Data Privacy and Protection - the Way Forward

[1st] Ms. Haritha. N
Symbiosis Centre for Information Technology,
Pune , India

[2nd] Mr. Karthick Deepan. S
Symbiosis Centre for Information Technology,
Pune , India

[3rd] Prof. Nisha TN
Symbiosis Centre for Information Technology,
Pune , India

***Abstract*-The growth of technology is digitally transforming various industries. Data is an integral part of the technological surge. Due to the digitalization, securing and protecting data is becoming a cumbersome task. The banking sector is one of the most critical sectors. It is handling highly confidential data of the people and has thus become the victim for most of the data breaches in the recent years. Various data breaches have led to the downfall of the Indian banking industry, whose repercussions have been high.**

Many renowned banks were the victims of cyber- attacks that took place from the year 2016 to 2019. The reason for the respective attacks were not explicitly mentioned in any public platforms. But, there are various ways in which this could have happened. The reasons range from specialized malwares to unprotected servers and old SWIFT transactions.

In this research paper, we will follow a case based approach to probe into these biggest data breaches of the banking industry, analyze the reason behind the data attacks, and perform a detailed analysis on the various causes that led to the attacks that left the entire Indian banking industry aghast. We will also be focusing on the control recommendations like implementation of sandbox model, implementing on-demand scanning and on-access scanning for the same in order to pave a data breach free road to the future.

Keywords—Cyber-attacks, cyber security, Obfuscation ,data breaches, banking sector, control recommendations, sandbox model, on-access scanning, on-demand scanning

I. INTRODUCTION

Data is a main constituent of all the major sectors like banking and finance, healthcare, Information Technology etc. Technology is changing which is in turn is changing the nuances of all the industries. In all these changes, data is used in ethical and in both unethical means. Data privacy is a growing concern worldwide. There are certain industries in which data privacy is highly significant. A small exposure of private data will cost a lot in terms of money and reputation. One of those sectors which is sensitive towards data privacy is banking.

Though implementing various controls and techniques, the data breaches continue at a steady rate in the banking industry. Various banks all over the world, are the victims of data breaches.

There were various instances of data breach which were prevalent in the banking sector from the year 2016 till 2019. More than 3 million cards were compromised, and the customers' personal details were leaked in the public space. Indian Banks data breach was reported in October 2016. The users reported unauthorized use of their cards in many parts of the world but predominantly in China. One of the biggest banks in India announced the blocking and replacement of almost 600,000 cards over the entire nation. An audit performed by SISA Information Security reported that the 2016 Indian Bank Data breach was due to malware injection and vulnerabilities in the Hitachi Payment System.

In 2018, a renowned bank was a victim of the hackers. The cards of various customers were cloned, and an amount of 94 crore was illegally transferred from various customer accounts. This was a biggest malware attack in the banking sector that resulted in monetary and reputational damage.

One of the renowned and largest banks in India, leaked account data of millions of customers on January 30th, 2019. The server of the bank which contained all the customer details was attacked due to the lack of password protection. The glitch however was resolved in the later stage but left with major losses. The fraud cases are growing in large numbers, where the frauds are happening due to various reasons ranging from of identity theft and aadhaar data scammers have compromised bank accounts and stolen money from those accounts.

In an age of technology integration, interdependence of data is becoming a major threat to privacy. Yet current regulation focuses on the sharing of information between two parties rather than multi-factor situations. This research is based on assessing the various factors that has led to data breaches in the banking sector. To analyze the reason behind the attacks, to research on the loopholes that were used to carry out the attacks and the future recommendations to prevent such attacks. This study can be used to provide information about the current trends of data privacy, and looking ahead at the scope of it in the banking sector. Apart from the banking sector, the research will also provide insights about the general data protection and privacy and how India as a country can nurture itself technologically to forbid unexpected events in the near future.

II. LITERATURE REVIEW

Several Banks, in India and globally have become a brunt for data breaches and data related issues. In 2016, India witnessed one of the biggest data leakage issue. Various leading banks were the victims of this attack. This attack took place due to the malware infection, which was detected six weeks later. The infection compromised many transactions. Malicious attacks could have been anything ranging from viruses, Trojan horses, and botnets [2]. As per the reports from CERT-In, it alerted the banks on the backdoor Trojans. Trojan horse programs cannot replicate themselves, in contrast to some other types of malware, like viruses or worms. A Trojan

horse can be attached to a software, or it can be spread by tricking users into believing that it is a useful program.

There are two terms known and "packer" and "compressor" which are used to describe the components that change the binary structure of the files. This is done by reducing the spaces in the files. A file when becomes from uncompressed to compressed, becomes undetectable. [1] The compression takes place with the help of various compression algorithms. Many such compression algorithms when run, goes undetectable by creating a new binary signature. The credentials of the users are thus compromised this way. [1]

The cards of various customers were cloned, and a whooping amount of 940 million was illegally transferred from various customer accounts in one of leading banks. This was a biggest malware attack in the banking sector that resulted in monetary and reputational damage. There are various reasons which are speculated. One of it could be, the ATM or the Point Of Sale banking switch that was targeted in the bank attack. This switch is a component that provides terminal support which forms as an interface to core banking solution, and connectivity to various networks, which includes networks ranging from regional to international. [3] The bank attack unlike the other attacks was more advanced, well-planned, operation that focused on the bank's infrastructure. The major reasons for this attack would be creation of a proxy switch. The payment details were never sent to the Core Banking Systems (CBS), but were sent to the proxy switch. This resulted in attackers sending fake responses by authenticating the transactions. [3] Apart from the ATM Switch, reports claim that the SWIFT Environment was also compromised. SWIFT is an inter-bank communication. It has been adopted by large sample of banks – 6848 banks across 29 countries in 2017 [4]. Attacking the SWIFT system, might be a common way for the hackers to perform their act. The reason this behind this can be predicted to be an outdated SWIFT System [4].

Many IT-based banking products, services and solutions are available today. A few of them are, Phone Banking, ATM, Credit, Debit and Smart Cards, Net Banking & SWIFT Network [5]. Due to the bloom of IT, many cyber related crimes pose a high risk to certain industries. The recent attack on one of the banks, occurred due to the negligence of the employees, where the server was not password protected. The bank uses a quick text message method, to help the customers who do not have smart phones. This is a process in which the customer's phone number is identified and the details are collected based on that and then sent as a text message. The scenario in which the server is password-less, allows the user to see the in and out of the messages travelling over the network. The lack of password protection may result from, for example, the possibility that an attacker could have modified the function of the public-access terminal with a spyware program. [6] A Spyware is a software that gathers the user information with the help of user's internet connection without the user's knowledge. The Spyware has the ability to record all that happens in a network including the transactions [5].

Audits play an integral part in any sector. The significance of audits in banking sector is tremendous. Every bank must have an internal audit committee. The internal audit group should perform activities free of doubt and interference [7]. The relationship between the internal audit and banking supervision is important for evaluating the work of the audit department in the bank. This includes testing management processes in identifying, measuring, monitoring and controlling risks [7].

III. ANALYSIS

The research is focused on the three major attacks which have created great impacts in the Indian banking history. The attacks were mainly due to malware infections and lack of password protection. We will be analyzing on how these malware infection has occurred, what might have been the possible way of the infection, implications of lack of password protection in servers and databases. The servers and the databases which are not password protected, can be easily tracked using spyware. The working of spyware and the attack of it on the devices will be discussed further. Good standards and procedures can resolve the problems of such mishaps in the future. Analyzing the current audit practices and providing enhancement suggestions in the audits practices will also be a part of focus. The efficient techniques in the processes of the banks and to improve the audit process will also be discussed further in this paper.

A. Case 1 - 2016 Indian Banks Data Breach:

Many renowned banks in India, were the victims of data breach in the year 2016. The attack was due to the malware attack in the Hitachi payment systems. According to SISA, the attack claimed to be a very sophisticated one. The attack was capable of spreading itself at an alarming rate throughout the entire payment system. The hackers created a dummy code book capturing all the numbers between 0000 to 9999 in order to steal the PIN that is used for cash withdrawal and transactional purpose. SISA did not reveal the details or the reasons of the attack pertaining to the confidentiality aspects of their client (Hitachi). Though the exact way of propagation of the attack is not revealed, there are many ways in which this could have been carried out.

1) The Malware:

The malware that affects the payment systems in called as POS Malwares. POS malwares were first discovered in the 2008 in which the visa cards were exploited. The attackers using the malware extracted the magnetic stripe data from the memory.

2) Working of magnetic stripe cards:

When the card is moved in the card reader, voltage is induced in the device. The voltage is then amplified, and recorded on a processor/device which later authenticates and carries out the transaction. The information is captured on a track basis (track 1 and track 2). Track 1 data gives the information about the card holder, name and account number. Track 2 stores the information related to the card.

3) Propagation of the attack:

The card skimming attack that led to massive data breach is a multi-step process.

a) The attacker gains access to the network
b) Traversal to gain access to the payment system within the network
c) Installation of the malware

d) Exfiltration using the staging server

Attacker gains access to the network using external network system, if the system is weak. This could be done in many ways ranging from SQL injection on the server or by accessing a periphery device that is not password protected. There are various tools in which the attackers locate and access the systems with the Cardholder Data Environment (CDE). The basic and the simplest method is to gain the user credentials, which could have been possible using various techniques like brute force, password hash extraction, key logging, attaining the domain control access etc. Once the attackers gain access to the CDE, the malware can be installed, which thus results in the exposure of the data in the payment system therefore resulting in leakage. RAM scrapping malwares are those which collect the credit card numbers which are read into the computer memory. The gathered data is then stored in the temporary system and then extracted using exfiltration. The data reaches the external system by hopping through the internal network. During exfiltration is when the staging server comes in to the picture. Staging server is the one in which communicates on a regular basis with the payment system during transaction. The RAM scrapping malware is targeted to the staging server where the information is collected and stored until it is sent to the attacker. The data which is gathered is also transferred to many internal systems until it reaches the final external system. The compromised external system could be like a targeted FTP server that belongs to any third party. Apart from malware, various Trojan also could also be the possible reasons for the data breach. Trojans like Dexter, Alina, BlackPOS, Citadel and many more.

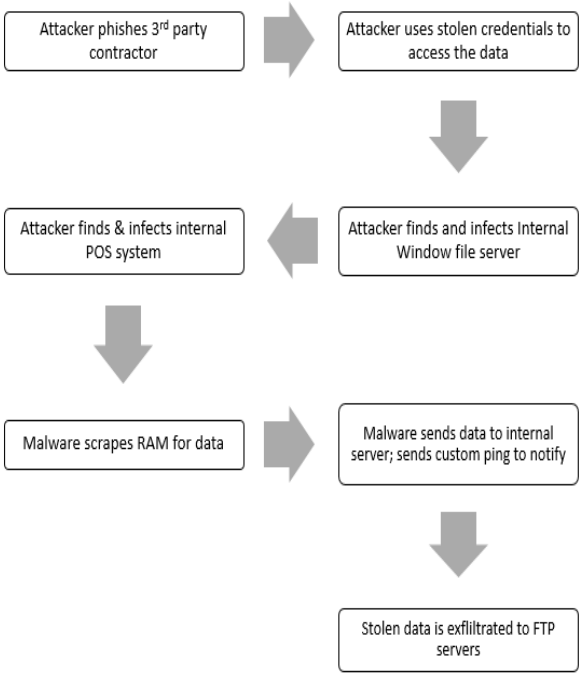

Fig. 1

B. Case 2 - Year 2018:

In 2018, a renowned bank was a victim of data breach where a whooping sum of 940 million was illegally transferred from various customer accounts. The reason for the attack was due to the compromise of the ATM switch and the glitches in the SWIFT transaction network.

1) Working of ATM Switch:

The bank attack was due to the compromise of the ATM switch. The picture below provides a reference of the ATM switch architecture.

ATM switch is responsible for performing the authentication during any ATM transaction. Any change in the PIN or any transaction is authenticated by the ATM Switch. In cases when a different bank's card is used to perform the transaction, the ATM Switch verifies that the card is original or not and checks to whom it belongs to.

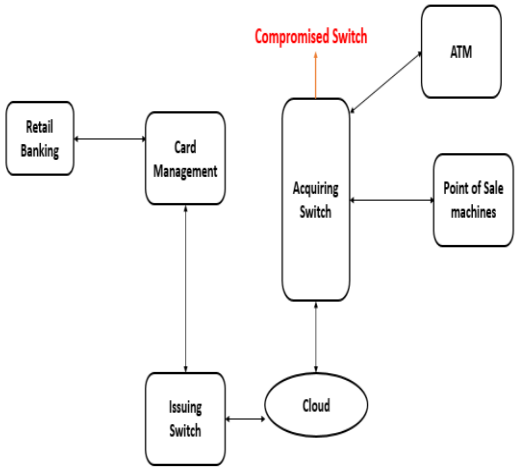

Fig. 2

2) ATM Switch breach during bank attack:

In this bank attack, the hackers created a proxy server by bypassing the firewall of the ATM switch. Using the proxy server, they carried out various self-authorized transactions. More than 12,000 transactions were performed and the banks were unaware about the incident for the next 48 hours. As per the Maharashtra Investigation Board, the evidences were wiped off completely and the accountability for the attack was not mapped to any group due to the mentioned reason.

Obfuscation is a process which is used to anonymize the cyber-attacks. They hide everything ranging from fingerprints and the signature of the code. This is carried out by variety of techniques. The techniques include packers, crypters, dead code instructions and many more. The packers will compress the packages. Compressed packages become undetectable. Crypters encrypt the malware programs thus making it undetectable by the anti-virus software. Unnecessary codes can be added to a malware to disguise its appearance.

Analysis of the bank case, arrives to a conclusion that the using one of the many obfuscation techniques, the hackers could have erased their identity and performed the attack in such a way that it could not be traced back.

3) SWIFT Network Compromise

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is used to propagate financial transactions worldwide. This is used to send and receive information regarding the transaction in a safe, secure and reliable way. The compromise of SWIFT system could have been using two methods – Hacking and Malwares. The hacking of the system is done in three ways – Access the bank system, steal the credentials and propagate throughout the system.

Attacker scans the finds out the potential system and connects to it. On the other hand, the malwares gather the system information, get the system infected and controls the SWIFT Transaction.

C. Case 3 – Year 2019:

One of the leading government owned banks of India was a victim of the data breach in the recent days. The quick text methodology of the bank which is called Bank Quick, was a loophole found out by the attackers, using which the data was extracted.

1) Bank Quick:

Bank Quick is a text and a call-based system, which is a quick and easy way for the customers to enquire about their bank details. Using Bank Quick, the customers can send a text or give a missed call to retrieve the information. It was highly acclaimed among the people, who do not have smartphones or have a limited data availability. If the customer wants to check the balance of the account, the customer could simply send 'BAL', in which the bank server will identify the phone number and give back the details accordingly. Apart from the balance enquiry, the system can also help in blocking the ATM cards, perform enquiries about loans.

2) Reason and propagation of the attack:

The data of all the customers were archived and stored in the server which was hosted in Mumbai. The database as such was not password protected. The password-less database paved way to the exposure of millions of data. There were more than three million transactions that happened on a single day, the details of which were available to anyone who could access the database. The server also allowed access to the archived messages that went two months back. There are various ways of extracting data from the database which includes, Brute-force attack, privilege escalation, SQL Injection and many more. But the major cause for this apart from the lack of password protection is predicted to be the presence of unpatched vulnerabilities. Though the group responsible for attack has not yet been found out, it is predicted that a single person might have acquired the access to the database that contained all the information and might have extracted all the data.

IV. CONTRIBUTIONS AND RECOMMENDATIONS

According to NIST 800-83, there are various techniques to prevent and handle the malware incidents. It is classified in to preparation, detection and analysis, containment/eradication/recovery. Enforcement of content filtering software that uses deep learning and machine learning mechanisms helps to filter the malicious content. Analysis of the anti-virus software and emphasizing more on on-access scanning and on-demand scanning. Host based and network based anti-virus scanning techniques can also help until a certain extent. Implementation of security models like sandbox helps in assuring Confidentiality and Integrity of the data. For malware attacks, there has to be more emphasis on firewall protection and anti-virus installation which promises continuous patch updates. For database protection, an automated way of capturing the transactions that are happening in the database will help to some extent. Organizations that have weak audit trail mechanisms will not be aware of who the end user is, what was the change that was performed by the end user. Enhanced audit trail mechanisms should be put in place. On the whole, the factor of accountability will be lost if there is no proper audit trail mechanism. There should be a strong separation of duties between database administrators and database server platforms and their working. For a chunk of information in the database, the categorization of the sensitivity could be done and encryption should be applied accordingly. The audits must be carried out on people related controls rather than focusing much on process, system and technology perspective.

REFERENCES

[1] Haagman, D., & Ghavalas, B. (2005). Trojan defence: A forensic view. *Digital Investigation*, *2*(1), 23-30
[2] Scott, S. V., Van Reenen, J., & Zachariadis, M. (2017). The long-term effect of digital innovation on bank performance: An empirical study of SWIFT adoption in financial services. *Research Policy*, *46*(5), 984-1004.
[3] Bhasin, M. (2007). Mitigating cyber threats to banking industry. *The Chartered Accountant*, *50*(10), 1618-1624.
[4] Cerruti, J. A., Nusser, S., Schoudt, J. T., Stefani, G., & Wilcox, E. (2011). *U.S. Patent No. 7,921,454*. Washington, DC: U.S. Patent and Trademark Office.
[5] Dumitrescu, M. I. B. (2004). Internal audit in banking organisations. *Biatec*, *12*, 7.
[6] Casaló, L. V., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review*, *31*(5), 583-603.
[7] Breslin, J., Borgia, E., & De Gottal, G. (2007). *U.S. Patent Application No. 11/763,030*.
[8] Bamoriya, P. S., & Singh, P. (2011). Issues & Challenges in Mobile Banking In India: A Customers' Perspective. *Research Journal of finance and accounting*, *2*(2), 112-120.
[9] Tebaa, M., Zkik, K., & El Hajji, S. (2015). Hybrid homomorphic encryption method for protecting the privacy of banking data in the cloud. *International Journal of Security and Its Applications*, *9*(6), 61-70.
[10] Kumar, T. R. (2012). Information technology in banking sector. *Asia Pacific journal of marketing and management review*, 25-33.
[11] Nie, J., & Hu, X. (2008, December). Mobile banking information security and protection methods. In *2008 International Conference on Computer Science and Software Engineering* (Vol. 3, pp. 587-590). IEEE.
[12] Rodríguez, R. J. (2017). Evolution and characterization of point-of-sale RAM scraping malware. *Journal of Computer Virology and Hacking Techniques*, *13*(3), 179-192.