Chapter 54
Analysis of Data Validation Techniques for Online Banking Services

Shadi A Aljawarneh
Jordan University of Science and Technology, Jordan

ABSTRACT

The insufficient preparation for the information and communication technologies revolution led to few offering online transaction platforms, information security features, and credit facilities. One of the security concerns is a lack of data validation. Data that is not validated or not properly validated is the main issue for serious security vulnerabilities affecting online banking applications. In this chapter, the influences of security issues on world banks will be discussed. A number of data validation methods will be also reviewed to date to provide a systematic summary to banking environment. Based on the advantages and disadvantages of each method, the IT developer will decide which is best suited to develop the systematic online banking application. From this analysis, a global view of the current and future tendencies of data validation will be obtained and therefore provision of possible recommendations for solving the security and privacy issues for the online banking services.

BACKGROUND

The rate of successful act of bypassing protection mechanisms and gaining access to computer system is sharply increased. Good examples can be found in Saudi Arabia, the United Arab Emirates, Lebanon, and Jordan. Above 20% of banks operating in the North Africa and Western Aisa, offer online services, from simple banking facilities to payment schemes (Ben-Jadeed & Molina, 2004). For instance, Lebanese banks now offer online services by moving some documentary credit procedures online to facilitate and guarantee e-commerce procedures (Aljawarneh et al, 2014).

The recent online banking facilities have not yet found their way to Libyan banking. Amongst the Arab nations, Libya has the finest reputation in the bankers but the worst banking services (Libyan investment, 2007). Essential electronic banking services, such as ATMs and mobile banking are limited

DOI: 10.4018/978-1-5225-3422-8.ch054

unless in some commercial banks. Most Libyan banks are still using manual banking techniques to carry out their services. It seems that there is no good networking among Libyan banks and their branches due to poor IT infrastructure. Consequently, security measures are not up to the standard required in the Libyan banking industry. There is a great concern about security issues that regulate e-banking activities in Libya, such as potential fraudulent activities, errors in conducting customer transactions, in addition to the lack of security measures such as e-laws and legislation (Abukhzam & Lee, 2010).

The United Arab Emirates Central Bank has adopted Secure Sockets Layer (SSL), Public Key Infrastructure (PKI), and smart card technology to activate online banking, and payment gateways that are being implemented by some of the large national players (Dutta & Coury, 2003).

However, because of information security concerns, most Small and Medium Enterprises (SMEs) in the Arab world ((refers to Arabic-speaking states and populations in North Africa and Western Asia) depend on conventional interactions and have not moved their operations online. Almost all of Arab banks websites are still informational without any online interaction among their customers. With little training and poor levels of awareness, SMEs do not take benefits from online accessing to new markets and inter-Arab trade potential (Dutta & Coury, 2003), for example as in Egypt and the western region of North Africa including five countries: Morocco, Algeria, Tunisia, Libya, and Mauritania. As a result, the insufficient preparation for the Information and communication technologies (ICT) revolution led to few offer transaction platforms, security features, and credit facilities for SMEs to motivate access technology.

For example, generally speaking, the major drawback of e-commerce in Libya is the lack of security, which scared people to use the Internet. Web applications need to be secured and people should be educated regarding security issues (Hamed, 2010).

The several banks (such as Citibank, HSBC, Lloyds TSB, National Bank of Abu Dhabi and Emirates NBD) across the United Arab Emirates are currently fighting to restore lost confidence in its online banking system after criminals used counterfeit credit cards to withdraw large quantities of funds from cash machines. Losses are expected to be several million dollars. This estimation of increase is expected to continue (Internet Security.ca, 2011).

In this chapter, we will focus on the main security issue which is the lack of data validation. Data that is not validated or not properly validated is the main issue for serious security vulnerabilities affecting online banking applications.

Therefore, the banks that have a web presence are increasingly worried for their reputations if the web system is subverted. This is because current security tools may not prevent the web system vulnerabilities. For example, with 4,396 new vulnerabilities disclosed in first half of 2010, total vulnerability count increased nearly 36% over the first half of previous year. This trend of increase is expected to continue (IBM, 2010).

Because inadequate data validation is a challenge, the Open Web Application Security Project (OWASP) mentioned the top ten security vulnerabilities effecting web. Several security issues in applications are caused by inadequate input validation including:

- Parameter manipulation, and therefore subversion of logic or security controls.
- Code injection, such as Cross Site Scripting, Structured Query Language (SQL) (MySQL, n. d.) Injection and Operating System command injection attacks (OWASP – 4 and 6).