



THE LIBYAN ACADEMY
SCHOOL OF APPLIED SCIENCES AND ENGINEERING
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

LIBYAN INTERNET BANKING SECURITY, EVALUATION AND AUTHENTICATION ENHANCEMENT

BY: EBTISAM IBRAHIM RADDAD

SUPERVISOR: DR. ALBAHLOUL ALFGHI

SUBMITTED IN PARTIAL FULFILLMENT FOR THE REQUIREMENTS OF THE
DEGREE OF MASTER OF SCIENCE

DEDICATION

To the most beautiful Queen, **MOM**: Because one day you had it a dream, today I turned it
into reality

إلى أجمل الملكات، **أمي**: لأنك حلمت بها يوماً، أضع رسالتي بين يديك اليوم حقيقة.

ACKNOWLEDGMENTS

I would like to seize the opportunity to express my deep gratitude:

To Dr. Bahlul Fgee for supervising my work and firstly for introducing me to the subject of Network Security which I became fascinated about.

To the committee, namely; Dr. Ahemd Arara, whose guidance was the key behind having this thesis in its final form, and Dr. Abubaker Elhuni, who supported my not only in this work but throughout the different stages of my study at the Academy.

To Dr. Mokhtar Mohamed Ashur, Dean of Applied Science and Engineering School at the Libyan Academy, for his inspiration, support, and beautiful mind. Simply for being the great person he is.

To all lecturers, book authors, the Libyan Academy staff, and everyone who contributed to my knowledge.

To all my family and friends:

My father who raised me to be independent and confident,

My grandparents whose prayers made doors of life open voluntarily,

My beloved sister, Asma, who guided me throughout life being a mother, a teacher, and a mentor,

My Sister/Friend, Amal, and my Friend/Sister, Ahlam, who believed in me when I stopped believing in myself,

And last but not least, to my five mermaids and Prince: Asma, Joud, Esra, Aya, little Robeen, and Ibrahim whose existence made me want to be a better Auntie.

ABSTRACT

Internet banking refers to several types of banking activities through which bank customers can get information and carry out most retail banking services through Internet. The majority of Libyan banks continue to conduct their banking transactions using traditional bank branches, and only few adopted the technology in its basic form. Having the Libyan banking industry in extreme need of essential change to enhance its banking system in order to follow global standards, it is about time to find studies offering real solutions.

Authentication mechanisms provide the cornerstone for security enhancement and are essential for any intended development. Traditional authentication methods include passwords and PINs are now inadequate to protect online users and organizations from ever more sophisticated attacks.

The purpose of this study is to evaluate the existing internet banking system by scanning and analyzing its activities against possible attacks in order to understand where the industry stands.

Also, the improvement to traditional authentication mechanisms followed is another aim. In this study, we answer two main questions to cover the two sides of authentication enhancement: which method is adequate to replace the traditional, and how global standards can be employed to achieve better security and compliance.

الخلاصة

يقصد بالصيرفة الالكترونية النشاطات المصرفية المختلفة التي يقوم بها زبائن المصارف للحصول على المعلومات والخدمات المصرفية عن طريق شبكة الانترنت. تستمر غالبية المصارف العاملة في ليبيا بتقديم المعاملات المصرفية بالطرق التقليدية عن طريق فروعها والتعامل المباشر مع زبائنهم، وقلة فقط من تلك المصارف تبنت تقنية الصيرفة الالكترونية في أبسط صورها.

ونظراً لأن صناعة المصارف في ليبيا في حاجة ماسة لتغييرات جذرية لتحسين منظومتها الخدمية واللاحق بركب التقنية العالمي، توجب وجود دراسات تتناول هذا الجانب وتقدم حلولاً ناجعة. طرق التحقق من الهوية تعد حجر الزاوية لتحسين أمان الصيرفة الالكترونية، وهي أساسية أيضاً لأي تطوير مقترح. فالطرق التقليدية للتحقق من هوية المستخدم والمتضمنة كلمة السر ورقم التعريف الشخصي غير مناسبة في أيامنا هذه لتوفير الحماية المطلوبة للمستخدمين والشركات ضد الهجمات التي تزداد تعقيداً يوماً بعد يوم.

الهدف من هذه الدراسة هو تقييم منظومة الصيرفة الالكترونية الموجودة حالياً في ليبيا بفحص وتحليل نشاطاتها مقابل الهجمات المحتملة لتوفير فهم أكبر للصورة العامة وأرضية للعمل على تحسينها.

كما يعد تطوير نظام تحقيق الهوية المطبق هدفاً آخر لهذه الدراسة. حيث ستم الإجابة على سؤالين رئيسيين يغطيان جانبي تحسين طرق التحقق من الهوية وهما: أي الطرق هي الأكثر ملائمة لاستبدال الطرق التقليدية المتبعة، وكيف يمكن الاستفادة من المعايير العالمية لتحقيق أمان أعلى لخدمات الصيرفة الالكترونية وجعلها أكثر مطابقة للأنظمة العالمية.

يقصد بالصيرفة الالكترونية النشاطات المصرفية المختلفة التي يقوم بها زبائن المصارف للحصول على المعلومات والخدمات المصرفية عن طريق شبكة الانترنت. تستمر غالبية المصارف العاملة في ليبيا بتقديم المعاملات المصرفية بالطرق التقليدية عن طريق فروعها والتعامل المباشر مع زبائنهم، وقلة فقط من تلك المصارف تبنت تقنية الصيرفة الالكترونية في أبسط صورها.

ونظراً لأن صناعة المصارف في ليبيا في حاجة ماسة لتغييرات جذرية لتحسين منظومتها الخدمية واللاحق بركب التقنية العالمي، توجب وجود دراسات تتناول هذا الجانب وتقدم حلولاً ناجعة.

TABLE OF CONTENTS

DEDICATION	i
ACKNOWLEDGMENTS	ii
ABSTRACT	iii
TABLE OF CONTENTS	v
LIST OF TABLES	viii
LIST OF FIGURES	ix
CHAPTERS	
1. INTRODUCTION	1
1.1. Background to the study	2
1.1.1. Importance of Internet Banking	2
1.1.2. Challenges to Internet banking.....	3
1.2. Research Question	4
1.3. Research Methodology	5
1.4. Thesis structure	6
2. SECURITY IN INTERNET BANKING	8
2.1. Components of security	8
2.2. Security Mechanism.....	11
2.3. Visibility of security mechanisms to users	12
2.4. Types of Online communication attacks.....	13
2.4.1. Attacks on Online Service Provider (OSP).....	14
2.4.1.1. Denial-of-service attack (DoS).....	15
2.4.1.2. Website/application manipulation	15
2.4.1.3. Brute-force attack	16
2.4.1.4. OSP security policy violation	16
2.4.2. Attacks on Communication Channel (CC)	17
2.4.2.1. Sniffing	17
2.4.2.2. Man-in-the-middle attack (MITM).....	17
2.4.2.3. Session hijacking	18
2.4.3. Attacks on End Users (EU)	18
2.4.3.1. User surveillance	18
2.4.3.2. Token/notes theft	19
2.4.3.3. Malware infection	19
2.4.3.4. Social engineering	19
2.4.3.5. Phishing	19
2.4.3.6. Pharming.....	19

2.4.3.7.Clickjacking	20
2.4.3.8.Man-in-the-browser attacks (MITB)	20
2.4.General security attitudes for financial transactions	21
3. AUTHENTICATION IN AN INTERNET BANKING ENVIRONMANT	23
3.1.Typical authentication process	23
3.2.Authentication classes.....	25
3.2.1.Knowledge-based authentication (KBA)	25
3.2.2. Token-based authentication (TBA).....	26
3.2.3. Biometric-based authentication (BBA).....	27
3.3.Implementation mechanisms	29
3.3.1.Single-factor authentication	29
3.3.2. Multi-factor authentication.....	30
3.3.3. Multi-channel authentication	30
3.4.Authentication to an Internet bank.....	32
3.4.1.Two-factor authentication methods.....	32
3.4.1.1. EMV Card and Reader	33
3.4.1.2. Hardware & Software OTP Tokens	33
3.4.1.3. Hardware-based PKI tokens	33
3.4.1.4. Software-Based PKI Tokens	34
3.4.1.5. SMS-based OTPs.....	34
3.4.1.6. TAN Lists	34
3.4.1.7. Matrix cards.....	34
3.4.2. Two-factor authentication using mobile phones	35
4. LIBYAN INTERNET BANKING EVALUATION	38
4.1. Libyan Banks and Internet Banking	39
4.2. Internet Banking Security and Vulnerability Scanners	41
4.2.1. Vulnerability Scanners	41
4.2.2. Benefits and Limitations of Vulnerability Scanners	43
4.2.3. Types of Vulnerability Scanners	44
4.2.4. Web Vulnerability Scanners	45
4.2.5. Common Web Vulnerability Scanners	46
4.2.5.1. Acunetix Web Vulnerability Scanner	49
4.2.5.2. Qualys Web Vulnerability Scanner	50
4.2.5.3. Vega Web Vulnerability Scanner	51
4.3. Web security analysis	52
4.3.1. Vulnerability count and severity levels	52

4.3.2. Types of detected vulnerabilities	56
4.4. Authentication Security Analysis	64
4.5. Summary and obstacles	75
5. APPLIED AUTHENTICATION AND PROPOSED ENHANCEMENT	77
5.1.Product solution	77
5.1.1.Why 2FA?	78
5.1.2. Which method is right?.....	79
5.1.3 Bank selection criteria to adopt a solution.....	81
5.1.3.1. Customer usability	82
5.1.3.2. Effectiveness	83
5.1.3.3 Cost	84
5.1.4. Method selection summary.....	85
5.2. Guidance to authentication in an Internet banking environment	86
5.2.1 FFIEC guidance to authentication in an Internet banking environment.....	87
5.2.2 Implementing a layered system of security	88
5.2.2.1. Step 1: Risk management	88
5.2.2.2. Step2: Customer Authentication for High-Risk Transactions	88
5.2.2.3 Step3: Layered Security Programs	89
5.2.2.4 Step4: Effectiveness of Certain Authentication Techniques	90
5.2.2.5 Step5: Customer Awareness and Education	91
5.2.3. Compliance example	94
6. CONCLUSION AND RECOMMENDATIONS	95
6.1.Conclusion	95
6.2.Recommendations.....	96
6.3.Suggestions for future work.....	97
REFERENCES	98
BIBLIOGRAPHY	100
APPENDIX A	101
APPENDIX B.....	105
APPENDIX C.....	109

LIST OF TABLES

Table 2.1: Security Objectives.....	9
Table 2.2: Security Mechanisms in Internet Banking.....	11
Table 2.3: Visible Security Mechanisms.....	12
Table 3.1: Summary Table of Different Authentication Classes.....	28
Table 4.1: Banks existing and potential Internet banking and related Mobile service.....	40
Table 4.2: List of web vulnerability scanners.....	46
Table 4.3: Selected web vulnerability scanners summary and justification of choice.....	51
Table 4.4: Severity Levels.....	52
Table 4.5: Summary of conducted scans	53
Table 4.6: Top vulnerabilities by Acunetix	58
Table 4.7: Top vulnerabilities by Qualys	60
Table 4.8: Top vulnerabilities by Vega.....	63
Table 4.9: High vulnerabilities causes.....	69
Table 4.10: Summary of conducted authentication scans.....	66
Table 4.11: Top authentication pages vulnerabilities by Acunetix.....	70
Table 4.12: Top authentication pages vulnerabilities by Qualys.....	72
Table 4.13: Top authentication pages vulnerabilities by Acunetix.....	74
Table 4.14: Top authentication pages vulnerabilities by Vega.....	74
Table 4.15: Summary of obstacles and their solutions	76
Table 5.1: Comparison between authentication methods.....	80
Table 5.2: Method compliance to criteria	81
Table 5.3: Suggested authentication guidance checklist.....	92

LIST OF FIGURES

Figure 1.1: Stages of the Research Methodology.....	6
Figure 1.2: Structure of the Thesis.....	7
Figure 2.1: Internet Banking Activities.....	10
Figure 2.2: Applicable Attacks on the Main Three Communication Elements.....	14
Figure 2.3: (a) Non-persistent XXS Attack; (b) Persistent XSS Attack.....	16
Figure 2.4: Security Policy Violation.....	17
Figure 2.5: Man-in-the-Middle (MITM) Attack.....	18
Figure 2.6: DNS Spoofing Attack.....	20
Figure 2.7: Man-in-the-Browser (MITB) Attack.....	21
Figure 2.8: Showing Level of Concern about Financial Transactions Security.....	22
Figure 2.9: Concern for Fraudulent Access of an Account.....	22
Figure 3.1: Internet Bank Authentication Process.....	24
Figure 3.2: Smart Card.....	27
Figure 3.3: Different Hardware Token Types Used to Generate One-Time Pin.....	26
Figure 3.4: Single-Factor Authentication Mechanism.....	29
Figure 3.5: Multi-Factor Authentication Mechanism.....	30
Figure 3.6: Multi-Channel Authentication Mechanism.....	31
Figure 3.7: TAN and matrix card methods.....	35
Figure 3.8: General Architecture of Mobile Authentication.....	36
Figure 3.9: OTP Check.....	37
Figure 4.1: Libyan banking infrastructure.....	39
Figure 4.2: Internet and Mobile banking services in Libyan banks.....	41
Figure 4.3: Components of a vulnerability scanner	42

Figure 4.4: Comparison between total numbers of detected vulnerabilities.....	54
Figure 4.5: Comparison of total detected vulnerabilities (without info alerts).....	54
Figure 4.6: Comparison between numbers of detected vulnerabilities for BCD bank.....	55
Figure 4.7: Comparison between numbers of detected vulnerabilities for Eljumhuria.....	55
Figure 4.8: Comparison between numbers of detected vulnerabilities for Aman bank.....	56
Figure 4.9: Internet banking providers' different login screens	65
Figure 4.10: Comparison of total detected authentication vulnerabilities.....	67
Figure 4.11: Comparison of total authentication vulnerabilities (without info alerts).....	67
Figure 4.12: Comparison between detected authentication vulnerabilities for BCD.....	68
Figure 4.13: Comparison between detected authentication vulnerabilities for Eljumhuria.....	68
Figure 4.14: Comparison between detected authentication vulnerabilities for Aman.....	69
Figure 5.1: The cost of different banking channels.....	78
Figure 5.2: Criteria of solution adoption	82
Figure 5.3: Percentage of BCD compliance with FFIEC guidance.....	94

INTRODUCTION

Electronic banking- also referred as Online banking, Internet banking, e-banking, virtual banking and by other terms is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. Electronic banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet. Customers access electronic banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), kiosk, or Touch Tone telephone. While the risks and controls are similar for the various electronic banking access channels, this thesis will focus specifically on Internet-based services due to the Internet's widely accessible public network. Accordingly; the term "Internet Banking" will be used along this work. A narrower definition of Internet Banking subject of this work would be: Internet Banking is an electronic system that enables customers of a financial institution to conduct financial transactions on a website operated by the institution.

Distance banking services- known also as Home Banking- from the early 1980s were the start of modern online banking. The term "online banking" became popular in late 1980s. Online services started in New York in 1981 when four of the city's major banks (Citibank, Chase Manhattan, Chemical and Manufacturers Hanover) offered home banking services using the videotex system. Because of the commercial failure of videotex these banking services never became popular except in France where the use of videotex (Minitel) was subsidized by the telecom provider and the UK, where the Prestel system was used. In the late 1990s, many banks began to view Web-based banking as a strategic imperative. The attraction of banks to online banking are fairly obvious: diminished transaction costs, easier integration of services, interactive marketing capabilities, and other benefits that boost customer lists and profit margins.

Many consumers were hesitant to conduct monetary transactions over the web. It took widespread adoption of electronic commerce, based on trailblazing companies such as America Online, Amazon.com and eBay, to make the idea of paying for items online widespread. By 2000, 80 percent of U.S. banks offered e-banking. At Bank of America, for example, it took 10 years to acquire 2 million e-banking customers. In 2001, Bank of

America became the first bank to top 3 million online banking customers, more than 20 percent of its customer base. Online customers proved more loyal and profitable than regular customers. In October 2001, Bank of America customers executed a record 3.1 million electronic bill payments, totaling more than \$1 billion. In 2009, a report by Gartner Group estimated that 47 percent of U.S. adults and 30 percent in the United Kingdom bank online. Today, many banks are internet only banks without any physical- branch- representation [1].

1.1. Background to the Study

1.1.1. Importance of Internet Banking

Internet banking provides a number of advantages for both the banks and their customers. Internet banking has made life much easier and banking much faster and more pleasant, as it:

- Saves time spent on queuing in the Bank.
- Removes geographical limitations for small and medium size banks, thereby paving ways for international operation without limits.
- Has no time limitation i.e. banking transactions may be performed through out the day, week and from any place they can have access to the Internet.
- Provides efficient cash management for interest optimization.
- Provides convenience in terms of the capital, labor time and all the resources needed to make a transaction.
- Has assist banks to increase in data collection, data management, and financial engineering that have improved the ability of potential creditors to assess the creditworthiness of potential borrowers and to price the risk associated with those borrowers through standardized mechanisms such as credit scoring.
- Taking advantage of integrated banking services bank, clients may compete in new markets, gain access to new customers and grow their market share.
- Banking technological developments make it much easier and cheaper for customers to compare and contrast products and to establish multiple banking connections, which could alter the purchase decision-making process of the customer.

1.1.2. Challenges to Internet Banking

The internet banking being a relatively new technology- especially in Libya- faces a problem of acceptability. Then it has to battle with competition since competition is the driving force behind the introduction of the Internet banking. The banking system being an oligopolistic market (a market condition in which sellers are so few that the actions of any one of them will materially affect price and have a measurable impact on competitors), it is necessary for the internet bank to compete in the first place through the sub-strategy of product-service differentiation. To enhance the product-service differentiation; the internet should be exploited as a channel to build, maintain and develop long-term client relationships through the ready access to a broad and increasing array of products, service and low-cost financial shopping, rapid response to customer inquiries, and personalized product-service innovation. Another challenge prone to the Internet banking is transaction security, due to the open nature of the Internet; this is likely to emerge as the biggest concern among the Internet banks. Since transactions risk would create a significant barrier to market acceptance, its management and control are crucial for business reputation and the promotion of consumer confidence as well as operational efficiency. To safeguard this, it is imperative for the Internet bank to implement measure to protect client assets and information. The Internet banking is likely to be challenged by demographics; this can prevent some commercial banks future access to profitable, IT-seasoned customer segments. To exploit this challenge and increase market share, financial institutions must seek to attract and capture computer-literate Internet users who are young and educated as early as possible to supplying at low cost technologically innovative and sophisticated products and services such as globally mobile banking and e-financial transactions over the Internet.

Internet banking has also brought new challenges for bank management, supervisory and regulatory authorities.

Operational risk: Operational risk of Internet banking is the central of system availability and security to the dependability on new technology which provides services.

Security threats can be internal or external to the system, due to this, banking regulators and supervisors must check that banks have the right measures in place to secure data integrity and confidentiality. These security practices should be tested on regular basis by technical skilled persons to analyze network vulnerabilities and recovery preparedness. The integral part of the overall management of risk needs to include the management of the heightened

operational risks and supervisors need to include operational risks in their safety and soundness evaluations.

Legal risk: Electronic banking carries heightened legal risks for banks. Banks has grown geographically faster in terms of services which they render through Internet banking compared to the traditional banking method. In some cases, however, the banks rendering these services might not be fully acquainted with laws and regulations abiding in that area before offering such services, either with a permission (license) or not. When this permission is not there, a virtual bank not having adequate contact with its supervisor from the host country may find problems adapting to the regulatory changes. As a result, virtual banks being unaware unknowingly could go against the protection laws of a customer, including data collection and privacy. After which, they subject themselves to losses through lawsuits or crimes that are not prosecuted because of jurisdictional disputes. Money laundering has being on for some time now which is being facilitated by Internet banking due to the anonymity it affords. Many countries have issued proper rules for the identification of customers when an account is being opened.

Reputational risk: Bank's reputation can be damaged due to violation of security and disruptions to the availability of the system. Reputational risk is more dependent on the reliance on electronic delivery channels which in turn increases its potentials. For instance, a bank that offers electronic services experienced any problems that might lead to the lost in confidence customers have for electronic delivery channels in general, these problems can potentially affect other providers of Internet banking services. Reputational risks also stem from customer misuse of security precautions or ignorance about the need for such precautions. Security risks can be amplified and may result in a loss of confidence in electronic delivery channels [2].

1.2. Research Questions

The main aim of this research is to evaluate the existing online banking security in Libya and propose an authentication enhancement method to the existing. In order to achieve that the research asks the following questions:

- ✓ Are there security vulnerabilities in the existing Libyan internet banking security? And if yes, do they affect authentication?
- ✓ Considering the technical infrastructure and budget, can a secure and reliable authentication method be implemented and adopted to replace the existing?

1.3. Research Methodology

Research methodology is a way to systematically solve the research problem. It may be understood as a science of studying how research is done scientifically. In it we study the various steps that are generally adopted by the researcher in studying his research problem along with the logic behind them.

The basic types of research are as follows [3]:

- **Descriptive vs. Analytical:** Descriptive research is used to report a description on what has happened or what is happening where the researcher has no control on the variables. In analytical research, on the other hand, the researcher uses facts or information already available, and analyzes those to conclude a critical evaluation.
- **Applied vs. Fundamental:** Applied research aims at finding a solution for an immediate problem facing a society or an industrial/business organization, whereas fundamental research is mainly concerned with generalization and with a formulation of a theory. Gathering knowledge for knowledge's sake is termed fundamental research.
- **Conceptual vs. Empirical:** Conceptual research is that related to abstract ideas or theory. It generally used by philosophers or thinkers to develop new concepts or to reinterpret existing ones. While empirical research relies on experience or observation alone, often without due regard for system or theory. It is data-based research, coming up with conclusions which are capable of being verified by observation or experiment.
- **Quantitative vs. Qualitative:** Quantitative research is applicable to phenomena that can be expressed in terms of quantities. Qualitative research, on the other hand, generally aim to understand the experiences and attitudes of the research samples. These methods aim to answer questions about the 'what', 'how' or 'why' of a phenomenon.

Based on the above definitions, this work will use *Analytical* research type to answer our research questions.

The research is divided into two sequential phases- as illustrated by the below chart of figure 1.1 - leading to answering our research questions.

First Phase- Evaluation

- Register for a vulnerability scanner tool
- Run scans on the targeted website
- Understand result factors
- Analyze results to determine vulnerability levels

Second Phase- Enhancement

- Run scans on authentication pages and links
- Provide a roadmap toward authentication enhancement
- Suggest policies as part of the solution

Figure 1.1: Stages of the Research Methodology

1.4. Thesis Structure

Chapter 1 provides an introduction to the research, which will include research background, research question, research methodology containing a detailed explanation of the research approach, design and the structure of the research, and connections between research stages will be presented.

Chapter 2 will cover the first part of the literature review related to Internet security: its components, mechanisms, and types of attacks. The information contained in this chapter serve as a strong background to deeper understanding of the evaluation discussed in later chapter (namely; chapter 4)

Derived from its importance as a key focus when security of Internet banking is the subject **Chapter 3** covers authentication in Internet banking. Being the second part of the literature review this chapter explains concepts related to chapter 5. Authentication process, methodologies, the implementation of mobile devices are some of the topics of interest.

Chapter 4 and **Chapter 5** are where the application of the research methodology takes place. In these two chapters, we evaluate the existing Libyan Internet banking, explore vulnerabilities, and propose solutions. A review and background of used software and service websites consulted are also contained.

Derived from Chapters 4 and 5 work and based on the overall research chapters, **Chapter 6** will include the conclusion and findings. At this stage, the answers of all research questions are stated as well as some recommendations for future work to help future researches to start from where this work stopped and help building on its findings.

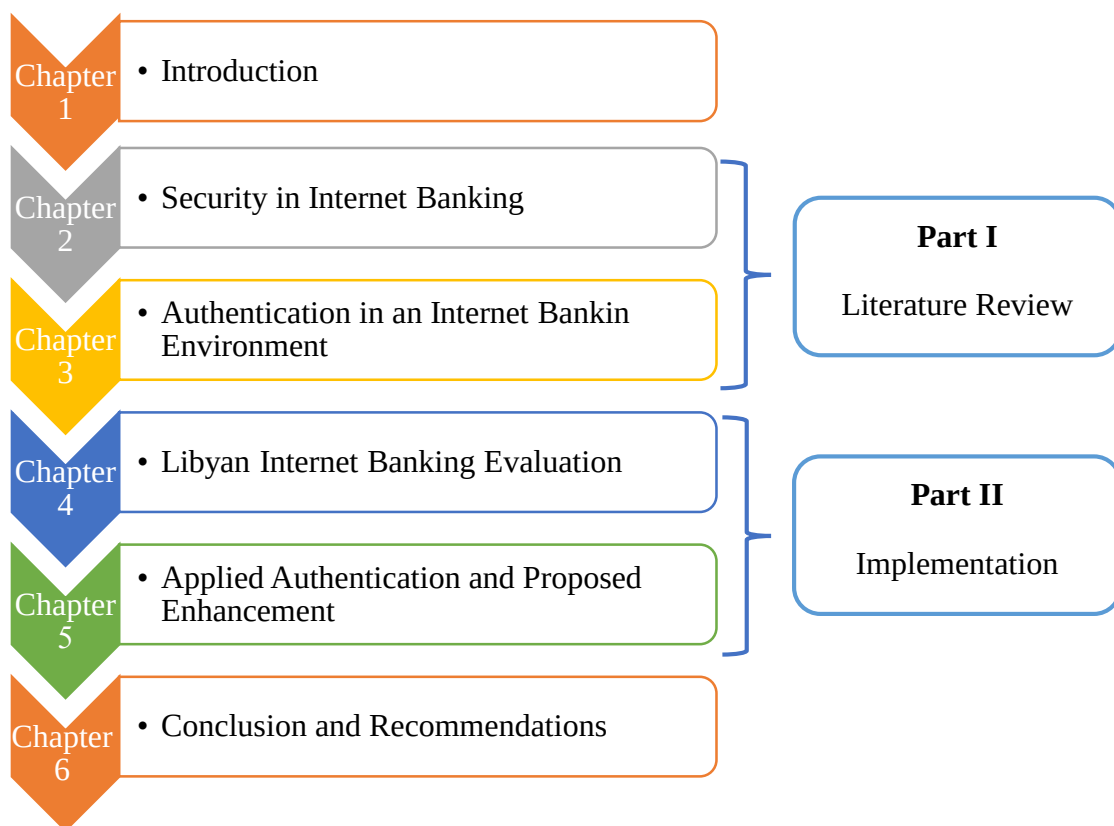


Figure 1.2: Structure of the Thesis

SECURITY IN INTERNET BANKING

Security, being a complex concept, has been defined by several researchers using diverse classification techniques. In general, security is defined as the protection against security threats. In electronic commerce, a threat would be defined as an event that can destroy, modify, waste, deny or disclose information or reduce efficiency of the data and network resources. These threats could appear at the client or the server side and these could originate due to human, system or communication errors.

To gain a in depth view of security, in this section a review of the components of security (Section 2.4.1), the meaning and types of security mechanisms (Section 2.4.2) and the interaction of users with these mechanisms (Section 2.4.3) are presented.

2.1. Components of Security

Security is primarily composed of a set of security primitives or objectives. Each of these objectives aims at protecting the systems and/or users against threats. The primary goals of security are Confidentiality, Integrity and Availability or the ‘CIA’ triad. Over time, several other objectives such as authentication and authorization have been identified and been included as an integral part of security. The most widely acknowledged security objectives of e-commerce and its applications are confidentiality, integrity, availability, authentication, authorization, non-repudiation and privacy.

Table 2.1 lists the definitions of these objectives. Each of the objectives from Table 2.1 covers areas of potential security breaches and attempts to provide a holistic view of the meaning of security in internet banking applications. While some objectives would implicitly imply that other objectives should be fulfilled (for example, confidentiality would require authentication to be achieved) other objectives can be achieved singularly [4].

Table 2.1: Security Objectives

Objective	Definition
Confidentiality	This ensures that the communication between the user/customer and the service provider is not accessible to other parties. Unauthorized access of information should be prevented. This should include confidentiality of information that is passed over the network during communication and also the confidentiality of information that is stored at different locations.
Integrity	During and after exchange of information, the content should remain unchanged and should be tamper free. This covers both accidental and intentional damage to information data. Integrity ensures that messages that are not created, modified, intercepted or deleted by unauthorised people.
Availability	The information required by users should be accessible when acquired by them. This ensures that the system is reliable and authorized personnel can access the services of an application within a desired time frame.
Authentication	Traditionally authentication deals with verification of parties who are communicating to guarantee that they are who they claim to be. Authentication must cover both, entity authentication and data authentication. They explain that entity authentication is the verification of the entities or people involved in a transaction. Data authentication is ensuring the data is valid at a particular point in time.
Authorization	This objective aims at making sure that the user accessing information has the right to view/manipulate this information. This also includes ensuring that users of e-commerce applications have the permission to send requests and communicate with the system.

Non-repudiation	The aim of this is to ensure that the party involved in initiating a transaction, sending any information, or receiving any information cannot deny it at a later instance of time.
Privacy	Privacy, though considered by some researchers a separate issue from that of security, has been included by many as part of the security objectives. From a customer's perspective, security and privacy may not be discrete concepts, and in most circumstances, security would imply privacy. Privacy is defined as the need to guarantee that the customer information is not accessible to unauthorized users and is not misused.

Internet banking transactions normally have a pre-defined set of steps that a user follows to perform the activities. Four steps defined these activities. Figure 2.1 lists these steps.

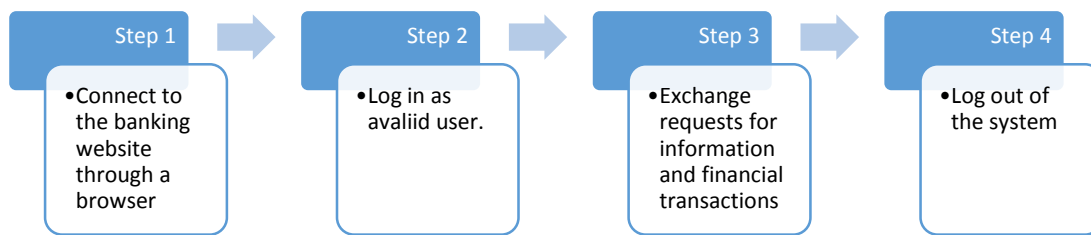


Figure 2.1: Internet Banking Activities

On analyzing each of these steps, the security objectives that were defined above can be mapped to security requirements for user activities. In Step 1, the user should be able to connect to the website within a reasonable period of time, hence dictating the need for the availability objective. Step 2 requires the user's login to be validated and the user should be able to access and manipulate his account information. Thus, authentication and authorization are needed. The third step involves communication of information over a network and therefore, this communication needs confidentiality, integrity and privacy. Through all four steps, the bank customer must be ensured that the transactions requests made by him would be followed through by the bank. This can be ensured by the non-repudiation objective. Thus, security for e-banking applications can be achieved through considering a combination of these seven objectives.

2.2. Security Mechanisms

In an attempt to provide extensive security support for e-commerce applications the objectives defined previously must be achieved using different measures. For a user, these measures are means of understanding and interacting with the security of a system.

Security cannot be defined only as technological measures. There are several mechanisms that are non-technical in nature such as policies, strategies, information listed on websites and so on. All these measures are solutions to countering the threats to the security of the applications and services. Hence, for this paper, security mechanisms are defined as the devices, technologies, methods, measures used to secure a particular system.

Authentication is considered to be one of the most critical security goals that must be achieved for e-banking. Along with that, Hawkins et al. (2000) state that currently most financial institutions including banks employ security mechanisms such as Secure Socket Layers (SSL), encryption of data that is transferred over the internet, digital certificates, etc. To protect customer information stored within their servers, they use firewalls, virus detection and protection methods, backup servers as some of the protective measures [4].

Table 2.2 shows examples of mechanisms currently employed by the internet banking industry to fulfil various security objectives. Some mechanisms are capable of achieving more than one objective, but their protective capability with respect to each objective may differ.

Table 2.2: Security Mechanisms in Internet Banking

Objective	Security Mechanisms
Confidentiality	Cryptography: includes encryption during data transmission and storage
Integrity	• Encryption. • Digital signatures. • Hash functions.
Availability	Back up servers.

Authentication	• Passwords (fixed and dynamic) • Hardware measures (such as USB tokens) • Digital signatures.
Authorization	Access control policies.
Non-repudiation	Digital signatures and certificates
Privacy	Policies and disclosures.

2.3. Visibility of Security Mechanisms to Users

Internet banking users would be informed through the user interface about the types of mechanisms used and their protection goals. From a user's perspective, the visibility of these security mechanisms through the user interface is an important aspect and hence the integration of these security mechanisms with the interface is important. Several features such as user name and password logins, informative error and warning messages, information on the encryption technologies used, symbols such as the padlock sign in browsers are security mechanisms that are visible to users. Each of these conveys the type of the mechanism used to secure the transaction between the user and system [4].

Table 2.3 provides a list of visible security mechanisms for different security objectives. While the indicators of security listed in the table do not form an exhaustive list of those used by all banking (and in general e-commerce websites), these are some of the most commonly appearing ones.

Table 2.3: Visible Security Mechanisms

Objective	Examples of Visible Mechanisms
Confidentiality	• Padlock Symbol in browser(indicates encrypted connection like SSL) • Warning messages when moving to unsecured network connections. • Presence of “https”.
Integrity	• Padlock Symbols • Warning/Error messages.

Availability	Reduced System Down-time.
Authentication	Login IDs and Passwords
Authorization	Login pages.
Non-repudiation	• Policy disclosure. • Padlock symbol indicating page is digitally signed.
Privacy	Privacy Policy disclosures.

2.4. Types of Online Communication Attacks

Since the introduction of the Internet and the tremendous growth of Internet users and e-commerce web applications, user identification and authentication have become major research areas charged with keeping pace and withstanding networking changes and increasing numbers of information security threats and attacks, evolving over time. These attacks use various technologies and techniques, and exploit various vulnerabilities; they have the potential to damage any of the three key elements involved in an online communication model. These three key elements are: the source, the transmission system, and the destination. In this research, source and destination are referred to as *end user (EU)* and *online service provider (OSP)*, respectively. The transmission system is referred to as the *communication channel (CC)*.

Figure 2.2 shows the applicable known attacks on each of the key elements of the online communication model [5].

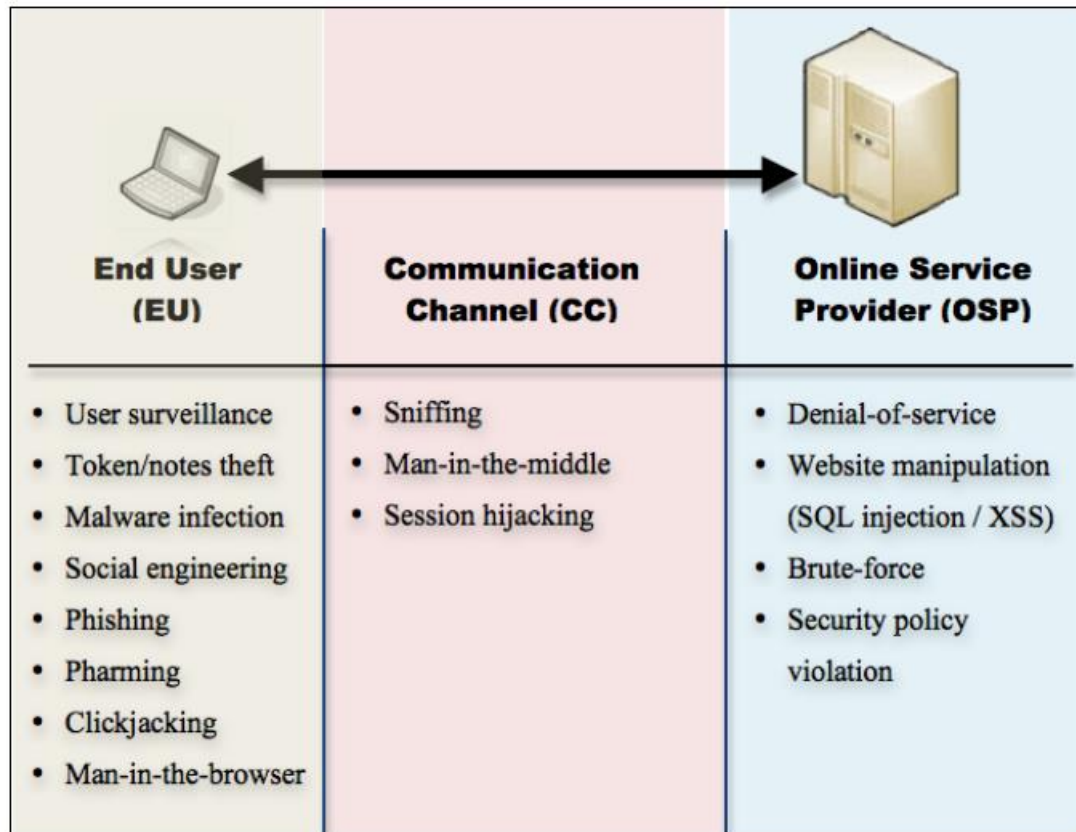


Figure 2.2: Applicable Attacks on the Main Three Communication Elements

2.4.1. Attacks on Online Service Provider (OSP)

An Online Service Provider (OSP) is any organization that provides an electronic service for users via the Internet. This includes Internet banking services provided by banks, electronic mail services provided by companies like Microsoft, Google, and Yahoo!, and other online services that are owned and managed by individuals and are hosted by different data centres around the world (e.g., Internet relay chat (IRC), social community forums, hosting services, online file sharing, blogging, and online gaming).

There are many reasons why attackers target OSPs. Some aim to utilize the OSP resources for illicit materials; they might store hacking tools and set the server to be part of a DDoS attack. Others attack OSPs to steal services or valuable files, to spy on friends and family members, or to build reputations, especially if attacking well-known high profile or secured organizations where there are clashes of interests related to politics and religion. The following sub-sections discuss the types of attacks that target OSPs.

2.4.1.1 Denial-of-Service Attack (DoS)

This type of attack aims at making the OSP's online services unavailable or unreachable to users, turning services down. Denial-of-Service (DoS) is about involving only one source (i.e., a single person or a group of people) to exhaust OSP resources, such as network bandwidth, computing power, or operating system data structures, and to limit or stop completely the delivery of services to end users.

2.4.1.2. Website/application Manipulation

Website/application attacks are considered the most common attacks targeting OSPs with 49% of total known OSP attacks. Manipulation of website site contents or the web application database can be very harmful and destructive in nature if recovery plans are not properly set by the OSP management. For example, an SQL injection type of attack, where database SQL statements are injected into the URL as a query string because of poorly designed web application, can allow the attacker to gain administrative privileges for a security-policy maintained web application. The attacker can also wipe all database records, and if there were no proper frequent backup rules set in place, especially for an interactive web application, updated frequently by the OSP and customers, this can cause severe implications for the OSP's reputation and its online business.

There are many types of website/application manipulation attacks; the most common ones are the SQL injection and cross-site scripting (XSS). The latter is usually used to hijack users' cookies or sessions. XSS comes in two forms: *non-persistent* and *persistent*. Nonpersistent attacks cannot be carried out unless the attacker is able to contact the victim user by e-mail or other means to pass a crafted link with a malicious code. Once the user clicks on the link, it opens a legitimate website the user visits that may have an account that is authenticated by a cookie stored in the user's machine. The malicious code injected in the link will be executed by the user's browser after it is rendered by the website the user visits. Depending on the code functions, it can copy the user's cookie or session and pass it on to the attacker (see Figure 2.3).

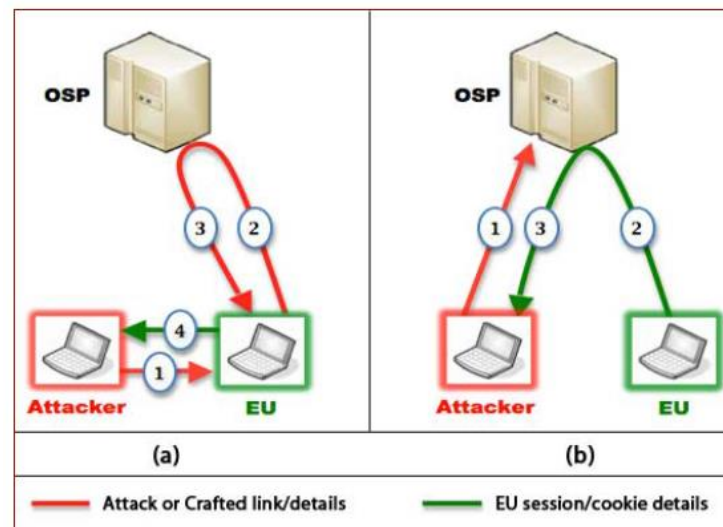


Figure 2.3: (a) Non-persistent XSS Attack; (b) Persistent XSS Attack

2.4.1.3. Brute-force Attack

This type of attack aims at compromising users' accounts at the server level by randomly checking the validity of usernames and passwords with infected zombie personal computers. Usually this happens in a distributed manner as discussed in DoS attacks. The response of the OSP is recorded and passed back to the original attacker. This can be either an invalid username and password or a valid session establishment, which normally means a valid username and password.

2.4.1.4. OSP Security Policy Violation

Security policy (SP) violation is defined as one of the factors that could result in a successful online banking attack. An employee may cause an internal security incident and expose customers' information if violating the OSP's security policies while there are weak access controls and logging mechanisms. This also could lead to unauthorized access to the OSP's servers.

In the digital world, improper definition of a web application's SP or violations to SPs could result in an attacker being able to acquire administrative privileges by attacking an employee's machine. This usually happens when an employee, who has administrative privileges to access the OSP's servers, is accessing the OSP local network while, at the same time, is connected to other public web services like e-mail, chatting, and social networking sites from the same machine. The computer here is the weakest link because personal computers are usually prone to attacks like viruses, worms, Trojans, and other common

malware (see Figure 2.4). A good security policy would strictly disallow employees to connect one machine to the local network and to the Internet at the same time.

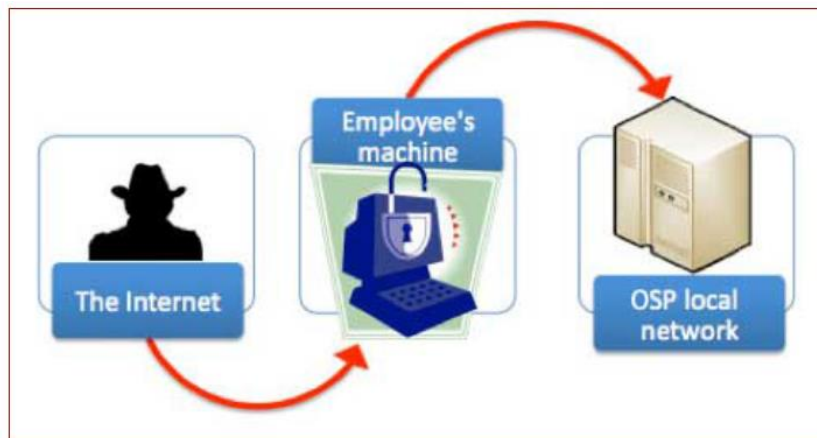


Figure 2.4: Security Policy Violation

2.4.2. Attacks on Communication Channels (CC)

This type of attack focuses on communication channels between the EU and OSPs. It could be limited to a local area network LAN (e.g., home or office networks) but could have a more far-reaching effect if an attacker is able to attack wide area networks (WAN) (e.g., telecommunication companies that provide Internet services to others). This section discusses three common attacks targeting CC: sniffing, man-in-the-middle (MITM), and session hijacking.

2.4.2.1 Sniffing

Sniffing is a type of attack that compromises the communication channel between the end user and the OSP. The attacker uses sniffing to listen to and interpret the data exchanged between the parties, and therefore, is able to capture factors sent by the user for authentication and authorization. This kind of attacks is passive and does not alter the data exchanged between the communicating parties.

2.4.2.2. Man-in-the-middle attacks (MITM)

This type of attack allows an attacker to intercept the data exchanged between the EU and the OSP. Unlike a sniffing attack, man-in-the-middle is a real-time attack and has the ability to alter captured packets and to capture sensitive information about other websites directly from the user's machine (see Figure 2.5).

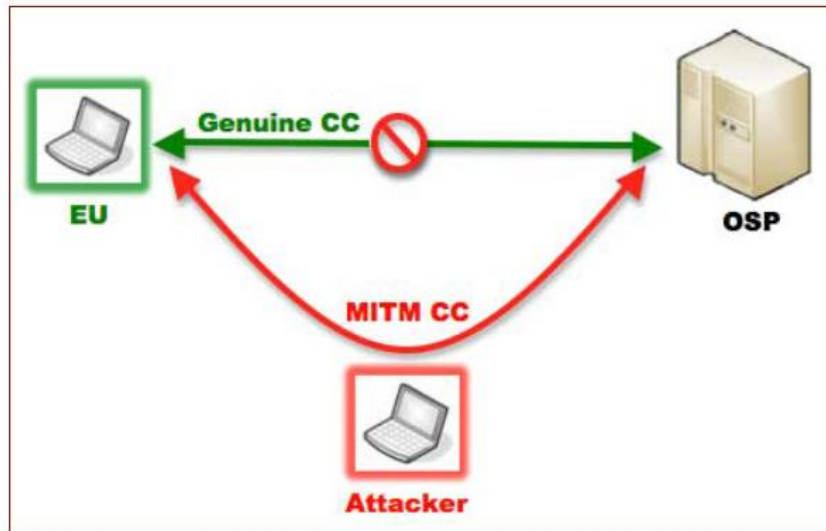


Figure 2.5: Man-in-the-Middle (MITM) Attack

The success or failure of MITM attacks is not based on bugs or un-patched software residing on the EU's machine nor does it depend on what users are browsing at the time when the attack is launched. It is solely a matter of whether the network the user is connected to is secured and trusted or not. Public networks (especially those which provide a Wifi connection feature) are always unsafe networks, no matter what website the user is intending to visit.

2.4.2.3. Session hijacking

Session hijacking is usually a result of other attacks like sniffing, phishing and pharming, and MITM attacks; it utilizes the user's connection session ID to spoof the user's identity.

2.4.3. Attacks on End Users (EU)

Users remain the weakest link in security. Online businesses' current attention is focused on the advances of attacks targeting OSPs and CCs while neglecting the end users who are the only element that cannot be technically controlled.

2.4.3.1. User surveillance

User surveillance is the use of hardware devices to monitor or record users' input to computers or teller machines (ATMs). It is electronic, over-shoulder surfing. This attack can capture user passwords/PINs used in the authentication process.

2.4.3.2. Token/notes theft

Token theft is another type of attack where users' tokens, like ATM bank cards, smart cards, mobile phones, OTP calculators, and other authentication tokens, are stolen. Although some of these tokens will not fully authenticate the attacker unless another form of authentication (e.g., PIN for ATM cards) is used, others do not need further authentication to be of benefit to the attacker. Examples of the latter the older versions of ATM cards, which are still used by some banks in different countries, that allow swiping the card into a card reader without the need to verify further by PIN number.

2.4.3.3. Malware infection

Malware could be a virus, a worm, a mobile code, a backdoor, a Trojan, or a rootkit. All have the ability to capture authentication factors once they are installed in a victim's machine.

2.4.3.4. Social engineering attacks

Social engineering attacks usually aim at stealing authentication factors by fooling the access credential holders. This type of attacks takes two forms: technical and nontechnical. The credential holders may be the customers who are the account holders or even the support help desk people who have administrative privileges to access and reset customer credentials. Non-technical social engineering attacks aim at deceiving users by means of convincing and trust building.

2.4.3.5. Phishing

Phishing is an example of technical, social engineering where the attacker designs and hosts a fake page or website, which has the same look and feel of a legitimate website. Then the attacker invites people to submit log-in credentials using e-mails or instant messaging (IM) that claim to be from a legitimate source but contain links to the fake spoofed page or website.

2.4.3.6. Pharming

Pharming is yet another social engineering attack that targets end-users. Pharming and phishing implement the same techniques to capture end-users' access credentials. However,

they use different strategies to complete this task. Unlike phishing, pharming attacks first compromise the user's machine to alter the host's file before the user is deceived and taken to a fake website. The host's file is a file residing in personal computers and used to speed up domain name resolution. When a user tries to access a domain name, if that domain name is not defined in the host's file, the machine will try to contact a domain name server (DNS) to resolve the IP address associated with the domain name. If it is defined in the local machine host's file, then there is no need to contact a DNS server.

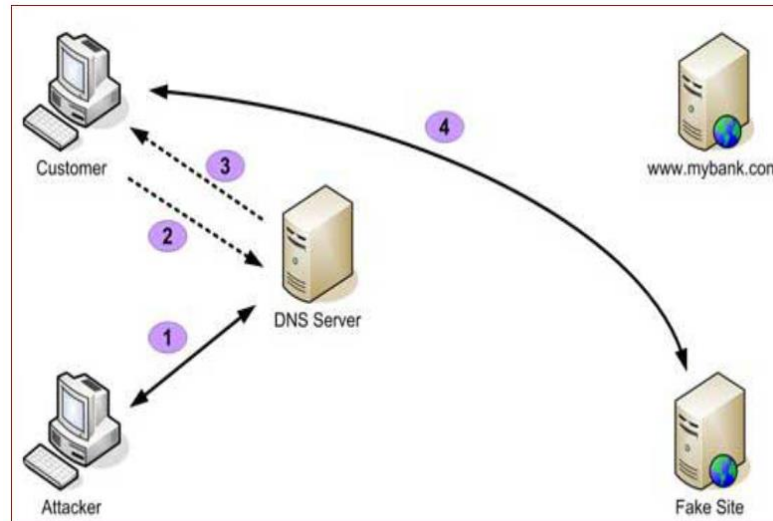


Figure 2.6: DNS Spoofing Attack

2.4.3.7. Clickjacking

Clickjacking, also known as user-interface (UI) redressing, is an attack technique based on HTML codes being used to hide a layer on top of the displayed contents to perform unexpected actions after the user clicks on it. Attacker can send an e-mail to a victim with an embedded video clip. The video clip has a play button, which, if clicked, installs malicious software into the user's machine. A clickjacking attack has the ability to allow an attacker to completely control the victim's desktop; thus, it hijacks the victim's active sessions or captures the authentication factors exchanged with other sites.

2.4.3.8. Man-in-the-browser attacks (MITB)

A man-in-the-browser attack is one of the recently developed attacks that target users' machines (specifically users' browser software). It is a malware type of attack that installs itself in the user browser and has the ability to intercept and modify transmitted details before they are sent out to the OSP (see Figure 2.7). It also intercepts replied details from the OSP and is able to modify them before they are displayed in the user's browser. All of these

alterations are performed in real-time and the user will find it difficult to identify the changes carried out by the MITB. [5]

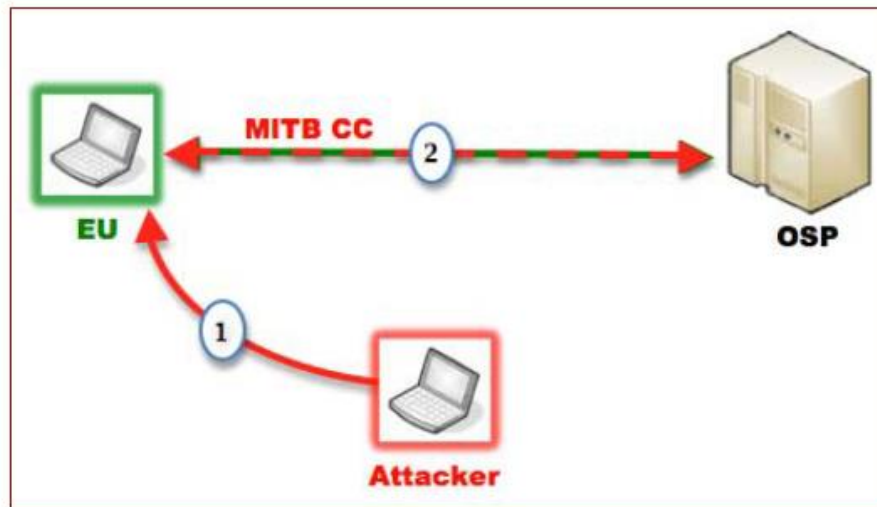


Figure 2.7: Man-in-the-Browser (MITB) Attack

2.5. General Security Attitudes for Financial Transactions

Results of a study conducted in 2008 [6] to assess the attitude towards conducting financial activities over the Internet is shown in Figure 2.8. Participants of the study were more concerned about accessing their on-line financial accounts compared to their email accounts. Participants' indicated that their level of concern was highly dependent on the computer that they need to use for accessing their accounts, particularly when accessing their financial accounts. However, they indicated that their level of concern was not as dependent on the Internet connection that they use (e.g., wireless or wired), or the location (e.g., school or internet cafe) where they access their information. As for their perceived level of safety for using different computers for financial transactions.

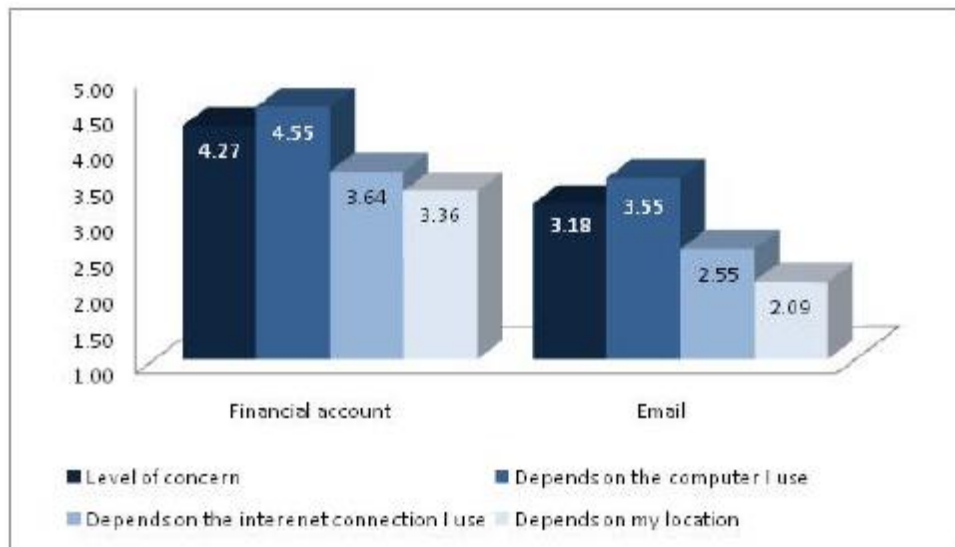


Figure 2.8: Showing Level of Concern about Financial Transactions Security

Another interesting survey was set out to find how trends in Internet security and data security, such as phishing, pharming, and data breaches, have affected consumer's perceptions and behaviors with internet banking. The study revealed that over one-fifth of all online consumers felt extremely threatened by online fraud. Two-thirds of the respondents stated they were nervous that someone would fraudulently access their online accounts, as shown in Figure 2.9. [7]

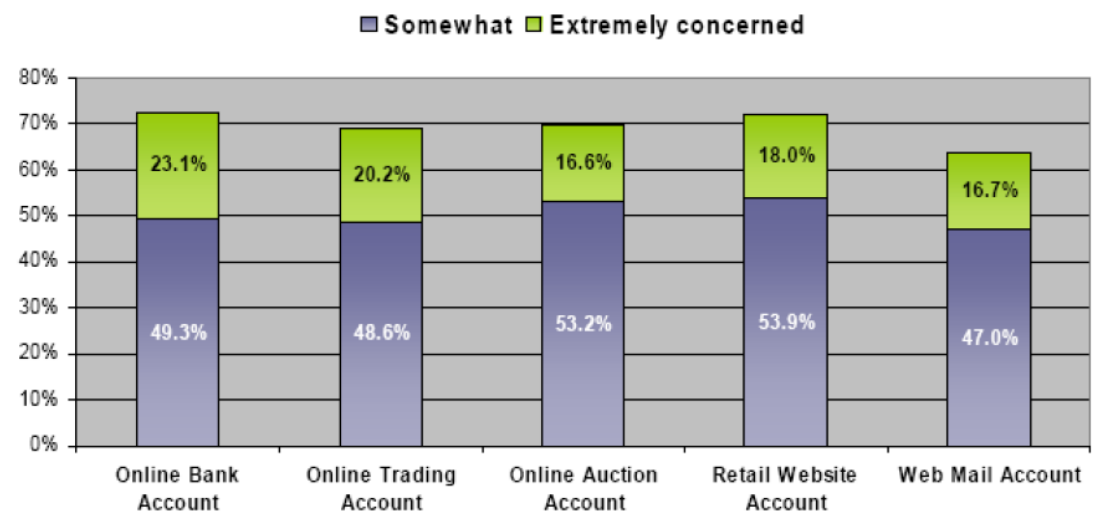


Figure 2.9: Concern for Fraudulent Access of an Account

The results prove to be very alarming for financial institutions, and further stress the importance of applying reliable security mechanisms.

AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT

In recent years, we have witnessed the increase of online-banking abuses. Since internet banking has been widely used, malicious and criminal users have become interested in it. Especially organized criminal attempts are on the rise. Consequently, more sophisticated attacks on internet banking have come up. Most recent trends go towards complex phishing (password fishing) attacks. These types of attacks are not pure technical attacks; they exploit on one hand psychological and sociological properties of users and on the other hand technical flaws and weaknesses.

As online transactions require new authentication methods, banks are trying to introduce new approaches in order to prevent attacks being successful and to increase security. The trend goes towards multiple-factor-authentication (mainly two-factor authentication). In fact most banks employ two-factor authentication yet in different ways. Besides usual username/password (or similar) approaches, additional tokens are applied for authentication in order to make internet banking more secure.

The main concern is that the continuous use of a security technology that does not improve security but makes applications harder to use for the customer. For example, the iTAN security measure does not raise the security level – but only bluffs security. On the other hand alternative approaches, which could raise security for users are not employed (or rarely employed). Based on those findings it is strongly recommends not to apply unnecessarily complex or cumbersome security technologies. Instead a cost-benefit-analysis should be applied to security technologies, which would asses how effective the protection is and what are the burdens for all the involved parties, including the bank's customers. [8]

3.1. Typical Authentication Process

This section provides a detailed description of the steps involved in the Internet bank authentication process (Figure 3.1):

1. The user visits a service provider's website and clicks on the authentication link.
2. The website shows authentication options and the user chooses his bank by clicking on the corresponding link.
3. The service provider generates an authentication request and redirects the user's browser with the request to the chosen Internet bank website.

4. The user authenticates to his bank by the authentication credentials issued by the bank.
5. The bank asks for permission to send the identification information of the user to the service provider.
6. After the user has agreed, the bank generates a digitally signed authentication token that contains the user's identifiable information, and redirects the user's browser with the token to the service provider.
7. The service provider verifies the token and continues with the authorization process.

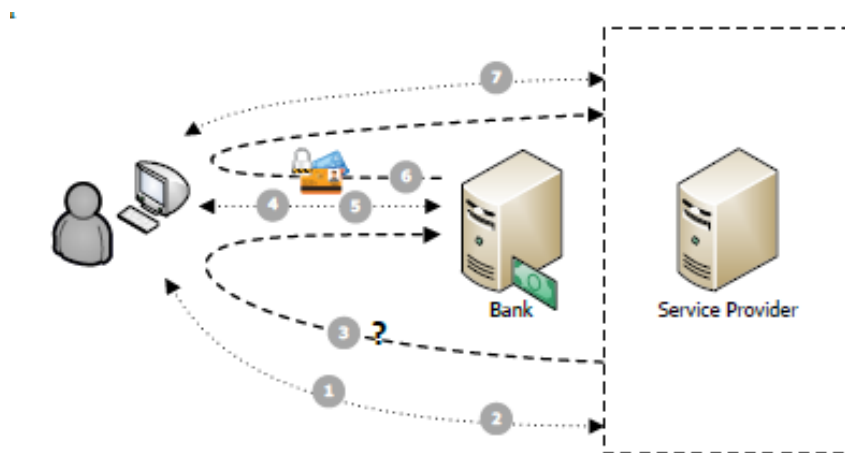


Figure 3.1: Internet Bank Authentication Process

The authentication request generated by a service provider must contain the service provider's identifier and, optionally, a specific return URL to which the user should be redirected after a successful authentication to the Internet bank.

In order to redirect the user's browser with an authentication message to the bank and from the bank to the service provider, a non-malicious type of cross-site request forgery is used. Usually a hidden HTTP POST form with the required message parameters is generated and automatically submitted with the help of JavaScript. It is possible that the service provider receives an authentication token without previously sending an authentication request message. This happens in case the user has initiated an authentication request from the bank's Internet bank e-services page. [9]

3.2. Authentication Classes

The verification process is usually based on authentication factors like facts, characteristics, behaviours, or knowledge known only to both the claimant and the verifier. Based on these authentication factors, the researchers have classified authentication in information technology into three classes: knowledge-based (KBA), token-based (TBA), and biometrics based (BBA). This section discusses these three classes and the possible implementation strengths and weaknesses of each in detail [5].

3.2.1. Knowledge-based Authentication (KBA)

KBA is also called *something the user knows* and it refers to the method of verifying a user's identity by matching one or more pieces of "secret" information supplied by an individual (claimant) against information sources associated with the claimant. KBA is the most common authentication approach used in most distributed systems today. This is due to many factors including simple implementation requirements, low implementation and administration costs, and a high level of user acceptance. A fixed password as an authentication factor is the most widely used KBA mechanism; it acts as the first line of defence against unauthorized access. After the user enters a secure password. The system will then consult a database or a data file to locate a matching record. Sometimes passwords are encrypted in the database so the comparison process is only done after the entered password is encrypted using the same encryption algorithms.

Despite the fact that passwords are the most commonly used KBA, it is clear that they still have several weaknesses and are vulnerable to different attacks. In order to overcome these weaknesses, some organizations have made use of system generated passwords. This could be counter-productive as system generated passwords tend to be very complex, and therefore, hard to remember. Consequently, users might write these passwords down and degrade the overall security of the system. The same goes for organizations that set password policies that include rules requiring user defined passwords to be very complex (i.e., force the use of special characters, combination of small and capital letters, and numbers).

One of the most common security mechanisms –especially in financial firms–applied to password authentication is to restrict the allowed number of invalid retries. Another common mechanism is to force the user to change the password regularly.

Making passwords complex, and therefore, hard to guess does not prevent other types of attacks like Trojans and sniffing. Even a strong password can easily be captured if a key-logger is used.

3.2.2. Token-based Authentication (TBA)

Sometimes referred to as *something you have (hold)*, is an authentication class based on tokens possessed by the user. The authentication principle does not rely on user's memory but rather on the ability of the user to prove the ownership of a token.

Several technologies have been used for authentication based on tokens. These include *smart cards and hardware token*.

The smart cards (see Figure 3.2), also known as challenge/response cards, are cards with a built-in chip used as memory and/or as a microprocessor. They are capable of performing computational algorithms and are able to store passwords and certificates. In computer systems, smart cards are used to allow single sign-ons and as an encryption factor to encrypt the file system. In financial firms, smart cards are used as ATM cards, credit/debit cards, fuel cards, SIM cards, and electronic wallets. In terms of security, smart cards use public key infrastructure (PKI) where the private key is stored in the card and cannot be copied. Usually it utilizes a two-factor authentication protocol where the token itself is considered one factor and a PIN the other. It limits the number of invalid trials before the card becomes inactive. Nevertheless, as for other token-based authentication, smart cards are prone to theft, and therefore, can be compromised, especially if the PIN number is written down on the card itself or is captured by covert user surveillance, such as over-shoulder sniffing or surveillance spy cameras. It has been estimated that around 25% of ATM card owners write down their PIN numbers on their card.



Figure 3.2: Smart Card

Hardware tokens also exist include USB drives, key fobs, and one-time pin (OTP) calculators (see Figure 3.3). Overall, token-based authentication offers better security than the traditional knowledge-based authentication and protects online users from guessing, interception, social engineering, and brute-force attacks. However, the tokens used to authenticate users can be shared or duplicated. Token-based authentication is also more expensive to deploy and maintain than knowledge-based authentication, especially when implemented on a large-scale.



Figure 3.3: Different Hardware Token Types Used to Generate One-Time Pin

3.2.3. Biometric-based Authentication (BBA)

Biometric authentication refers to the use of *physiological* and *behavioral* biometrics to authenticate users. This type of authentication relies on matching patterns of user characteristics or behaviors that are unique and distinguished [42] and assumes that similarities of these characteristics or behaviors cannot be found in two or more users.

Biometric authentication overcomes the drawbacks of other authentication classes but it has its own. Not all people are willing to put part of their body in a machine and some are disabled (e.g., lost fingers or eyes).

Biometric authentication's underlying technology is even more expensive than authentication technology involving tokens due to the high tech infrastructure required to process authentication data, especially if implemented on a large scale. Exact matches in biometrics authentication cannot be achieved due to the noise usually associated with the biometrics sensors such as sensing device, humidity and biometric position.

Avery important fact is that despite the high security offered by biometrics, they are not impossible to break.

Table 3.1 presents a summary of different authentication classes covered in the literature along with some examples currently implemented in the market.

Table 3.1: Summary Table of Different Authentication Classes

Class	Example	Advantage	Disadvantage
Knowledge-based (KBA)	-Secret questions -User ID and password -PIN	-High user acceptance -Easy to implement and administer -Cheap to deploy and maintain	-Can be shared -Users tend to re-use -Subject to guessing and reply attack -Prone to eavesdropping -Can be forgotten
Token-based (TBA)	-Magnetic stripe cards -Contactless cards -Smart cards -Badges -USB drives -Mobile software -Keys	-Ease of use and management -Cheap to implement -Better accountability as tokens are tangible -Matured and Widespread -High user acceptance	-Can be shared -Can be duplicated -Susceptible to loss and Damage -Can be stolen and reused -Requires hardware to replace -Limited lifetime
Biometrics based (BBA)	-Fingerprint -Face Iris -Voice print	-Difficult to share or duplicate -Repudiation unlikely -Forging difficult	-Expensive on wide scale -Availability issues

		-Cannot be lost or stolen	-Low user-acceptance -Accuracy issues -Reliability issues under abnormal conditions Patterns can be captured and replayed
--	--	---------------------------	--

3.3. Implementation Mechanisms

The previous section reviewed and discussed different authentication classes proposed in the literature. Many arguments, however, also exist in the literature and in industry about how these classes should be implemented in real applications. This section discusses different authentication mechanisms based on the classes covered by the previous section. These mechanisms are *single-factor*, *multi-factor*, and *multi-channel* authentication mechanisms [5].

3.3.1. Single-factor Authentication

This is the most basic and widely implemented authentication mechanism in information technology. Single-factor, in terms of security, is the weakest authentication mechanism among all other mechanisms (see Figure 3.4).

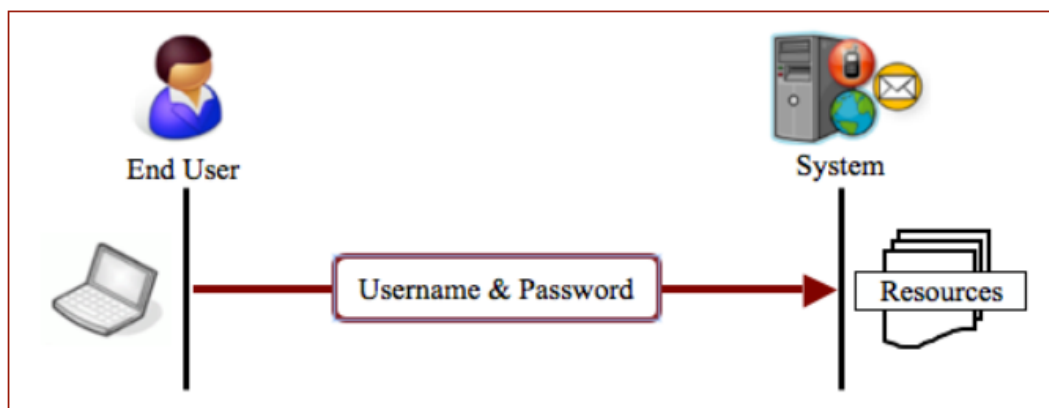


Figure 3.4: Single-Factor Authentication Mechanism

3.3.2. Multi-factor Authentication

It is the common mechanism adopted by financial institutions. It is implemented by adding extra authentication factors to the process of authenticating a user into a system (see Figure 3.5).

In terms of security, multi-factor authentication offers better protection against several attacks such as guessing, brute-force, and phishing. However, the one channel used in this mechanism is the weakest part because, if the channel is compromised, all factors exchanged between the end-user and the system can be captured accordingly.

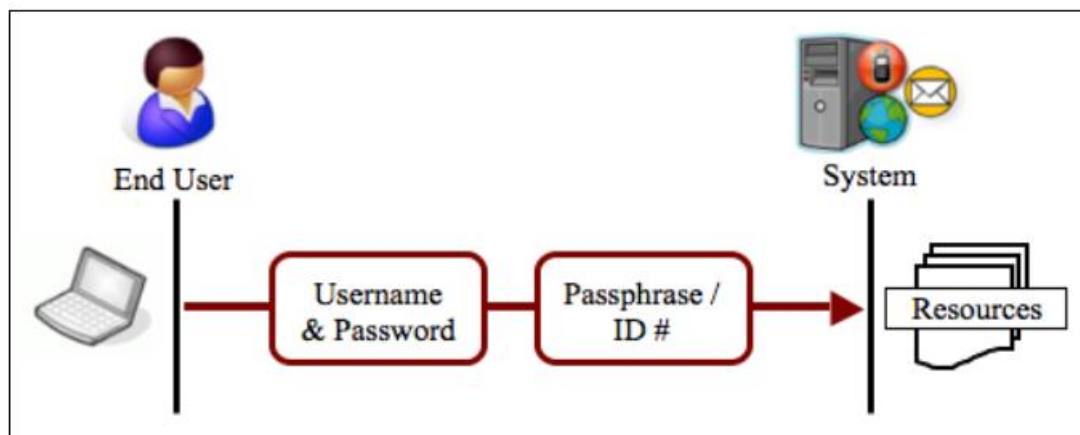


Figure 3.5: Multi-Factor Authentication Mechanism

3.3.3. Multi-channel Authentication

Although the multifactor authentication mechanism has improved overall security, it has not eliminated the fear of the kinds of attacks that could compromise all security levels. Figure 3.6 explains the mechanism.

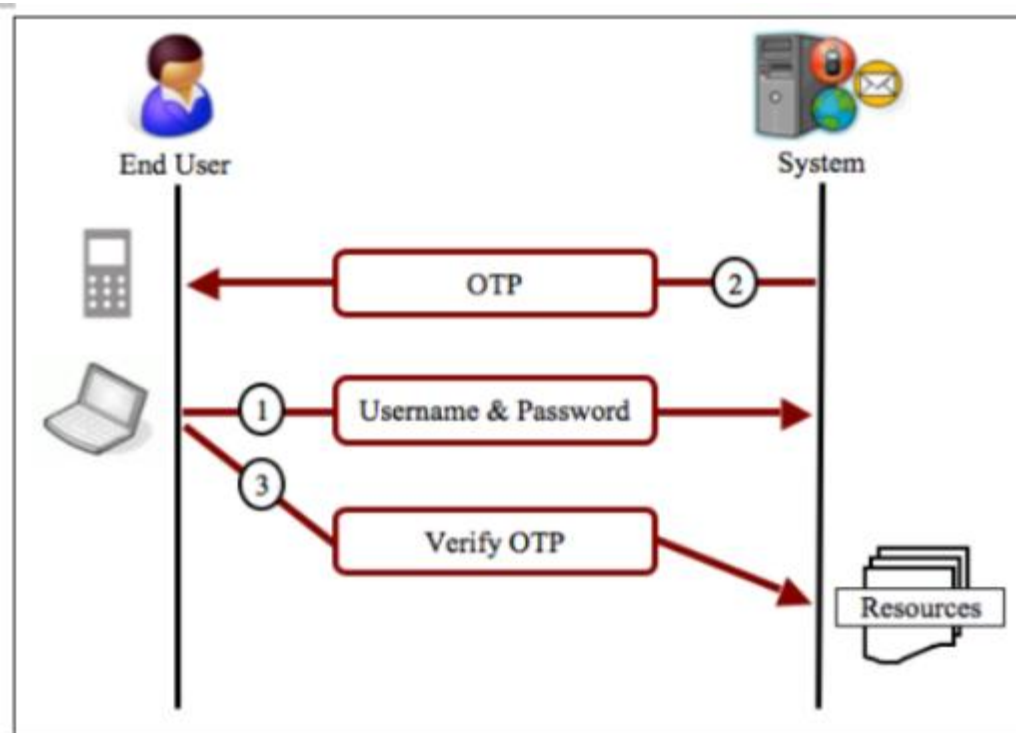


Figure 3.6: Multi-Channel Authentication Mechanism

Some organizations, especially financial firms, have improved the way multilevel authentication is implemented in online banking by integrating the multi-channel authentication (MCA) approach. MCA uses independent channels (e.g., web channel combined with mobile network channel), having the most commonly used channels for authentication along with the Internet channel are the telephone and cellular networks. For instance, the primary authentication factor is delivered using the web channel while the secondary authentication factor is delivered to the customer via an SMS using the mobile network infrastructure.

There are many commercial products and services, such as Identrica, SAINTlogin and Lloyds TSB, which offer multi-channel authentication services using telephone and mobile networks. Identrica requests the user to enter the access login details along with the mobile number into a login page. Then, to complete the login process, the user has to call a given number of the company. The company's system does not answer the call but checks the caller number to verify if it matches the customer's phone number who just submitted login credentials. If it matches, the user is allowed full access to the system.

MCA is currently offered by different commercial applications in a number of different ways. It is vital for any business to carry out a risk analysis and verify the need for MCA before implementing it.

3.4. Authentication to an Internet Bank

In this section we discuss in more detail the implementation approach of the most common authentication mechanism used by banks- being the research main focus, the two-factor authentication. As previously discussed another mechanisms are used by banks to further strengthen security (namely, multi-channel authentication) in combination with the two-factor, this section will cover the combined approach elements and implementation [10].

3.4.1. Two-Factor Authentication Methods

Whilst it is useful to try to counter specific attacks (and as part of a layered security strategy, we would always recommend this), the only long-term, strategic solution is to move away from the current dependence on static credentials.

Traditionally, all authentication mechanisms can be placed into one of the following three categories:

- ✓ Something you **know**—a secret, such as a password.
- ✓ Something you **are**—a biometric, such as a fingerprint.
- ✓ Something you **have**—a device or object or some kind, such as a credit card.
- ✓

With this approach, it can readily be seen that the problems with phishing arise from an overreliance on the first category. Strong authentication can be achieved by employing two different authentication credentials in parallel, from *different* categories. This is known as *Two-Factor Authentication (2FA)*.

For reasons of cost, complexity, reliability and privacy, biometrics are not widely used in banking. There are however a wide variety of low-cost, dependable security devices available.

Typically, such devices generate and display a *One-Time Password (or OTP)*. As the name suggests, an OTP is valid for a single use only, and many are also time-limited. Rather than being static, OTPs are *dynamic*—new OTPs can be generated on demand, from an inexhaustible sequence that is unique to each device.

The OTP is copied from the device to the web terminal by the customer. To the bank, knowledge of a valid OTP demonstrates proof of possession of the device, which when coupled with a traditional static password can offer an extremely effective defence against on-line attacks.

Any bank considering deploying 2FA must choose between a wide range of possible authentication devices. The following list, whilst not exhaustive, gives a representative sample:

3.4.1.1 EMV Card and Reader

MasterCard has devised a scheme based on existing retail banking smart cards and PINs. Dubbed the Chip Authentication Program (CAP), it has also been adopted by Visa, under the Dynamic Passcode Authentication (DPA) banner. The customer is supplied with a small, hand-held card reader, into which their existing EMV ‘Chip and PIN’ card is inserted. On entering the card PIN, the chip on the card is used to generate an OTP, which is displayed on the reader’s screen. Additional functions on the reader also support transaction authentication. The advantages include a high security, whilst by leveraging existing cards and issuance processes deployment and management costs are reduced. However, the user experience, whilst familiar, is more complicated than with other tokens.

3.4.1.2 Hardware & Software OTP Tokens

Many vendors offer OTP-generating tokens. They are available in a wide range of shapes and sizes, and many offer custom branding options. The simplest tokens are suitable for user authentication only. More advanced tokens incorporate a keyboard, making them suitable for transaction authentication. Most vendors employ proprietary algorithms to generate the OTPs.

3.4.1.3. Hardware-based PKI Tokens

A PKI system employs a *private key*, used to make *digital signatures* that are validated using a *public key*. The public key is held by the bank, and the private key by the customer. Chip-card or USB devices are commonly used to secure the customer’s private key. Since PKI tokens cannot generate OTPs, they must instead be connected to the customer’s PC.

Devices and keys are often managed using a *Certificate Authority*. They offer a high security level, although PC-based attacks may use the token illicitly. By including the ability to sign

transactions and other instructions, they offer great flexibility to banking applications. As a result, they are more common in business banking than consumer banking.

3.4.1.4. Software-Based PKI Tokens

Rather than storing PKI private keys in a physical device, they can also be stored on the customer's PC, protected by software. By eliminating the device, such systems offer significant cost savings in distribution and maintenance.

However, the software-based signing key may be vulnerable to PC-based attacks, and since the key is installed on a particular PC, customer mobility is reduced.

3.4.1.5. SMS-based OTPs

An appealing alternative to deploying tokens is to use something the customer already has—their mobile phone. In this case, the bank generates the OTP and sends it to the customer as an SMS message. The customer returns the OTP to the bank through their web browser. Naturally, this approach relies on the bank maintaining current details of the customer's telephone number and the customer being able to receive messages at the particular moment of logon.

Additionally, a transaction summary may be included in the SMS. This enables the user to detect fraudulently modified transactions.

3.4.1.6. TAN Lists

TAN (Transaction Authentication Number) lists are paper-based lists of one-time passwords. They are securely generated by the bank and issued to each customer.

The customer provides an OTP every time she logs on or submits a transaction. The OTPs are either used in sequence, or the bank requests a specific OTP using an index.

Whilst offering a lower security level, this low technology approach offers a combination of simplicity, reliability and low cost.

3.4.1.7. Matrix Cards

Also called grid card, this is a random grid of numbers or letters typically printed on a credit-card sized piece of plastic issued by the bank. The customer is prompted to supply the

contents of 2 or 3 cells during logon or when submitting a transaction. For example, the prompt “A4, C7” would give the log-on response “5, 8” using the card shown.

With similar advantages to TAN lists, the card format is convenient and durable. Whilst re-use of cells make the security analysis less clear, it also allows for a more flexible expiry policy.

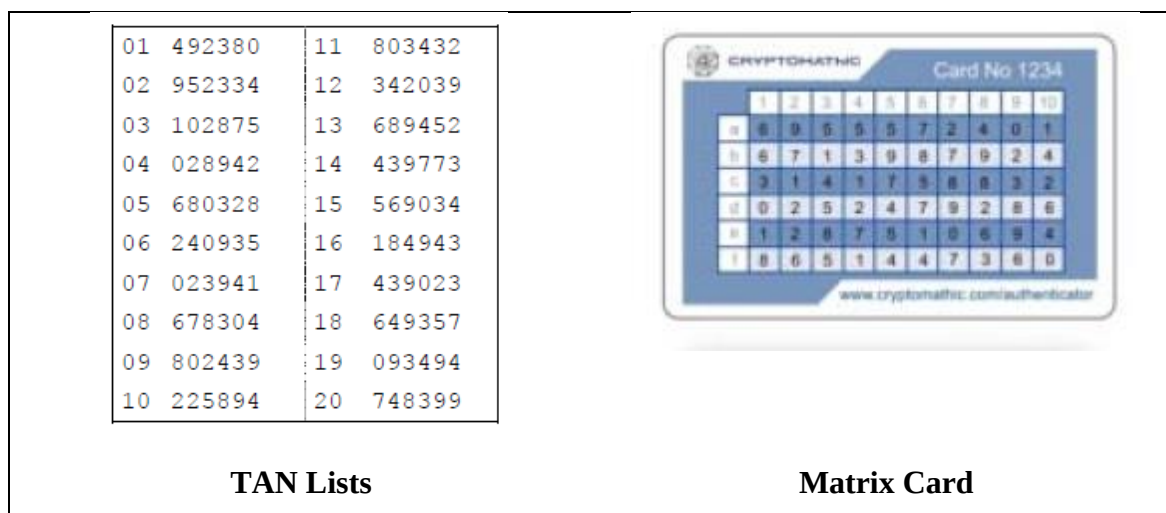


Figure 3.7: TAN and Matrix Card Methods

3.4.2. Two-Factor Authentication Using Mobile Phones

To authenticate users through a mobile phone requires certain components to be placed. Figure 3.8 shows the required components and the general architecture needed for the solutions described in this paper to work.

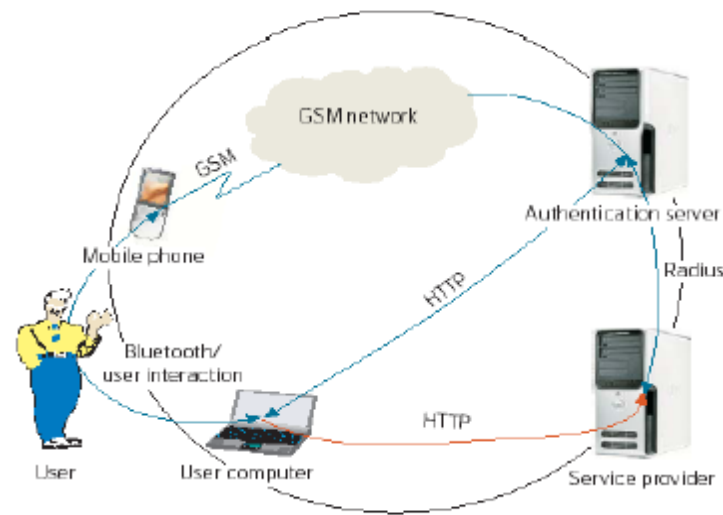


Figure 3.8: General Architecture of Mobile Authentication

The user must access to a computer connected to the internet and be in possession of a mobile phone with a working SIM card. If the computer and mobile phone are equipped with Bluetooth, higher usability can be obtained. Through the Internet browser on the computer the user can access web services provided by service providers. The service provider (SP) is connected to an Authentication Server (AS) that will handle the authentication on behalf of the SP. The AS is connected to the GSM network which enables it to communicate with the user's mobile phone and the operator's Authentication Center (AUC). The AS is composed of two parts, an authenticator and an AAA server. The authenticator communicates with the client and relays messages to the AAA server which handles the authentication.

When designing an authentication scheme which uses two separate devices that communicate over two different networks it is very important to ensure that it is the same user that controls both devices. This is done by ensuring that there is a "closed loop" going through all the components involved in the authentication as illustrated in Figure 3.8. The loop starts in the device requesting the service, the user's computer, goes through the network with SP and AS and then via mobile phone and back to the initial device, either by user interaction or Bluetooth.

One-Time Password is one of the simplest and most popular forms of two-factor authentication today. This solution builds on the same principle as the session ID check, that a user with a working phone is already authenticated through the GSM network. The difference is that the check is done by the server and therefore relieves the user from this

burden. The user starts the authentication procedure by entering his username. The session is redirected to the AS which creates an OTP based on the user's identity by a cryptographic hash function. The OTP is then sent to the user by SMS. When receiving the SMS the user types the OTP in the browser. The AS verifies that the OTP is correct and redirects the browser back to the service provider and the user is logged in. Figure 3.9 shows the message exchange of this solution. [11]

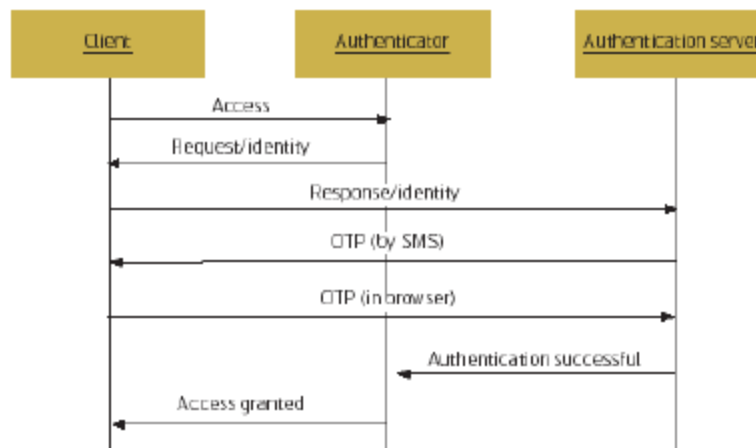


Figure 3.9: OTP Check

LIBYAN INTERNET BANKING EVALUATION

The Libyan authorities started to liberalize the national banking system in the mid-1990s, permitting the private ownership of banks. It is only since 2001, with the liberalization of foreign trade, that banks have experienced substantial changes in the banking system. Private sector clients no longer have to work through the large state-owned banks, and the commercial banks themselves are free to develop banking relationships abroad. They have been connected to the Society for World-wide Interbank Financial Telecommunication (SWIFT and Western Union system) since 2001 and no longer need to use the Libyan Arab Foreign Bank to make foreign payments and transfers .

However, competition between the five state-owned Libyan Public Commercial Banks has yet to emerge, and it is also expected that some privately-owned banks may enter the competition. Tight central controls have been in place for too long for immediate launch of innovative practices. However, the private sector banks are installing modern integrated banking systems and thus, are creating opportunities to attract large volumes of business from enterprises that want to use efficient payments systems.

As presented below in Figure 4.1 there are two types of banks under the control of the Central Bank of Libya: public and private sector banks. The state-controlled public banks in Libya consist of two major types: specialist and commercial banks.

Libyan public specialist banks (LPSBs) include: the saving and Real-Estate Investment Bank, the Development Bank, the Agriculture Bank, and the Libyan Arab Foreign Bank. Libyan public commercial banks (LPCBs) are: Eljumhuria Bank, Umma Bank, Sahara Bank, National Commercial Bank, and Elwahda Bank [12]. Libyan private banks consist of: Al-wafa Bank, Alejmaa Alarabi Bank, Mediterranean Bank, Aman Bank, the National banking corporation, United bank for Commerce and Investment, Assaray Trade and Investment Bank, North Africa Bank.

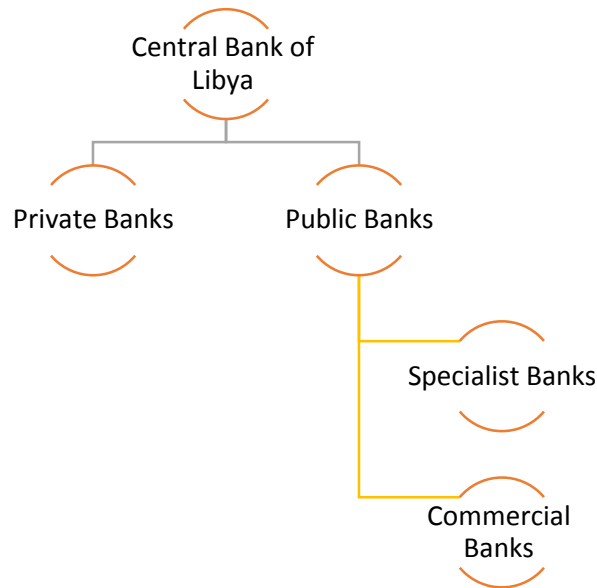


Fig 4.1: Libyan banking infrastructure

4.1. Libyan Banks and Internet Banking

In 2005, Bank of Commerce and Development (BCD) introduced the first Internet banking services in the country together with electronic magnetic cards such as Credit Card, VISA Credit Card, and VISA Electron Credit Card. Several years after, Aman Bank started to define itself as the first competitor being the second to initialize Internet banking. Although both the private banking sector and local banks are now free to establish and develop online banking technology, but among the all State-Owned Commercial Banks (SOCBs) only Eljumhuria Bank has recently joined the competition [13].

BCD again takes the lead by proving more convenience for its customers, by offering Mobile banking. This service sends SMS to order banking transactions and services, such as (balance, exchange rates). Soon competitors offered either simpler form of the service or even more advanced Mobile applications, which forms a good base to strengthen security as discussed later.

Table 4.1 provides a summary about banks offering Internet banking and/or Mobile services.

Table 4.1: Banks existing and potential Internet banking and related Mobile service

NO.	Commercial Bank Name	Internet Banking	Mobile	Mobile Service Remarks
Internet and Mobile Banking Service				
1	Eljumhuria Bank	YES	YES	Text only
2	BCD	YES	YES	Text only and Mobile application to be released soon
3	Aman Bank	YES	YES	Mobile application
Mobile Service Only				
4	United bank	NO	YES	Text only
5	National Commercial Bank	NO	YES	Text only
6	North Africa Bank	NO	YES	Mobile application
7	Elwahda Bank	NO	YES	Text only
Potential				
8	Sahara Bank	NO	NO	--
9	Al-wafa Bank	NO	NO	--
10	Alejmaa Alarabi Bank	NO	NO	--
11	Mediterranean Bank	NO	NO	--
12	National Banking Corporation	NO	NO	--
13	Assaray Trade and Investment Bank	NO	NO	--

As discussed in previous section 28% of the operating banks have absolutely no presentation on the Web. Analyzing the remaining 72%, only few provide Internet banking, others are trying to emerge and the majority can be considered a potential for both. Figure.4.2 below provides the exact percentage.

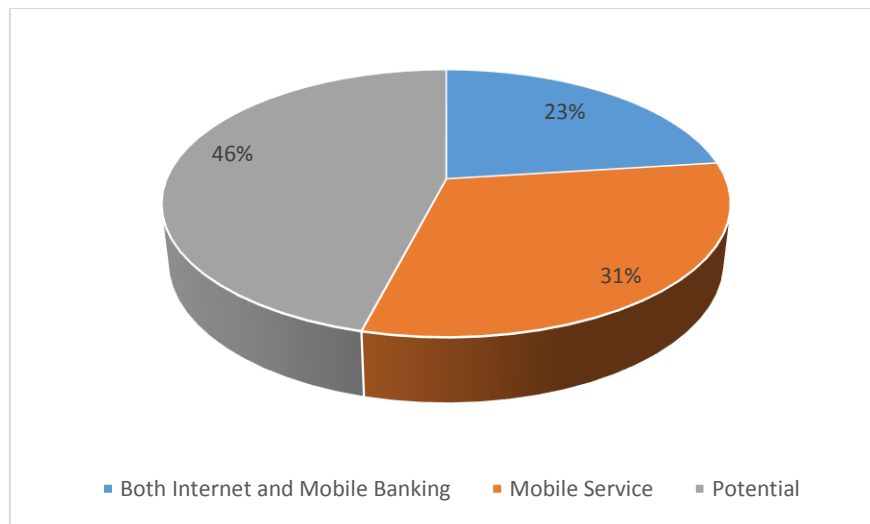


Fig 4.2: Internet and Mobile banking services in Libyan banks

4.2. Internet Banking Security and Vulnerability Scanners

Security is a very crucial element in Libyan banking as a whole, and it is absolutely essential for online banking, especially in the current situation in the country at a transitional point of government. This may require the imposing of more security arrangements, with the involvement of international high security companies in addition to the existing Internet banking security systems.

Although Libyan Internet banking services appear advanced in general and in particular in a developing country like Libya, it is still uncertain whether they are adequately protected by compatible online security. The level of customers' privacy is also unknown and needs to be investigated. In this research we will put web application security in general and Internet banking authentication security in particular under analysis using vulnerability scanners as a tool.

4.2.1. Vulnerability Scanners

A vulnerability scanner is software application that assesses security vulnerabilities in networks or host systems and produces a set of scan results. However, because both administrators and attackers can use the same tool for fixing or exploiting a system, administrators need to conduct a scan and fix problems before an attacker can do the same scan and exploit any vulnerabilities found. This article provides a general overview of vulnerability scanners.

A vulnerability scanner can assess a variety of vulnerabilities across information systems (including computers, network systems, operating systems, and software applications) that

may have originated from a vendor, system administration activities, or general day-to-day user activities:

1. Vendor-originated: this includes software bugs, missing operating system patches, vulnerable services, insecure default configurations, and web application vulnerabilities.
2. System administration-originated: this includes incorrect or unauthorized system configuration changes, lack of password protection policies, and so on.
3. User-originated: this includes sharing directories to unauthorized parties, failure to run virus scanning software, and malicious activities, such as deliberately introducing system backdoors.

In general, a vulnerability scanner is made up of four main modules, namely, a Scan Engine, a Scan Database, a Report Module and a User Interface. Figure 4.3 shows the architecture of these components [14].

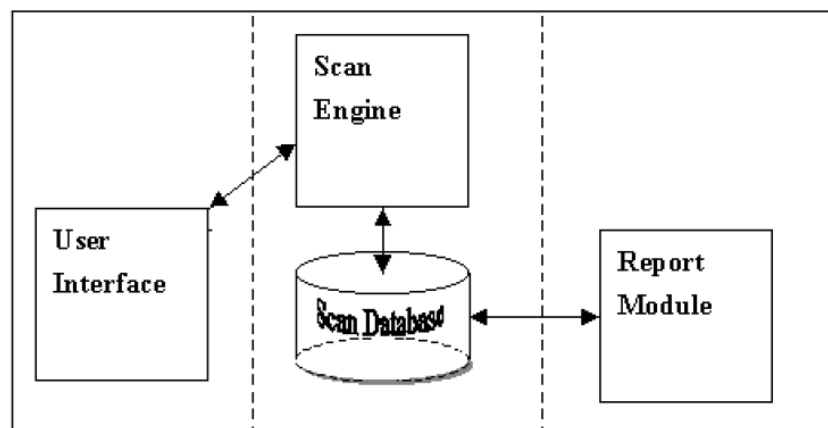


Fig 4.3: Components of a vulnerability scanner

1. The Scan Engine executes security checks according to its installed plug-ins, identifying system information and vulnerabilities. It can scan more than one host at a time and compares the results against known vulnerabilities.
2. The Scan Database stores vulnerability information, scan results, and other data used by scanner. The number of available plug-ins, and the updating frequency of plug-ins will vary depending on the corresponding vendor. Each plug-in might contain not only the test case itself, but also a vulnerability description, a Common Vulnerabilities and Exposures (CVE)2 identifier; and even fixing instructions for a

detected vulnerability. Scanners with an "auto-update" feature can download and install the latest set of plug-ins to the database automatically.

3. The Report Module provides different levels of reports on the scan results, such as detailed technical reports with suggested remedies for system administrators, summary reports for security managers, and high-level graph and trend reports for executives.
4. The User Interface allows the administrator to operate the scanner. It may be either a Graphical User Interface (GUI), or just a command line interface.

4.2.2. Benefits and Limitations of Vulnerability Scanners

Firstly, a vulnerability scanner allows early detection and handling of known security problems. By employing ongoing security assessments using vulnerability scanners, it is easy to identify security vulnerabilities that may be present in the network, from both the internal and external perspective.

Secondly, a new device or even a new system may be connected to the network without authorization. A vulnerability scanner can help identify rogue machines, which might endanger overall system and network security.

Thirdly, a vulnerability scanner helps to verify the inventory of all devices on the network. The inventory includes the device type, operating system version and patch level, hardware configurations and other relevant system information. This information is useful in security management and tracking.

The drawbacks of vulnerability scanners are: [14]

1. Snapshot only: a vulnerability scanner can only assess a "snapshot of time" in terms of a system or network's security status. Therefore, scanning needs to be conducted regularly, as new vulnerabilities can emerge, or system configuration changes can introduce new security holes.
2. Human judgement is needed: Vulnerability scanners can only report vulnerabilities according to the plug-ins installed in the scan database. They cannot determine whether the response is a false negative or a false positive¹. Human judgement is always needed in analysing the data after the scanning process.

3. Others: a vulnerability scanner is designed to discover known vulnerabilities only. It cannot identify other security threats, such as those related to physical, operational or procedural issues.

In addition, many vulnerability scanners rely on “plug-ins” to determine potential vulnerabilities. Plug-ins are part of the knowledge database (or scan database) of the vulnerabilities that the scanner is capable of detecting. These databases may be named differently (such as “Scanning Profile”) in different scanner products, but the term “plug-ins” will be used in this article. The finite number of plug-ins can be another drawback with vulnerability scanners. A scanner can only check for those vulnerabilities that it “knows”, by cross checking with the presence of its corresponding installed plug-in set. It cannot identify those vulnerabilities that don’t have a plug-in. Not all scanners need plug-ins. For example, port scanners do not need any plug-ins as they just scan a target range of ports.

4.2.3. Types of Vulnerability Scanners

Vulnerability scanners can be divided broadly into two groups: network-based scanners that run over the network, and host-based scanners that run on the target host itself.

a) Network-based scanners

A network-based scanner is usually installed on a single machine that scans a number of other hosts on the network. It helps detect critical vulnerabilities such as mis-configured firewalls, vulnerable web servers, risks associated with vendor-supplied software, and risks associated with network and systems administration. Different types of network-based scanners include:

1. Port Scanners that determine the list of open network ports in remote systems;
2. Web Server Scanners that assess the possible vulnerabilities (e.g. potentially dangerous files or CGIs) in remote web servers;
3. Web Application Scanners that assess the security aspects of web applications (such as cross site scripting and SQL injection) running on web servers. It should be noted that web application scanners cannot provide comprehensive security checks on every aspect of a target web application. Additional manual checking (such as whether a login account is locked after a number of invalid login attempts) might be needed in order to supplement the testing of web applications.

b) Host-based scanners

A host-based scanner is installed in the host to be scanned, and has direct access to low-level data, such as specific services and configuration details of the host's operating system. It can therefore provide insight into risky user activities such as using easily guessed passwords or even no password. It can also detect signs that an attacker has already compromised a system, including looking for suspicious file names, unexpected new system files or device files, and unexpected privileged programs. Host-based scanners can also perform baseline (or file system) checks. Network-based scanners cannot perform this level of security check because they do not have direct access to the file system on the target host.

This study scope is to evaluate Internet banking in its narrow definition being an electronic system that enables customers of a financial institution to conduct financial transactions on a website operated by the institution. Thereon, Web application scanners will be used as evaluation tools, and in the following sections more details are covered.

4.2.4. Web Vulnerability Scanners

Website security is today's most overlooked aspect of securing an enterprise and should be a priority in any organization. Increasingly, hackers are concentrating their efforts on web-based applications – shopping carts, forms, login pages, dynamic content, etc. Hackers already have a wide repertoire of attacks that they regularly launch against organizations including SQL Injection, Cross Site Scripting, Directory Traversal Attacks, Parameter Manipulation (e.g., URL, Cookie, HTTP headers, web forms), Authentication Attacks, Directory Enumeration and other exploits.

Web applications – shopping carts, forms, login pages, dynamic content, and other bespoke applications – are designed to allow your website visitors to retrieve and submit dynamic content including varying levels of personal and sensitive data. If these web applications are not secure, then your entire database of sensitive information is at serious risk. A Gartner Group study reveals that 75% of cyber-attacks are done at the web application level. [15]

Why are web applications vulnerable?

- Websites and web applications are easily available via the internet 24 hours a day, 7 days a week to customers, employees, suppliers and therefore also hackers.

- Firewalls and SSL provide no protection against web application hacking, simply because access to the website has to be made public.
- Web applications often have direct access to backend data such as customer databases.
- Most web applications are custom made and, therefore, involve a lesser degree of testing than off-the-shelf software. Consequently, custom applications are more susceptible to attack.
- Various high profile hacking attacks have proven that web application security remains the most critical. If your web applications are compromised, hackers will have complete access to your backend data even though your firewall is configured correctly and your operating system and applications are patched repeatedly.
- Network security defense provides no protection against web application attacks since these are launched on port 80 which has to remain open to allow regular operation of the business. It is therefore imperative that you regularly and consistently audit your web applications for exploitable vulnerabilities.

4.2.5. Common Web Vulnerability Scanners

Table 4.2 provide a listing of vulnerability scanning tools currently available in the market according to the Open Web Application Security Project (OWASP). [16]

Table 4.2: List of web vulnerability scanners

No.	Name	Owner	License	Platforms
Commercial/ Available Free with Limited Capability				
1	Acunetix WVS	Acunetix	Commercial / Free (Limited Capability)	Windows
2	Burp Suite	PortSwiger	Commercial / Free (Limited Capability)	Most platforms supported
3	Nexpose	Rapid7	Commercial / Free (Limited Capability)	Windows/Linux

4	Websecurify Suite	Websecurify	Commercial / Free (Limited Capability)	Windows, Linux, Macintosh
5	Contrast	Contrast Security	Commercial / Free (Limited Capability)	SaaS or On-Premises
Commercial				
6	AppScan	IBM	Commercial	Windows
7	BugBlast	Buguroo Offensive Security	Commercial	SaaS or On-Premises
8	GamaScan	GamaSec	Commercial	Windows
9	Hailstorm	Cenzic	Commercial	Windows
10	IndusGuard Web	Indusface	Commercial	SaaS
11	N-Stealth	N-Stalker	Commercial	Windows
12	Netsparker	MavitunaSecurity	Commercial	Windows
13	AppSpider	Rapid7	Commercial	Windows
14	ParosPro	MileSCAN	Commercial	Windows
15	Proxy.app	Websecurify	Commercial	Macintosh
16	Retina	BeyondTrust	Commercial	Windows
17	WebApp360	TripWire	Commercial	Windows
18	WebInspect	HP	Commercial	Windows
19	SOATest	Parasoft	Commercial	Windows / Linux / Solaris
20	Trustkeeper Scanner	Trustwave SpiderLabs	Commercial	SaaS
21	WebReaver	Websecurify	Commercial	Macintosh

Open Source				
22	Grendel-Scan	David Byrne	Open Source	Windows, Linux and Macintosh
23	Vega	Subgraph	Open Source	Windows, Linux and Macintosh
24	Wapiti	Informática Gesfor	Open Source	Windows, Unix/Linux and Macintosh
25	Wikto	Sensepost	Open Source	Windows
26	Xenotix XSS Exploit Framework	OWASP	Open Source	Windows
27	Zed Attack Proxy	OWASP	Open Source	Windows, Unix/Linux and Macintosh
28	Grabber	Romain Gaucher	Open Source	Python 2.4, BeautifulSoup and PyXML
29	Nikto	CIRT	Open Source	Unix/Linux
30	GoLismero	GoLismero Team	GPLv2.0	Windows, Linux and Macintosh
31	w3af	w3af.org	GPLv2.0	Linux and Mac
Cloud Based				
32	IKare	ITrust	Commercial	N/A
33	AVDS	Beyond Security	Commercial / Free (Limited Capability)	N/A
34	QualysGuard	Qualys	Commercial	N/A
35	Securus	Orvant, Inc	Commercial	N/A
36	Sentinel	WhiteHat Security	Commercial	N/A
37	WebScanService	German Web Security	Commercial	N/A

When researching vulnerability scanners, it is important to find out how they are rated for accuracy (the most important metric) as well as reliability, scalability and reporting. If accuracy is lacking, you will end up running two different scanners, hoping that one picks up vulnerabilities that the other misses. In this study, we are combing through three sets of scanning results for this propose.

Vulnerability scanners are either software-based or cloud-based, and here we are using both in order to achieve more accuracy, take advantage of their strengths, and also experience their limitations.

Software-Based Vulnerability Scanners are either commercial or open sourced. In order to expand our search one of each is used. One of the well-known and more highly rated commercial vulnerability scanners is Acunetix, and Vega is a good choice for a well-developed open source scanners.

Cloud-based are a newer type of vulnerability scanners which are delivered on-demand as Software as a Service (SaaS). Products such as Qualys Vulnerability Management provide continuous, hands-free monitoring of all computers and devices on all network segments.

An overview of each of the scanners that are used in this study is provided in the following three sections, as well as Table 4.3 that shows a summary and justification of choice.

4.2.5.1. Acunetix Web Vulnerability Scanner

Acunetix Web Vulnerability Scanner is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injection, Cross site scripting and other exploitable vulnerabilities. In general, Acunetix Web Vulnerability Scanner scans any website or web application that is accessible via a web browser and uses the HTTP/HTTPS protocol.

Acunetix Web Vulnerability Scanner offers a strong and unique solution for analyzing Off-the-shelf and custom web applications including those utilizing JavaScript, AJAX and Web 2.0 web applications. Acunetix has an advanced crawler that can find almost any file. This is important since what is not found cannot be checked.

Main scanner features are [15]:

1. Uses a technology called Acunetix AcuSensor to retrieve a listing of all the files present in the web application directory and add the files not found by the crawler to the crawler output. Such files usually are not discovered by the crawler as they are not accessible from the web server, or not linked through the website.
2. Provides details such as source code line number, stack trace or affected SQL query which lead to the vulnerability are listed. Recommendations on how to fix the vulnerability are also shown.
3. Various reports can be generated on completed scans, including Executive Summary report, Developer report and various compliance reports such as PCI or ISO 270001.

4.2.5.2. Qualys Web Vulnerability Scanner

Qualys Web Application Scanning (WAS) is a cloud service that provides automated crawling and testing of custom web applications to identify vulnerabilities including cross-site scripting (XSS) and SQL injection. The automated service enables regular testing that produces consistent results, reduces false positives, and easily scales to secure a large number of websites. Proactively scans websites for malware infections, sending alerts to website owners to help prevent black listing and brand reputation damage.

Built on the world's leading Cloud security and compliance platform, Qualys WAS frees you from the substantial cost, resource and deployment issues associated with traditional software products. Known for its fast deployment, ease of use, and unparalleled scalability (scan thousands of web applications), Qualys WAS is relied upon by leading companies around the world.

As part of the award-winning Qualys Cloud Platform, Qualys WAS helps you truly reduce risk by automatically finding the official and “unofficial” apps that may be hiding in your environment. Main scanner features are [17]:

- **Immediate deployment** — no hardware to set up, always up-to-date
- **Global scalability** — add more apps anytime, throughout the world
- **Multiple, unified solutions** — one console for WAS, WAF, VM and more
- **Centralized management** — apply policies consistently across apps
- **XML APIs** — publish data to other enterprise systems (e.g., SIEM)

4.2.5.3. Vega Web Vulnerability Scanner

Vega is a free and open source scanner and testing platform to test the security of web applications. Vega can help you find and validate SQL Injection, Cross-Site Scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities. It is written in Java, GUI based, and runs on Linux, OS X, and Windows. Vega can be extended using a powerful API in the language of the web: Javascript, and it was developed by Subgraph in Montreal.

Vega includes a website crawler powering its automated scanner. Vega can automatically log into websites when supplied with user credentials.

Main scanner features are [18]:

- **GUI-Baseb** — Vega has a well-designed graphical user-interface.
- **Multi-Platform** — Vega is written in Java and runs on Linux, OS X, and Windows.
- **Extensible** — Vega detection modules are written in Javascript. It is easy to create new attack modules using the rich API exposed by Vega.

Table 4.3: Selected web vulnerability scanners summary and justification of choice

Scanner	Scanner Base	Capability	Main Features
Acunetix	Software-based	Commercial / Free (Limited Capability)	• Detailed vulnerability description and solution • Variety of reports • Deep scan using both crawler and AcuSensor
Qualys	Cloud-based	Cloud/ (Limited Capability)	• Free substantial cost • Unparalleled scalability • Immediate deployment • Free version provides compliance reports • Free version includes vulnerability solution
Vega	Software-based	Open source	• GUI-based • Multi-platform • Extendable

4.3. Web Security Analysis

In order to answer the first research question and together with the information covered in previous sections of this chapter, the scope of this study is to cover the following in detail:

- ✓ Only three Libyan banks are currently offering Internet Banking. Namely, BCD, Aman and Eljumhuria Bank all their websites are scan targets.
- ✓ Severity levels have to be clearly defined.
- ✓ Causes of detected vulnerabilities, their impact, and recommended solutions if any will be sated.
- ✓ Three web vulnerability scanners will be used, and a comparison between obtained results will take place.

4.3.1. Vulnerability count and severity levels

One of the key components of the scan results is the list of all vulnerabilities found in the scan target during the scan. The alerts are categorized according to four severity levels as shown in Table 4.4 [15]:

Table 4.4: Severity Levels

Symbol	Severity Level	Description
	High Risk Alert Level 3	Vulnerabilities categorized as the most dangerous, which put the scan target at maximum risk for hacking and data theft.
	Medium Risk Alert Level 2	Vulnerabilities caused by server misconfiguration and site coding flaws, which facilitate server disruption and intrusion.
	Low Risk Alert Level 1	Vulnerabilities derived from lack of encryption of data traffic or directory path disclosures.
	Informational Alert	These are items which have been discovered during a scan and which are deemed to be of interest, e.g. the possible disclosure of an internal IP address or email address, or matching a search string found in the Google Hacking Database, or information on a service that has been discovered during the scan.

In order to start our analysis three scans against each of the three banks web application were conducted using our three selected web scanners. Appendix A shows all screen shots of the completed scans.

Conducting three web vulnerability scans on the three websites involves long waiting hours to get the scan results, due to the number of pages and lines checked and the fact that the internet speed in Libya is a hold back.

As a result, Table 4.5 shows the exact number of detected vulnerabilities under each of the alert categories as well as the total sum.

Table 4.5: Summary of conducted scans

Bank	Number of Detected Vulnerabilities					
	High	Medium	Low	Info	Total	Total without Info threats
Using Acunetix						
BCD	0	2	13	56	71	15
Eljumhuria	1	33	11	5	50	45
Aman	1	28	12	50	91	41
Using Qualys						
BCD	0	23	18	88	129	41
Eljumhuria	1	7	14	23	45	22
Aman	1	3	4	33	41	8
Using Vega						
BCD	0	3	0	106	109	3
Eljumhuria	19	18	3	69	109	40
Aman	10	1	9	89	109	20

Extracting from the Table 4.5, Figure 4.4 provides a comparison between the results obtained by each of the scanners with regard to the total number of vulnerabilities. From the figure, Acunetix defines Aman as the most vulnerable while Qualys defines it as the least. Vega believes that all three websites are same as vulnerable.

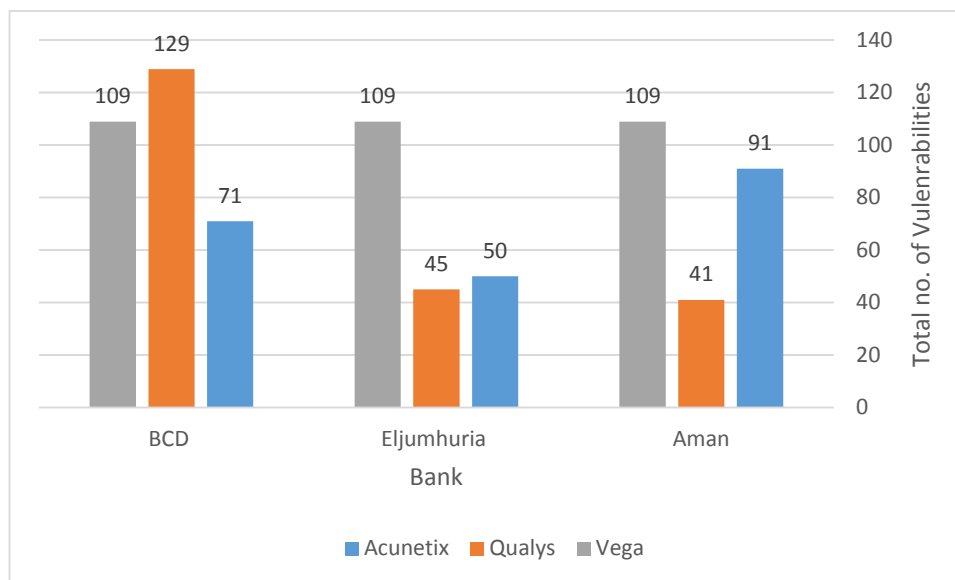


Fig 4.4: Comparison between total numbers of detected vulnerabilities

If we exclude information alerts, we obtain the results shown in Figure 4.5 where both Acunetix and Vega agree that the least vulnerable is BCD and the most is Eljumbhuria. Also both Acunetix and Vega give close results for the vulnerabilities detected, while Qualys in addition to the difference in the numbers detected it proves low when both Acunetix and Vega say high and vice versa.

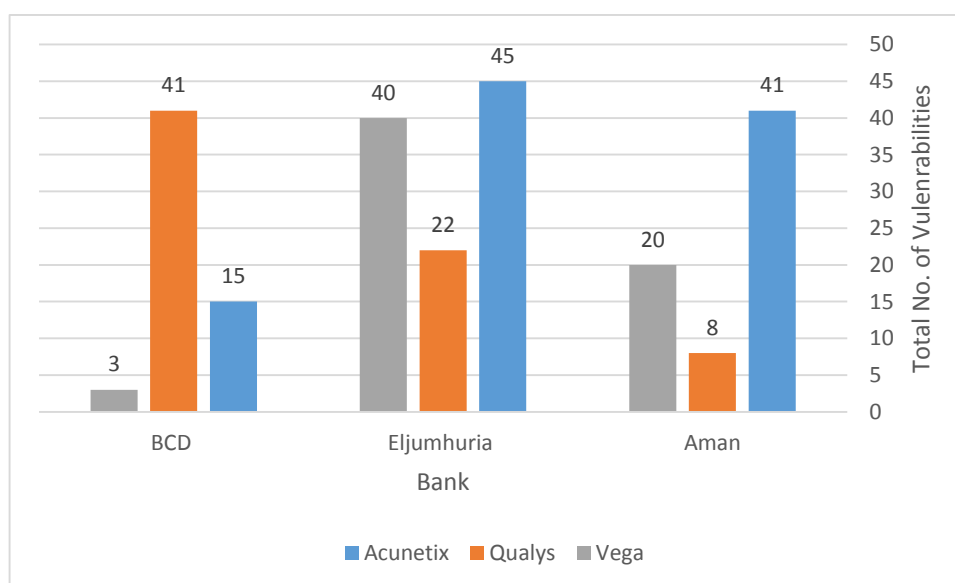


Fig 4.5: Comparison between total numbers of detected vulnerabilities (without info alerts)

In order to dig deeper, the obtained results for each bank by the three scanners are compared after being classified according the severity level. Figure 4.6 shows the results comparison of BCD bank where all three scanners believe BCD does not suffer from any high level vulnerabilities. Qualys detects more medium and low threats while Vega detects the highest number of information alerts.

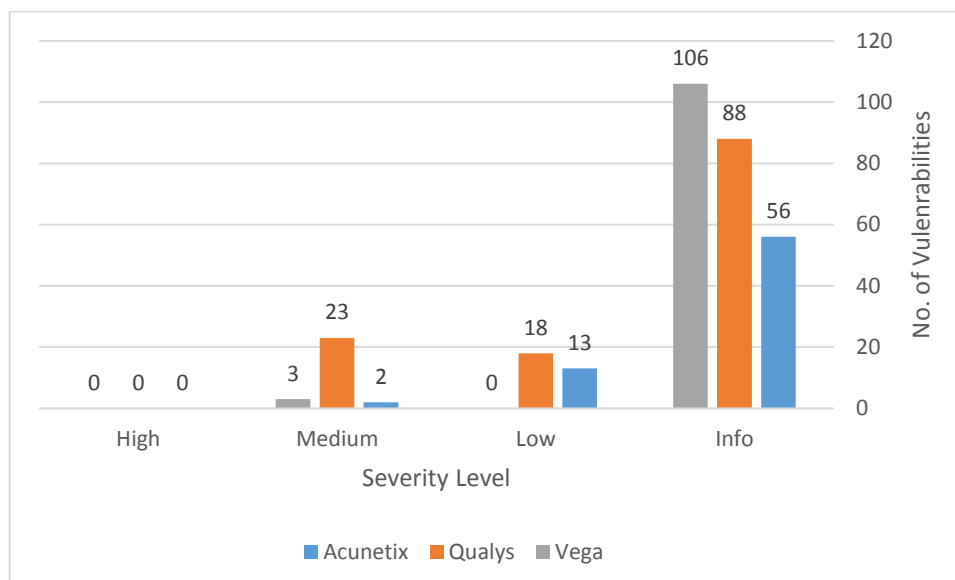


Fig 4.6: Comparison between numbers of detected vulnerabilities for BCD bank

Figure 4.7 illustrates Eljumhuria bank results. Vega again detects the highest number of information alerts. Acunetix and Qualys believe high alerts are minimal while Vega shows serious level of alerts. Results of medium and low alerts varies by scanner.

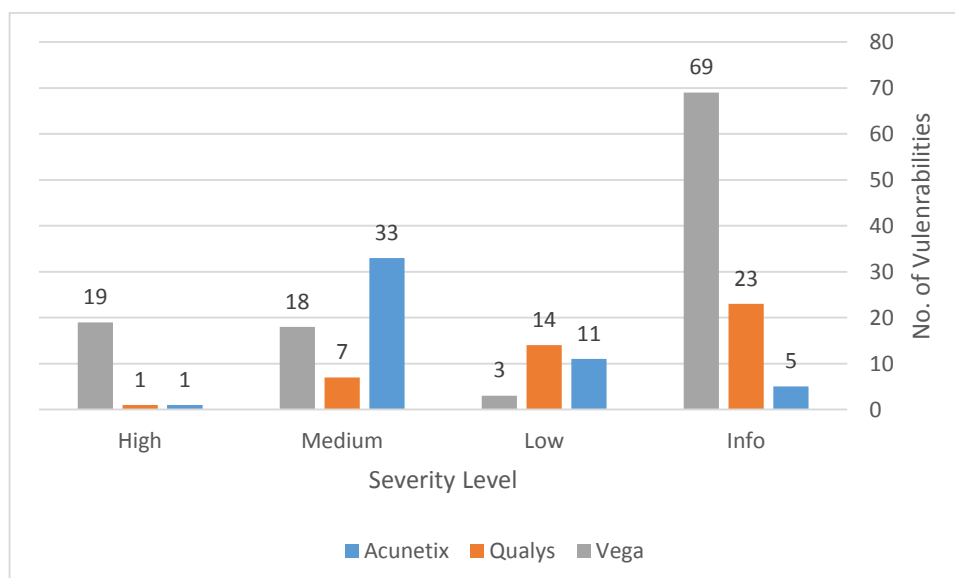


Fig 4.7: Comparison between numbers of detected vulnerabilities for Eljumhuria bank

Aman bank results are shown in Figure 4.8. again Acunetix and Qualys believe high threats are minimal for this website while Vega disagrees. Vega detects the highest number of information alerts while medium and low categories vary.

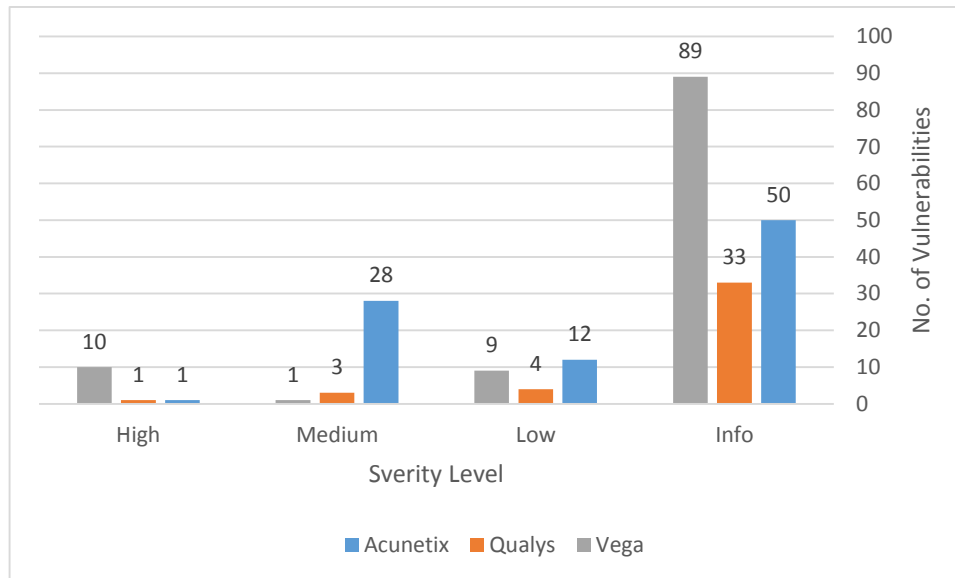


Fig 4.8: Comparison between numbers of detected vulnerabilities for Aman bank

4.3.2. Types of detected vulnerabilities

Appendix A shows an overview of vulnerabilities detected by each of the used scanners. The three scanners vary in the information they give about the detected vulnerabilities. Manly:

- ✓ Acunetix provides a very good description of the vulnerability
- ✓ In addition to a good description, Qualys provides in its free version- used in this study- suggested solutions to the detections. Also provides compliance reports of those against OWASP security standards.
- ✓ Vega –being an open source software- provides only numbers and a very brief title of the vulnerabilities detected.

In order to gain a deeper understanding of the results Tables 4.6, 4.7, and 4.8 state the top vulnerabilities, and a full description, its impact, and a solution of each where applicable. Each table shows the results of a corresponding scanner separately.

When creating the tables to provide a summary the following was:

- ✓ In top vulnerabilities mentioned are either sole detection of severity level or the groups of the higher numbers in their severity level.
- ✓ Along to the end of this research vulnerabilities that where defined by the scanner as of no impact on security will not be mentioned, those lay in either low or informational vulnerability group.

Table 4.6: Top vulnerabilities by Acunetix

Severity Level	Vulnerability Type	Description	Impact
BCD Bank			
Information	GHDB	This is a simple search for a login page. Attackers view login pages as the "front door" to a site, but the information about where this page is stored and how it is presented can provide clues about breaking into a site.	Breaking into the site
Eljumbhuria Bank			
High	Cross site scripting	Also referred to as XSS. Allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because the browser cannot know if the script should be trusted or not, It will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.	Malicious users may inject Javascript, VBScript, Active X, HTML or Flash into a vulnerable application to fool the user in order to gather data from them. The attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.
Medium	HTML form without CSRF protection	Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.	An attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Aman Bank			
High	Long password denial of service	By sending a very long password (1.000.000 characters) it's possible to cause a denial a service attack on the server. This may lead to the website becoming unavailable or unresponsive. Usually this problem is caused by a vulnerable password hashing implementation. When a long password is sent, the password hashing process will result in CPU and memory exhaustion. This vulnerability was detected by sending passwords with various lengths and comparing the measured response times. Consult details for more information.	An attacker may cause the website to become temporarily/indefinitely unavailable or unresponsive.
Medium	Application error message	This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception..	The error messages may disclose sensitive information. This information can be used to launch further attacks.

Table 4.7: Top vulnerabilities by Qualys

Severity level	Vulnerability type	Description	Impact	solution
BCD				
Medium	SSL Server Allows Anonymous Authentication Vulnerability	The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. A vulnerability exists in SSL communications when clients are allowed to connect using no authentication algorithm. SSL client-server communication may use several different types of authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the communications are vulnerable to a man-in-the-middle attack."	An attacker can exploit this vulnerability to impersonate your server to clients.	Disable support for anonymous authentication.
Low	SSL Certificate - Subject Common Name Does Not Match Server FQDN	An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.	A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.	Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

		A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.		
Eljumbhuria Bank				
High	EOL/Obsolete Software SNMP Version Detected	Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks." The authentication of clients of earlier versions of SNMP is performed only by a "community string", in effect a type of password, which is transmitted in cleartext.	The system is at high risk of being exposed to security vulnerabilities. Since the vendor no longer provides updates, obsolete software is more vulnerable to viruses and other attacks.	Disable or remove SNMPv1/2c authentication. Use SNMP version 3 authentication
Medium	Web Server Stopped Responding	The Web server stopped responding to 3 consecutive connection attempts and/or more than 3 consecutive HTTP requests. Consequently, the service aborted testing for HTTP vulnerabilities. The vulnerabilities already detected are still posted.	The service was unable to complete testing for HTTP vulnerabilities since the Web server stopped responding.	Check the Web server status.
Low	Path-Based Vulnerability	A potentially sensitive file, directory, or directory listing was discovered on the Web server.	The contents of this file or directory may disclose sensitive information.	Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Aman				
High	Microsoft Windows HTTP.sys Remote Code Execution Vulnerability (MS15-034)	Windows is prone to a remote code execution affecting the HTTP protocol stack (HTTP.sys). The vulnerability is caused when the HTTP protocol stack (HTTP.sys) improperly parses crafted HTTP requests. Microsoft has released a security update that addresses the vulnerability by correcting the way that HTTP.sys handles requests.	The vulnerability could allow remote code execution if an attacker successfully sends crafted HTTP requests to an affected Windows system	Refer to MS15-034 for further information.

Table 4.8: Top vulnerabilities by Vega

Severity Level	Vulnerability Type
BCD	
High	Character set not specified
Eljumbhuria	
High	Cross site scripting
Medium	Local Filesystem paths found
Low	Form password with autocomplete enabled
Info	Unsafe or unrecognized character set in response body
Aman	
High	Shell injection
Medium	Local Filesystem paths found
Low	ASP/ASPX error detection
Info	Interesting Meta tag detected

Extracting from the previous top vulnerability tables, and although scanners give close vulnerability numbers and agree in some cases on the severity level of the threat. Interestingly, each scanner believes the type of vulnerability to be different. Examining all types of vulnerabilities for all three banks against all the three scanners would be out of scope, so here we state a good example by examining only high alerts and see what each scanner thinks the cause of vulnerability is. Table 4.9 shows the type of vulnerability each scanner believes that it is the main cause of the high alerts detected.

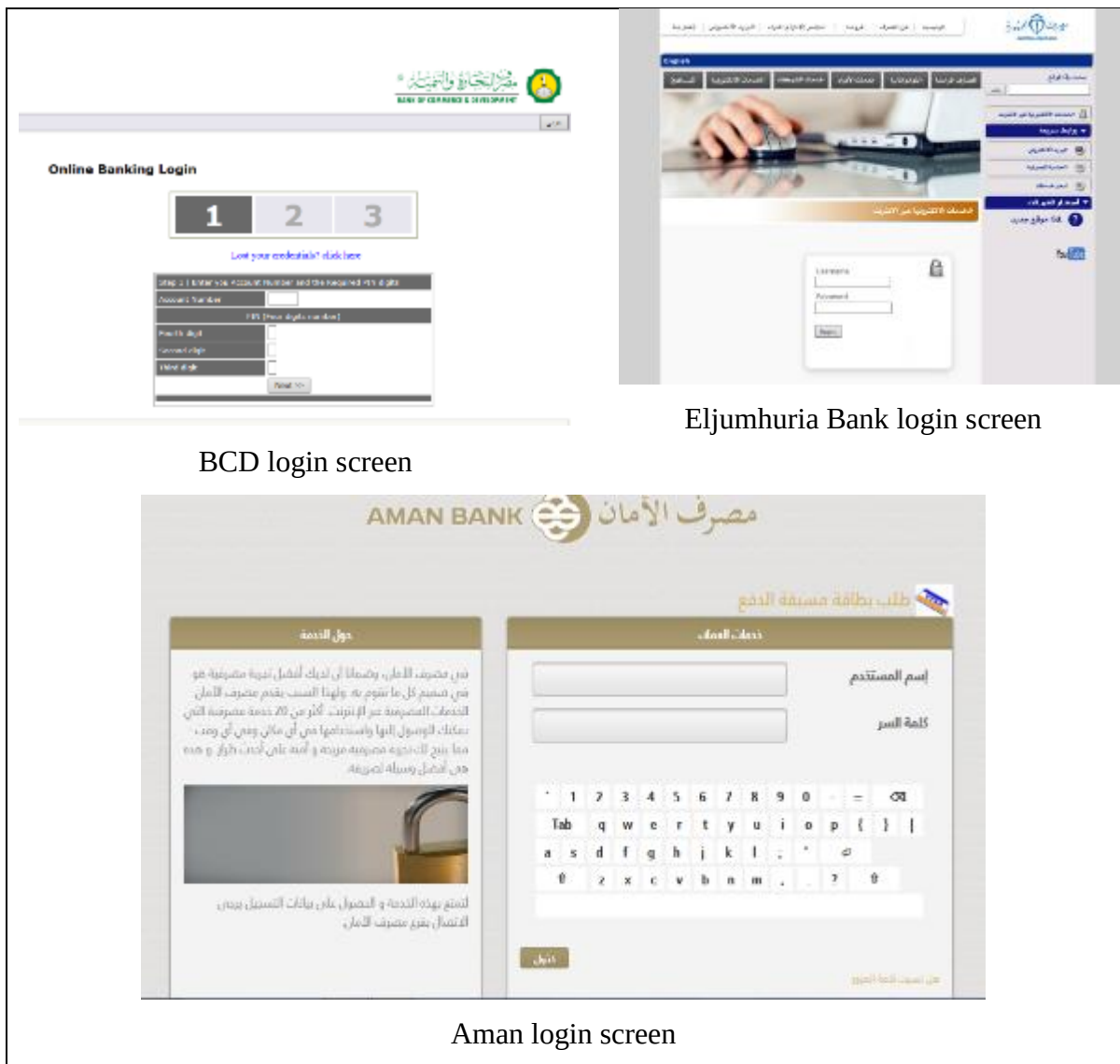
Table 4.9: High vulnerabilities causes

Bank	Vulnerability Scanner		
	Acunetix	Qualys	Vega
BCD	N/A	N/A	N/A
Eljumbhuria	Cross site scripting	EOL/Obsolete Software SNMP Version Detected	Cross site scripting
Aman	Long password denial of service	Microsoft Windows HTTP.sys Remote Code Execution Vulnerability (MS15-034)	Shell injection

4.4. Authentication Security Analysis

Despite the leading advantage of the banks already offering Internet banking, by checking the login page, they are using the very basic KBA (knowledge-based authentication) class and users are only asked to provide only a password and user name to be able to login. BCD as always tries to lead the competition and asks for specific digits of a PIN previously provided to the customer, figure 4.9 shows the login interface used in each bank.

The authentication PIN used by BCD, in addition to the username and the password, is a random code from the code card. The same challenge code is asked again until it has been entered correctly. This should prevent an attacker from brute-forcing favorable challenges for codes that he may have captured previously.



BCD login screen

Eljumhuria Bank login screen

Aman login screen

Fig 4.9: Internet banking providers' different login screens

It is obvious from these initial information that the existing authentication is questionable and a more efficient solution must be implemented not only to ensure login security but also to allow banks to extend their basic query services to a global standard of services.

Here we dig more in depth by running a scan by a vulnerability scanner ONLY to the login page, as to assess the full function we need actual credentials to be entered which unfortunately are unavailable. Similar to the steps followed in section 4.3 of this chapter we start by running the three vulnerability scanners against the login page in order to test authentication vulnerability. Appendix B shows screen shots of all scans conducted. Table 4.10 provides a summary of the numbers of detected vulnerabilities.

Table 4.10: Summary of conducted authentication scans

Bank	Number of Detected Vulnerabilities					
	High	Medium	Low	Info	Total	Total without Info threats
Using Acunetix						
BCD	0	0	1	1	2	1
Eljumhuria	0	5	4	2	11	9
Aman	0	1	18	0	19	19
Using Qualys						
BCD	1	7	9	29	46	17
Eljumhuria	0	5	6	27	38	11
Aman	0	2	5	607	614	7
Using Vega						
BCD	1	0	0	1	2	1
Eljumhuria	3	0	1	2	6	4
Aman	3	0	1	12	16	4

Figure 4.10 shows a comparison between the total number of alerts detected by each of the three scanners for each of the three banks. Qualys here gives an odd result when run against the authentication page of Aman bank as well as a notable gap compared to the very close results obtained by both Acunetix and Vega.

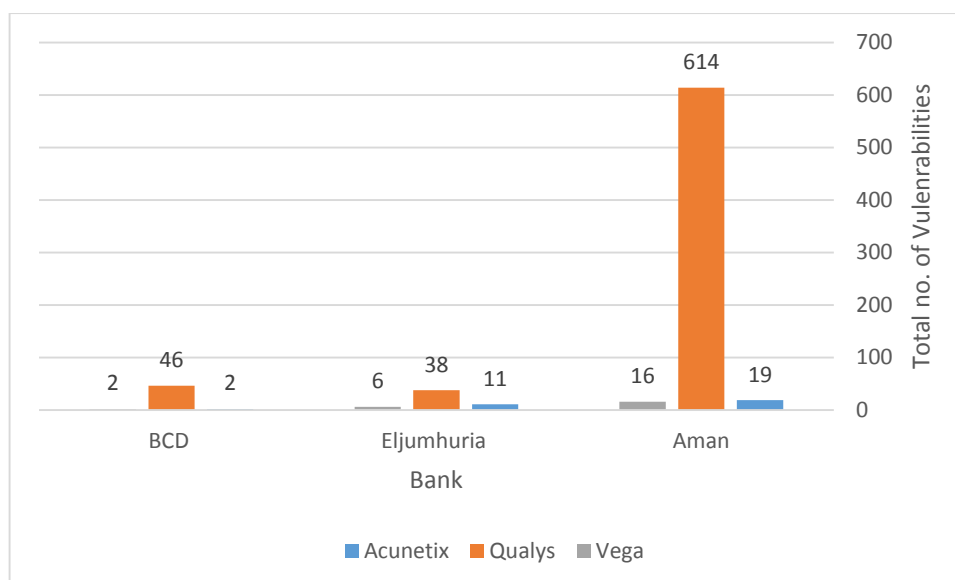


Fig 4.10: Comparison between total numbers of detected authentication vulnerabilities

In order to get a better sense of the obtained results, information alerts will be excluded. Figure 4.11 illustrates how Acunetix and Vega agree that BCD again is the least vulnerable while Qualys believes is the most.

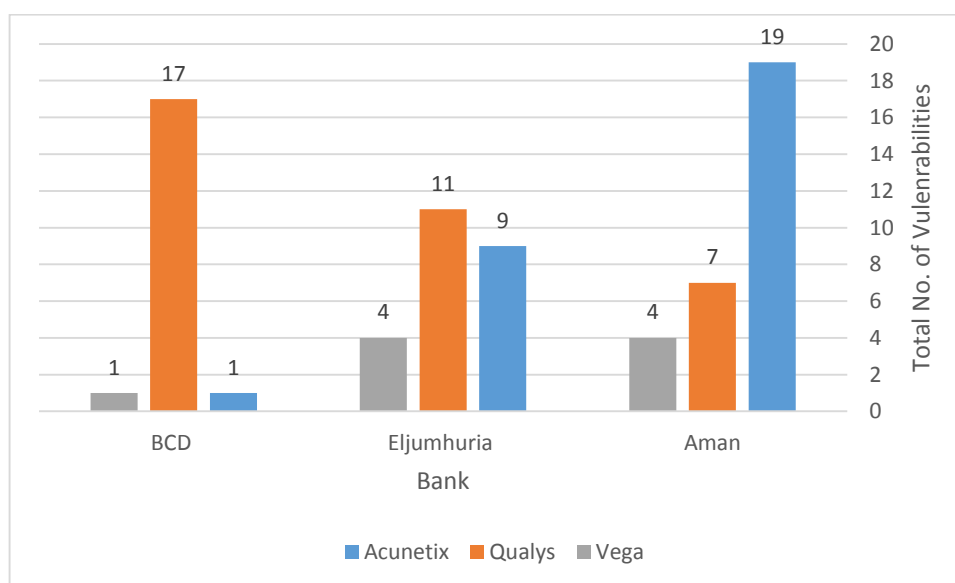


Fig 4.11: Comparison between total numbers of detected authentication vulnerabilities (without info alerts)

Now it is time to analyse bank authentication separately with enough details of severity levels. From the comparison in Figure 4.12 two out of the three scanners believe BCD has a high authentication vulnerability. Otherwise, acunetix and Vega show very close results while Qualys sets notable difference.

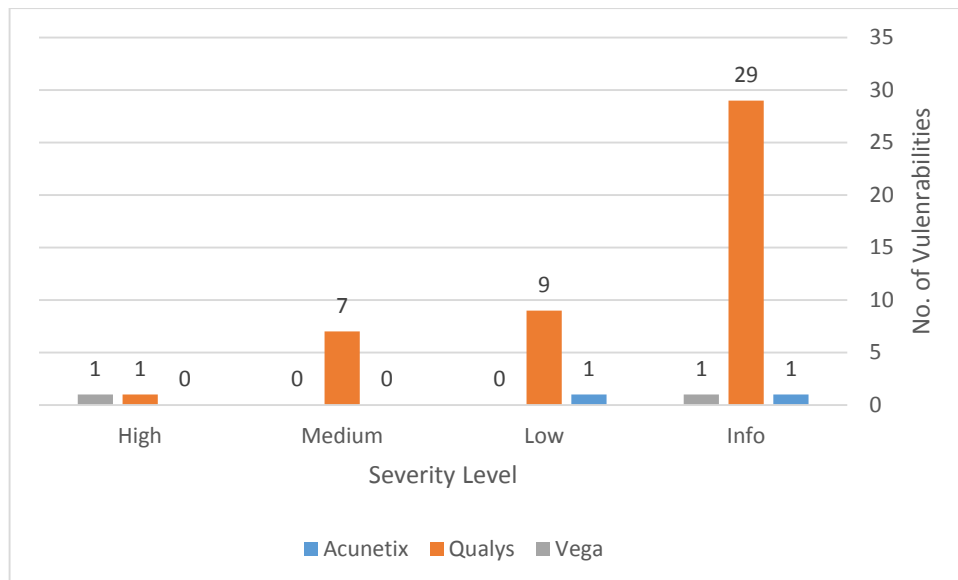


Fig 4.12: Comparison between numbers of detected authentication vulnerabilities for BCD

Unlike BCD, Figure 4.13 shows that only Vega believes Eljumhuria authentication suffers from high alerts while the other two scanner classify it as high alert free.

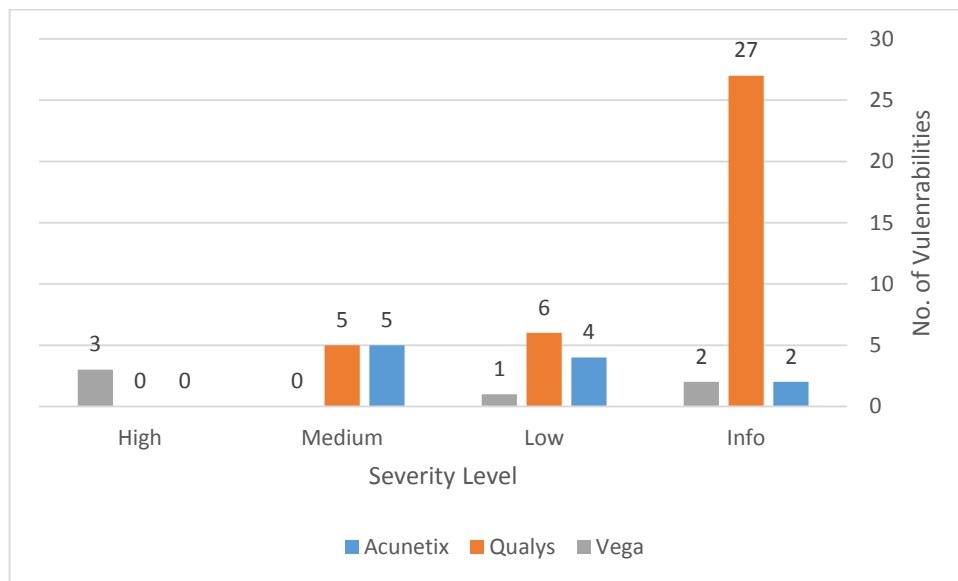


Fig 4.13: Comparison between numbers of detected authentication vulnerabilities for Eljumhuria bank

Figure 4.14 shows that the cause of the odd number affecting the total number of detected vulnerabilities by Qualys comes from information alerts. Again, only Vega believes Aman authentication suffers from high alerts while the other two scanner classify it as high alert free.

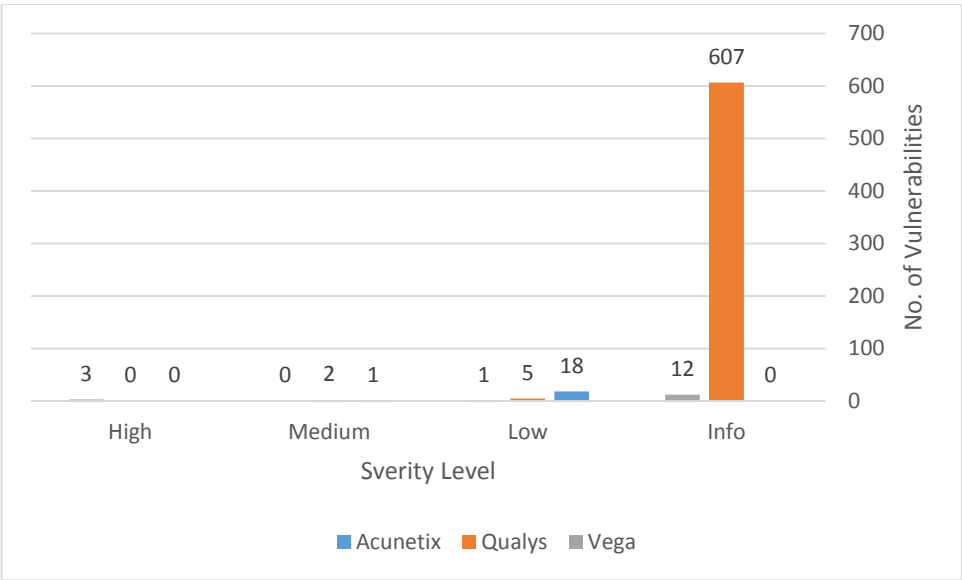


Fig 4.14: Comparison between numbers of detected authentication vulnerabilities for Aman bank

Continuing with the same steps followed in section 4.3 and guided by appendix B. types of vulnerabilities and their descriptions for each of the scanners are listed in Tables 4.11, 4.12, and 4.13.

Table 4.11: Top authentication pages vulnerabilities by Acunetix

Severity Level	Vulnerability Type	Description	Impact
BCD Bank			
Low	Clickjacking: X-Frame-Options header missing	Clickjacking (User Interface readdress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.	The impact depends on the affected web application.
Information	Microsoft IIS version disclosure	The HTTP responses returned by this web application include a header named Server. The value of this header includes the version of Microsoft IIS server.	The HTTP header may disclose sensitive information. This information can be used to launch further attacks.

Eljumbhuria Bank			
Medium	HTML form without CSRF protection	User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.	A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.
Aman Bank			
Medium	URL redirection	This script is possibly vulnerable to URL redirection attacks. URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.	A remote attacker can redirect users from your website to a specified URL. This problem may assist an attacker to conduct phishing attacks, trojan distribution, spammers.

Table 4.12: Top authentication pages vulnerabilities by Qualys

Severity Level	Vulnerability Type	Description	Impact	Solution
BCD				
High	EOL/Obsolete Software: Microsoft SQL Server 2005 (SP0) RTM Detected	Microsoft SQL Server 2005 RTM (SP0) release was detected on the host. Technical support for this RTM release has ended. No further bug fixes, enhancements, security updates or technical support is available for this release.	The system is at high risk of being exposed to security vulnerabilities. Since the vendor no longer provides updates, obsolete software is more vulnerable to viruses and other attacks.	Update to the latest service pack or a currently supported service pack.
Eljumbhuria Bank				
Medium	Web Server Stopped Responding	The Web server stopped responding to 3 consecutive connection attempts and/or more than 3 consecutive HTTP requests. Consequently, the service aborted testing for HTTP vulnerabilities. The vulnerabilities already detected are still posted.	The service was unable to complete testing for HTTP vulnerabilities since the Web server stopped responding.	Check the Web server status.
Aman				
Medium	Host Responds to One ICMP Request Multiple Times (Smurf Variant)	We have detected that a host belonging to the same class C (whose IP address is given in the report) responds to an	If a malicious user sends an ICMP echo-request packet to your network broadcast address, then numerous ICMP echo-reply packets will be generated (since all live hosts on the class C network will reply). By spoofing the source address	We strongly advise that you prevent unauthorized users from reaching broadcast address. To do so, filter these IP broadcast addresses on your router or firewall (IP layer protocol). Note, that there could be several

		ICMP echo request with two or more replies.	of the ICMP packet (i.e., a victim IP), a malicious user can flood the victim IP without difficulty by using the network as an amplifier (the destination IP would be your broadcast address). Since the source IP address was spoofed, it's difficult to trace the malicious user.	broadcast addresses if you're using subnetting on your network.
--	--	---	---	---

Table 4.13: Top authentication pages vulnerabilities by Vega

Severity Level	Vulnerability Type
BCD	
High	SSLv2 support
Info	Character set not specified
Eljumbhuria Bank	
Info	Unsafe or unrecognized character set in response body
Aman	
High	Session cookie without secure flag
Low	ASP/ASPX error detection

Now it is time to examine low alerts causes (as it is the most variant category, having both high and medium with many not applicable field) and see what each scanner thinks the cause of vulnerability is. Table 4.14 shows the type of authentication vulnerability each scanner believes that it is the main cause of the high alerts detected.

Table 4.14: Low authentication vulnerabilities causes

Bank	Vulnerability Scanner		
	Acunetix	Qualys	Vega
BCD	Clickjacking: X-Frame-Options header missing	Many (9 different)	N/A
Eljumbhuria	Clickjacking: X-Frame-Options header missing	Many (6 different)	Form password with autocomplete enabled
Aman	-Cookie without HTTP only flag set -Cookie with secure flag set	- Cookie Does Not Contain The "HTTPOnly" Attribute - Cookie Does Not Contain The "secure" Attribute	ASP/ASPX error detection

4.5 Summary and obstacles

Extracting from the chapter a simple summary of the main findings would be:

- ✓ Both Acunetix and Vega find BCD the least vulnerable and Aman Bank is the most.
- ✓ Results of the total number of vulnerabilities of both Acunetix and Vega are very close. On the other hand, Qualys not just give different reading but shows high number where both showed low and vice-versa.
- ✓ When it comes to severity of web application vulnerabilities, all three scanners couldn't detect any high alerts for BCD.
- ✓ Vega showed the highest information alerts numbers when detecting overall website vulnerabilities.
- ✓ Results of medium and low severity vulnerabilities varied significantly between the three scanners.
- ✓ Scanners differ in the type of information provided about detected vulnerabilities. While Vega provides only titles of vulnerabilities Acunetix provides a detailed description as well as the impact of the vulnerability on the system. Qualys goes even further to provide solutions and compliance reports in the free version.
- ✓ Although two scanners may give close vulnerability numbers and even same severity levels but most of the time they believe of different causes –type-of the vulnerability.
- ✓ Testing authentication vulnerability, Acunetix and Vega found BCD the least vulnerable while Qualys found the reverse.
- ✓ The bad news is that only in BCD authentication two scanners found high level alerts (Vega and Qualys).
- ✓ Two scanners (Acunetix and Qualys) found Aman and Eljumburia high authentication alert free, while showed three high vulnerabilities for each.

To make the above available and the listed information easy to extract number of obstacles were faced, Table 4.15 lists some of them and a brief of the solution made.

Table 4.15: Summary of obstacles and their solutions

No.	Challenge	Solution
1	Commercial vulnerability scanners are very expensive and most trial versions allow very limited number of scans- two most of the time. Also reports, solutions, and compliance reports are prohibited.	Subscription with more than an account made more scans possible, and using more than one scanner made more information available.
2	Open source software are known of the complexity of their installation, the use of poor GUI, and the many errors obtained after the actual download of the program. Finding the right software was a challenge and involved hours of downloading.	All available open source scanners were downloaded as well as packages of needed kits to successfully run the program. Not all turn to a success but eventually the right software was used.
3	Mainly, only website owners are allowed to run scans to their websites, as a verification file must be implemented in the script to ban hackers from using such tools.	This limitation appears more when using the commercial software online. In order to turn around it the scanner was downloaded to the computer
4	Long hours were needed to perform a single scan due to internet speed and the line-by-line checks used by the scanner. In this study a total number of 18 scans were conducted.	Patience!
5	Collection of data about Libyan banking structure from the information available on the Internet was a challenge as no much information are there. Also IT researches about Libya are rarely found, and even when found are not specific to the topic.	Bank visits, social network, university library access, building on similarities, and other resources were used to overcome the lack of data.
6	Testing the authentication page needs actual credentials giving by the bank after opening an account with them. Asking your social network to help does not work, as those remain private information.	The scan was run on the authentication page (login page) instead.

APPLIED AUTHENTICATION AND PROPOSED ENHANCEMENT

In this chapter, we work to answer the second research question and try to propose an authentication enhancement solution to the Libyan Internet banking club "members" and to those who have the potential to join.

We start by explaining how the business case for deploying two-factor authentication extends beyond a simple ‘fraud minus costs’ calculation to include a wide range of other factors. Our aim is to ensure strategic decision makers fully understand the range of opportunities for business development and cost reduction offered by two-factor authentication, and thereby enable a more positive, realistic business case.

Secondly, we present our vision of a secure, scalable, flexible and token-vendor independent authentication infrastructure, supporting a comprehensive range of authentication methods. The approach enables banks to offer the optimal user experience across a range of applications and channels, whilst reducing development and deployment costs and avoiding token-vendor lock-in.

Finally, and as an essential part of the proposed solution, we discuss what should be followed by the sector and imposed the umbrella (Central Bank of Libya) as a guidance to a secure Internet banking and authentication.

5.1. Product Solution

The importance of Internet banking is obvious for several reasons. Firstly, it offers a cost efficient alternative to telephone and branch banking due to the relatively low capital and maintenance costs, and its fully-automated processing of most transactions see figure 5.1. Secondly, it offers unparalleled customer convenience by enabling 24-hour access to a wide range of services.

The development is no longer just driven by the banks’ desire to reduce costs: first and foremost it is a manifestation of customers’ demand to access bank services online— at any time and from any location [10].

This section will cover a full roadmap towards choosing the right product solution to financial institutions in light of their requirements. It also highlights main factors to consider that might be sometimes overlooked when taking the decision of adopting a specific solution.

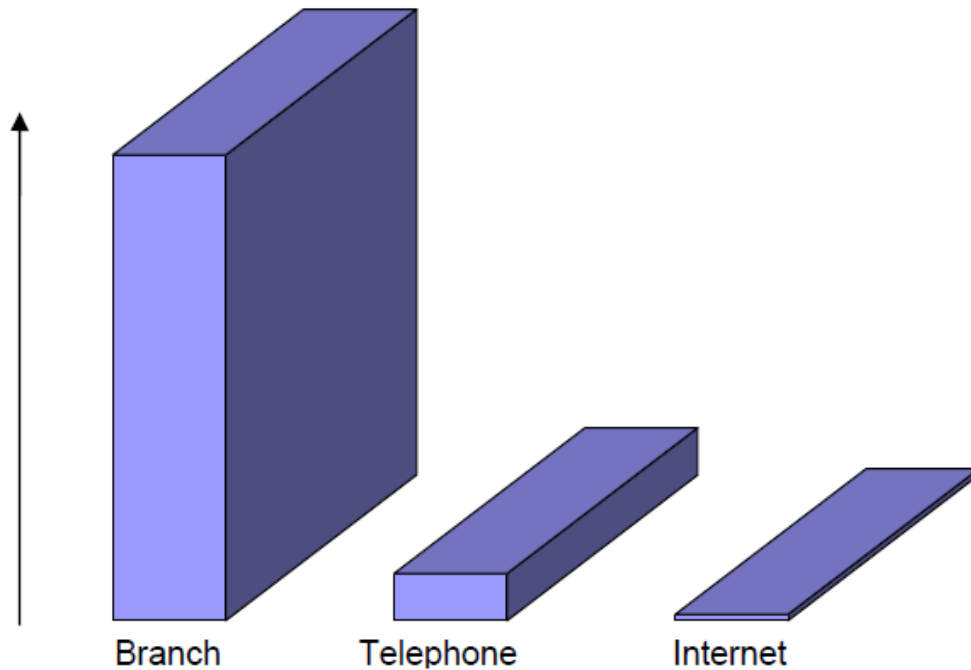


Figure 5.1: The cost of different banking channels

5.1.1. Why 2FA?

A small number of successful attacks against 2FA-enabled Internet banking systems have led to press reports that 2FA as a general approach has been ‘broken’. The reality is rather more complex, as we shall discuss below.

An attacker may obtain a valid OTP from a customer using the same methods as those used to obtain a static password. If the bank has deployed a simple system with 2FA used for login only, this attack may succeed.

To understand how to mitigate or eliminate this risk, it is first necessary to understand how attackers operate. Rather than one individual or organization being responsible, attacks are carried out by loose associations of individuals or groups, each with their own specialist role. Different parties cooperate, each providing a service: creating a fake web site, sending spam email, collecting passwords, and finally using those passwords to obtain cash. Passwords and other credentials are bought and sold between groups. This takes time. Since most OTPs

include an expiry mechanism, the attacker's standard operating model is no longer effective, and a considerably more complicated model of real-time attacks is being adopted. This explains the continuing technological advances in on-line attacks which we discussed earlier. Is this a never-ending arms race, or will there eventually be an outright winner? Happily, the strongest forms of 2FA available today offer a long-term, provably secure solution. The key is to move from authenticating the customer, to authenticating the transaction which the customer wishes to perform.

The user experience remains simple: the user simply enters the beneficiary account number and transaction amount into their authentication device, by means of an integral keyboard. The OTP thus created acts as a digital signature on those transaction details—even if obtained by an attacker, the OTP cannot be used for *any* other purpose.

Whilst this step may not be necessary today, many banks are deploying 2FA solutions with the option to upgrade to transaction authentication in the future. By this route, their customers first gain familiarity with the simplest form of the technology, and the bank is strategically placed to respond to future threats.

5.1.2. Which method is right?

To compare authentication methods, they must each be assessed against a range of criteria:

- ✓ **Usability**—ease of deployment and use, portability and reliability
- ✓ **Effectiveness**—how effective is it against a wide range of simple and advanced attack scenarios?
- ✓ **Cost**—initial purchase, deployment, support, lifetime and replacement

Figure 5.1 illustrates the advantages and disadvantages to consider for each authentication method

Table 5.1: Comparison between authentication methods

No.	Method	Method Advantages	Method Disadvantages
1	Software OTP token	-Simple to use -Many users already carry -capable smart phones -Timely authentication -Low cost	-User authentication only on simple applications -Applications can be compromised
2	CAP/DPA	-Transaction & user authentication -Card PIN provides 2nd factor— no need for separate password -Simple deployment	-Cost of card readers -Possible card reissuing costs -Usability for some customers
3	Matrix Card/ TAN list	-Small form-factor -Low cost -Easy to use	-User authentication only -Lower security level -Easy to copy -Relatively short lifetime
4	SMS	-Transaction & user authentication -Timely authentication -Low initial cost -Most users already carry mobile phones	-Customer management expensive -Availability to all customers -Availability of coverage -Ongoing cost of SMS messages
5	PKI token (hardware/software)	-Transaction & user authentication -Highly secure digital signature	-Low user mobility -Vulnerable to PC Trojans -Hardware costs (high) -High integration and support costs -Internet channel only
6	Static and partial password/PIN	-Useful as second factor -Familiar to all customers	-Very low security if sole method -Password reset/PIN mailer costs

A simple yet interesting presentation of the above methods against usability, cost and effectiveness criteria is shown in Table 5.2. Green, yellow and red colors correspond to the compliance with the factor tested, where green is compliant, yellow is partially compliant, and red is questionable.

Table 5.2: Methods compliance to criteria

Method	Usability	Cost	Effectiveness
Software OTP token			
CAP/DPA			
Matrix Card/ TAN list			
SMS			
PKI token (hardware/software)			
Static and partial password/PIN			

5.1.3. Bank selection criteria to adopt a solution

As we have seen, there are a wide range of two-factor authentication devices available, each with their own advantages and disadvantages. Combined with vendor spin and confusing media reporting, this often leads to confusion and internal conflict within the bank as to the best approach to take. Given the large investment required, and the visibility of the decision to customers, the end result can be procrastination and delay.

A business case for 2FA should not be based solely on ‘fraud minus cost’, as this is overly simplistic. Additional factors including potential loss of business, reputational damage, cost savings and opportunities for growth need to be considered to ensure a broader and more accurate business case is created. [10]

Figure 5.2 presents our suggested criteria to adopt the right solution and this section provides a full explanation of each of its components.

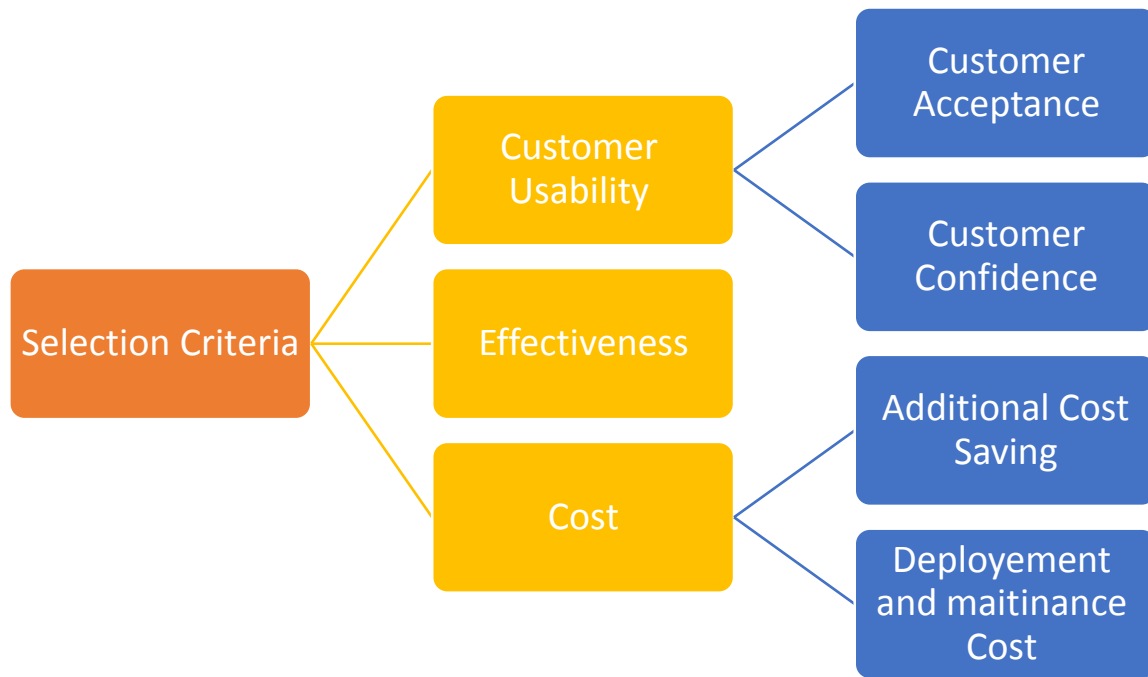


Figure 5.2: Criteria of solution adoption

5.1.3.1. Customer usability

Usability has two consideration: Customer acceptance and customer confidence in the applied method.

a) Customer Acceptance

The most important factor to consider is *always* customer ease-of-use. People will simply not use systems they find difficult, and so a positive customer response is essential to the success of any deployment. Also, with large banking customer bases, if even 1% of customers require telephone support, the total deployment cost increases dramatically. The authentication method or mix of methods selected must be simple, intuitive and reliable.

Customer attitudes towards a particular 2FA technology are best established through market research. Whilst internal opinion-gathering can act as a rough guide, it is important to remember that bank staff are not a good representation of customers in general. Surveys of customer opinion often produce surprising results, which only serves to underscore their value. By obtaining meaningful data, sufficient assurance of customer acceptance be demonstrated, thereby resolving internal debate and enabling additional resources to be committed with confidence.

b) Customer Confidence

Several customer surveys have highlighted security concerns as obstacles to the uptake of Internet banking. They are also frequently cited as a major factor in people moving away from on-line services to more expensive channels.

2FA is unique amongst anti-fraud technologies in its visibility to the customer, and is therefore uniquely placed to placate such fears. Conversely, the impact to consumer confidence and reputation of doing nothing, whilst the attack emails and media reports continue, must not be underestimated.

Being seen to be secure can help to achieve business targets by driving the uptake of Internet banking. Even for existing web users, increased confidence leads to increased usage for a wider range of transactions.

Visibly better security can also act as a competitive differentiator to boost migration from other banks, either for security reasons or because a more appealing technology is offered. Placing a device in every customers' wallet or pocket is also a powerful marketing opportunity, an ideal vehicle for driving brand awareness.

5.1.3.2. Effectiveness

Any assessment of potential savings arising from fraud reduction must start with current fraud levels. Extrapolating from past data to project future losses typically shows a growing exposure.

Any such estimates must also take into account the intrinsic insecurity of non-2FA systems, and the rapid ability of attackers to package and commoditise today's advanced attacks to deliver them *en masse* tomorrow. Failing to invest in 2FA can be seen as a 'ticking bomb', waiting for a fraud explosion.

In addition, it's important to recognize the fraud where it is occurring. Most banks currently refund defrauded customers in full, leaving the bank open to first-party fraud. Whilst this can be addressed through careful processes, these are costly and time-consuming. By forcing

active customer participation in each transaction, 2FA reduces the opportunity for first-party fraud and increases the scope for the bank to disclaim liability in suspicious cases.

Lastly, card-not-present (CNP) fraud must be considered alongside Internet banking fraud. E-commerce transactions can be secured by integrating 2FA into 3-D Secure systems (MasterCard SecureCode / Verified by Visa). In some countries, this approach is being extended to incorporate mail order and telephone order (MOTO) transactions.

5.1.3.3. Cost

In addition to the initial cost two cost considerations must be in mind when choosing the right method:

a) Additional Cost Savings

By using 2FA to present a more difficult target, the overall volume of attacks is likely to be reduced. Operational costs in researching and shutting down such attacks are thus reduced, freeing resources for more productive work. A similar workload reduction for front-line staff currently handling fraud claims can also be expected.

In addition, once deployed and proven effective, 2FA may allow current expenditure on complementary anti-phishing technologies and services to be reduced or even eliminated. Finally, deployment of 2FA technology may enable existing processes elsewhere to be reengineered, with considerable cost savings. One UK bank realised that 2FA enabled them to automate their call centre customer authentication process—the resulting savings were sufficient to cover the *entire* deployment costs. Strong, automatic customer authentication also increases the range of services that can be offered without the involvement of an operator.

b) Deployment and Maintenance Costs

Having considered the full range of potential benefits, it is of course essential to consider the full costs, and to devise a strategy to extract the greatest return on the necessary investment. Device costs comprise the initial purchase price, together with the costs associated with packaging and delivery. Reliability and robustness must be taken into account when calculating re-issuance costs due to device failures, and the lifetime of the device also considered. Market acceptance of charging either for the initial device or for replacements varies between countries.

The second component to consider is the cost of the necessary supporting infrastructure. Rather than tightly coupling the 2FA system to the Internet banking application, a dedicated authentication system offers numerous advantages: it allows multiple applications and channels to leverage the investment; it provides a consistent user experience across applications and channels; and it reduces the Internet banking development resources required.

Large banks typically offer a range of products to a variety of market segments. Each product has its own security requirements, and its own budget, and there can be a huge variation in acceptance of authentication technology across different customer groups. A central authentication server must therefore be sufficiently flexible to offer a hybrid approach, in which certain products or customers use one kind of authentication, whilst a different approach is used in parallel elsewhere.

As well as being better able to support today's requirements, a flexible authentication server can enable longer-term cost savings. By not tying the bank to a particular vendor, on-going device costs are more easily controlled. And the ability to switch devices or device modes enables the bank to react rapidly to new attacks.

The final component in the cost calculation is resource costs: project management, development, operations and customer support. An efficient and effective infrastructure strategy minimises the first three of these; the last must be addressed through careful choice of a simple authentication method coupled with clear customer communication, refined through experience obtained by an initial pilot deployment.

5.1.4. Method selection summary

- ✓ For the "potential" Libyan banks to adopt Internet banking and from establishment cost perspective: comparing the branch cost with the Internet banking cost, the decision should be easy to take.
- ✓ For the three banks today providing Internet banking: considering the very basic authentication methods used, it is about time to adopt more efficient solutions.
- ✓ Internet banking services already provided by Libyan banks stay very basic and do not exceed queries about integrated accounts and bank statement print out. In order

to expand provided services a solution to enhance current authentication method must be implemented.

- ✓ There is no such a thing as "the right product solution for all banks". The right product have to do with the bank itself and with what it is visible to its base of customers.
- ✓ The way to choosing the right solution for a specific bank starts with testing it against acceptability, cost and effectiveness.
- ✓ When deciding to go for one specific method solution customers' test of confidence has to prove positive.
- ✓ There are hidden sources of cost when implementing a certain method rather than the cost of establishment, those sources must be carefully considered.

5.2. Guidance to authentication in an Internet banking environment

One of the best worldwide practices when it comes to security measures enforcement and assurance is the placement of a guidance. The purpose of this guidance is mainly to enforce risk management framework and to provide institutions with an overview of pertinent regulatory issues, and to offer suggestions on how to apply existing consumer laws and regulations to new electronic financial services.

The range of existing security standards and guidance is wide: The International Standard – ISO 27001 family, NIST Special Publication 800-53, The Open Web Application Security Project (OWASP), Payment Card Industry (PCI) standards, Sarbanes Oxley Act, The Security Technical Implementation Guide (STIG), The Web Application Security Consortium (WASC) and others are just few examples.

Authentication- being the focus of this chapter and the most critical part of the internet banking system- has to have a specific guidance. In this section, we choose to talk about Federal Financial Institutions Examination Council (FFIEC) authentication guidance because of the following main reasons:

- ✓ It is specific to financial institutions
- ✓ It is specific to authentication
- ✓ It has the most specialized updated guidance
- ✓ Comes in several issues each rectifies the previous
- ✓ It is considered to be the guide for most of the American financial institutions
- ✓ There is an IT handbook for each step of the procedure

5.2.1. FFIEC guidance to authentication in an Internet banking environment

The Federal Financial Institutions Examination Council (FFIEC) is an interagency body which promotes uniformity and consistency in the supervision of financial institutions through establishing uniform principles, standards and report forms for financial institution regulatory agencies. [19]

Regulatory Agencies:

- ✓ Board of Governors of the Federal Reserve System (FRB);
- ✓ Federal Deposit Insurance Corporation (FDIC);
- ✓ National Credit Union Administration (NCUA);
- ✓ Office of the Comptroller of the Currency (OCC); and
- ✓ Consumer Financial Protection Bureau (CFPB)

The “Authentication Guidance” issued by the FFIEC continues to evolve as new technologies emerge and as changes occur in the fraud environment that financial institutions are faced with:

- ✓ August 2001: Authentication in an Electronic Banking Environment
- ✓ October 2005: Authentication in an Internet Banking Environment (Replaced 2001 Guidance)
- ✓ June 2011: Supplement to Authentication in an Internet Banking Environment

The “2001 Guidance” focused on risk management controls necessary to authenticate the identity of retail and commercial customers accessing Internet-based financial services

The “2005 Guidance” replaced the 2001 Guidance and provided a risk management framework for financial institutions offering Internet based products and services to their customers.

The “2011 Supplement” reinforced the 2005 Guidance’s risk management framework and updated the Agencies’ expectations regarding customer authentication, layered security, or other controls.[19]

5.2.2. Implementing a Layered System of Security

The concept of customer authentication in the 2005 Guidance is broad, including more than the initial authentication of the customer when he or she connects to the financial institution at login. Since virtually every authentication technique can be compromised, the FFIEC maintains that financial institutions should not rely solely on any single control for authorizing high-risk transactions, but rather institute a system of layered security that includes the following steps [20]:

Step1: Risk Assessments

Step2: Customer Authentication for High-Risk Transactions

Step3: Layered Security Programs

Step4: Effectiveness of Certain Authentication Techniques

Step5: Customer Awareness and Education

5.2.2.1. Step 1: Risk management

Financial institutions should review and update their existing risk assessments as new information becomes available, prior to implementing new electronic financial services, or at least every twelve months. Updated risk assessments should consider, but not be limited to the following factors:

1. Changes in the internal and external threat environment
2. Changes in the customer base adopting electronic banking;
3. Changes in the customer functionality offered through electronic banking; and
4. Actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry.

5.2.2.2. Step2: Customer Authentication for High-Risk Transactions

"high-risk transactions" are electronic transactions involving access to customer information or the movement of funds to other parties. However, more customers (both consumers and businesses) are conducting online transactions. The Agencies believe that it is prudent to recognize and address the fact that not every online transaction poses the same level of risk.

Therefore, financial institutions should implement more robust controls as the risk level of the transaction increases.

Financial institutions should implement layered security, as described herein, utilizing controls consistent with the increased level of risk for covered transactions. Additionally, they should offer multifactor authentication to their customers.

5.2.2.3. Step3: Layered Security Programs

Layered security is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control. Layered security can substantially strengthen the overall security of Internet-based services and be effective in protecting sensitive customer information, preventing identity theft, and reducing account takeovers and the resulting financial losses.

Effective controls that may be included in a layered security program include, but are not limited to:

1. fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response;
2. the use of dual customer authorization through different access devices;
3. the use of out-of-band verification for transactions;
4. the use of "positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account;
5. enhanced controls over account activities; such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (e.g., days and times);
6. internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities;
7. policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud;
8. enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels; and

9. enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk.

The Agencies expect that an institution's layered security program will contain the following two elements, at a minimum.

a) Detect and Respond to Suspicious Activity

Layered security controls should include processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to:

- ✓ initial login and authentication of customers requesting access to the institution's electronic banking system; and
- ✓ initiation of electronic transactions involving the transfer of funds to other parties.

b) Control of Administrative Functions

For business accounts, layered security should include enhanced controls for system administrators who are granted privileges to set up or change system configurations, such as setting access privileges and application configurations and/or limitations. These enhanced controls should exceed the controls applicable to routine business customer users. For example, a preventive control could include requiring an additional authentication routine or a transaction verification routine prior to final implementation of the access or application changes. An example of a detective control could include a transaction verification notice immediately following implementation of the submitted access or application changes.

5.2.2.4. Step4: Effectiveness of Certain Authentication Techniques

a) **Device Identification**

This typically uses a cookie loaded on the customer's PC to confirm that it is the same PC that was enrolled by the customer and matches the logon ID and password that is being provided. Simple device identification as described above can be distinguished from a more sophisticated form of this technique which uses "one-time" cookies and creates a more complex digital "fingerprint" by looking at a number of characteristics including PC configuration, Internet protocol address, geo-location, and other factors.

Institutions should no longer consider simple device identification, as a primary control, to be an effective risk mitigation technique.

b) Challenge Questions

The amount of information about people that is readily available on the Internet and the information that individuals themselves make available on social networking websites makes basic challenge questions inadequate for authentication. As a result, institutions should require sophisticated challenge question systems that require the customer to correctly answer multiple “out of wallet” questions that do not rely on information that is often publicly available.

5.2.2.5. Step5: Customer Awareness and Education

A financial institution's customer awareness and educational efforts should address both retail and commercial account holders and, at a minimum, include the following elements:

- ✓ An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts with Internet access;
- ✓ An explanation of under what, if any, circumstances and through what means the institution may contact a customer on an unsolicited basis and request the customer's provision of electronic banking credentials;
- ✓ A suggestion that commercial online banking customers perform a related risk assessment and controls evaluation periodically;
- ✓ A listing of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk, or alternatively, a listing of available resources where such information can be found; and,
- ✓ A listing of institutional contacts for customers' discretionary use in the event they notice suspicious account activity or experience customer information security-related events.

Table 5.3 presents a summary of the guidance in a simple checklist to help the use of financial institutions.

Table 5.3: Suggested authentication guidance checklist

Risk management	
Review and update the existing risk assessments to include:	
Changes in the internal and external threat environment	☐
Changes in the customer base adopting electronic banking	☐
Changes in the customer functionality offered through electronic banking	☐
Actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry	☐
Customer Authentication for High-Risk Transactions	
Make sure to use:	
Multifactor authentication is offered mainly to high-risk transaction.	☐
Layered Security Programs	
Program must include:	
Fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response	☐
Use of dual customer authorization through different access devices	☐
Use of out-of-band verification for transactions	☐
Use of "positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account	☐
Enhanced controls over account activities; such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (e.g., days and times)	☐
Internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities	☐
Policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud	☐
Enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels	☐
Enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk	☐

Processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to login and initiating a transaction	☐
Enhanced controls for system administrators who are granted privileges to set up or change system configurations	☐
Effectiveness of Certain Authentication Techniques	
Make sure to use:	
Sophisticated form of device identification technique	☐
Multiple “out of wallet” questions as challenge questions	☐
Customer Awareness and Education	
customer awareness and educational efforts should include:	
An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts with Internet access	☐
An explanation of under what, if any, circumstances and through what means the institution may contact a customer on an unsolicited basis and request the customer's provision of electronic banking credentials	☐
A suggestion that commercial online banking customers perform a related risk assessment and controls evaluation periodically	☐
A listing of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk, or alternatively, a listing of available resources where such information can be found	☐
A listing of institutional contacts for customers' discretionary use in the event they notice suspicious account activity or experience customer information security-related events	☐

5.2.3. Compliance example

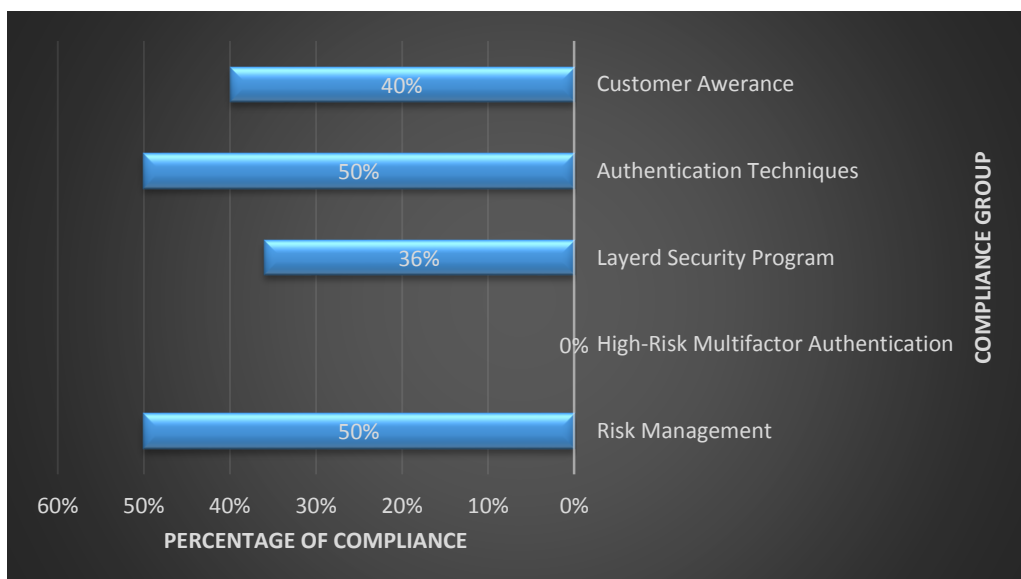
In order to provide a better sense of how the suggested guidance can be encouraged, BCD was chosen to give a rough idea about where it stands if eventually CBL decides to apply such a guidance. Studying policies and standards compliance is out of the scope of this work, but giving such an example for the bank that is believed to provide relatively fair level of security helps in understanding how the first step of applying a guidance could be.

Referring to Appendix C, and by simply filling in the pre-prepared checklist by an IT professional from BCD bank, we find:

- ✓ Overall bank compliance cannot be calculated as not all four compliance groups have the same weight.
- ✓ Due to the basic services provided online many items were checked false
- ✓ None of the five compliant groups proved to be fully compliant with the guide, and none exceeded 50%.
- ✓ Due to the non-existence of a multifactor authentication, the compliant group including it turned non-compliant

Figure 5.3 provides a summary of the percentage of compliance with FFIEC guidance for each of the five compliance groups.

Figure 5.3: Percentage of BCD compliance with FFIEC guidance



CONCLUSION AND RECOMMENDATIONS

The aim of this study is to evaluate the security of the Libyan Internet banking and to suggest solutions to enhance the authentication methods in use, after evaluating them being an essential part of the overall evaluation. In this chapter, we summarize the outcome of the study with a conclusion, followed by some recommendations and suggestions for future researches.

6.1. Conclusion

Libyan Internet banking is in its early stages. Almost 30% of the banking sector has absolutely no presence on the Web, while only few banks are currently offering a basic form of Internet services- mainly account queries. Authentication methods used are also simple, inadequate and not fulfilling customer security needs.

Efforts from the Central Bank of Libya CBL to provide a guide to the banks working under its umbrella for -either or both- Web presentation and Internet banking almost does not exist. Furthermore, CBL own presence on the Web is humble and its security is also questionable.

Working on such an unexplored topic has its pros and cons. From the negative side, the collection of data remains the main challenge. However, the findings throughout the way adds to the excitement and pushes towards wanting to know more. Summary of those finding comes below:

1. The existing Web security is vulnerable to a relatively high number of attacks. Although, severity differs from one bank to another.
2. Services provided by Libyan internet banking are in the simplest form (mainly account queries) as well as the lack of useful tools and sophistication of a normal international bank presence on the web, yet the number of detected vulnerabilities is high while it should be much lower considering the simplicity of what is offered.
3. Surprisingly, the Central Bank of Libya website, vulnerability, range of services do not set a good example. Furthermore, no guidance to Internet security, Internet banking and/or authentication is in place or being supervised.

4. The cost of establishing a branch is much higher than adopting Internet banking solution. Libyan banks still working the traditional way have great potential to turn to a smarter solution for cost-efficiency perspective.
5. Being the first to introduce Internet banking in Libya, Bank of Commerce and Development, is still the leader with the least severity level and a relatively low number of vulnerabilities.
6. Security scanners are used to help detecting vulnerability and in order to achieve reliable results and wider sense of where our online security stands, more than one security scanner is normally used. The reason behind this is that scanners tend to give different evaluation to the same service as well as a different range of information ranging from naming the vulnerability to finding the exact fixing to the script line.
7. Banks offering Internet banking services use one factor authentication, which is unreliable method of authentication and not used anymore to authenticate customers of Internet banking services.
8. Talking about authentication in general and financial institutions' authentication in particular, two-factor authentication has been widely replacing traditional single-factor authentication, as well as proving to provide adequate protecting to high-risk transactions against possible attacks.
9. When it comes to choosing authentication method and/or solution product there is no such a thing as "the right solution for all". Each financial institution has its specific considerations that must be taken in account before making the right decision.
10. There are many standards and guidance specialized in the security of financial institutions. Following those is the best practice to ensure ultimate Internet banking service.

6.2. Recommendations

Recommendations of this section are directed to financial institutions in order to enable them catch up with the World's latest technologies in practice. As an outcome of this study, we recommend the following:

1. Very powerful yet expensive vulnerability scanner tool are in the market. Some have features of checking web-applications line-by-line and suggest defense measures by predicting program reactions. Those have to be adopted as enhancers to bank web security and considered as an intelligent investment.

2. Benefits of Internet banking were discussed in detail in this work. Investment of the banking sector in this regard is highly recommended and eventually will turn rewarding to those who chose to adopt smart business solutions.
3. Single-factor authentication is not in use today in almost all financial institutions worldwide. Libyan banks offering Internet banking must turn to a two-factor authentication.
4. The way to adopt the right solution for a specific bank starts with testing it against usability, cost and effectiveness.
5. When choosing to implement certain authentication method, hidden sources of cost-rather than the initial deployment cost must not be overlooked.
6. In this work we present one of the world's most powerful guidance to financial institutions online security, as well as an initiative easy to follow checklist. CBL is encouraged to enforce and supervise a security guide on sector banks, either by creating a derivation from the existing or joining one of the bodies.
7. GSM network as well as smart phones are widely used by bank customers, making multi-channel authentication a technology to consider. Libyan GSM network coverage efficiency and other factors must be also considered.

6.3. Suggestions for future work

As previously stated, the topic of Internet banking in general and its security in particular are relatively new to Libya. Country specialized researches are only few and mainly covering the economic side rather than technical, which allows a lot of research based on this work or handling the topic from a different aspect. Some suggestions would be:

- ✓ Banking network security instead of web application security is a rich research subject where firewalls and other network components can be assessed.
- ✓ Fixing vulnerability of one of the banks' website can be a very interesting subject to work on.
- ✓ Suggesting a unique authentication solution using a multi-factor, multi-channel authentication.
- ✓ Applying a guidance standard on operating banks.
- ✓ Create an Internet banking application to expand the number and nature of the existing Internet banking services.

REFERENCES

1. Online banking, Wikipedia, [Online Resource], available from: http://en.wikipedia.org/wiki/Online_banking.
2. Olowookere Sunday & Popo-ola E. Arnold (January 2008). Accessing e-banking based on resilient transaction.
3. Luis M. Camarinha-Matos (2012). Scientific Research Methodologies and Technique, L. M. Camarinha-Matos, 2009-2012.
4. Kritika Law RITIKA LAW (2007). Impact of Perceived Security on Consumer Trust in Online Banking.
5. Al Fairuz, Mohamed Ali Suleiman (2011). An Investigation into the Usability and Acceptability of Multi-channel Authentication to Online Banking Users in Oman.
6. Nima Kaviani, Kirstie Hawkey, Konstantin Beznosov (2008). A Tow-Factor Authentication Mechanism Using Mobile Phones.
7. Gregory D. Williamson (2006). Enhanced Authentication In Online Banking.
8. Marko Holbl, CEPIS LSI Security (2007). Authentication Approaches for Online-Banking, Bakground Paper.
9. Arnis Parsovs (2012). Security Analysis of Internet Bank Authentication Protocols and their Implementations
10. Cryptomathic A/S White Paper. (2012). Two-Factor Authentication for Banking, Building the Business Case.

11. Professor T.Venkat Narayana Rao, Vedavathi K (2011). Authentication Using Mobile Phone as a SecurityToken
12. CBL Central Bank of Libya, (2007) *General news*, [Online Resource], available from: <http://www.cbl.gov.ly/en/>
13. Ahmed E. A. Mohamed (2013). Improving the Libyan customers' trust and acceptance for online banking technology, University of Salford.
14. The Government of the Hong Kong Special Administrative Region (February 2008). An overview of vulnerability scanners.
15. "Web vulnerability scanner – Network vulnerability scanner ", [Online Resource], available from: www.acunetix.com.
16. Vulnerability scanning tools, [Online Resource], available from: www.owasp.org
17. Web application scanning,[Online source], available from: www.qualys.com
18. Vega vulnerability scanner, [Online Source], available from: <https://subgraph.com/vega/>
19. Matthew Clohessy. FFIEC Customer Authentication Guidance: Authentication in an Internet Banking Environment .
20. Federal Financial Institutions Examination Council (2011). Supplement to Authentication in an Internet Banking Environment.

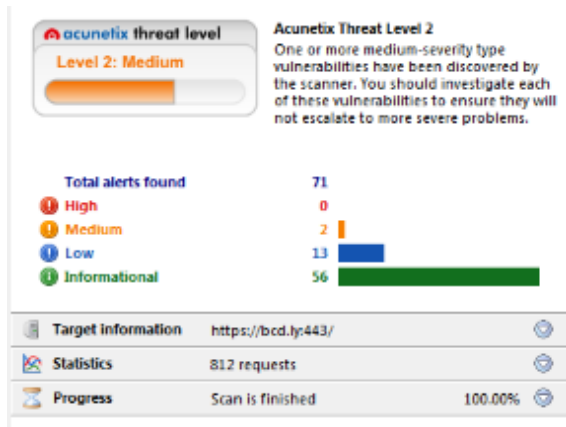
BIBLIOGRAPHY

1. SecureAuth white paper (September 2015). FFIEC authentication compliance using SecureAuth idP.
2. Federal Financial Institutions Examination Council (2011). Guidance on electronic financial services and consumer compliance.
3. Fadi Aloul, Syed Zahidi, and Wassim El-Hajj. Two factor authentication using mobile phones, American University of Sharjah and College of Information Technology, UAE.
4. O.B. Lawal, A. Ibitola, and O.B. Longe (March 2013). Internet Banking Authentication Methods in Nigeria Commercial Banks.
5. Nima Kaviani and Konstantin Beznosov. A two factor authentication system using mobile phones
6. Mohammad Mohsin (2010). Adoption of e-Banking in Context of a Developing Country, Pakistan. COMSATS Institute of Information Technology, Islamabad.
7. Yudit María (April 2010). PCI DSS Case Study: Impact in Network Design and Security. Rochester Institute of Technology.
8. Walter Sprenger (September 2008). Security Trends eBanking. Compass Security.
9. Finacle from Infosys. What the Future of Online Banking Authentication Could Be.
10. Manal Adham¹, Amir Azodi¹, Yvo Desmedt^{2,1}, and Ioannis Karaolis¹. How to Attack Two-Factor Authentication Internet Banking

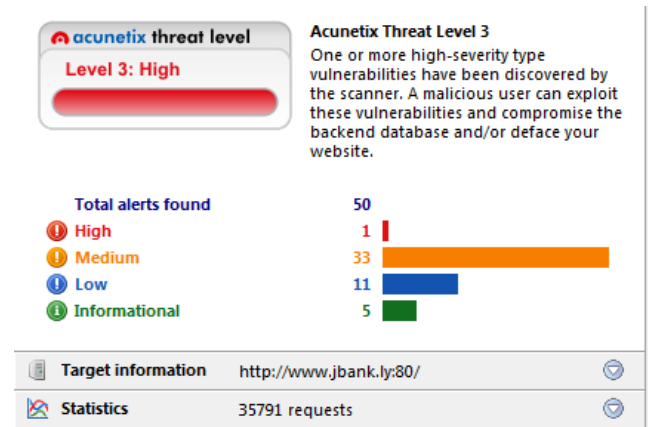
APPENDIX A

Web Vulnerability Scan Results

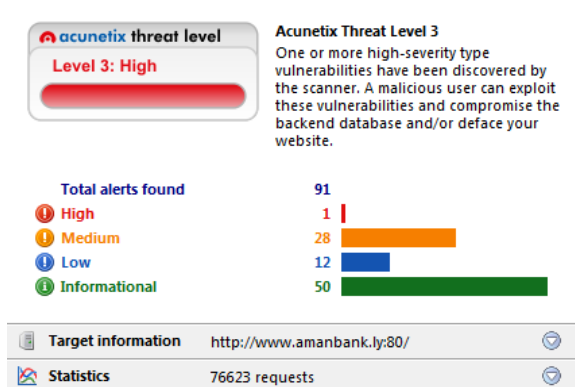
Using Acunetix



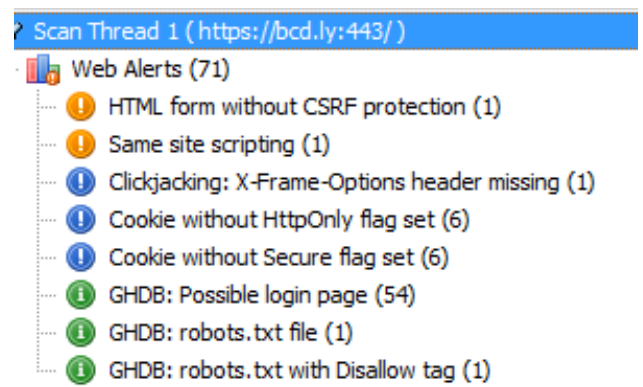
BCD vulnerability scan result



Eljumbhuria vulnerability scan result



Aman Bank vulnerability scan result



BCD Bank detected vulnerability overview

Scan Thread 1 (http://www.jbank.ly:80/)

Web Alerts (50)

- ❗ Cross site scripting (verified) (1)
- ❗ HTML form without CSRF protection (28)
- ❗ Unencrypted __VIEWSTATE parameter (3)
- ❗ User credentials are sent in clear text (2)
- ❗ ASP.NET debugging enabled (1)
- ❗ ASP.NET version disclosure (1)
- ❗ Clickjacking: X-Frame-Options header missing (1)
- ❗ Cookie without HttpOnly flag set (2)
- ❗ Cookie without Secure flag set (3)
- ❗ Possible sensitive directories (1)
- ❗ Possible virtual host found (2)
- ✅ Broken links (1)
- ✅ Microsoft IIS version disclosure (1)
- ✅ Password type input with auto-complete enabled (3)

Eljumburia detected vulnerability overview

Scan Thread 1 (http://www.amanbank.ly:80/)

Web Alerts (91)

- ❗ Long password denial of service (1)
- ❗ Application error message (12)
- ❗ ASP.NET error message (1)
- ❗ HTML form without CSRF protection (3)
- ❗ Same site scripting (1)
- ❗ Unencrypted __VIEWSTATE parameter (10)
- ❗ User credentials are sent in clear text (1)
- ❗ ASP.NET version disclosure (1)
- ❗ Clickjacking: X-Frame-Options header missing (1)
- ❗ Cookie without HttpOnly flag set (2)
- ❗ Cookie without Secure flag set (4)
- ❗ File upload (2)
- ❗ Login page password-guessing attack (1)
- ❗ OPTIONS method is enabled (1)
- ✅ Broken links (40)
- ✅ GHDB: Typical login page (6)
- ✅ Microsoft IIS version disclosure (1)
- ✅ Password type input with auto-complete enabled (3)

Aman detected vulnerability overview

Using QUALYS

More Results Quick Tour Upgrade Now Entsem Ibrahim 3 Scans Remaining

View by: OWASP Report Patch Report **Threat Report** Print Report

BCD External Host Vulnerability Report 05 November 2015 at 9:32PM (GMT+0200)

41 Vulnerabilities Detected **0** HIGH Risk **23** MED Risk **18** LOW Risk **88** INFO Gathered

https://bcd.ly/
109.78.237.177
bcd.ly
Ubuntu / Linux 3.x
Rescan URL

Filter by: All (41) Level 5 (0) Level 4 (4) Level 3 (10) Level 2 (17) Level 1 (1) Info (88) Search for Title, Category, CVE ID or QID

All Scan Results 1 - 25 of 129

Vulnerability	Severity
SSL Server Allows Anonymous Authentication Vulnerability	High
SSL Server Allows Anonymous Authentication Vulnerability	High
SSL Server Allows Anonymous Authentication Vulnerability	High
ISC BIND Query Processing Denial of Service Vulnerability	Medium
Mail Server Accepts Plaintext Credentials	High
Web Server Stopped Responding	High
Web Server Stopped Responding	High
Mail Server Accepts Plaintext Credentials	High
POP3 Server Allows Plain Text Authentication Vulnerability	High
Slow HTTP POST vulnerability	Medium

SSL Server Allows Anonymous Authentication Vulnerability

QID: 38142 CVE Base: 5.1 Port: 455
CVSS Temporal: 4.1 Category: General remote services
CVE ID: -

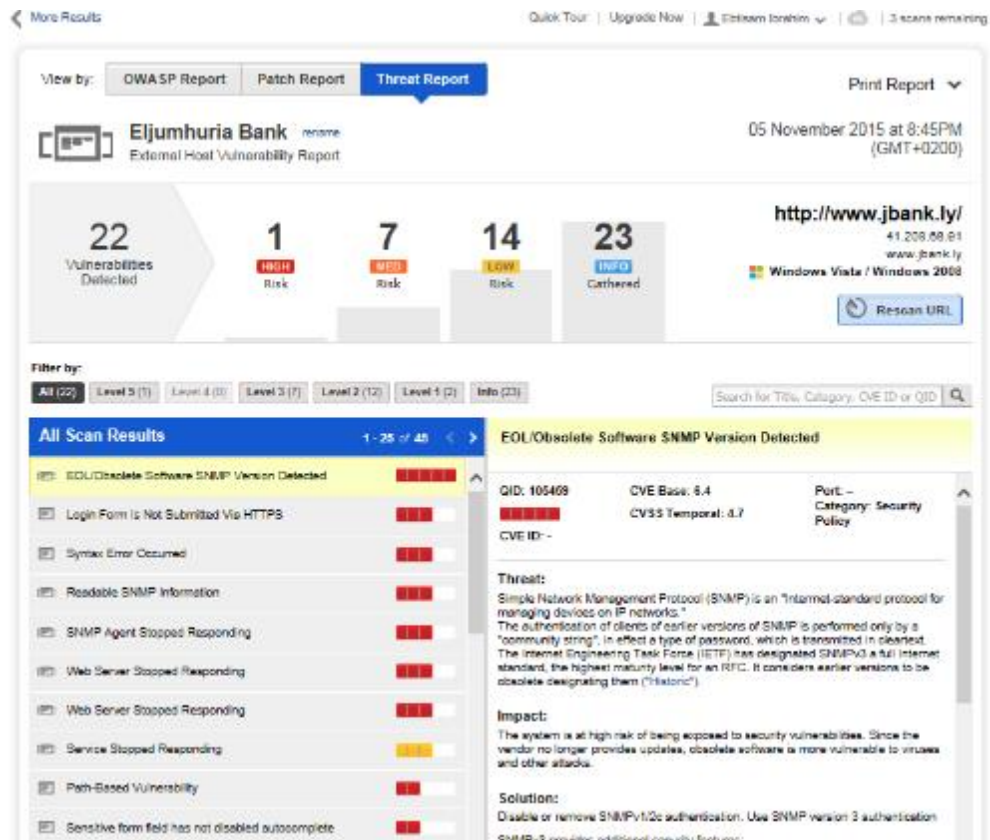
Threat:
The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. Most common Web browsers like Microsoft Internet Explorer, Netscape and Mozilla do not use anonymous authentication ciphers by default.

A vulnerability exists in SSL communications when clients are allowed to connect using no authentication algorithm. SSL client-server communication may use several different types of authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the communications are vulnerable to a man-in-the-middle attack.

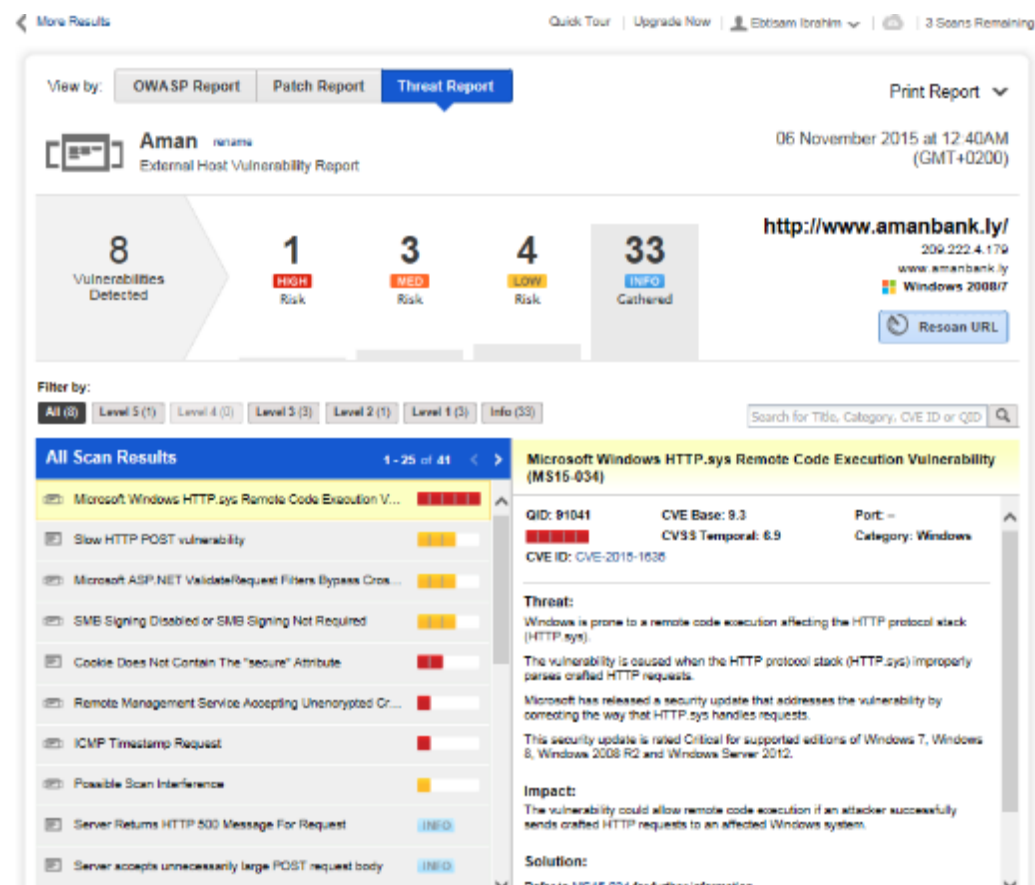
Impact:
An attacker can exploit this vulnerability to impersonate your server to clients.

Solution:
Disable support for anonymous authentication.

BCD vulnerability scan result



Eljumphuria vulnerability scan result



Aman Bank vulnerability scan result

Using Vega

Scan Info		
		
Scan Alert Summary		
High		(None found)
Medium		(3 found)
Local Filesystem Paths Found	1	
PHP Error Detected	1	
Possible XML Injection	1	
Low		(None found)
Info		(106 found)
News Feed Detected	1	
Possible AJAX code detected	14	
Interesting Meta Tags Detected	14	
Cookie Secure Flag Not Set	2	
Cookie HttpOnly Flag Not Set	2	
Character Set Not Specified	67	
Blank Body Detected	6	

BCD vulnerability scan result

Scan Info		
		
Scan Alert Summary		
High		(10 found)
Session Cookie Without Secure Flag	3	
Session Cookie Without HttpOnly Flag	2	
Cleartext Password over HTTP	2	
SQL Injection	5	
Cross Site Scripting	7	
Medium		(18 found)
Local Filesystem Paths Found	18	
Low		(3 found)
Form Password Field with Autocomplete Enabled	2	
ASP/ASPX Error Detected	1	
Info		(69 found)
Unsafe Or Unrecognized Character Set In Response Body	43	
Possible AJAX code detected	16	
Character Set Not Specified	9	
Blank Body Detected	1	

Eljumhuria vulnerability scan result

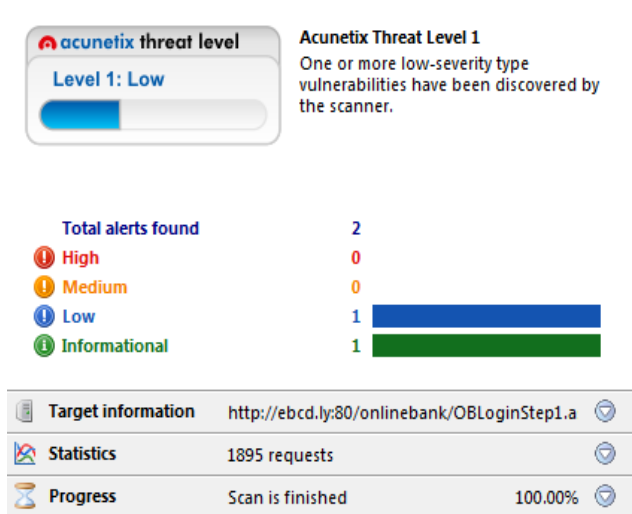
Scan Info		
		
Scan Alert Summary		
High		(10 found)
Session Cookie Without Secure Flag	1	
Cleartext Password over HTTP	1	
Shell Injection	5	
SQL Injection	2	
Bash "ShellShock" Injection	1	
Medium		(1 found)
Local Filesystem Paths Found	1	
Low		(9 found)
ASP/ASPX Error Detected	8	
Form Password Field with Autocomplete Enabled	1	
Info		(89 found)
Interesting Meta Tags Detected	72	
Form File Upload Detected	7	
Blank Body Detected	10	

Aman Bank vulnerability scan result

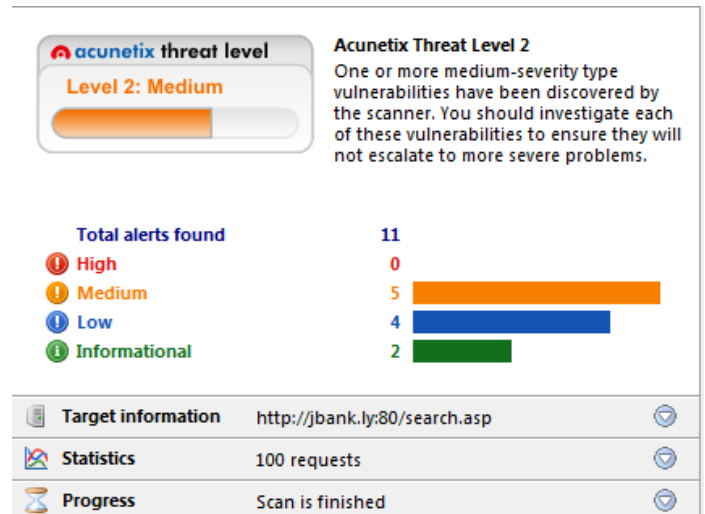
APPENDIX B

Authentication Page Scan Results

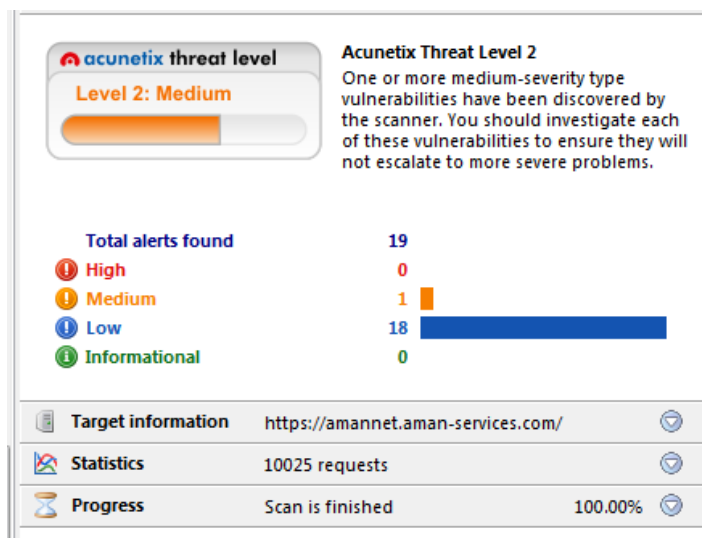
Using Acunetix



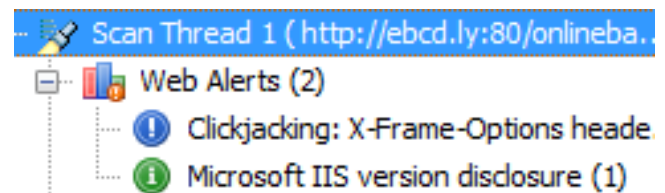
BCD authentication page vulnerability scan result



Eljumbhuria authentication page vulnerability scan result



Aman authentication page vulnerability scan result



BCD authentication page detected vulnerability overview

Scan Thread 1 (http://jbank.ly:80/search.a...

Web Alerts (11)

- HTML form without CSRF protection ...
- User credentials are sent in clear te...
- ASP.NET version disclosure (1)
- Clickjacking: X-Frame-Options heade...
- Cookie without HttpOnly flag set (1)
- Cookie without Secure flag set (1)
- Microsoft IIS version disclosure (1)
- Password type input with auto-comp...

Eljumphuria authentication page detected vulnerability overview

Scan Thread 2 (https://amannet.aman-services.com/)

Web Alerts (19)

- URL redirection (1)
- Clickjacking: X-Frame-Options header missing (1)
- Cookie without HttpOnly flag set (8)
- Cookie without Secure flag set (8)
- Session Cookie scoped to parent domain (1)

Aman authentication page detected vulnerability overview

Using QUALYS

More Results Quick Tour Upgrade Now Ebtisam Ibrahim 3 Scans Remaining

View by: OWASP Report Patch Report **Threat Report** Print Report

Vulnerability Scan External Host Vulnerability Report 06 November 2015 at 1:21PM (GMT+0200)

17 Vulnerabilities Detected 1 HIGH Risk 7 MED Risk 9 LOW Risk 29 INFO Gathered https://www.ebcd.ly/online... 66.148.120.45 www.ebcd.ly Rescan URL

Filter by: All (17) Level 5 (1) Level 4 (0) Level 3 (7) Level 2 (7) Level 1 (2) Info (20) Search for Title, Category, CVE ID or QID

All Scan Results 1 - 20 of 46

Item	Severity
EOL/Obsolete Software: Microsoft SQL Server 2005 (SP0) RTM	High
Windows Remote Desktop Protocol Weak Encryption Met...	High
FTP Server Does Not Support AUTH Command	High
SSL Server Supports Weak Encryption Vulnerability	High
Windows Remote Desktop Protocol Uses Weak Private Key	High
SSLv3 Padding Oracle Attack Information Disclosure Vul...	High
SSL/TLS use of weak RC4 cipher	High
Microsoft Remote Desktop Service Not Using Additional...	High
Cookie Does Not Contain The "secure" Attribute	High
Cookie Does Not Contain The "HTTPOnly" Attribute	High

EOL/Obsolete Software: Microsoft SQL Server 2005 (SP0) RTM Detected

QID: 105371 CVE Base: 10 Port: -
CVSS Temporal: 7.4 Category: Security Policy
CVE ID: -

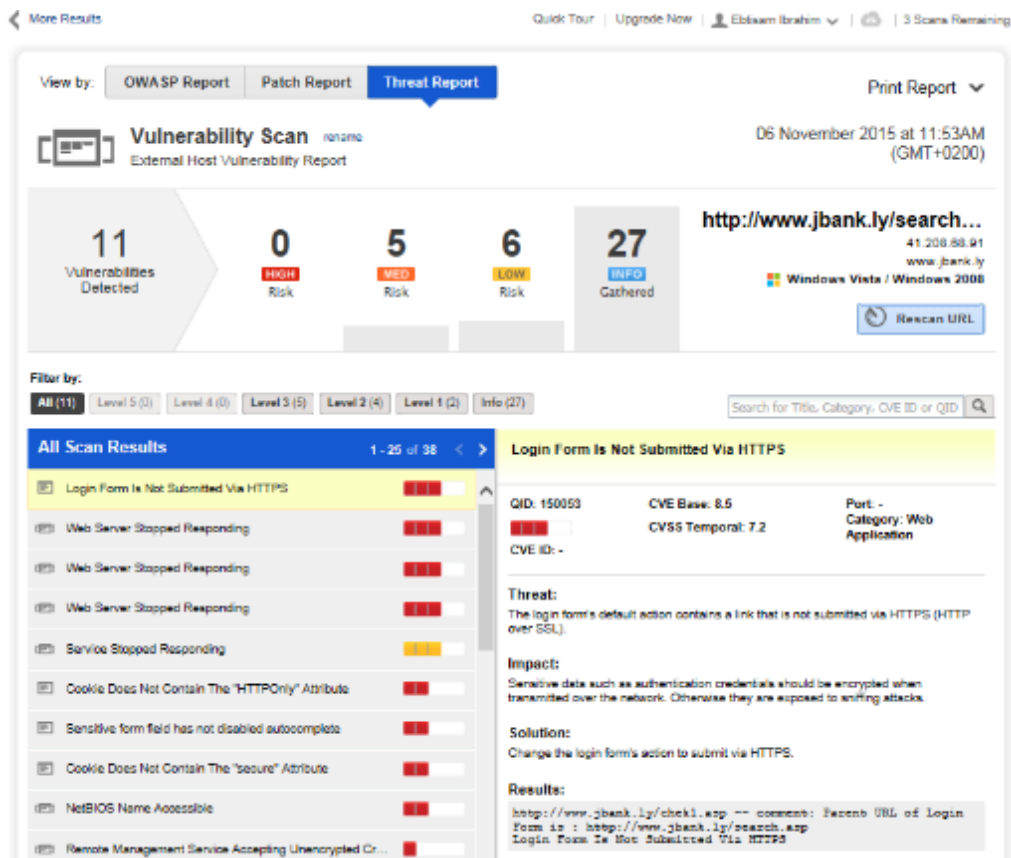
Threat:
Microsoft SQL Server 2005 RTM (SP0) release was detected on the host.
Technical support for this RTM release has ended. No further bug fixes, enhancements, security updates or technical support is available for this release.

Impact:
The system is at high risk of being exposed to security vulnerabilities. Since the vendor no longer provides updates, obsolete software is more vulnerable to viruses and other attacks.

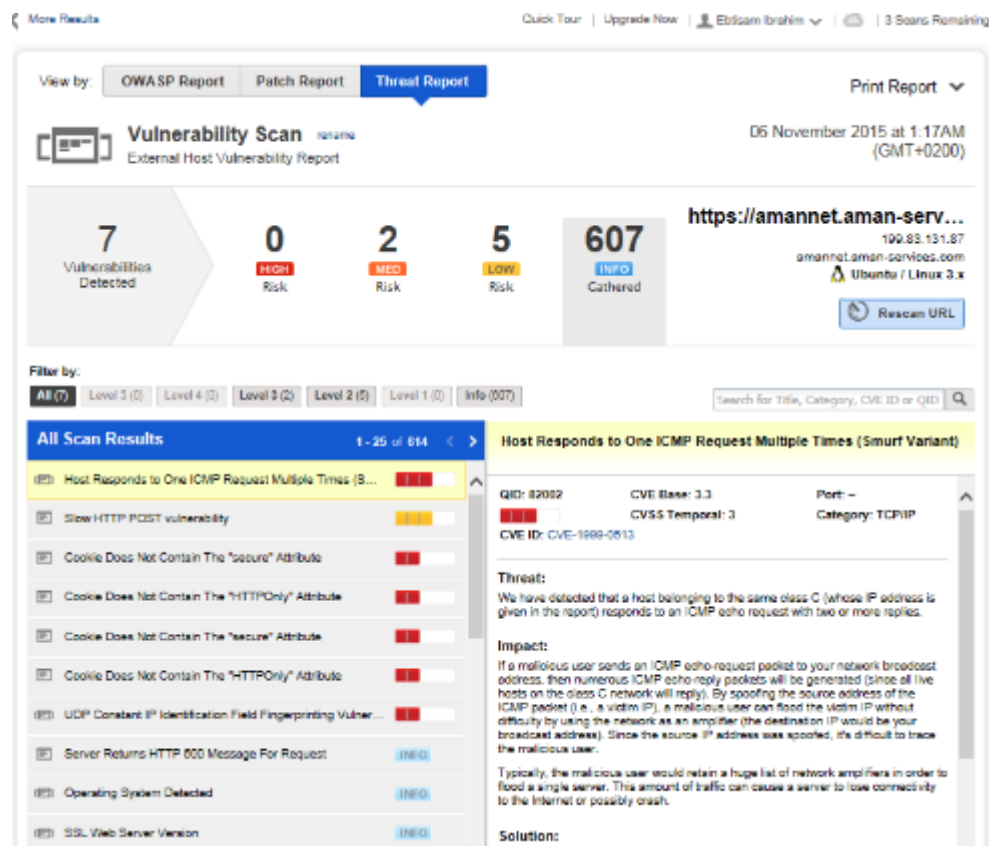
Solution:
Update to the latest service pack or a currently supported service pack.

Results:
9.0.1399

BCD authentication page vulnerability scan result

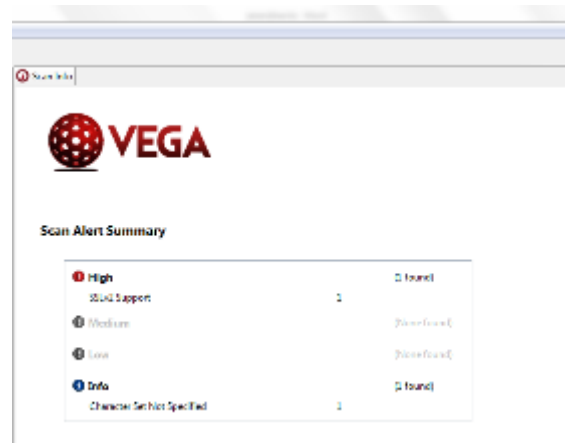


Eljumbhuria authentication page vulnerability scan result

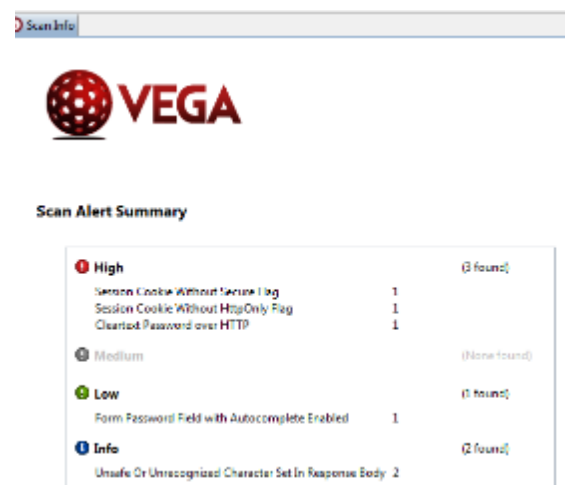


Aman authentication page vulnerability scan result

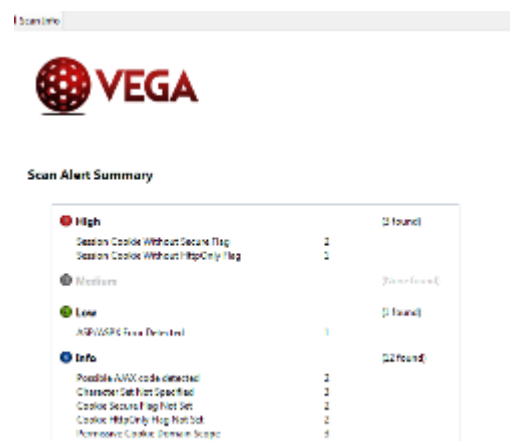
Using Vega



BCD authentication page vulnerability scan result



Eljumbhuria authentication page vulnerability scan result



Aman authentication page vulnerability scan result

APPENDIX C

Bank of Commerce and Development

Dear IT Responsible,

Please dully fill in the check boxes below with ✓ or ✗ as applicable:

Risk management	
Review and update the existing risk assessments to include:	
Changes in the internal and external threat environment	✗
Changes in the customer base adopting electronic banking	✓
Changes in the customer functionality offered through electronic banking	✗
Actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry	✓
Customer Authentication for High-Risk Transactions	
Make sure to use:	
Multifactor authentication is offered mainly to high-risk transaction.	✗
Layered Security Programs	
Program must include:	
Fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response	✗
Use of dual customer authorization through different access devices	✗
Use of out-of-band verification for transactions	✗
Use of "positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account	✗
Enhanced controls over account activities; such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (e.g., days and times)	✗
Internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities	✓
Policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud	✗
Enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels	✓

Enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk	✗
Processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to login and initiating a transaction	✓
Enhanced controls for system administrators who are granted privileges to set up or change system configurations	✓
Effectiveness of Certain Authentication Techniques	
Make sure to use:	
Sophisticated form of device identification technique	✓
Multiple “out of wallet” questions as challenge questions	✗
Customer Awareness and Education	
customer awareness and educational efforts should include:	
An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts with Internet access	✗
An explanation of under what, if any, circumstances and through what means the institution may contact a customer on an unsolicited basis and request the customer's provision of electronic banking credentials	✓
A suggestion that commercial online banking customers perform a related risk assessment and controls evaluation periodically	✗
A listing of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk, or alternatively, a listing of available resources where such information can be found	✗
A listing of institutional contacts for customers' discretionary use in the event they notice suspicious account activity or experience customer information security-related events	✓

Name and Signature	Khawla Swesi- IT Department, Ben Ashour Branch
Date	08/11/2015