Stock Exchange Threat Modeling, EGX as a Case Study

Ehab ElShafei(✉) and Nashwa AbdelBaki(✉)

Nile University, Giza, Egypt
{e.elshafei,nabdelbaki}@nu.edu.eg
http://www.nileu.edu.eg

Abstract. Cyber crime is a growing threat affecting all business sectors. Stock Exchanges, a financial services sector, are not far from it. Trading stocks via Internet exposes the process to cyber threats that might take advantage of a system defect to breach security and cause possible harm. Online Trading websites are protected by various security systems. Digital Certificate, which is based on Secure Socket Layer (SSL) protocol, is an example. This research examines implementation of Digital Certificate in online trading servers. This evaluation helps to identify security weaknesses and take actions for protection improvement.

Keywords: SSL/TLS · Security · Electronic trading · Stock exchange

1 Introduction

Stock Exchange Markets provide a service to trade stocks and bonds. They have multiple roles in the economy [?] such as raising capital for companies, government capital raising for development projects and mobilizing savings for investment. Additionally, it is an indication of the general trend in the economy for a particular country. For many years, stock exchanges were physical locations where buyers and sellers met and negotiated. With the improvement in communication technology in the late 20th century, traders started to transact from remote locations in what became known as electronic trading (etrading).

There are clear indications attest that the electronic crime threat in stock markets is an increasing threat, with the possibility of significant costs [3,4]. Therefore, implementing an effective information security measures and controls has become a critical success factor for all parties (regulators, brokerage companies and individual investors) to ensure a safe environment for electronic trading. Hereby, a threat modeling has to be developed and be followed for optimizing environment security.

Threat modeling is a method for improving security by identifying assets that needs protection and weaknesses. Then defining actions reduce the effects of threats to the system. In stock exchange environment, the web servers are

A.E. Hassanien et al. (eds.), *Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2017*,
Advances in Intelligent Systems and Computing 639, DOI 10.1007/978-3-319-64861-3_19

companies assents that need a protection. Digital Certificate is one of the technologies required to maintain the protection. It is based on Secure Socket Layer (SSL) [6] and Transport Layer Security (TLS) [8] protocols. SSL/TLS protocols are considered the de facto standard for providing secure communication over the Internet. The protocols have evolved over years to fix the weaknesses and drawbacks detected, add protection against discovered attacks and support new cryptographic algorithms that were defined.

Several security assessments should be conducted to make sure that stock exchange markets are aligned with recent cyber threats. Moreover, companies should evaluate their systems and implemented technologies to identify any weakness. Then take actions toward enhancing the protection of their clients' information.

The rest of this paper is organized as following. Section 2 demonstrate the previous studies related to cyber threats in stock exchange. Followed by Sect. 3 which define the threat modeling for this environment. Section 4 introduce SSL/TLS protocols background, the known attacks and deployment best practices. The case study is presented in Sect. 5. The security assessment, its results and discussion are presented in Sect. 6. The conclusion is presented in Sect. 7 along with future work.

2 Preceding Studies

Most of studies that are related to Stock Exchange analyze the markets performance. It provides economic advices and recommendations to investors. Other studies discuss the regulations that protects the trading environment, listed companies and investors, from frauds. In the digital era, there is no enough studies evaluate how vulnerable are stock markets to cyber threats.

This research is an effort to introduce the cyber threats that may target electronic trading in stock markets. It starts with defining a threat modeling, which is discussed in the next section.

3 Threat Modeling

Threat modeling is an endless process that consists of defining assets that needs protection. Followed by, identifying the role of each component with respect to these assets. Then, creating a security profile for each component, identifying prospective threats, prioritizing it. Determine where the most effort should be applied to keep a system secure is the key to threat modeling.

In an online trading environment, web servers are companies assets that need to be protected. Digital Certificate is the standard solution for that purpose. It protects the communication between clients and server. In addition, it provides a mechanism for servers identifications.

As part of the threat modeling, it is important to understand the technical security background, terminologies, attacks and best practices of the selected technology area. The next section introduces The SSL/TLS Protocols.

4 SSL/TLS Protocols Background

Security was not taken into consideration in Internet design. The main aim was sharing information between different parties. As Internet grows, all information sent over open network could be eavesdropped, tampered, or forged. The development history is introduced in [16,17]. SSL 1.0 was not released to the public. A number of security flaws discovered in SSL 2.0, which was released in 1995, led to the design of SSL 3.0 [6] that was released in 1996.

IETF adopted it and released Transport Layer Security (TLS) in 1999 as an Internet standard RFC2246 [8]. After seven years, TLS 1.1 defined in RFC4346 [18]. In 2008, TLS 1.2 was defined in RFC5246 [19] which is the latest release. All TLS versions were further refined in RFC6176 [20] by removing their backward compatibility with SSL 2.0.

Nowadays, SSL/TLS are the dominant protocols for securing network communication. This section introduces how do they work, followed by their known attacks. In the end, the deployment best practices are presented.

4.1 SSL/TLS Known Attacks

During the 20-years of SSL development, several defects were found. They were fixed due to the flexible architecture of SSL. This section lists the known attacks [21] that are related to this research (1) Heartbleed (2) BEAST (3) POODLE (SSL/TLS) (4) Attacks on RC4 algorithm (5) owngrade attack.

Applying SSL/TLS deployment best practices is the best way to overcome these issues.

4.2 SSL/TLS Deployment Best Practices

When SSL/TLS is configured improperly, a false impression of security is given where the communications could be at risk. This section presents deployment best practices, that are related to this research topics, introduced by [22,23] to ensure secure communication.

Extended Validation (EV) certificates are issued only after thorough offline checks. EV certificates are more difficult to forge, provide slightly better security, and browsers present them in a better treatment.

Secure Protocols: SSL/TLS family consists of five protocols. (1)&(2) SSL2/3 are insecure and must not be used. (3) TLS1 when used with careful configuration, it can almost be made secure. (4)&(5) TLS 1.1/1.2 should be the main protocols as it offer important features that are unavailable in earlier versions.

Perfect Forward Secrecy: PFS [24] is a protocol feature that enables secure conversations, which are not dependent on the server's private key. If a server is configured to support forward secrecy, then a compromise of its private key can't be used to decrypt past communications recorded by third party.

Client-Initiated Renegotiation: Renegotiation [25,26] allows parties to stop exchanging data in order to renegotiate how the communication is secured.

The server may need to do it, but there is no known need for client to. It may expose the server to Man-in-the-middle (MITM) attack [27]. Thus, it should be disabled. In addition, insecure server renegotiation should be disabled in result of discovering an authentication gap vulnerability in Nov 2009.

TLS compression: compression [?] can be used by attackers to decrypt part of data transmitted. As very few web browsers support TLS compression, it is unlikely that clients will experience any performance issues by disabling it on the servers.

HTTP Strict Transport Security: HSTS [28] does not allow any insecure communication with the web site that uses it. It achieves this goal by automatically converting all plain-text links to secure ones. Adding support for HSTS is the single most important improvement for the SSL security of the web sites. New sites should always be designed with HSTS in mind and the old sites converted to support it wherever possible.

5 Case Study: The Electronic Trading in the Egyptian Exchange (EGX)

The Egyptian Exchange (EGX)[29] is one of the oldest stock markets established in the Middle East. It traces its origins to 1883. It introduces the online trading via the Internet in 2006. The regulation for the electronic and online trading were issued by The Egyptian Financial Supervisory Authority (EFSA) [30]. The regulation presents IT Infrastructure requirements (systems, servers' roles, network (WAN), and security) as with other requirements, which a brokerage company must implement to get a license after inspection.

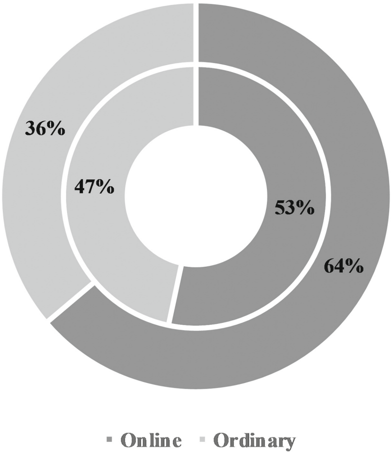


Fig. 1. Trading methods

5.1 Electronic Trading Trends

It is worthy to know the weight of online trades compared to ordinary trades. This helps identifying the risk and estimating the losses of being under attack. Figure 1 compares the trading methods for Q4Y16 according to data published by EGX. The outer ring shows that the online trades value is 87.5 Billion EGP, which represents 53% of all traded value. Whereas, the online trades number is approx. 2.6 Million trades, which represents 64% of all trades number as presented by the inner ring.

The predicament is, What if cyber attacks targeted wide range of brokerage companies in an organized way! The least loss would be preventing investors for trading electronically. The worst-case scenario is executing unauthorized orders to create a confusion state. Subsequently, it could lead to market crash, where sudden dramatic decline of stock prices result a significant loss of investors' wealth. The investors lose the trust in the stock market and/or the stock market lose its reputation. Protecting the online trading process is the protection for the whole Egyptian stock market from unfortunate events.

6 SSL/TLS Digital Certificates Assessment

This assessment addresses the online trading regulation [30] point 11, concerned of websites digital certificates. Brokerage companies have to deploy a valid digital certificate in their online trading web servers for encryption and for identification.

It addresses many security aspects such as "Confidentiality". Secure communication ensures that no other parties know the transmitted data, which is one state of information lifecycle. It provides protection against many attacks such as eavesdropping and man-in-the-middle attacks. Another security aspect is "Availability". SSL certificate provides a mechanism for clients to identify the correct website which is a protection against phishing.

The Selection criteria is the list of brokerage companies that executed online trading orders in Q4Y16. According to EGX statistics, 103 companies executed online trading orders.

SSL server test approach consists of four steps (1) Look at a certificate to verify that it is valid and trusted. (2) Inspect server configuration in three categories a. Protocol support, b. Key exchange support, c. Cipher support. (3) Combine the categories scores into an overall score (from 0 to 100). Category with 0 will push the overall score to 0. Then, a letter grade is given. (4) Apply a series of rules to handle some server configuration aspects that cannot be expressed via numerical scoring. Rules may reduce the grade or increase it.

Several parameters are collected by this assessments: (i) Secure Protocols supported by websites, (ii) whether the website supports (Secure Renegotiation, Secure Client-Initiated Renegotiation, TLS Compression, Forward Secrecy, and Strict Transport Security (HSTS)) or not. Finally, (iii) the overall website rating.

The websites are assessed between March 26 and 29, 2017. The data analysis results are presented in next section.

6.1 Assessment Results

It is found that from 103 websites, only 85 (82.5%) are available for assessment, whereas 18 (17.5%) websites cannot be evaluated. All upcoming figures are for evaluated websites only.

The first result of data analysis is concerned about Secure Protocols supported by websites. Figure 2 shows that the most secure protocols TLS 1.2 and TLS 1.1 are supported by approx. 35% of websites. TlS 1.0 is supported by 98.8%, almost all websites. Furthermore, The insecure protocols SSL 3 & SSL 2 are supported by 81% and 56.5% respectively of websites. Analysis shows that only 14% of websites do support secure protocols TLS 1.x and do not support insecure SSl x.

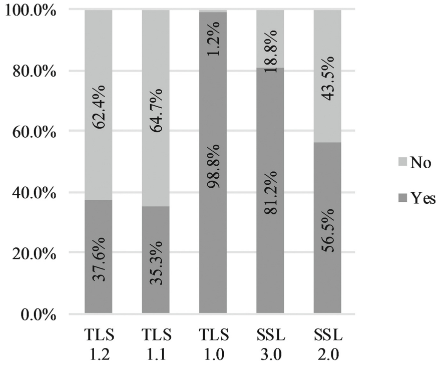


Fig. 2. Supported secure protocols

Concerning Attacks, Fig. 3 presents that 97.6% and 94.1% are not vulnerable to Heartbleed and BEAST respectively. Moreover, almost 70% of website are not vulnerable to POODLE (SSL & TLS). Furthermore, 90% of websites are vulnerable to attacks on RC4. Finally, almost 80% of websites are vulnerable to protocol downgrade attack.

Figure 4a presents various features that are discussed in Sect. 4.2. (1) Only 6% of websites use Extended Validation (EV) certificate. (2) "Secure Renegotiation" is supported by 90% of websites. While (3) "Client-Initiated Renegotiation" is not supported by 94%. (4) "TLS compression" is not supported by all websites. (5) "Strict Transport Security" are not supported by almost 98% of websites. Lastly, Fig. 4b shows that "Forward Secrecy" is supported by 50% of websites, half of them use weak key exchange.

The overall rating for the websites is shown in Fig. 5. It is found that almost 35% of websites have good overall rate (A, B & C). While 64% of websites have F grade.

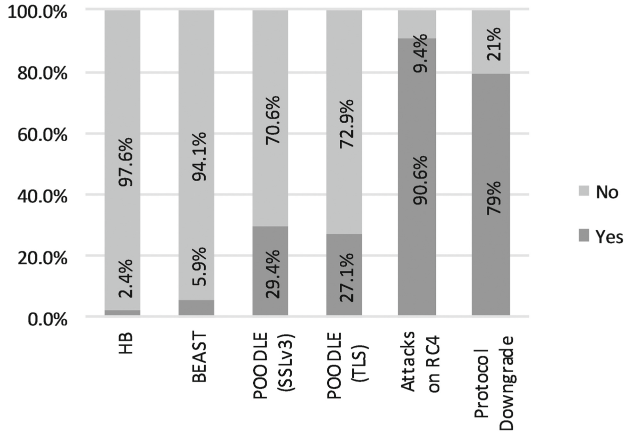
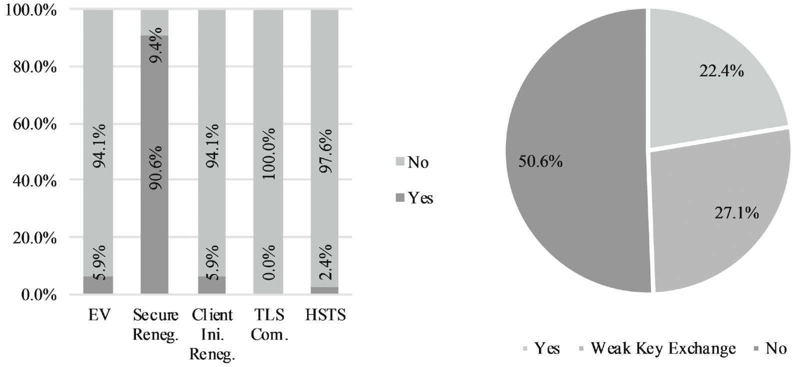


Fig. 3. SSL/TLS known attacks



(a) Various Features

(b) Forward Secrecy

Fig. 4. SSL/TLS best practices

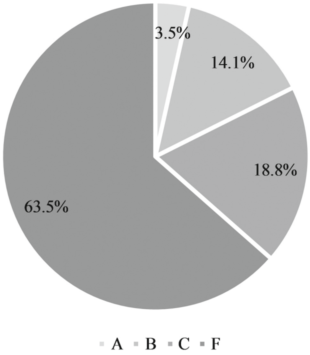


Fig. 5. Websites overall rating

6.2 Assessment Discussion

The results shed the light on critical issues.

Only 14% of websites may be considered secure as they do support TLS 1.x protocols and do not support SSL x. This also implies, that 86% of websites are vulnerable to protocol downgrade attack. Though all modern Internet browsers prefer to use TLS 1.0, which is supported by all websites, a hacking tool or a MiTM attacker may force clients browsers to use SSL 2.0, as present in Sect. 4.1, then take advantage of its weak to attack clients' sessions. It is worth mentioning that these attackable websites are used for trading 63% of EGX trading value, more than 55 Billion EGP.

The websites that have EV certificate are only 6% of websites, Thus, Only their clients are considered protected from Phisihing attacks. This is very poor rate. Though, [31] concluded that some users may neglect signs placed outside of their attention such as EV certificate does. Educating clients, in order to pay attention to these notification, is the most recommended action by Anti-Phisihing Working Group (APWG) to fight it. Brokerage companies should be encouraged to use EV Digital Certificates over standard type.

In addition, "Strict Transport Security" (HSTS) is not supported by almost all websites. This could be used by an attacker to gain unauthorized access to clients' information, the same way as LinkedIn vulnerability found in June 2014 [32]. The poor HTTPS/SSL implementation allows an attacker to intercept a user's communication and to attempt MitM attack against the website as presented in Sect. 4.1.

"Forward Secrecy", which is not supported by 50% of websites, could be led to ravel clients' trading history if (i) the private key used by this websites is identified by an attacker (ii) this attacker was recording the clients' encrypted sessions. Therefore, all websites should support "Forward Secrecy".

7 Conclusion

The developed threat modeling for stock exchange determine that the most effort should be applied to online trading servers. Digital Certificates, which are based on SSL/TLS protocols, are considered as the countermeasures to prevent, or mitigate the effects of threats to the environment.

The results emphasize that there is a particular lack of attention towards information security as demonstrated in the case study. The regulation, as a high level document, is good if it is considered as baseline. Thus, companies cannot depend on it for security technologies deployment. Guidelines should be released to help implementing technologies, related to regulation, best practices. Moreover, the regulator should monitor the companies constantly and pay attention to those who violate the regulation.

Needless to say that more assessments needed to complete the whole picture. These assessments aim to make sure that all regulation points are well covered by brokerage companies. Regulation point 3 is an example. Do brokerage companies follow firewalls deployment best practices? Do they maintain and update their technologies (operating systems, services such as mail & web, database engines, network equipment, antivirus, firewall, IPS, ... etc.) to the latest release that cover volubilities found in the previous versions or not? Another subject is "Software Security". Is the trading web application used is protected from Buffer Overflow, SQL injection ... etc.? All these assessment are considered as future work.

References

1. Ngare, E., Nyamongo, E.M., Misati, R.N.: Stock market development and economic growth in Africa. J. Econ. Bus. **74**, 24–39 (2014)
2. Ayadi, R., Arbak, E., Naceur, S.B., De Groen, W.P.: Financial development, bank efficiency, and economic growth across the Mediterranean. In: Economic and Social Development of the Southern and Eastern Mediterranean Countries. Springer, pp. 219–233 (2015)
3. Tendulkar, R.: Cyber-crime, securities markets and systemic risk. In: IOSCO Staff Working Paper, pp. 3–11 (2013)
4. Rashid, F.Y.: Cyber attacks against stock exchanges threaten financial markets: Report (2013). http://www.securityweek.com/cyber-attacks-against-stock-exchanges-threaten-financial-markets-report
5. Shostack, A.: Threat Modeling: Designing for Security. Wiley, New York (2014)
6. Frier, A., Karlton, P., Kocher, P.: The SSL 3.0 protocol. Netscape Commun. Corp. **18**, 27–80 (1996)
7. Barnes, R., Thomson, M., Pironti, A., Langley, A.: Deprecating secure sockets layer version 3.0. Technical report, Internet Engineering Task Force (2015)
8. Dierks, T., Allen, C.: The TLS protocol, version 1.0. The Internet Engineering Task Force (1999)
9. Polk, T., McKay, K., Chokhani, S.: Guidelines for the selection, configuration, and use of transport layer security (TLS) implementations. NIST Spec. Publ. **800**(52), 32 (2014)
10. Hamid, K., Suleman, M.T., Ali Shah, S.Z., Akash, I., Shahid, R.: Testing the weak form of efficient market hypothesis: empirical evidence from Asia-Pacific markets. Int. Res. J. Finan. Econ. **58**, 121–133 (2010)
11. Fenghua, W., Zhifang, H., Zhifeng, D., Xiaoguang, Y.: Characteristics of investors'risk preference for stock markets. Econ. Comput. Econ. Cybern. Stud. Res. **48**(3), 80–99 (2014)
12. Coffee Jr., J.C., Sale, H., Henderson, M.T.: Securities Regulation: Cases and materials. Foundation Press, New York (2015)
13. Hussain, S., Kamal, A., Ahmad, S., Rasool, G., Iqbal, S.: Threat modelling methodologies: a survey. Sci. Int. (Lahore) **26**(4), 1607–1609 (2014)
14. Alsaadi, E., Tubaishat, A.: Internet of things: features, challenges, and vulnerabilities. Int. J. Adv. Comput. Sci. Inf. Technol. **4**(1), 1–13 (2015)
15. Andrea, I., Chrysostomou, C., Hadjichristofi, G.: Internet of things: security vulnerabilities and challenges. In: 2015 IEEE Symposium on Computers and Communication (ISCC). IEEE, pp. 180–187 (2015)
16. William, S.: Cryptography and Network Security, 4/E. Pearson Education India, New Delhi (2006)
17. McKinley, H.L.: SSL and TLS: A Beginners' Guide. SANS Institute (2003)

18. Dierks, T., Rescorla, E.: The transport layer security (TLS) protocol, version 1.1. The Internet Engineering Task Force (2006)
19. Dierks, T., Rescorla, E.: The transport layer security (TLS) protocol, version 1.2. The Internet Engineering Task Force (2008)
20. Turner, S., Polk, T.: Prohibiting secure sockets layer (SSL) version 2.0. The Internet Engineering Task Force (2011)
21. Sheffer, Y., Holz, R., Saint-Andre, P.: Summarizing known attacks on transport layer security (TLS) and datagram TLS (DTLS). Technical report, The Internet Engineering Task Force (2015)
22. Ristic, I.: Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications. Feisty Duck, London (2013)
23. Seltzer, L.: Best practices and applications of TLS/SSL. https://www.symantec.com/content/en/us/enterprise/white_papers/b-best-practices-applications-of-tls-ssl_WP.pdf
24. Huang, L.S., Adhikarla, S., Boneh, D., Jackson, C.: An experimental study of TLS forward secrecy deployments. IEEE Internet Comput. **18**(6), 43–51 (2014)
25. Rescorla, E., Ray, M., Dispensa, S., Oskov, N.: Transport layer security (TLS) renegotiation indication extension. Internet Engineering Task Force (IETF) (2010)
26. Giesen, F., Kohlar, F., Stebila, D.: On the security of TLS renegotiation. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM, pp. 387–398 (2013)
27. Prentow, T.S., Krarup, M.V.: MITM attacks on SSL/TLS related to renegotiation (2009)
28. Hansen, R.: Strict communications transport security, uS Patent App. 14/172,899 (2014). https://www.google.com/patents/US20140250296
29. EGX Egyptian exchange (2017). http://www.egx.com.eg
30. EFSA. Egyptian financial supervisory authority (2017). http://www.efsa.gov.eg
31. Dhamija, R., Tygar, J.D., Hearst, M.: Why phishing works. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, pp 581–590 (2006)
32. Khandelwal, S.: Millions of linkedin users at risk of man-in-the-middle attack (2014). http://thehackernews.com/2014/06/millions-of-linkedin-users-at-risk-of.html