncyclic attack graph. Noncyclic attack graphs provide an intuitive aid in threat analysis. We dissert that such a formal interpretation is indispensable to precisely understand how noncyclic attack graphs can be framed up during design and analysis. We provide an educational semantics, based on a mapping to attack stack, which abstracts from the internal structure of a Noncyclic attack graph, we study transformations between Noncyclic attack graphs, and we study the attribution and the projection of a Noncyclic attack graph.

General Terms: Smart Card, Attack Graph, Security.

Keywords: No Cyclic attack Graph, Authentication, integrity,

1. Introduction
The development of smart card systems faces security threats to both the card and its environment [8]. Issues related to readers, protocol implementations, the smartcard's hardware security features [6] or a combination of logical and physical attacks [5] are of legitimate concern. The attackers must be classified by their expertise, goals and budget to discover the source of the possible attacks. In a complete system the card readers, the communication lines, and the interfaces between the elements, even the standards of each element and the compatibility between them must be considered. The smart card is not itself the goal. It is the tool for reaching goals and is only a small part of the system. The possible abstract view of attack relations are shown through the path matrix.

	A	B	C	D	E	F	G
A	1	0	0	1	1	0	1
B	0	1	1		1	0	0
C	1	0	1	1	1	0	1
D	1	0	0	0	0	0	0
E	1	0	1	1	1	0	1
F	0	0	0	1	0	1	0
G	0	0	0	0	0	0	1

Table 1.1

TERMINAL-A
TERMINAL OWNER-B
ISSUER-C
DATA OWNER-D
CARD HOLDER-E
MANUFACTUER-F
DEVELOPER S/W MANUFACTUER-G

Three conditions must be present in order for an attacker to carry out an attack against a defender's system.1. The defendant must have vulnerabilities or weaknesses in their system.2. The threat agent must have sufficient resources available to exploit the defender's vulnerabilities. This is known as capability.3. The threat agent must believe they will benefit by performing the attack. The expectation of benefit drives motivation. Condition 1 is completely dependent on the defender. Whether condition 2 is satisfied depends on both the defender and the threat agent. The defender has some influence over which vulnerabilities exist and what level of resources will be required to exploit them. Different threat agents have different capabilities. All the elements of a smart card system have their own specific threats [4].They could be attacked in various ways (see the relevant chapters on [7]) or member parties could attack each other within a smart card system [3].Several publications mentioned above have organized the attacks into a custom-built classification. These taxonomies detail and discuss each type of attacks or attack classes, but the system analyst needs to draw the growing impact of the attacks in the case of a working smart card system. Moreover, the system changes during the design,

development or even working stage, and these changes have to be handled dynamically. Software producers also contribute to the Smart Card security - they should offer their products with properly encrypted data and transfers.

2. Smart Card Security

Security is basically the protection of something valuable to ensure that it is not stolen, lost, or altered. The term "data security" covers the wide range of applications and has great impact on everyone's daily life. The security issues related to smart card come into existence due to assembly and the Authentication procedure of smart card. The smart card is a memory card that uses an embedded micro-processor of the smart card reader machine perform required operations specified in the protocol. Kocher et al. [9] and Messerges et al. [10] pointed out that all existing smart cards cannot prevent the information stored in them from being extracted by techniques such as by monitoring their power consumption. Some other reverse engineering techniques are also available for extracting information from the smart cards. That means once a smart card is stolen by an attacker, he can extract the information stored in it. A good password authentication scheme should provide protection from deferent possible attacks against the authentication procedure of smart card. Smart card used data security system using cryptographic mechanism. Smart card support: Confidentiality, Non Repudiation, Data integrity, Authentication as well as Key generation and key distribution. For Opaque the Authentication, Cryptography is intuitive technique to be used as authentication mechanism. Some security information is stored that could uniquely identify the user this could either use digital certificate, user name password pair or combinative of private-public key pair. Static authentication can be used with symmetric cryptography, where the card issuer generates a digital signature on the smart card. The terminal is authenticated by card through a PIN, after that, it sends the signature to the terminal. At the terminal, Encryption and decryption of data take place and the card only to confer this signature as a password. This means that card does not to do processing but it is continuator of legitimate communication. Public key cryptography will need to be Implemented on the card itself to take amenability of security, Providing a real time dynamic signature to the terminal or host.[11] leach has suggested the public key cryptography for smart card Authentication.[13] verschuren use a combinative Public key and Symmetric key for Smart card Authentication. Urien [12] introduces the perception of a secure and open architecture, where the smart card is not iron bound to any specific application. This new outlook will focus on smart card as internet card. As security is concerned, Cryptography plays main role to provide security , cryptography is integral decomposing of data and network security but it solely does not provide full and competitive solution. There are some serious issues with cryptography (a) Key distribution or Key Exchange (b) safe storage, (c) good key generation. The number of Authentication schemes has been purposed for smart card authentication some of them have faced different possible attacks.

3. Fundamental Concept

The "No cyclic attack graph" concept [1] gives the chance not only to itemize but also to organize in a manageable structure all possible attacks and many attributes of them. In this paper, "Smart card noncyclic attack graph" is introduced. The attack graph is an "and-or" graph where the goal to be reached is on the top and the lines represent the ways where threats could come from. The 'AND' lines must both happen in order to reach the parent node, while in case of 'OR' lines it is enough that one of them is realized. The lowest cost path can be determined to any intermediate node or to the root-node. Each node can have a cost, a chance of occurrence, or even a 'required tools' value connected with it. It is also possible to identify the most probable way from any point in the no cyclic graph to the root. A detailed explanation with many samples about attack noncyclic graph methodology can be found in [2]. New parameters (e.g. The significance of the attack on an exact system) and its value range can be added. The available papers on this topic provide the top-level smart card attack types that can be logical, physical, or social based on the type ; hardware, software or firmware by the target. Sometimes the attacks belongs to multiple types, therefore this classification method is not well suited to the noncyclic attack graph creation. It is possible to build mixed classifications where the elements produce a cross linked net (such as in the figure above), but this is also not the best solution for a noncyclic graph with multiple parameters, which must each have input values to serve different calculations. The existing papers help to itemize and understand the possible attacks, and they can be put in place in a noncyclic graph based on the three main threats against confidentiality, availability and Integrity.

4. Smart card attack Graph

Attributes provide a powerful analysis tool for penetrability scenarios. They help us to grapple the attacks which may with a high probability and which countermeasures should be applied. However, to get micro analysis, it is necessary to have exact values associated with all the nodes of a Non Cyclic Attack Graph. One strategy is to ask experts to offer the values. Another strategy is to engage numerous people, such as the system owner, developers and administrators, to carry out the task both the strategy can be very time consuming, costly and highly error-prone, depending on the tree complexity and the number of attributes. Thus, numerous approaches have been proposed, allowing us to deduce values for one node, based on values already associated with other nodes, or to combine values for several attributes in order to deduce the value of another attribute. As mentioned above, the first level in the noncyclic attack graph has three sub-modes: confidentiality, integrity and availability. In this sample the value domain for the each attribute except probability, Contains three values: Cheap in the range from 1 to 3, Average in the range from 4 to 7, Difficult in the range from 8 to10 and for each node in the Non cyclic attack graph **.**Taking into consideration the exact value of the ranges and the rules used for calculating, each node has its own value. These values can be recalculated if the noncyclic graph or the ranges are modified. Noncyclic attack graphs grow quickly as the builder goes deeper and deeper to the leaves. The noncyclic attack graph for smart card authentication scheme is given below.

1 <OR> Confidentiality

1.1 <OR> Obtain PIN

1.1.1 <OR> User Conduct

1.1.1.1 Written down

1.1.1.2 Find

1.1.2 <OR> dictionary attack.

1.1.2.1 Online

1.1.2.2 Offline

1.1.3 <OR> Guess

1.1.3.1 Field test

1.1.3.2 Luck

1.2 <OR> Masquerade as communicator

1.2.1 Analyze data

1.2.2 Sniff data

1.3 <OR> Unauthorized access

1.3.1 Smart Card Stolen

1.3.2 Plain Text

1.3.3 Built-in code...

2 <OR> Integrity

2.1 <OR> Algorithm

2.1.1 Weak Random Number

2.1.2 <OR>Weak conception

2.1.2.1 Weak Random Number

2.1.2.2 Test code

2.1.3 <OR> Outsider influence

2.1.3.1 <OR> HW + OS

2.1.3.1.1 Key& Memory Reading

2.1.3.1.2 Timing Analysis Attack

2.1.3.1.3 Frequency Manipulation

2.1.3.1.4 <OR> Cryptanalysis

2.1.3.1.4.1 Decrypt the message itself

2.1.3.1.4.2 <OR>Break Asymmetric Encryption

2.1.3.1.4.2.1 Brute force breaks asymmetric encryption

2.1.3.1.4.2.2 Mathematically break asymmetric key

2.1.3.2 <OR> Reverse engineering

2.1.3.2.1 <OR> Side Channel attack

2.1.3.2.1.1 Timing attack

2.1.3.2.1.2 Acoustic cryptanalysis attacks

2.1.3.2.1.3 Differential fault analysis

2.1.3.2.2 Optical analysis

2.2 <OR> Protocol(s)

2.2.1 Bad algorithm

2.2.2 Bad design

2.2.3 Bad implementation

3 <OR> Availability

3.1 <AND> Block access

3.1.1 Block PIN

3.1.2 Block PIN2/PUK

3.2 <OR> Denial of Service

3.2.1 Break Communication

3.2.2 Overwhelmed the server

3.3 <OR>Destroy Hardware

3.3.1 <OR> Card damage

3.3.1.1 Physical damage

3.3.1.2 Logical

3.4<OR> Reflection Attack

3.4.1 Weak Request/Response algorithm

3.4.2 Weak Implementation

3.4.3 Spoof IP

3.4.4 Overwhelmed with a reply

5. Risk Analysis of Smart Card Attack

The Non cyclic attack graph model comprises some sort of parameter computation rules; the equivalent Non cyclic attack graphs should have the same value. Otherwise, the Non cyclic attack graph values depend on the order of attacks and even though different analysts could come up with equivalent Non cyclic attack graphs, their results will not be comparable. We chose a set of attribute values to calculate the risk of attack. We require estimating values of attributes for each node. Attribute are cost-The amount of effort referring to e.g., Equipment or software costs, educational expenses, development costs and resources require for attack. Difficulty-The technical or social skill level needed for the attacker to succeed. Probability-The implicit chance that the attack will succeed could be based on heuristics of similar attacks or perceptional estimations. Impact-This describes how much of the attacker's goal is achieved, when the attack realizes, or how much impact is generated in the system. Impact is a number from 1 – 10 .The value domain for the each attribute except probability, Contains three values:

Cheap in the range from 1 to 3, Average in the range from 4 to 7, Difficult in the range from 8 to10 and for each node in the Non cyclic attack graph .The risk is computed from the other three parameters using the formula
Risk = (probability*impact) /cost
First, we transformed the attribute values into natural numbers. The risk is generally accepted to be the combination of two factors: In order to understand the risk, our model needs to include the impact of each attack. This can be achieved by a simple extension to the Non cyclic attack graph model. The impact can occur at any level in the tree. Although some attack impacts occur when an attacker performs an exploit (at a leaf node), much larger impacts typically occur at higher levels in the tree. The Table 1.2 is given below to compute the value of whole Non cyclic attack graph with respect to the above discussed attributes.

	And-Sub Tree	Or- Sub Tree
Probability	$\prod_{i}^{n} p_i$	$\frac{\sum_i^n P_i}{n}$
Cost	$\sum_{i}^{n} C_i$	$MIN_i^n C_i$
Impact	$\frac{\sum_i^n P_i \cdot m_i}{n}$	$MAX_i^n m_i$
Difficulty	$MAX_i^n d_i$	$MIN_i^n d_i$
Confidence	$MIN_i^n f_i$	$MAX_i^n f_i$

Table 1.2

5. Conclusions

Non cyclic attack graphs provide a formal methodology for analyzing the security of systems and subsystems. They provide a way to think about security, to capture and reuse expertise about security, and to respond to changes in security. Security is not a product -- it's a process. Non cyclic attack graphs form the basis of understanding that process. The advantage of a Non cyclic attack graph is that in the future every new attack type can be inserted or existing node values can be modified and the attack ways can be recounted. It is also possible to connect different Non cyclic attack graphs. Smart card systems are used with biometry or cryptology many times, where both could have their own Non cyclic attack graph. The situation is the same true with the card readers or any other CAD (PCs, laptops or mobile phones), which have their own Non cyclic attack graphs. The creation of a smart card attack graph could involve other areas, both directly and also indirectly influenced areas producing an 'attack forest' of information technology. Last but not least, such an Non cyclic attack graph could help the smart card project managers for planning their project (what are the risks and their cost?), helps the developers using the tree as a checklist when they design their applications (what \must be considered?) and also helps auditors who check the security of a system or an implementation (what kind of controls have been applied?). This work is also a research project and all the enthusiastic interested parties are welcome to add their own tree or small forest to turn the security jungle in a manageable oasis.Like any security analysis, creating attack trees requires a certain mindset and takes practice.

6. References

[1] Bruce Schneier: 'Secrets and Lies' attack trees:

[2] Terrance R. Ingoldsby: Understanding Risk Through Attack Tree Analysis, CSI Computer Security Journal, Spring 2004, Volume XX, Number 2. pp 33-59

[3] Bruce Schneier, Adam Schostack: Breaking Up Is Hard To Do: Modelling Security Threats for Smart Cards, Usenix Workshop on Smartcard Technology, February

[4] David Corcoran: Security-related Exposures and Solutions in Smartcards,Information Security Bulletin, November 2000. pp. 13-22.

[5] Zoltán Kincses: On avoidance of attacks against the pin error counter of smart cards, (CS) – The Fourth Conference of PhD Students in Computer Science 2 Szeged, Hungary, July 2004. Abstract on pp. 68:

[6] Michael Lamla: Hardware attacks on smart cards – overview, Eurosmart SecurityConference, 2000. Marseille, pp. 31-39.

[7] Ross Anderson: Security Engineering – A Guide to Building Dependable Distributed Systems, 2001. John Wiley & Sons Inc.

[8] Wolfgang Rankl, Wolfgang Effing: Overview about Attacks on Smart Cards, 2003,Munich, from their own 'Smart Card Handbook' (John Wiley & Sons, ISBN: 0-470-85668-8).

[9] P. Kocher and B. Jun, \Differential power analysis," Proceedings of Crypto '99, pp. 388-397, Springer-Verlag, 1999.

[10] T. S. Messerges, E. A. Dabbish, and R. H. Sloan,Examining smart-card security under the threat of power analysis attacks," IEEE Transactions on Computers, vol. 51, no. 5, pp. 541-552, 2002.

[11] Leach J. Dynamic authentication for smart cards,Computers & Security, Vol 14 No 5 1995, Volume: 14 Issue: 5 pp.385-389 (5 pages)

[12] P. Urien, "Internet card, a smart card as a true Internet node", Computer Communications, 2000, pp.1655-1666.

[13] Verschuren T., Smart Access: Strong Authentication on the Web, Computer Networks and ISDN system 1998,pp 1511-1519