Cybercrime in "Credit Card Systems": Case Study on the 2014 Korean Credit Bureau Data Leak

Walter. T. Mambodza[1], Robert T. R. Shoniwa[2,]V. M. Shenbagaraman[3]

[1, 2] SRM University, School of Computer Sciences,
Kattankulathur, Kanchipuram, National Highway 45, Potheri, Tamil Nadu 603203, India

[3]SRM University, Faculty of Management,
Kattankulathur, Kanchipuram, National Highway 45, Potheri, Tamil Nadu 603203, India

Abstract: ***As technology is advancing Credit card systems have become the corner stone of E-commerce-related payments. People have become dependent on online payment systems. The increase in its importance causes a lot of privacy and security concerns. The researchers performed a business case analysis on the 2014 internal attack on the Korean Credit Bureau's databases focusing on the stolen credit card details of customers. A study on literature review was conducted to identify the possible threats, formulate solutions and develop a framework as a countermeasure from future attacks.***

Keywords: privacy, security, threats, ecommerce, framework

1. Introduction

More than 100 million South Korean credit card and account details have been stolen and sold to marketing firms, with the President and U.N. Secretary General also among the victims. According to Reuters, around 130 people have joined a class action suit against their credit card providers in what is expected to be the first in a storm of furious litigation. Local Korean media claimed that most South Koreans who own a credit card have been affected. The country's population stands at around 50 million and the number of affected people is up to 20 million. An employee of Korea Credit Bureau, who was ironically responsible for new software development to detect credit card fraud, stole the data in 2012 using a USB device, claim prosecutors.

2. Review of Literature

"The paper highlights unique characteristics of technologies of the e-commerce world as compared with traditional payment systems and the way these characteristics may be exploited to compromise payment. Focus has been upon aspects such as loss of collateral information through techniques such as aggregation and disaggregation of payment systems and use of third party intermediaries." Stephen Burns [1].

"E-commerce is now used to complete many very important transactions. However, due to the threat of cybercrime, these transactions are at risk and this can result in loss of critical data if not protected well. A range of possible threats exist that can compromise these transactions and this can be resolved by using known and trusted mechanisms (e.g. authentication) to secure them. Further research can be done on the tools used to discover and deal with the listed aspects of cybercrime as well as how the two entities interact and affect each other." N. Leena [2].

"Many cybercrimes are now being committed from distant locations outside national borders. Through the strategic targeting of financial institutions such crimes can ultimately derail a nation's productivity. This was found to be true and in response, national security organizations in the EU and the USA put in place guidelines and policies to help avoid and handle such crimes as a united front. Increasing the scope to include industrial or national power-grid management institutions can be done in future. This is with the goal of dealing with homegrown threats which can cause the same problems from within the country's borders." Raluca Georgiana [3].

"A discussion on some of the issues in the state of information security as it pertains to e-commerce. Topics include the neglect for information security in the heads of e-commerce pioneers, intrusions and consequences that have been revealed to the general public, and a few notes about the future. It is perhaps those who consider security as a core function of e-business that will be the long-term beneficiaries of this revolution." David J. Olkowski Jr [4].

"With the business of e-commerce booming, more and more sensitive information is being passed around on the web. Financial and identity information are constantly at risk of being stolen as more and more users take advantage of the ease of doing business online through web applications. The purpose of this paper is to discuss one particularly salient security threat that this creates: session hijacking. It is important to protect our session data at both the network and application levels. There is need for continuous monitoring and testing of the network." Mark Lin [5].

"The robots.txt file will impact your page rank rating with search engine providers. Configuration errors can result in web site revenue losses. A misconfigured robots.txt file can also lead to information disclosure, a foothold to system compromise. A basic understanding of this simple text file can prevent e-commerce problems and security issues. Robots.txt can be a source of information disclosure from either comments or sensitive directories and files. Sensitive information can be exposed to the public via search engines and can lead to site compromise or private information exposed to competitors." Jim Lehman [6].

“A clear and emerging new channel in the space of banking and payments is mobile. A key challenge with gaining user adoption of mobile banking and payments is the customer’s lack of confidence in security of the services. The mobile banking and payments ecosystem is complex and dynamic. Security and the perception of security will clearly play a role in who ends up dominating. A foundation element of that trust is the security of products and services.” Vanessa Pegueros [7].

“Advancements in information technology have driven the information security discipline to the forefront in the quest to protect customer data. Sound privacy policy for an organization must be supported by the appropriate information security infrastructure. The highest priority is confidentiality. Information security enables organizations to operate responsibly with sensitive customer data. As the new information security technologies are created, firms need to assess their impact on privacy policy.” Alan Pacocha [8].

“Thousands of people use their credit cards every day, to make payments over the internet. But giving out their credit card numbers make many of them feel insecure and others even reluctant to use the internet. SET is safer than other payment methods and the insecurity barrier in front of e-commerce is getting pulled down.” Onur Arikana [9].

“Today, the public enjoys shopping and banking from the comfort of their home while companies save money on processing transactions and hiring employees. However, with any innovation, there are obstacles to overcome before the venture is deemed successful. In e-business, encompassing any transaction via the internet, the information exchange can be simple. The law needs to adopt policies stating companies must report successful break-ins. It should be mandatory to report security breaches such as gaining access to databases or exposing financial information without regard to its reputation.” Changyin Zhou, Chunru Zhang [10].

“This paper analyzes the building blocks of trusted smart phone and proposes a framework to provide a trusted platform for mobile electronic payment. The paper outlines the security measures which are applied to smart phone to make it trustworthy. The secure smart phone acts as an e-wallet and serves as a key component for the electronic payment systems. Furthermore, it proposes a mobile payment framework, in which the secure smart phone acts as an e-wallet.” Kimberly Lemiux [11].

3. Research Gap

Cybercrime has come into existence due to the emergence of buying and selling of goods and services using electronic means. However most transactions involve the use of money and various mechanisms have been devised to make electronic commerce a success. The use of plastic money, digital money, e-wallets, e-cash, online payment systems and service provision has become rampant. Credit cards from companies such as VISA, MAESTRO and MasterCard are now being used world-wide to make payments. However a lot of problems and attacks have been on the increase due to the use of these methods. A lot of researchers have done research and from the review of literature many attacks come from external sources but for this research our focus is going to be cybercrime in e-commerce from an internal source.

4. Objectives of the Study

- To perform a business case analysis on the Korea Credit Bureau
- To review literature on related cases or research to come up with solutions to the problems
- To create a secure framework for credit card bureau

5. Scope and Limitations of the Study

There are various cybercrime in e-commerce but our research will focus on the loss of customer credit card details from Korea Credit Bureau. The limitations of the study are that the research is based on the information provided by various newspapers and websites only.

6. Methodology

The researchers came across an article on the huge data leak at the Korean Credit Bureau in 2014. Further primary investigation through the use of magazine and newspaper articles from reputable sources such as the Washington Post and Reuters proved two points:

- There had been other information security incidents that had occurred in the recent past in Korea
- There was also a growing number of cases regarding data leaks and theft of client information in developed countries such as Korea and the USA

This highlighted a major problem in the developed world regarding the use of credit cards. A study was then done to prove whether a country’s economic development has any form of correlation to the number of credit card related crimes. This was done through the analysis of published articles on this topic and related aspects. To add to that, some other articles claimed that due to the rapidly closing technological divide between More Economically Developed Countries (MEDCs) and Less Economically Developed Countries (LEDCs),it would most likely be just a matter of time before these cases became common to more countries in the world. This then led to the research team looking into other incidents related to crimes involving credit cards while using the Korean Credit Bureau case as the chief reference.

A number of cases were noted from newspaper articles, magazines as well as journal papers. However, there was a certain norm followed by most of the papers. This was basically that most of the cases that the research team came across were mainly focused on attacks from external entities. Less were on the threat from internal attackers who, according to another paper, are actually a much bigger threat to organizations than external hackers.

This aspect then led to the analysis of studies on why this is so which came to prove that it was because of a number of factors including the reputation of an organization that contributed to this. This logically made sense since an organization has to look out for itself and not compromise its profit-making capabilities as was highlighted in another article. Therefore, using the available data on cybercrime, the researchers then decided to focus on the aspect of internal security breaches and a possible solution to them.

The analysis of the available data then led to the design of the proposed internal security framework. This framework involves a number of basic aspects to be considered when implementing a company's security policy and related mechanisms. Due to the constantly changing technological landscape, it would not be ideal to specify what algorithms and software should be used to optimally implement the framework. However, in order to paint a better picture, currently used and recently created information security tools were used to better explain the workings of the proposed framework. The overall findings of the study were then summarized and possible solutions to the Korea Credit Bureau case were also highlighted after an analysis of similar incidents in other countries. Any other concepts that were discovered during the research process but did not fall within the predefined scope were then added to possible suggestions for the future

7. Analysis of Korean Credit Bureau Data Leak

7.1 Relationship between involved entities

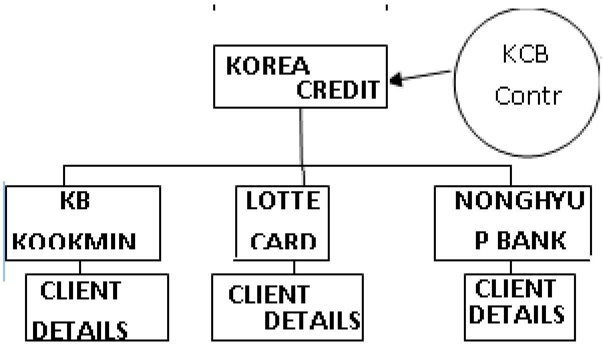

Figure 1: Relationship between entities involved in Data Leak

The Korea Credit Bureau (KCB) is a company that offers risk management and fraud detection services to banks and credit card companies in South Korea. These banks include KB Kookmin Bank, Lotte Card and Nonghyup Bank. This means that selected individuals at the Korea Credit Bureau have access to the databases located on the internal servers at these three companies. It should be noted that the three mentioned are also the ones who were the worst affected by this incident. A lot of crucial data was compromised including:

- Personal identification numbers
- Credit ratings
- Credit card details
- Contact details

However, passwords were not taken.

When and how the leak occurred

The employee was a temporary consultant at the Korea Credit Bureau who had access to a number of the databases. This was because he had been hired to work on the Company's Fraud detection system and was thus given access to the databases. The employee had access to a number of databases on the internal servers of the three companies in question. The incident occurred for a period of one and a half years from October 2012 up till December 2013. During that time, the contractor used his external hard drive to copy client details from the databases of the firms involved. He then sold the data to phone marketing companies.

Customers affected by the Leak

Korea, like most developed nations, relies heavily on the credit card system. According to Reuters, the average Korean citizen has up to five credit card accounts. With that in mind, it was also found out by the Financial Supervisory Service (FSS) that through this leak, a total of up to 20 million South Koreans had their personal details revealed. In a country with a population of 50 million citizens, that means approximately 40% of the country's population was affected by this attack.

Detection of Leak

The incident was only identified in late 2013 when a forensic audit was being undertaken. In a review by the Financial Supervisory Commission (FSC) it was discovered that the companies had been negligent in preventing the breach.

Impact of the Leak

Most of the affected customers have decided to cancel their accounts with the affected banking institutions. Others chose the option to apply for new cards. There could be a rise in identity theft cases due to the leaking of the customers' personal details. These details included ID Numbers, contact details as well as credit ratings and home addresses. Knowledge of this data is all a criminal would need to undertake identity theft.

According to the Financial Supervisory Commission (FSC) in Korea, the banks affected were fined for neglecting their duties during this incident. They were also banned from issuing new credit cards for the period from the point the verdict was reached. The perpetrator and the managers of the phone marketing companies he sold the details to were also arrested. The credit card firms involved were also ordered to cover any financial losses their customers would have incurred due to the incident. However, nothing could be done about the ripple effects regarding the leaked personal details. Given the window period during which the contractor committed the crime, the details cannot be retrieved again and the damage has already been done. The breach also triggered a reaction from the FSC and other regulators to review all financial firms and also how the firms protect customer data.

8. SWOT Analysis

The researchers performed a SWOT analysis on the case and this was the result from the analysis

Table 1: SWOT Analysis

STRENGTHS	WEAKNESSES
• Efficient validation of potential creditors • The bureau has updated database of creditors details	• System is not foolproof and databases are not secure • Weak company policy regarding the use of removable media • The employee who developed system was the one who stole information
OPPORTUNITIES	THREATS
• -Reliable source of information, so easy to sell information to competitors or in the market • -Loss of customer confidentiality	• Law suit from customers and credit providers • Loss of goodwill • Risk of identity theft for client

9. Findings

- The company policy regarding the use of removable media was weak
- There method used to allocate user privileges for separate duties was inefficient
- The database was not secured and was easily accessible with records visible in plain text
- They did not frequently monitor database access logs
- They did not perform audit trails at regular intervals

10. Suggestions

Credit card bureau should use the framework below (illustrated in figure 2) to ensure security:

- Have strong company security policies by following Generally Acceptable System Security Protection (GASSP guidelines. For example, the policies should allow the use of software that prevent the use of removable media on important servers
- To encrypt information stored on database to make it difficult to access by using encryption techniques such as FHE (Full Homomorphic Encryption) and PHE (Partial Homomorphic Encryption)
- Use appropriate intrusion detection system (IDS) types such as Anomaly Based IDS for the Korea Credit Bureau scenario
- To secure databases by passwords by using hashing algorithm such as SHA-1 and MD5
- To change customer credentials such as credit card passwords regularly.
- Perform audit trails at regularly intervals
- Implement effective physical security
- Use monitoring tools such as installing access controls and CCTV on server rooms
- Manage and distinctly separate user access levels and privileges through methods such as indistinguishable obfuscation.
- Establish Baseline controls.

11. Future Scope of the Study

Future work consists of coming up with other security related methods of protecting an information asset. This can be done by taking into consideration the confidentiality, integrity, usefulness, possession, authenticity and availability of information.

12. Conclusion

Organizations should not only worry about the possible threats and attacks from outside the organization but should ensure a secure environment to protect their systems from both the inside and the outside. Cybercrime exists everywhere and this analysis paves a way for security specialists to enhance the cyber security within their respective organizations.

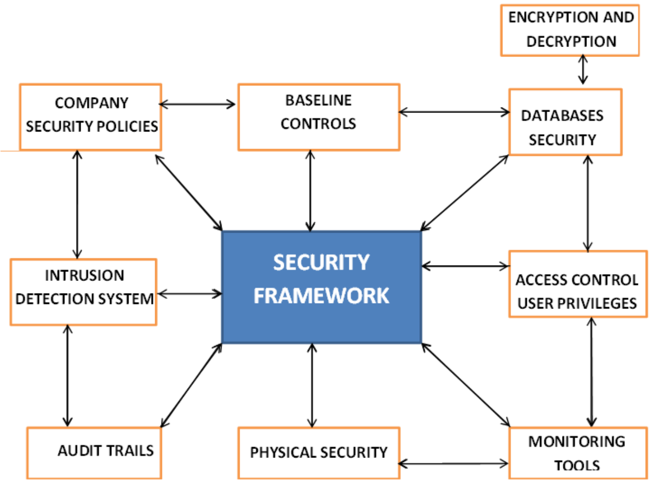
ENCRYPTION AND DECRYPTION
COMPANY SECURITY POLICIES
BASELINE CONTROLS
DATABASES SECURITY
INTRUSION DETECTION SYSTEM
SECURITY FRAMEWORK
ACCESS CONTROL USER PRIVILEGES
AUDIT TRAILS
PHYSICAL SECURITY
MONITORING TOOLS

Figure 2: Security Framework designed by the researchers for cyber security

References

[1] Stephen Burns, Unique characteristics of ecommerce technologies and their effects upon payment systems, Oriental Journal of Computer Science & Technology Vol. 4(1), (2011)

[2] N. Leena, Cyber Crime Effecting E-commerce Technology, Oriental Journal of Computer Science & Technology Vol. 4(1), (2011)

[3] Raluca Georgiana, Borderless Crime: Computer Fraud, Database Systems Journal vol. III, no. 1/2012

[4] David J. Olkowski, Jr, Information Security Issues in E-Commerce, SANS Whitepapers

[5] Mark Lin, An Overview of Session Hijacking at the Network and Application Levels. SANS Whitepapers

[6] Jim Lehman, Robots.txt, SANS Whitepapers

[7] Vanessa Pegueros, Security of Mobile Banking and Payments, SANs whitepapers

[8] Alan Pacocha; Using Security to protect the privacy of customer information; SANs whitepapers

[9] Onur Arikan; "SET" To pull down the insecurity barrier in front of e-commerce, SANs whitepapers

[10] Changying Zhou,Chunru Zhang; A Trusted Smart Phone and Its Applications in Electronic Payment

[11] B. R. R. Rantala, "Bureau of Justice Statistics Special Report Cybercrime against Businesses, 2005."

[12] S. Ó. Ciardhuáin, “An Extended Model of Cybercrime Investigations,” pp. 1–22.

[13] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, “CRS Report for Congress the Economic Impact of Cyber-Attacks.”

[14] R. Popa, “Borderless Crime-Computer Fraud,” Database Syst. J., vol. III, no. 1, pp. 49–58, 2012.

[15] M. I. L. R. Ustad, “private enforcement of cybercrime on the electronic frontier,” pp. 63–116, 2002.

[16] J. Govil and J. Govil, “Ramifications of cybercrime and suggestive preventive measures,” in 2007 IEEE International Conference on Electro/Information Technology, 2007, pp. 610–615.

[17] K. O. Shea, “Cyber Attack Investigative Tools and Technologies For more information :” no. May 2003.

[18] B. Sahu, N. Sahu, S. K. Sahu, and P. Sahu, “Identify Uncertainty of Cyber Crime and Cyber Laws,” in 2013 International Conference on Communication Systems and Network Technologies, 2013, pp. 450–452.

[19] “Infosecurity - Data on 350,000 Epson Korea customers compromised.” [Online]. Available: http://www.infosecurity-magazine.com/view/20412/data-on-350000-epson-korea-customers-compromised. [Accessed: 25-Feb-2014].

[20] “Infosecurity - Credit Card Details of 20 Million South Koreans Stolen.” [Online]. Available: http://www.infosecurity-magazine.com/view/36535/credit-card-details-of-20-million-south-koreans-stolen/. [Accessed: 25-Feb-2014].

[21] “Almost 40% of South Korea Hit in Major Credit Card Hack.” [Online]. Available: http://mashable.com/2014/01/20/south-korea-credit-hack/. [Accessed: 25-Feb-2014].

[22] “Theft of Data Fuels Worries in South Korea - NYTimes.com.” [Online]. Available: http://www.nytimes.com/2014/01/21/business/international/theft-of-data-fuels-worries-in-south-korea.html?_r=0. [Accessed: 25-Feb-2014]

Author Profiles

Walter. T. Mambodza is a student studying towards an MTech in Information Security and Cyber Forensics at SRM University. He holds a BTech (Hons) degree in Computer Science from Harare Institute of Technology (2011).

Robert T.R. Shoniwa is a student also studying towards an MTech in Information Security and Cyber Forensics at SRM University. He also holds a BTech (Hons) degree in Computer Science from Harare Institute of Technology (2012)

Dr. V. M. Shenbagaraman is a Professor of Systems at SRM University. His areas of specialty are e-banking, Information security and ERP. He is a chartered Electronics and Communication Engineer from the Institution of Engineers, Kolkatta. He holds an MBA in Finance and IT from University of Madras. He obtained his Ph.D from Pondicherry Central University, India.(2010)