E-Banking Security:
Threats, Challenges, Solutions, and Trends

4

Fabio Diniz Rossi
https://orcid.org/0000-0002-2450-1024
Federal Institute of Education, Science, and Technology of Farroupilha, Brazil

Rumenigue Hohemberger
Federal Institute of Education, Science, and Technology of Farroupilha, Brazil

Marcos Paulo Konzen
https://orcid.org/0000-0002-8765-970X
Federal Institute of Education, Science, and Technology of Farroupilha, Brazil

Daniel Chaves Temp
https://orcid.org/0000-0002-9724-1331
Federal Institute of Education, Science, and Technology of Farroupilha, Brazil

INTRODUCTION

There are several types of banks, such as public, private, corporate, development, investment, among other functions, but all have as an essential prerogative the provision of services related to individuals, companies, industries and government money. They range from lending and financing of real estate and vehicles to significant trade-maintaining transactions in the country.

Based on this importance of the banks, security must be applied in the day-to-day of these institutions, because the virtual world is a dangerous place, and without some security control, the tendency is for there to be attempts to steal local money, at the time of looting, among other situations of danger and threats.

Online banking, electronic banking or e-banking consists of the user achieving the most diverse banking operations that are not made within the physical banking agencies. Generally, such transactions are carried out via the Internet, ranging from bank totem to mobile devices.

It has changed people's behavior over the way they spend money since financial transactions can be carried out with just one click. At first glance, this ease and practicality lure the consumers in the sense that their money is safe in and by the financial institution. However, most banking threats are transparent to customers (Singh et al., 2006). It is difficult to quantify the damage of a cyber attack to any financial institution since the impact is not only economic, but other elements make measurement difficult, such as damage to the image and reputation of organizations, loss of confidence in the institution and the loss of potential customers. Therefore, the cost of a cyber attack for an institution may represent a considerably more significant amount than the amount extracted by the attackers.

Although e-banking has been a reality for several years, it is only after 2004 that the incidents began to be reported (Kolodinsky et al., 2004). As a result, e-banking use has declined since threats are reported, but in recent years it has gained strength due to other factors, such as new cryptographic algorithms.

DOI: 10.4018/978-1-5225-9715-5.ch060

None of this is useful when it is the consumer who agrees to be stolen, and this is what most viruses do. Fraudsters take advantage of the innocence of consumers and their inexperience in information security. At the same speed as security techniques advance, threats about such techniques are created (Carminati et al., 2018).

The damage caused by the frauds reaches values in the order of millions of dollars worldwide every year. All these frauds cause customers embarrassment and a lengthy process of adaptation and high costs for the affected banks (Al-Furiah and Al-Braheem, 2009). This chapter, therefore, presents a landscape on all issues ranging from the threat, the challenges to addressing a viable solution to such a threat, and future security perspectives that can prevent new threats from arising that cannot affect online banking transactions.

This chapter presents the following contributions:

- A new taxonomy for classifying threats to e-banking environments.
- A list of new threats that will be organized within the new taxonomy.
- A discussion of such threats and the challenges to address a solution to these threats.
- A review of some trends on e-banking security mechanisms.

From the above, one can note that scams in e-banking environments are not exhaustive, as with each new day a new threat arises. Proposals such as that in this chapter update state-of-the-art concerning new risks and new mechanisms for protecting banking transactions.

This chapter proposes a new e-banking fraud taxonomy, and it presents several types of frauds classified inside such new taxonomy. After, this chapter discusses the advantages and disadvantages offered by the many types of e-banking security proposals. Afterward, we will summarize the work, making it possible to view challenges, trends and future perspectives.

E-Banking Fraud Taxonomy

This chapter proposes a novel taxonomy on security in banking systems, divided into two parts: the first part consists of an approach that organizes and classifies cyber attacks on banking environments, and a second part is an approach that organizes and categorizes current methods of security against cyber attacks discussed in the first part of the taxonomy.

The evolution of computing and new technologies has changed the way data manipulation and information have undergone various changes. As for money, online banking has emerged to make life easier for people, bringing added convenience and agility to the day-to-day operations of our daily activities. Checking balances, transferring amounts and making purchases over the internet is a reality today, but many people still have a bit of a fear of doing this.

Figure 1 shows target-based cyber attacks. Therefore, the attack can be directed to the client and its devices and applications, to the server that supports the banking service and receives client requests, or attacks on the communication between client and server. Threats directed at client devices or applications are mostly idealized through viruses or their variations and require some form of client acceptance (implicit or explicit). Threats to servers or infrastructure that supports banking services are less frequent but usually, occur through cloned services. Threats over the communication infrastructure between clients and the server usually occur through redirecting the network flow to fake sites.