Cyber security in Banking: Challenges, Solutions and Trends

Rachael Fernandez, Salma Shalaby, Noora Fetais

KINDI Center for Computing Research
Qatar University

Abstract

The banking sector is becoming more smarter as cyber technology solutions are implemented for the sake of security of the banking services and the convenience of the customers. However, these solutions come at a price, as they expose the banking services to cyber threats and attacks. This paper provides a short review of the current trends and challenges faced by the banking industry with respect to cyber security. It also outlines the best practices and solutions to overcome these difficulties.

1. INTRODUCTION

As the banking sector is becoming increasingly modern, there has been a significant increase in the number of threats and security breaches that financial services and banks face. According to the 2011 Data Breaches Investigation Report, the banking sector was the third highest industry group that faced data breaches and the second highest industry group in terms of the number of data records that were compromised [1]. However, banking customers continue to embrace the use of internet banking, digital wallets, mobile banking and ATMs, and these in turn lead to an even greater risk of exposure to cyber-attacks.

Financial sectors possess assets that can be broadly classified under the following three types:

1. Personal data of the customer: This information refers to the unique identification of every customer and includes details like card number, account number and other customer information like name, date of birth etc.
2. Access to the banking network: Gaining unauthorized access to the banking network could lead to fraudulent transactions. This leads to varying credit and debit account balances between the bank and its customers.
3. Insider Information: Just like other businesses, the financial sector also possesses information, which could give its recipients a competitive edge over the business. These include information like capital market information, company's financial data etc. [2]

Cyber-criminals are constantly on the lookout to compromise these assets by either tricking the customer or gaining access to the banking network. The data breaches that occur could result in a loss of trillions of dollars a year, but more importantly the reputation of the banks are at stake.

Cyber security experts agree that cyber-attacks against the

financial sector are more sophisticated and more frequent when compared to other business sectors [3]. According to Symantec's Internet Security Threat Report 2018, the bankcard fraud rates were 1.8 times higher than they were in 2014 [4]. The year 2014 also witnessed Emotet, a banking Trojan for the first time that was used for phishing campaigns against bank customers. Security researchers discovered that Emotet was a banking malware that was designed to steal sensitive and private information from computers. Emotet was dormant for a period of 2 years before it began to resurface in 2017 during which its activities increased by 2000%. According to proofpoint Q2 Quaterly threat report, Panda Banker, Emotet, UriZone Banker Ursnif and The Trick were some of the most prominent banking malware in 2018 [5]. The financial trojans that were targeted at customers began to steal not only online banking credentials but also cryptocurrency wallet details in addition to any other details that would maximize the profit of those cyber-criminals responsible for the attack [4].

On the other hand, some cyber criminals directly attack the bank's network and not the customer. The hacker tries to gain access to the banking network that contains the ledger of the bank, which in most cases is built on a centralized database. Once the hacker gains access to the network, the bank's assets can be easily manipulated. However, the current trend of blockchain offers a solution to this problem by using distributed ledgers that record the transactions leaving no opportunity for attackers to create fraudulent transactions.

As the number of attacks against the financial sector is constantly on the rise, this creates a need for banking services to adopt a proactive approach and be more responsive to cyber security requirements.

The rest of the paper is organized as follows, Section 2 will review the challenges that the banking sector faces. Section 3 will offer some cyber security solutions to solve these challenges. Section 4 will highlight some of the current trends in the financial sector followed by the conclusion of the paper in Section 5.

2. CHALLENGES

The challenges that each sector and organization vary from one another. For example, the level of security that customers expect from a movie-streaming website would be much lower than what they expect from a banking or health care website.

Cyber-attacks aimed at the banking sector are done with the purpose of affecting the following aspects of information security [6][7]:

1. Confidentiality: It refers to the protection of data from unauthorized disclosure. It could also involve disclosure of information by legitimate users who pass the

information to illicit sources. Loss of confidentiality could lead to reputation loss.

2. Availability: This means that the system and data is accessible to authorized users as and when needed. This is necessary for running a business without any disruptions. Disruptions could lead to loss of revenue.

3. Integrity of information: This ensures that data is protected from unlawful modifications, insertion or deletion of data.

As banks rely on the trust of their customers, a reputation loss would generally impact them more than financial loss. Hackers tend to attack the financial sector to exploit these aspects of information security.

Bouevert et al. noted that the financial sector was exposed to higher cyber risk than other sectors due its dependence on highly interconnected networks and a centralized database [7]. Some of the attacks that the banking sector faces are:

a. Banking Malware: These malware are specifically developed to steal user's credentials for banking websites. They are spread by cyber criminals to infect a victim's computer by tricking them into opening a malicious email attachment or by visiting a website that has been compromised. The trojan then waits for the victim to visit a banking website before stealing sensitive information. The trojan uses one of the following two methods to steal the victim's information:

1. The malware uses a keylogger to capture the banking credentials of the victim or uses web injects to add extra fields to the forms to extract more information from the victim.

2. It redirects the victim to a fake website similar to the original website of the banks. Once the victim enters their credentials, the captured details are sent to the original website.

The malware now has complete control of the victim's account with the stolen credentials and is free to perform any illegal activity.

b. Attack vectors: An attack vector is defined as the means by which an attacker can gain access to a computer network with a malicious intent [8]. Some of the attack vectors aimed at banking services are [9]:

1. Credential Stealing Attack: Hackers try to gain access to the victim customer's credentials, either by using a banking malware or by phishing for it.

2. Channel Breaking Attack: The communication between a client and server is intercepted by posing as a legitimate server to the client and vice

versa.

3. **Content Manipulation Attack:** Also known as the Man-in-The-Browser (MiTB) attack, it takes place in the application layer between the user and browser. The hacker gains privileges to manipulate the user's data, whilst the user remains unaware of the attack.

4. **ATMs:** ATMs have always been a popular target for stealing customer information. Criminals fit skimming devices in ATMs to capture magnetic stripe information when the user swipes the card in the ATM. The ATM keypads are sometimes also fit with clear cases to capture the PIN of the user. These details would then be used to create counterfeit credit cards. In other cases, ATMs were reported to have been infected with malware which were capable of storing the magnetic stripe information and PIN without the need for hardware devices.

c. **Phishing:** It is another popular method to gain user's credentials by sending out spoof emails to fool the victim into divulging sensitive information. It has been reported that 30,000 phishing attacks take place each month globally. Of these attacks, 80% of them are targeted at banking institutions [10].

d. **Insider Attacks:** The Insider Threat Study Report examined 23 incidents in the banking and finance sectors between 1996 and 2002 [11]. Of these incidents, 87% of the cases used simple user commands to carry out the incidents, 70% of the cases were carried by exploiting systemic vulnerabilities and 78% of the incidents were carried out by authorized users with active computer accounts. These numbers imply that most incidents in the banking and finance sectors required minimal technical skill from insiders to successfully carry out the attacks.

e. **Distributed Denial of Service Attacks (DDoS):** These types of attacks attempt to make a service unavailable by overwhelming the server with excessive traffic. Cybersecurity expert Ryan noted that the latter half of 2012 saw an increased number of sophisticated DDoS attacks against financial institutions [3]. DoS attacks are generally considered "noisy" as they are easily noticeable. However, these attacks may serve as a distraction while hackers attempt other types of attacks [3][8].

3. SOLUTIONS

Though it is not possible to protect ourselves from every attack, we can reduce the risk and probability of an attack by using stronger and better authentication measures and

by employing better policies in the workplace. These solutions are proposed for better security for both customers and employees alike.

1. **Raise awareness:** Employees and customers should be made aware of phishing attacks and instructed not to open unidentified e-mails. Resources to report suspected phishing attacks should also be made available to them.
2. **Update Operating System, Software and Anti-Virus:**

   Hackers spot vulnerabilities in systems and tend to

TABLE I

BLOCKCHAIN TYPES

	Public Blockchain	Private Blockchain	Consortium Blockchain
Management	Anyone	Single organization	Multiple Organizations
Data Access	Public	Private	Public
Participants	Anonymous Permissionless	Known Identities Permissioned private	Known Identities Permissioned public
Application	Bitcoin, Ethereum	Banks Blockchains	The Blockchain Insurance Industry Initiative (B3I)

   exploit them. Hence, all software on the system should be updated to the newest version as and when they are released.

3. **Network Insight:** The banking network should be investigated to identify vulnerabilities.
4. **Administrator access:** Employees should be given ”least” privileges that will help them to do their work. Administrator privileges should be reserved only for employees whose work would be stalled without it.
5. **Biometrics:** Authentication measures like retina scanning, fingerprint authentication are becoming increasingly used for security and authentication. They can be used for added security in ATMs by replacing the conventional PIN.
6. **E-Banking Solutions:** Customers should be made aware of the importance

of using stronger passwords and authentication measures. In [12], the author suggests the use of three-factor authentication consisting of : 1) Passwords 2) tokens like smart-card and finally the use of 3) biometrics for better security. Measures like password length and application timeouts should be employed for better security [3].

4. TRENDS

Some of the current trends that works on ensuring security in the financial sector are cryptocurrency and blockchain.

A. CRYPTOCURRENCY

Cryptocurrency is the system that utilizes cryptography for secure transfer of electronic coins [13]. The first cryptocurrency was Bitcoin, it was introduced in 2009 by Satoshi Nakamoto. Since then, it became the most known cryptocurrency even with the evolution of other cryptocurrencies. When Satoshi Nakamoto created bitcoins, he, she or they did not reveal their identity. There could be many reasons behind this ambiguity, but the most convincing one is that the users will start thinking that the creator is getting some profit for each transaction [14]. The whole idea behind cryptocurrency is having secure digital transactions without the need of a third party or a financial institute to complete the transaction. To eliminate the third party, the typical centralized system should change to a distributed system and this is what Nakamoto came up with.

Having pure peer-to-peer (p2p) transaction will allow the transfer of money; however, this approach leads to double spending problem. Unlike the fiat currency, there is no physical representation of electronic money. A transaction

could be seen as sending an electronic file via email, where A is the sender and B is the receiver. The problem is that the sender A still has the file even after sending it to B, so it can be sent again. If we consider the money scenario, then this file will represent an amount of money that can be respent again after the first transaction [13]. To avoid such a problem, all the transactions should be recorded in a ledger. According to Nakamoto, the problem with having centralized ledger or a trust-based model is that it limits the small transactions because of the fees (mediation costs) [15]. Also, the governmental meddling might lead to inflation of the currency.

The failure of centralized economic systems encouraged Satoshi Nakamoto to make bitcoin completely decentralized to avoid single authority control. The decentralization

of transactions is done using blockchain that is a single universal digital ledger that is accessible by all the nodes in the network. Meaning that each node in the network has a copy of the transactions ledger [14]. As its name implies, blockchain consists of blocks where each new block holds a set of new transactions. Each of these transactions reference the previous transactions in the chain, which shows the set of transactions that a bitcoin has passed through before reaching this point. As blockchain does not depend on a controlling financial institution, there must be a way to verify that a transaction is valid and that the sender has enough bitcoins to send. Here comes the role of miners who work on detecting transaction requests, gathering them, validating them and finally add them to the chain as new blocks.

To add a new block to the chain, miners go through Proof of Work (PoW) process. When new transactions are issued, the miners put them in a block and try to hash this new block. The produced hash must start with a certain number of zeros and here comes the challenging part, as there is no way to predict the value produced by the hash function. Thus, miners add a random number (nonce) to the data such that the hash changes when the nonce changes. The miners keep running the hash function using different nonce at each run until one of them get the correct number of zeros. The first to find a satisfactory solution announces the new block to all the other miners to check it and append it to the chain [16]. Because PoW is computationally expensive and wastes power new cryptocurrencies appeared that follows different consensus algorithms like Proof of Stake (PoS) that is used by peercoin. In peercoin, instead of depending on the computational power of the miner it depends on the ownership of the currency, thus, users with more currency

has higher probability to issue the next block [17].

B. BLOCKCHAIN

Blockchain lays under the Distributed Ledger Technology (DLT) and works as a secure database for storing transactions. It emerged in 2009 to serve Bitcoin, which is the first known cryptocurrency. Although the main goal of cryptocurrencies is to eliminate central control by banks and governments, banks started to utilize the blockchain, which is the core technology behind cryptocurrencies, to facilitate transactions.

Generally, the block contains main data, current hash and previous hash. The main data represents the transactions information. The current hash represents the hash of all the content of the block and the previous hash is the hash of the preceding block. The fact that each block has the hash of the previous block constructs chain and builds the ledger up.

Blockchain is divided into three types: Public blockchain, Consortium blockchain

and Private Blockchain. Table 1 illustrates the difference between them. Public blockchains can be accessed by anyone like in the Bitcoins network. In Consortium blockchains data is available to public, but it is controlled by a set of known entity. Private blockchains are controlled by a set of known entities and data access is restricted [18].

Blockchain comes with several benefits to the banks and the financial systems in general. It speeds up the transactions, eliminates mediators, reduces the costs, helps in fraud reduction and improves the security. Payments clearing and settlements is a complicated process that involves several steps making it time and money costly[19]. Both Interbank and Interbank transactions requires middleman, blockchain eliminates the need of intermediaries. It facilitates point-to- point transactions, as there is no need for a third-party, which increases the efficiency and reduces the cost. In 2016, Standard Charted bank and fintech start-up Ripple succeeded in their first cross-border transaction using blockchain platform. Processing such payments usually takes two days, but using blockchain, the transfer was done in 10 seconds only [20]. Another plus of eliminating intermediaries is lowering the fees by removing the intermediary banks charges and the cost of foreign exchange and compliance costs.

One of the main challenges that faces centralized databases, used by traditional banking systems, is that they are a single point of failure (SPOF) meaning that if the database failed or got attacked, the whole system will fail. The distributed nature of blockchain makes SPOF attacks impossible; each node will have a copy of a ledger preventing such attack. Additionally, since all the blocks are connected; any change will affect the rest of the blocks in the chain and it will be easily detected by the network which ensures the integrity of the data.

5. **CONCLUSION**

Though the risk of cyber-attacks and the sophistication of the attacks against the financial sector is constantly evolving, good cyber security practices and a proactive approach can help to mitigate the risks and intensities of the attacks. Newer technologies like blockchain and cryptocurrencies also help in combating several disadvantages of conventional banking practices.

REFERENCES

1. M. Goudie, A. Hutton, C. David Hylender, J. Niemantsverdriet, Novak, D. Ostertag, C. Porter, M. Rosen, B. Sartin, P. Tippett, T. Bosschert, E. Brohm, C. Chang, M. Dahn, R. Dormido, B. Van Erck, K. Evans, E. Gentry, J. Grim, C. Hill, A. Kunsemiller, K. Lee, W. Lee, K. Long, R. Perelstein, E. Telemaque, D. Todd, Y. Uzawa, J. A. Valentine, N. Villatte, M. Van Der Wel, P. Wright, T. Beeferman, C. Dismukes, P. Goulding, and C. Neal, "2011 Data Breach Investigations Report," Verizon RISK Team, Tech. Rep., 2011.
2. M. Ula, Z. Bt Ismail, and Z. M. Sidek, "A Framework for the Governance of Information Security in Banking System," Journal of Information Assurance & Cybersecurity, vol. 2011, p. 12, 2011.
3. J. W. Ryan, A Resource Guide for Bank Executives: Executive Leadership of Cybersecurity, 2014.
4. Symantec, "ISTR Internet Security Threat Report Volume 23," Symantec, Tech. Rep., 2018.
5. ACSC, "Threat Report," Australian Cyber Security Center, vol. 1, p. 40, 2016.
6. G. W. Peters and E. Panayi, Banking Beyond Banks and Money. Springer, Cham, 2016.
7. A. Bouveret, S. Christo, T. Gaidosch, V. Haksar, E. Kopp, R. Maino, M. Patnam, C. Rochon, H. Poirson-Ward, N. Stetsenko, A. Toure´, A. Tiffin, C. Wilson, and K. Wiseman, Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. International Monetary Fund, 2018.
8. C. Roberts, "Biometric attack vectors and defences," Computers and Security, vol. 26, no. 1, pp. 14–25, 2007.
9. M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis, "How to Attack Two-Factor Authentication," Fc 2013, pp. 322–328, 2013.
10. N. S. Singh and D. Vijay, "Analysis of Different Vulnerabilities in Auto Teller Machine Transactions," Journal of Global Research in Computer Science, vol. 3, no. 3, pp. 2010–2012, 2012.
11. M. R. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, and Moore, "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," CarnegieMellon Software Engineering Institute, Tech. Rep., 2005. [Online]. Available: http://www.sei.cmu.edulpublications/pubweb.htnml
12. A. Fatima, "Journal of Internet Banking and Commerce E-Banking Security

Issues-Is There A Solution in Biometrics?" Journal of Internet Banking and Commerce, vol. 16, no. 2, 2011.

13. E. Dourado and J. Brito, "Cryptocurrency," in The New Palgrave Dictionary of Economics. London: Palgrave Macmillan UK, 2016, pp. 1–9.
14. P. K. Kaushal, A. Bagga, and R. Sobti, "Evolution of bitcoin and security risk in bitcoin wallets," in 2017 International Conference on Computer, Communications and Electronics (Comptelix). IEEE, 7 2017, pp. 172–177.
15. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Tech. Rep. [Online]. Available: www.bitcoin.org
16. ANDY EXTANCE, "BITCOIN AND BEYOND," Tech. Rep., 2015.
17. S. King and S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," Tech. Rep., 2012.
18. I.-C. Lin and T.-C. Liao, "A Survey of Blockchain Security Issues and Challenges," International Journal of Network Security, vol. 19, no. 5, pp. 653–659, 2017.
19. Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," Financial Innovation, 2016.
20. John Cusack, "Blockchain, A game-changer in the fight against financial crime?" 2017. [Online]. Available: https://www.sc.com/fightingfinancialcrime/perspectives-controls-blockchain.html