E-Banking: Security risks, previsions and recommendations

Meriem Tabiaa[1], Abdellah madani[2] and Najib El kamoun[3]

[1] LAROSERI Laboratory ,Chouaib Doukkali University, El jadida , Morocco
[2] LAROSERI Laboratory ,Chouaib Doukkali University, El jadida , Morocco
[3] STIC Laboratory ,Chouaib Doukkali University, El jadida , Morocco

Summary
Nowadays, the expanded use of the Internet and the establishment of advanced technology systems lead to a wide and an international increase in the use of the online banking (also known as e-banking).
However, the e-banking technology can be impacted by a range of fraud incidents and cyber-attacks. The present article aims to give a clear definition of the e-banking term. Also, it will describe the nature of the above mentioned. Finally, it will provide recommendations and suggestions in order to develop and strengthen the security aspect of the electronic banking

Key words:
E-banking; online banking; attacks; security, security of e-banking.

1. Introduction

Over the past few years, thanks to the spectacular technological leap, the number of the offshore services has remarkably increased. Thus, we have moved, in a very short time, from the era of postal mail to the digital era. E-banking is one the major services that has made life simple and easy; a user can now do a lot of things while he is sitting on a sofa. This goes from transferring money to applying for a credit.

Studies show that e-banking has multidimensional advantages for both individuals and companies, but it is not without some challenges and issues related to the security and the interest of customers [1]. Since security is considered to be one of the main preoccupations for both large and small organizations, electronic banking systems are also confronted to cyber-attacks just like any other system connected to the Internet.

This study will mainly focus on the security aspect of the « e-banking » technology in the context of scientific research perspective. The first part of this paper will present the e-Banking in a general way. It defines this vague term, presents its services and also lists the advantages and risks related to this technology. The second part will be dedicated to the analysis of previous works in order to identify it limits, challenges and issues. Finally, the third part will be devoted to the types of attacks and recommendations and suggestions in order to develop and strengthen security.

2. Overview of e-Banking

"Electronic Banking" or "e-Banking" is a fuzzy term; it can be defined in several ways. In a simple way, this may mean providing information or services by a bank to its customers, via a computer, a television, or a mobile phone.

The definition of e-banking, a contraction of electronic banking, varies greatly from one author to another. Authors sometimes refer to distinct aspects, sometimes to the same thing, or overlap partly [2], below some definitions are given:

- Electronic banking: refers to the provision of retail and small value banking products and services through electronic channels. Such products and services can include deposit-taking, lending, account management, the provision of financial advice, electronic bill payment, and the provision of other electronic payment products and services such as electronic money [3].
- Electronic banking or e-banking: form of banking where an account is maintained via the Internet rather than, or as well as, at a bank branch [4].
- E-banking: web-banking, pc-banking, net-banking, home-banking, etc. Different terms refer to the “Electronic Banking”. Thanks to the web, you have the possibility to manage your account from your home [2].

The fact that there are several definitions is not a coincidence, but rather by going back in the history of e-banking since its launch in 1981 in the USA with the first service [5][6][7], passing through its evolution and its arrival in Europe [8][9] can explain the vague term of e-Banking.

Manuscript received November 5, 2017
Manuscript revised November 20, 2017

2.1 One bank and different families

When it comes to e-banking, we have to distinguish between banks whose activities are 100% based on the Internet and those whose Internet activity supports (mobile banking), not to mention the traditional bank. We can distinguish three main families: First, “bricks and mortar” (traditional banks) [10]. Secondly, “clicks and mortar” and finally the “Pure Players”. We will focus on the last two families:

- Clicks and mortar: or click-and-click business models is “the integration of the Internet channel and the traditional retail channel (bricks and mortar)” [11]. In the banking context, the click and mortar bank is the bank that has a physical agency, while offering its same services on the internet.
- Pure player: are companies that do not have an up-front store presence and sell products only via the internet [12]. If we project this definition on banks, we will have a 100% electronic bank without tangible facilities and which provides services to its customers throughout the Web.

2.2 Services offered by the electronic banking:

Services offered by electronic banking to the customers are merely a fusion between the services of the traditional bank ("bricks and mortar") and technology/automation, which exceeds by far services offered by the traditional bank.

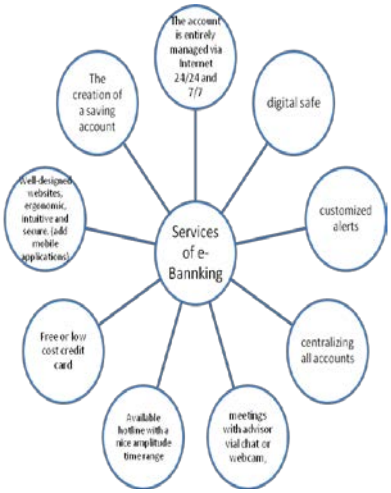
Services of e-Bannking
The account is entirely managed via Internet 24/24 and 7/7
digital safe
customized alerts
centralizing all accounts
meetings with advisor vial chat or webcam,
Available hotline with a nice amplitude time range
Free or low cost credit card
Well-designed websites, ergonomic, intuitive and secure. (add mobile applications)
The creation of a saving account

Fig. 1 Services offered by e-Banking

2.3 Advantages and risks of e-Banking:

There are many e-Banking advantages: for the customer and the electronic bank both [13]. As there are benefits, there are risks and issues too associated with this technology. We can name two types of electronic banking risks: general and application risks. General risks may include access to physical equipment, logical access to systems, and information technologies. Application risks could be the result of an error situation, for example, application information is not available in real-time due to a system failure [14]. The table below represents the advantages and the risks of this technology, in a general way:

Table 1: The advantages and the risks of e-Banking

Advantages	***Risks***
➢ To the customer : - Reducing his time in making different account’s operations, - Saving money, - Having access to his services at any time he would like to, in addition to the accessibility of the services via Internet [13]. ➢ To the bank: - Having a decrease in expenses and an increase in profitability, - Less paperwork since the administrative tasks are computerized - Access to the service would be at anytime, the need of the personnel and the investments for the development of the infrastructure are remarkably reduced because of the absence of physical agencies. [13]	➢ General risks [14] ➢ Application risks [14], ➢ Credit risk [15], ➢ Market risks [15], ➢ Strategic Risk[15] , ➢ Reputation risk [15] , ➢ Legal risk [3], ➢ Operational risk [3]

The latter risk (operational risk) is very important for our study, and means the risk of direct or indirect loss resulting from inadequate processes or failure for people and systems or external events. This type of risk is related to:

- Maintenance, design and implementation systems,
- Misuse of products and services by the customer,
- Security risk: In the absence of appropriate security checking, not only hackers could damage the bank by disclosing the personal data of customers, but also third parties can destroy the information system by injecting harmful viruses. In addition to external attacks, banks are exposed to fraud [3]…

3. Literature Review

The ease of use of e-Banking platforms is in conflict with security because most users are not able to complete the installation of the applications and systems of the electronic bank while respecting the instructions which generates security problems related to the knowledge and motivation of users. This is why a team carried out an in-depth study, the first of its kind on CAPTCHAs deployed in electronic banking around the world. The aim of this study was to prevent malicious connections middle man) for banking transactions. The study proposed a new set of image processing and recognition techniques, but limits this technology to unexplored and replaced by other alternative solutions such as those based on hardware tokens [16].

Still in the same context, following an on-line survey of the bank's security problems in Malaysia, the results suggested that most end-users experience many difficulties, especially with regard to technical terminology, security and other technical problems. What prompted the researchers revealed a conclusion is that the developer should find the best way to provide clear explanations so that it can accommodate any type of users so that they can understand the technical terminology and meaning functionality even though banks are well equipped with many security features such as SSL and digital certificates [17].

Other researches were more generous. They classify attacks and vulnerabilities which affect the online systems banking while linking them with the security models present at the time. This study also revealed that the weakest link in the chain is the user, in order to obtain authentication and identification information using social engineering or using malware, what was recommended is to develop a security model to detect frauds and real-time attacks based on the data mining and pattern recognition methods [18]. This contribution joins the study which was able to demonstrate that the common problem, affecting the information security and the confidentiality of customers, is the lack of security control of the electronic service provider that can harm the loss of confidentiality. Besides, another problem is the subsequent misuse of confidential customer information, as in the case of identity theft [19].

As for malwares, one of the most complicated and dangerous financial malwares called Emmental, has been identified and modeled. The result of the research was able to prevent these malware from entering the computer, classifying and registering their behavior and providing ways to block them. They also incited the authorities to redefine, conceive and implement secure banking services such as: secure Internet, secure mobile applications, secure electronic money, etc. They mentioned that today, attacks are more complicated, combined and wider, then more former and common solutions are no longer used and there is a need for new more powerful methods [20].

Also, there is a solution for detection of behavioral anomalies proposed for banks in order to detect the financial transactions made in suspicious circumstances, but this solution is implemented in the internal systems only, hence its limitation [21]. And finally, one of the most relevant results revealed that even the strongest passwords can be easily guessed with dictionary attacks or via Keyloggers (via sniffers, snoopware,). In order to overcome this risk, electronic banks have included virtual keyboards in their applications, but the risk remains latent when a hardware Trojan in the VGA screens can capture any sensitive information inserted via a virtual keyboard, which constitutes a new security challenge in mobile banking [22].

We can notice that: The majority of the works put the light on a certain type of attacks, without proposing solutions, or they propose arbitrary and traditional solutions without taking into account the development of technology and IoT. Without forgetting that when we approach the e-banking; it is a whole connected system, from the internal system of the bank, to the end customer while passing through a transmission channel. Also the risks related to a connection via a browser can be similar as different to a connection via the application. Thus, there is no work which puts in set: The definitions, the global risks and the analysis of the security aspect. The objective of the next section will be dedicated for the analysis of the security aspect, the presentation of the risks and attacks and the proposition of the recommendations and solutions which banks can adopt to enhance the security of their platforms.

4. Analysis and studies of the security in e-Banking:

4.1 The impact of security breaches:

In addition to the advantages, the banking industry has faced cyber threats due to Internet connectivity. The main challenge for the e-banking sector is the intensive use of information technology applications related to the e-banking. This leads to threats of electronic security, cyber-attacks on the profile of customers, embezzlement, fraud in terms of data messages, the confidentiality of anti-theft customers, the secret of financial transactions [23].

Many statistical reports provide examples on the dimension and the effects of security breaches in e-Banking. According to the SANS survey of 2016, which measures the state of risk and security in the financial sector, the financial services industry is under the deluge of ransom and hacking attacks, which are increasing dramatically [24].

According to Symantec in its latest report released in 2016; more than 430 million new unique pieces of malware in 2015 and 36% more than the previous year was detected. Symantec researchers have discovered a new Android phishing Trojan that incites the users to enter their banking information by creating a fake login page over legitimate banking applications. Threats such as "Dridex" use exclusively spam e-mail campaigns and include real company names into the sender's address and the body of the e-mail [25].

Another study reveals that 60% of bank managers agree that online identity theft has been identified by their bank. While the attack through malicious code and a denial of service attack were agreed by 54% of the executives. In fact, the attacks inspired by Wikileaks against the main of e-commerce sites fueled the interest of the fraudsters. The cases of hacking as well as credit card fraud or ATM have also been identified or reported in banks. The sophistication of phishing, vishing and spoofing attacks are also identified and confirmed by 76% of the bank's executives. The phishing, the falsification, the hacking and the identity theft online are some of the main challenges for banks [26].

4.2 Types of attacks:

In order to propose security models and radical solutions, it is necessary to understand and to determine, at first, the attack methods and the existing vulnerabilities on which they are based [26]. The search attempted to categorize and classify the diverse sorts of attacks against the e-banking in different ways. The main security threats or attacks of electronic banking platforms are; denial of service, illegitimate use, disclosure of information and repudiation [27]. Other researchers have presented a classification for the current attacks on the online banking systems [28]. Another study proposed a hierarchy causes that included three main categories; legitimate access, control of devices, and theft of property [29]. There is a model (Attack Weapon Model) that presents the main and the effective attacks, explains how to exploit inherited vulnerabilities (social engineering and phishing attacks) and takes control of software (malicious software) and identity theft of a legitimate user (fake pages of websites and malicious software). Such a grouping is one of the lowest and most regular used for attacks on the online banking system [19].

From another angle, the objective of an attacker can vary. The attacker may attempt to exploit vulnerabilities specific to the operating systems, where he can try again not to authorize entry on a website leading to a denial of service to clients [30]. Here is a non-exhaustive list of the types of attacks:

Table 2: Types of attacks

Type of attack	***The definition***
DOS attack	Denial-of-service attack is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled [31].
Ransomware attack	This malware takes advantage of people’s fear of revealing their private information, losing their critical data, or facing irreversible hardware damage [32]. Ransomware is computer malware that installs covertly on a victim's device and that either mounts the crypto viral extortion attack from crypto virology that holds the victim's data hostage [33].
Man-In-The-Middle attack	(MITM, sometimes called a "bucket brigade attack") [34], MITM targets the actual data that flows between endpoints, and the confidentiality and integrity of the data itself, the common scenario involves: Two endpoints (victims) and a third party (attacker). The attacker has access on communication channel between two endpoints, and can manipulate their messages. As a result, the attacker has convinced both victims that they use secure channel, but in reality it has access to all encrypted messages [35].
Phishing	is an online identity theft, which attempts to steal sensitive information such as username, password, and online banking details from its victims [36]. This is a type of semantic attack [37][38][39], in which attackers try to fool and steal money from legitimate Internet users sending e-mails rather than exploiting bugs in computer software. The attacker creates a fraudulent web site which has the look-and-feel of the legitimate website. Phishing e-mails employ a variety of tactics to trick people into disclosing their confidential information such as usernames, passwords, national

	insurance numbers and credit/debit card numbers [37] [40].
Pharming	Pharming attacks a sophisticated version of phishing attacks. The attacker inject Trojans and/or worms into users' computers or the DNS server that causes different types of attacks (modifying users' hosts file, DNS cache poisoning, domain hijacking, static domain spoofing, etc.).This kind of attack will redirect web users to the forged page in order to get their privacy information, account passwords or other important information. The terrible danger of pharming attack is that even if the users carefully check the URL before they visit a website, they cannot find any exception [41][42].
Vishing	Voice phishing is the criminal practice of using social engineering over the telephone system to gain access to private personal and financial information from the public for the purpose of financial reward [43]. Voice phishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals [44].
Spoofing	When the adversary pretends to be the legitimate transmitter to spread false messages, or be the legitimate receiver to filch confidential information [45].
Disclosure of Information:	The dissemination of information to anyone who is not authorized to access that information. These threat actions can cause unauthorized disclosure: Exposure, interception, inference, intrusion [46][47].
Repudiation attack	A repudiation attack happens when an application or system does not adopt controls to properly track and log users' actions, thus permitting malicious manipulation or forging the identification of new actions. This attack can be used to change the authoring information of actions executed by a malicious user in order to log wrong data to log files. Its usage can be extended to general data manipulation in the name of others, in a similar manner as spoofing mail messages. Repudiation refers to a denial of participation in all or part of the communication [48].
Social engineering attack	The authors define social engineering as "the science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity" [49]. There are many models and taxonomies concerning social engineering attacks The most commonly known model is Kevin Mitnick's social engineering attack cycle as described in his book, The art of deception: controlling the human element of security [50].
Port scanners	In this type of attack, the attacker uses various techniques to steal the sensitive information, by sending different types of signals to the system to retrieve the message and get the acknowledgement to ensure the details of the communication channel. The main focus is to collect the important information related to hardware and software used by the system to plan ahead for the type of attack, which can be performed on such system [51].
Password cracking	Consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc… [52].
Trojans	Trojan attacks are intended to affect normal circuit operation, potentially with catastrophic consequences in critical applications in many different domains. They can also aim at leaking secret information from inside a chip through covert channels or affect the reliability of an IC(integrated circuit) through undesired process changes that cause device/interconnect wear-out and long-term reliability issues [53].

5. Previsions, Recommendations:

Online banking is carried out by a series of transactions in diverse environments between the end user and the system. These transactions are always vulnerable to hacker attacks. As a result, from the threats listed previously, it became essential to design and to develop models of effective security in order to offer an online safe access.

Without mentioning traditional solutions and methods [19] and based on the reports and previsions (forecasts) of several renowned organizations, many actions are recommended. it should be taken into consideration when implementing security policies or developing new technological and practicable solutions. Better still, these organizations have begun to form partnerships, which is a "must" for continued growth in front of these risks.

According to the predictive study led by "Symantec" and raised several results, we found that Malware without file will increase, Secure Sockets Layer's abuse will pull in increased Phishing sites using HTTPS, drones will be used for attacks of espionage and explosions [54]. As for "McAfee", the machine learning of social engineering attacks is accelerated and sharing the intelligence of the threat makes big progress [55].

And, at the end, for "Gartner", always known for their ability to put percentages beside their predictions; until 2018, more than 50% of IoT device manufacturers will not be able to cope with threats arising from weak authentication practices. This prediction is rather revealing, and what was recommended; Push the industry towards authentication standards, but companies should identify the authentication’s risks, establish identity assurance requirements and use high security measures [59]. By 2019, the use of passwords and tokens in medium-risk applications will decrease by 55% due to the introduction of recognition technologies. To solve this, companies should look for products that focus on developing a continuous trust environment with a good user experience, while using biometric and analytical resources [56].

Also, by 2022, the majority of companies and organizations will be based on the Block Chain [56]. Thanks to the block chain service platform, the number of transactions can be considerably reduced, as well as their costs, and the transaction time can be shortened. The world's 42 largest financial giants, including JP Morgan chase, Citibank, Goldman Sachs Group, have invested massively in the research, development and service platform of the Block Chain [57].

To summarize, in order to combat these attacks, it is also necessary to initiate education and sensitization of the consumers, this action should be carried out in collaboration with the government and other private organizations. The education should be organized to ensure that the users understand the sensitivity of the data, the level of confidentiality and the mechanisms allowing to securing the transaction [26]. It also implements "on the point" security models with technology and meets requirements and standards. This says that it is necessary to plan collaboration with the technology industries and the banks.

6. Conclusion

With the development, the extension of advanced instruments and innovation have gradually permeated our daily lives, the requirement of the digital security has grown. To improve our cybernetic defenses, industry must cooperate. Banks should consider security issues as a major aspect of their administration offerings. Similarly, it is committed to providing secure management of online situations in light of the propelled security methods. The security and the insurance of the data exchanged between the customers and the bank are, for all the accounts, a difficult incentive in the field of e-Banking. The man in the middle, the phishing and data leakage, for example, cannot be completely destroyed, but it can be moderated by identifying it in time. The adequacy of e-Banking is based on its confidentiality, integrity and non-repudiation.

As Thomas Edison reportedly said last century:"There's a way to do it better — find it."

References

[1] J. Jayaram and P. N. Prasad, “Review of E-banking System and Exploring the Research Gap in Indian Banking Context,” Int. J. Innov. Res. Dev., vol. 2, no. 2, pp. 407–417, 2013.

[2] C. DENOEL, L’E-BANKING REMPLACE-T-IL LA BANQUE TRADITIONNELLE OU LA COMPLETE-T-IL. Mémoire de Master: Sciences de Gestion: Université de Liège, 2008.

[3] E. BANKING, “Risk Management FOR Electronic Banking AND Electronic Money Activities,” 1998.

[4] J. Midgley, “Financial inclusion, universal banking and post offices in Britain,” Area, vol. 37, no. 3, pp. 277–285, 2005.

[5] M. J. Cronin, Banking and Finance on the Internet. John Wiley & Sons, 1998.

[6] Charline Allen, “The Home Banking Dilemma.” .

[7] M. Edwards, “Computer Giants Giving a Major Boost to Increased Use of Corporate Videotex,” Commun. News, 1984.

[8] B. Wire, “Stanford federal credit union pioneers online financial services,” Bus. Wire June, vol. 21, p. 1995, 1995.

[9] K. procopio, “BofI Holding Inc. Changes Name of Bank Subsidiary to BofI Federal Bank".,” SEC.gov, 03-Oct-2011. .

[10] R. Sousa and C. A. Voss, “Service quality in multichannel services employing virtual channels,” J. Serv. Res., vol. 8, no. 4, pp. 356–371, 2006.

[11] F. Bernstein, J.-S. Song, and X. Zheng, “‘Bricks-and-mortar’ vs.‘clicks-and-mortar’: An equilibrium analysis,” Eur. J. Oper. Res., vol. 187, no. 3, pp. 671–690, 2008.

[12] K. K. Boyer, “E-operations: a guide to streamlining with the Internet,” Bus. Horiz., vol. 44, no. 1, pp. 47–54, 2001.

[13] R. Kalra and B. Narayan, “E-Banking: Advantages, Challenges and Opportunities in the Indian Context,” AADYA-Natl. J. Manag. Technol. NJMT, vol. 7, pp. 1–10, 2017.

[14] M. Georgescu, “Some issues about risk management for e-banking,” 2005.

[15] P. Saraçi and S. Shterbela, “E-BANKING USAGES IN ALBANIA: CASE STUDY OF SHKODRA REGION.”

[16] M. Hertzum, N. Jørgensen, and M. Nørgaard, “Usable security and e-banking: Ease of use vis-a-vis security,” Australas. J. Inf. Syst., vol. 11, no. 2, 2004.

[17] F. N. Mahmadi, Z. F. Zaaba, and A. Osman, “Computer Security Issues in Online Banking: An Assessment from the Context of Usable Security,” in IOP Conference Series: Materials Science and Engineering, 2016, vol. 160, p. 012107.

[18] S. Li, S. Shah, M. Khan, S. A. Khayam, A.-R. Sadeghi, and R. Schmitz, “Breaking e-banking CAPTCHAs,” in Proceedings of the 26th Annual Computer Security Applications Conference, 2010, pp. 171–180.

[19] L. Peotta, M. D. Holtz, B. M. David, F. G. Deus, and R. T. De Sousa, “A formal classification of internet banking attacks and vulnerabilities,” Int. J. Comput. Sci. Inf. Technol., vol. 3, no. 1, pp. 186–197, 2011.

[20] S. Geramiparvar and N. Modiri, “Security as a Serious Challenge for E-Banking: a Review of Emmental Malware,” Int. J. Adv. Comput. Res., vol. 5, no. 18, p. 62, 2015.

[21] S. Kiljan, K. Simoens, D. D. Cock, M. V. Eekelen, and H. Vranken, “A Survey of Authentication and Communications Security in Online Banking,” ACM Comput. Surv. CSUR, vol. 49, no. 4, p. 61, 2016.

[22] P. Peris-Lopez and H. Martín, “Hardware Trojans against virtual keyboards on e-banking platforms–A proof of concept,” AEU-Int. J. Electron. Commun., vol. 76, pp. 146–151, 2017.

[23] Z. Hussain, D. Das, Z. A. Bhutto, M. Hammad-u-Salam, F. Talpur, and G. Rai, “E-Banking Challenges in Pakistan: An Empirical Study,” J. Comput. Commun., vol. 5, no. 02, p. 1, 2017.

[24] H. G.Mark, “SANS Institute Survey Reveals 2016’s Biggest Cyber Security Threats and Risks in the Financial Sector,” Dec-2016. .

[25] Symantec, “Internet Security Threat Report Internet Report »VOLUME 21,” Apr-2016. .

[26] A. Bamrara, “Evaluating database security and cyber attacks: A relational approach,” J. Internet Bank. Commer., vol. 20, no. 2, p. 1, 2015.

[27] E. Abu-Shanab and S. Matalqa, “Security and Fraud Issues of E-banking,” Proc. Int. J. Comput. Netw. Appl., vol. 2, no. 4, pp. 179–187, 2015.

[28] M. Vrancianu, L. A. Popa, and others, “Considerations regarding the security and protection of e-banking services consumers’ interests,” Amfiteatru Econ. J., vol. 12, no. 28, pp. 388–403, 2010.

[29] G. C. Dalton, R. F. Mills, J. M. Colombi, R. A. Raines, and others, “Analyzing attack trees using generalized stochastic Petri nets,” in Information Assurance Workshop, 2006, pp. 116–123.

[30] T. P. S. Brar, D. Sharma, and S. S. Khurmi, “Vulnerabilities in e-banking: A study of various security aspects in e-banking,” Int. J. Comput. Bus. Res. 6 127, vol. 132, 2012.

[31] M. McDowell, “Understanding denial-of-service attacks,” Natl. Cyber Alert Syst. Cyber Secur. Tip ST04-0152004, 2004.

[32] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, “Cutting the gordian knot: A look under the hood of ransomware attacks,” in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 2015, pp. 3–24.

[33] M. PATYAL, S. SAMPALLI, Q. YE, and M. RAHMAN, “Multi-layered defense architecture against ransomware.”

[34] R. Perlman, C. Kaufman, and M. Speciner, Network security: private communication in a public world. Pearson Education India, 2016.

[35] M. Conti, N. Dragoni, and V. Lesyk, “A survey of man in the middle attacks,” IEEE Commun. Surv. Tutor., vol. 18, no. 3, pp. 2027–2051, 2016.

[36] N. A. G. Arachchilage and S. Love, “A game design framework for avoiding phishing attacks,” Comput. Hum. Behav., vol. 29, no. 3, pp. 706–714, 2013.

[37] S. Purkait, “Phishing counter measures and their effectiveness–literature review,” Inf. Manag. Comput. Secur., vol. 20, no. 5, pp. 382–420, 2012.

[38] A. Aggarwal, A. Rajadesingan, and P. Kumaraguru, “Phishari: automatic realtime phishing detection on twitter,” in eCrime Researchers Summit (eCrime), 2012, 2012, pp. 1–12.

[39] B. Schneier, “Semantic attacks: The third wave of network attacks,” Crypto-Gram Newsl., vol. 14, 2000.

[40] C. E. Drake, J. J. Oliver, and E. J. Koontz, MailFrontier. Anatomy of a Phishing Email. February, 2006.

[41] S. Gaudin, “Pharming attack slams 65 financial targets,” InformationWeek, 2007.

[42] J. Kirk, “’Pharming’attack hits 50 banks,” 2007.

[43] J. LaCour, “Vishing campaign steals card data from customers of dozens of banks,” 2014.

[44] M. B. Romney and P. J. Steinbart, Accounting information systems. Boston: Pearson, 2012.

[45] Q. Xiong, Y.-C. Liang, K. H. Li, Y. Gong, and S. Han, “Secure transmission against pilot spoofing attack: A two-way training-based scheme,” IEEE Trans. Inf. Forensics Secur., vol. 11, no. 5, pp. 1017–1026, 2016.

[46] J. Tang, D. Wang, L. Ming, and X. Li, “A scalable architecture for classifying network security threats,” Sci. Technol. Inf. Syst. Secur. Lab., 2012.

[47] K. D. Loch, H. H. Carr, and M. E. Warkentin, “Threats to information systems: today’s reality, yesterday’s understanding,” Mis Q., pp. 173–186, 1992.

[48] X. S. Yang Xiao and D.-Z. Du, Wireless network security. 2013.

[49] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, “Social engineering attack framework,” in Information Security for South Africa (ISSA), 2014, 2014, pp. 1–9.

[50] K. D. Mitnick and W. L. Simon, The art of deception: Controlling the human element of security. John Wiley & Sons, 2011.

[51] T. K. George and P. Jacob, “Vulnerability analysis of E-transactions in the Banking Industry, with a specific reference to malwares and types of attacks,” Int. J. Comput. Sci. Inf. Secur., vol. 12, no. 6, p. 48, 2014.

[52] R. Veras, C. Collins, and J. Thorpe, “On Semantic Patterns of Passwords and their Security Impact.,” in NDSS, 2014.

[53] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, “Hardware Trojan: Threats and emerging solutions,” in High Level Design Validation and Test Workshop, 2009. HLDVT 2009. IEEE International, 2009, pp. 166–171.

[54] Symantec, “Internet Security Threat Report , VOLUME 21, APRIL 2016,” Apr-2016. .

[55] intel security, “McAfee Labs 2017 Threats Predictions,” Nov-2016. .

[56] Gartner, “Predicts 2017 : treath and vulnerability management,” Nov-2016. .

[57] Q. Ya-Ping and S. Run-Jie, “Research on Block Chain Based on Innovative Management Mode,” DEStech Trans. Eng. Technol. Res., no. ssme-ist, 2016.

Meriem Tabiaa was born in Morocco in 1987. She obtained her Masters in computer science from “faculty of Science of El jadida” in 2012. She is currently studying for a doctorate at Chouaib Doukkali University in Morocco. Her field of interest is Modeling and assessment of the security of company’s information systems, especially on e-banking technology.

Abdellah Madani is currently a Professor and PhD Tutor in Department of Computer Science, Chouaib Doukkali University, Faculty of Sciences, El Jadida, Morocco. His main research interests include optimization algorithms, text mining, traffic flow and modelling platforms. He is the author of many research papers published at conference proceedings and international journals.

Najib Elkamoun received his Ph.D. degree in Optical and Microwave Communication from the National Polytechnic Institute of Grenoble, France, in 1990. He is currently Professor Researcher at Faculty of Science, University Chouaib Doukkali, El Jadida, Morocco. With over 20 years of expertise in information technology and communication, he has conducted several thesis and overseas missions in e-learning and telecommunication networks. His research interests include High Speed Network Architectures (MPLS), Mobility Management, security and QoS in Emerging Networks (MANET, VANET and WSN), Wireless Communications and Traffic Engineering for Computer