International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Dominant Attacks on Smart Card Based Transaction

Sivakumar Nadarajan
Research Scholar, PG and Research Department of Computer Science J.J. College of Arts and Science,
Bharathidasan University, Tiruchirappalli, Tamil Nadu, India

ABSTRACT

The smart card (SC) is icon of the current information epoch. Smart card technology is created out there in the market to gain access for product & services, verifying identity, establishment & to facilitate trade. Smart cards are secure devices that enable positive user identification & that they are multi-functional, value effective devices which will be simply adapted for each physical & logical access. This paper discuss concerning basic nature of smart card & therefore the attacks on smart card system. For the longer term of smart card to be bright, it's vital to look into many aspects & factors particularly those resulted due to the rapid advancement in info & communication technology.

Keywords: Smart Card, Multi-Functional, Attacks, User Identification, Market.

I. INTRODUCTION

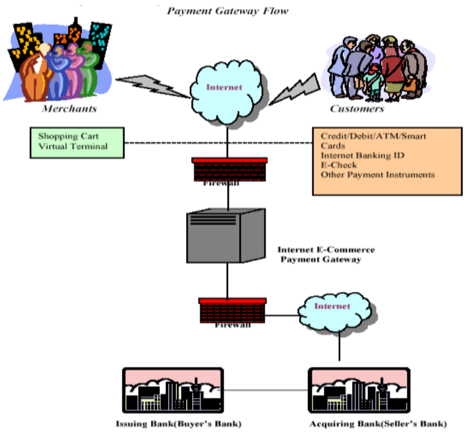
A smart card seems to be credit card however instead of simply having a magnetic stripe, it contains an embedded microprocessor, that makes them safer. The microprocessor is below a gold contact pad on one side of the card. The integrated circuit chip (ICC) is for reading & process data. they'll be used for specific forms of identification, banking transactions, telephone prepayment cards, security authentication, credit cards, mass transit system access, & electronic toll collection & with GSM mobile phone devices. once a smart card is used, identification are often confirmed through an entered password or by scanning it with a reader device. For the next level of security, biometrics (which may be a finger, hand or eye retinal scan) are often used with the card. Recently mexico government has issued 2M smart cards for poor folks for their money benefits & distributing food. during a fresh survey it's found that twenty seventh of smart card applications used within the banking, eighteen is used within the welfare & health, & 15 august 1945 within the transportation. it's additionally applicable in alternative applications like radio security, metering, telecommunications & identification.

II. BASICS OF PAYMENT GATEWAY

Whenever a client buys one thing from a virtual shopping mall, the Payment entry comes within the image for the subsequent functions:

- ✓ Authorising- validatory the buyer's credit/debit card details
- ✓ Clearing- Transferring the transaction to merchant's bank
- ✓ Reporting- Recording all transactions

The following is the steps concerned during a Payment gateway transaction.


Payment Gateway Flow
Merchants
Internet
Customers
Shopping Cart
Virtual Terminal
Credit/Debit/ATM/Smart Cards
Internet Banking ID
E-Check
Other Payment Instruments
Firewall
Internet E-Commerce Payment Gateway
Firewall
Internet
Issuing Bank(Buyer's Bank)
Acquiring Bank(Seller's Bank)

Step one- consumer visits a shopping web site and selects the products or services and clicks on the "Buy" button. A message is sent to the web site concerning the consumer's need to buy and create payment.

Step two- the web store's server, once receiving the message from the customer, adds its digital certificate to identify the mall. This message is currently known as a "Digital Order" and also includes the consumer's ip address and transaction amount. The Digital Order is currently sent to the Payment gateway over a secure network. Security is ensured by data encryption.

Step three- based on the Digital Certificate, the Payment entryway authenticates the web store.

Step four- The Payment entryway offers various payment choices on a screen to the customer.

Step five- client chooses the specified payment option, that is transmitted via the secure link to the Payment entryway.

Step six- The Payment entryway sends the payment details to the effort bank (in case of card transactions) or seller's bank (as termed for different instruments).

Step seven- The acquiring bank sends the data to the buyer's issuing bank (in case of card transactions) or buyer's bank (as termed for different instruments) over a secure link.

Step eight- based on the credit limit and also the payment instrument's validity, the issuing bank either accepts or rejects the transaction. The confirmation/rejection message is transmitted to the Payment gateway through the acquiring bank.

Step nine- The Payment entryway then transmits digital receipts to the shopping website as well as the client.

Step ten- The web store will ship the goods/services to the customer.

As opposed to the lengthy offline method, the online version might at the most require 30-40 seconds.

III. ATTACKS ON A SMART CARD

Since a large variety of parties are concerned in any smart card primarily based system, there are many forms of attacks that have to be thought of. Here we'll look at the attacks by the system participants against each other.

A. Terminal against the Cardholder

These are the simplest attacks to grasp. When a cardholder puts his card into a terminal, he's trusting the terminal to relay any input and output from the card accurately. The power for a rogue terminal to do damage in this environment is critical, and it's not possible for the cardholder to discover this sort of fraud within the context of one terminal. Prevention mechanisms in most smart card systems center around the fact, that the terminal only has access to a card for a brief amount of your time. code on the card might limit the amount of damage a rogue terminal could do. However, there are prevention mechanisms that involve having the user own the smart card terminal, like one attached to a personal computer. the real prevention mechanisms, though, don't have anything to do with the smart card/terminal exchange; they're the back-end process systems that monitor the cards and terminals, and flag suspicious behavior.

B. Cardholder against the issuer

Such attacks target the integrity and authenticity of information or programs keep on the card. These attacks are made attainable by the issuer's decision to use a smart card system wherever the cardholder holds knowledge for the issuer or different party. using the pay telephone application as an example, if the phone were to use an account-based system, wherever a simple card holds a very long account number that's utilized by the phone company to dereference an account keep on a back-end system, then there are account approximation and theft attacks based on the numbers. this kind of system will be increased by adding a challenge/response or inverted hash chain mechanism for sending replay resistant passwords. If the card issuer chooses to put bits that authorize use of the system within the card, they should not be shocked when those bits are attacked. These bits can be authenticated account numbers, or it can be a system with a key buried within the card, on the idea that this key can't be extracted, and correct completion of the protocol indicates that the card has not been tampered with. These systems all rest on the questionable assumption that the protection perimeter of a smart card is adequate for their functions.

C. Cardholder against the software Manufacturer

When the card is issued to an assumed hostile user, the idea exists that the card won't have new software loaded onto it. this can be implemented by the use of preissuance stages with various one-way transformations being employed by the card manufacturer to make sure that the software isn't tampered with. The underlying assumption is also that the split between card owner and software owner is unassailable, and depends on the separation being strong. However, attackers have shown a remarkable ability to urge the appropriate hardware sent to them to aid in launching an attack.

D. Cardholder against the data Owner

Data stored on the card should be shielded from the cardholder in several cases. In some cases, the cardholder isn't allowed to grasp that information. A building access card, for instance, may have a secret worth within the card; information of this value may permit the cardholder to make additional access cards. In different cases, the cardholder is allowed to grasp the worth, however not allowed to alter it. If the card may be a stored-value card, and also the user will modification the value, he will effectively mint money. There are 2 essential characteristics of these attacks. One, the card should act as a secure perimeter, preventing the cardholder from accessing the information within the card. during this context, the card may have to be fairly assured that it'll find and reply to attacks with a minimum of control over its environment. And two, the offender has access to the card on his own terms. he's allowed to take the card into his laboratory and perform no matter experiments he desires so as to learn how they work. There are several winning attacks against the information within a card. These attacks include reverse-engineering and defeating tamper resistance, fault analysis, and facet channel attacks like power and timing analysis.

E. Issuer against the card Owner

Many of the system guess that issuer holds the best-interests of the card-holder. It is not essentially the case, & a malicious issuer will launch many attacks against cardholders. These attacks are usually privacy invasions of 1 kind or another. smart card systems that serve as a substitute for money should be designed very fastidiously to keep up the anonymity and unlinkability that are a property of cash money. Attacks or design failures will well reduce the privacy of the system. Alternately, a system could also be sold as having additional privacy than it in truth offers, permitting the issuer to assemble knowledge surreptitiously about the cardholders. features introduced into the card because the system matures might alter initial characteristics of the system with substantial impact on the privacy of the system. this will count as associate attack by the institution because the cardholder is never asked or ready to recognise the protection impact of a modification to the system created by the institution. These changes are usually not elective from the customer's viewpoint; the sole decisions are to simply accept the upgrade or leave the system. Lastly, this sort of attack could also be disbursed by the issuer, or by the hardware or software designer, together with terminals, while not the information or consent of the issuer.

F. Cardholder against the Terminal

These attacks are terribly delicate. These involve fake or changed cards running rogue software, with the intent of subverting the protocol between the card and therefore the terminal. good protocol style mitigates the danger of those varieties of attacks, which might be created harder by hard-to-forge physical aspects of the card (e.g., the photograph on Visa and MasterCard cards), which might be checked by the terminal owner manually. Note that digital signatures on the software aren't effective here since a knave card will forever lie about its signature, and there's no way for the terminal to see within the card. defensive against this type of attack needs another function split: the cardholder should not be able to manipulate the information within the card.

G. Terminal Owner Against the issuer

In a pre-paid phone card system, the terminal controls all communication between the card and also the card issuer (generally the back-end of the system). during this system, the terminal will always falsify records that don't have anything to do with the smart card, refuse to record transactions, etc. The terminal may also fail to complete one or more steps of a transaction to facilitate fraud or produce client service difficulties for the issuer. By failing to complete the action of debiting a card, a terminal will cheat the issuer, or by finishing a transaction and not giving service (i.e., a pay phone) will produce a service nightmare. These attacks don't seem to be associated with the smart card nature of the system, and area unit merely attacks against the connection between the terminal owner and also the card issuer. Some systems attempt to mitigate this threat by having the card and back-end laptop build a secure affiliation through the terminal. several systems use observance on the rear finish to scale back the effectiveness of those attacks.

H. Impersonation Attack

These attacks are based on dynamic the roles played by various parties. The essential character of such an attack is that a celebration is transformed, resulting in an sudden set of motivations for that party. once a card is taken, the new cardholder has lost all interest in maintaining the safety of the account, and presumably within the physical integrity of the card. Thus, once a system assumes that the info keep on a card is secure as a result of the interests of the cardholder and issuer are aligned, a vulnerability is opened by the stealing of the card. observance attacks will attack the privacy of the transactions created by the cardboard or the secrecy of PIN or alternative information. The latter is maybe a precursor to a full of life attack, not essentially within the domain of the smart card protocol.

I. Third Party Attacks using stolen Cards

The distinction between this attack and an attack by the cardholder is that, the thief doesn't have access to any secret info needed to activate the card and also the thief has solely a restricted amount of your time to hold out his attack before the cardholder can notice that his card has been taken. Hence, all the attacks by the cardholder are potential with the subsequent addition: the thief isn't involved with any long-term repercussions against the legitimate cardholder. it's potential to create defenses into the system either at the card's or at the issuer's level. At the card level, there ar perimeter and anomaly defenses out there. The perimeter defense is that the card will contemplate many bad PIN tries to be indicative of attack. The anomaly observeion defense would be for the cardboard to store history info and detect a pattern change in its use. this is an aggressive demand, however in those cases wherever a card is used offline, it should make sense to boost a flag of some kind, probably requiring contact with its issuer before extra use to allow the rear finish system an opportunity to create a additional elaborate or sophisticated call, or maybe merely to defend the system against card duplication.

IV. MEASURES TO COUNTER THE ATTACKS

A. Prevention

The first step within the design is to review the protection of each link within the security chain. it's important to that no weak link exists, as this may be the doubtless point of attack. one amongst the foremost common oversights is to assume the people working with the system are not at risk of various temptation or threats. A designer that overlooks this puts the system and people in danger. Potential attackers usually seek for the best come on their investment, therefore a security designer should make sure that each part of the system is secure enough to deflect potential attackers to a a lot of profitable target.

B. Detection

The next step is to design in strategies of detection. One should assume each part may be a potential target. even as banks have panic buttons for the tellers and perimeter security alarms, therefore ought to systems, that use revolving credit technology. strategies to detect, live and isolate fraudulent activity are very important to the safety management. credit card systems tolerate a precise quantity of fallacious activity, however is measurable and regarded a part of doing business.

V. CONCLUSION

This paper presents an in depth study of the smart card system attack and conjointly this paper discuss varies components concerned in authentication techniques using smart card. a final purpose to think about is that security may be a unending battle. As technology improves, either side of the battle have higher tools to figure with. revolving credit manufacturers invest various dollars on improving the protection and that they leverage the millions invested with by the element providers. This paper attempt to study the smart card system, varied styles of attacks that it's susceptible to and measures to counter such attacks. Finally, further investigation must be allotted in the future to seek out the matter on the smart card security system.

VI. REFERENCES

[1]. Sebastien Canard , Herve Sibert "Votinbox - a voting system based on smart cards"France Telecom, Research and Development, 42 rue des Coutures, BP 6243, F-14066 Caen Cedex 4, France.

[2]. Rahul J. Jadhav, Dr.Pralhad K. Mudalkar "Smart Card Based e-PDS System"International Journal of Advanced Research in Computer and

Communication Engineering, Vol. 2, Issue 10, October 2013.

[3]. Sivakumar Nadarajan, Dr.Balasubramanian Ramanujam, "Encountering Imbalance in Credit Card Fraud Detection with Metaheuristics"Advances in Natural and Applied Sciences. 10(8); Pages: 33-41,2016.

[4]. V. K. Narendira Kumar and B. Srinivasan, Receipt-Free Electronic Voting Scheme with Smart Card Using Blind Signature, International Journal of Computer Communications and Networks (IJCCN), 2(3), pp 27-42, 2012 IJCCN 2, 3, Article 3 (December 2012),

[5]. Jurlind Budurushi, Stephan Neumann and Melanie Volkamer "Smart Cards in Electronic Voting: Lessons Learned from Applications in Legally-Binding Elections and Approaches Proposed in Scientific Papers"

[6]. Ding Wang, Ping Wang, Chun-guang Ma and Zhong Chen "Robust Smart Card based Password Authentication Scheme against Smart Card Security Breach"

[7]. Sudarshan K. Valluru "Design and Assemble of Low Cost Prepaid Smart Card Energy Meter - A Novel Design"International Journal on Electrical Engineering and Informatics-Volume 6, Number 1, March 2014

[8]. K. Eswar Kumar, Ashok Kumar Yadav, Dr. T. Srinivasulu "Smart Card based Robust Security System"International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 2, Issue 5 (March 2013)

[9]. Jorge Ferrari Robert Mackinnon, Susan Poh Lakshman Yatawara "Smart Cards: A Case Study"International Technical Support Organization , http://www.redbooks.ibm.com

[10]. Sivakumar Nadarajan, Dr.Balasubramanian Ramanujam, "Article: Enhanced Anomaly Detection in Imbalanced Credit Card Transactions using Hybrid PSO".International Journal of Computer Applications 135(10):28-32, 2016.

[11]. Shen, J.-J., Lin, C.-W., and Hwang, M.-S., "Security Enhancement for the Timestamp-Based Password Authentication Schemes using Smart Cards", Computers & Security, Vol. 22, No 7, Elsevier, 2003, pp. 591-595.

[12]. Yang, W.-H. and Shieh, S.-P., "Password Authentication Schemes with Smart Cards", Computers & Security, Vol. 18, No. 8, Elsevier , 1999, pp.727-733.

[13]. Chan, C.-K. and Cheng, L. M., "Cryptanalysis of a Timestamp-Based Password Authentication Scheme", Computers & Security, Vol. 21, No. 1,Elsevier, 2002, pp. 74-76.

[14]. Fan, L., Li, J.-H., and Zhu, H.-W., "An Enhancement of Timestamp-Based Password Authentication Scheme", Computers & Security, Vol. 21, No. 7, Elsevier, 2002, pp. 665-667.

[15]. Sivakumar Nadarajan, Dr.Balasubramanian Ramanujam, "Fast and Effective Credit Card Fraud Detection in Imbalanced Data using Parallel Hybrid PSO"International Journal of Advanced Research in Science, Engineering and Technology, Vol. 3, Issue 9 , September 2016