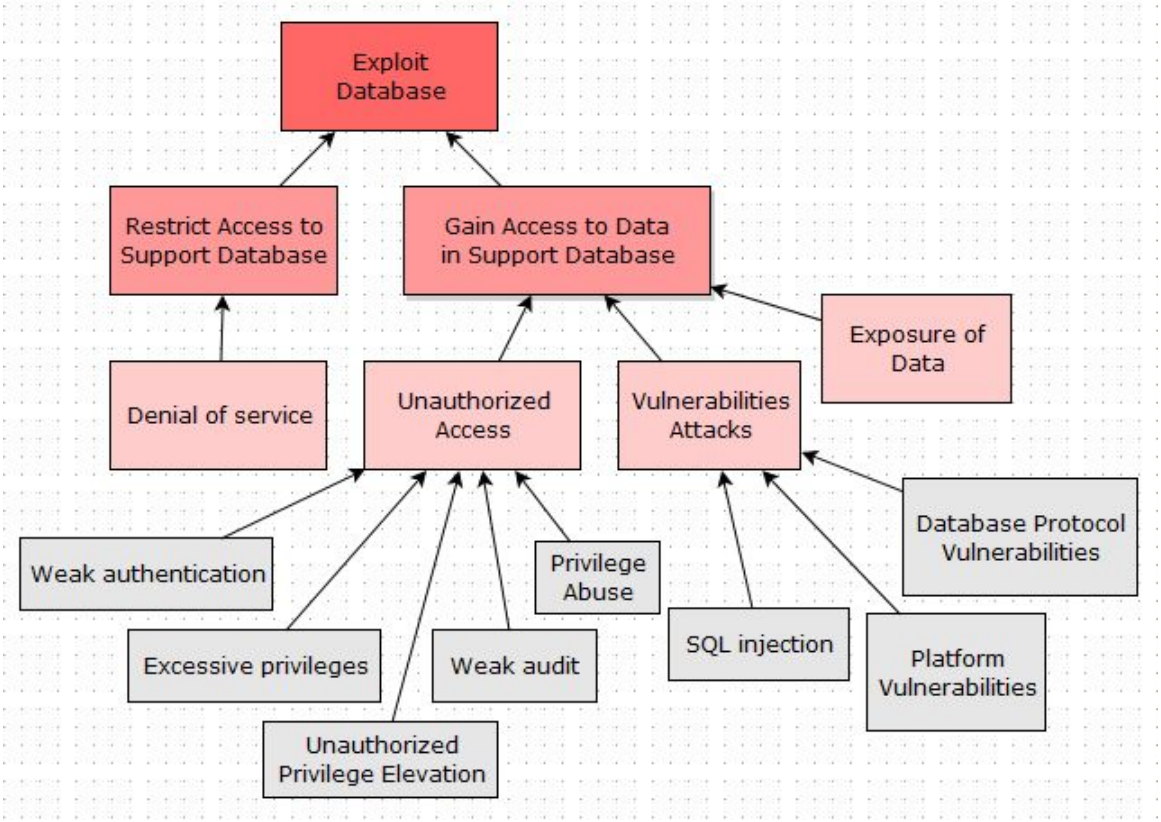
CS4203 Assessment 2
Threats and Mitigation

Student ID: 080010830

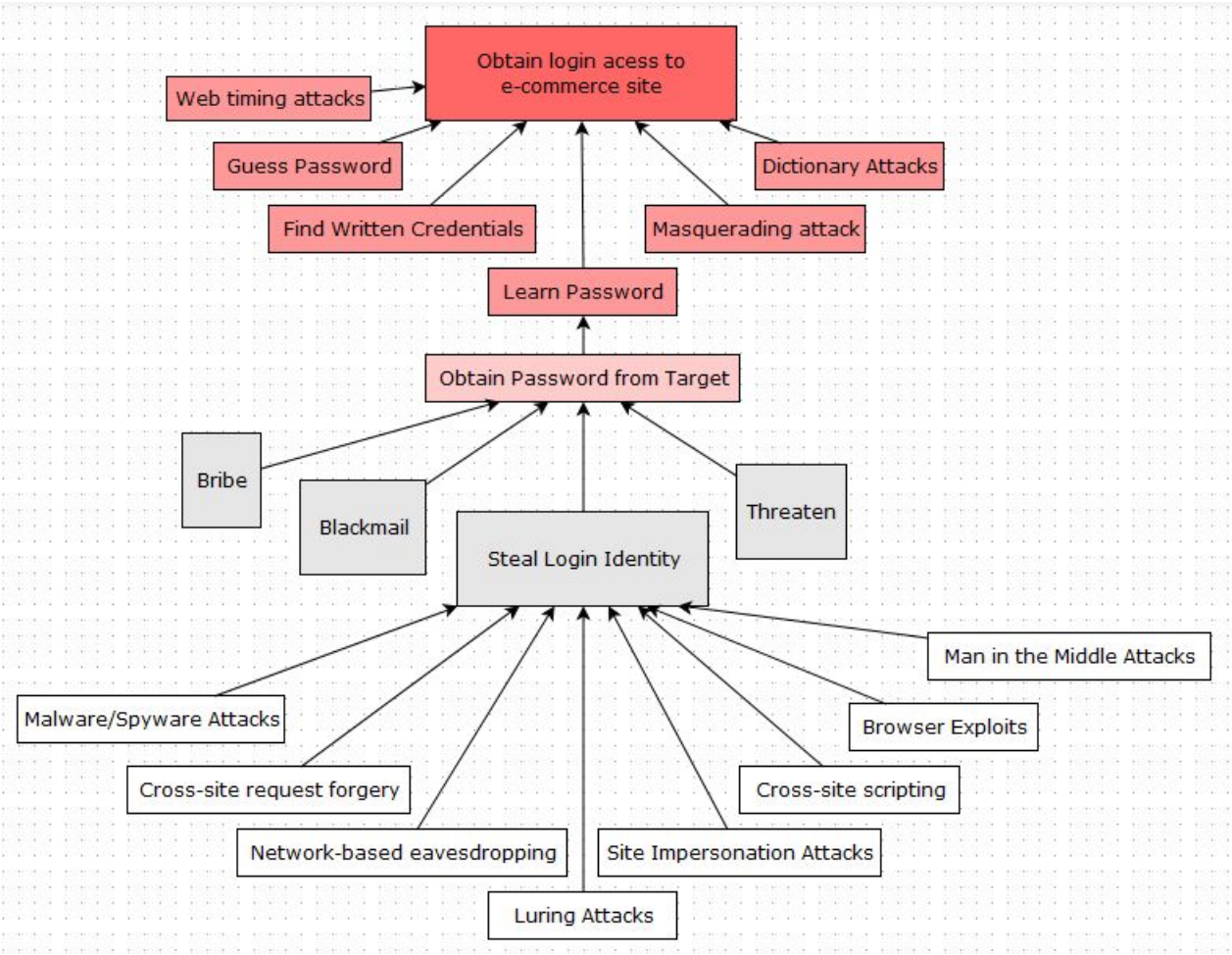
April 26, 2012

1 Threat Trees

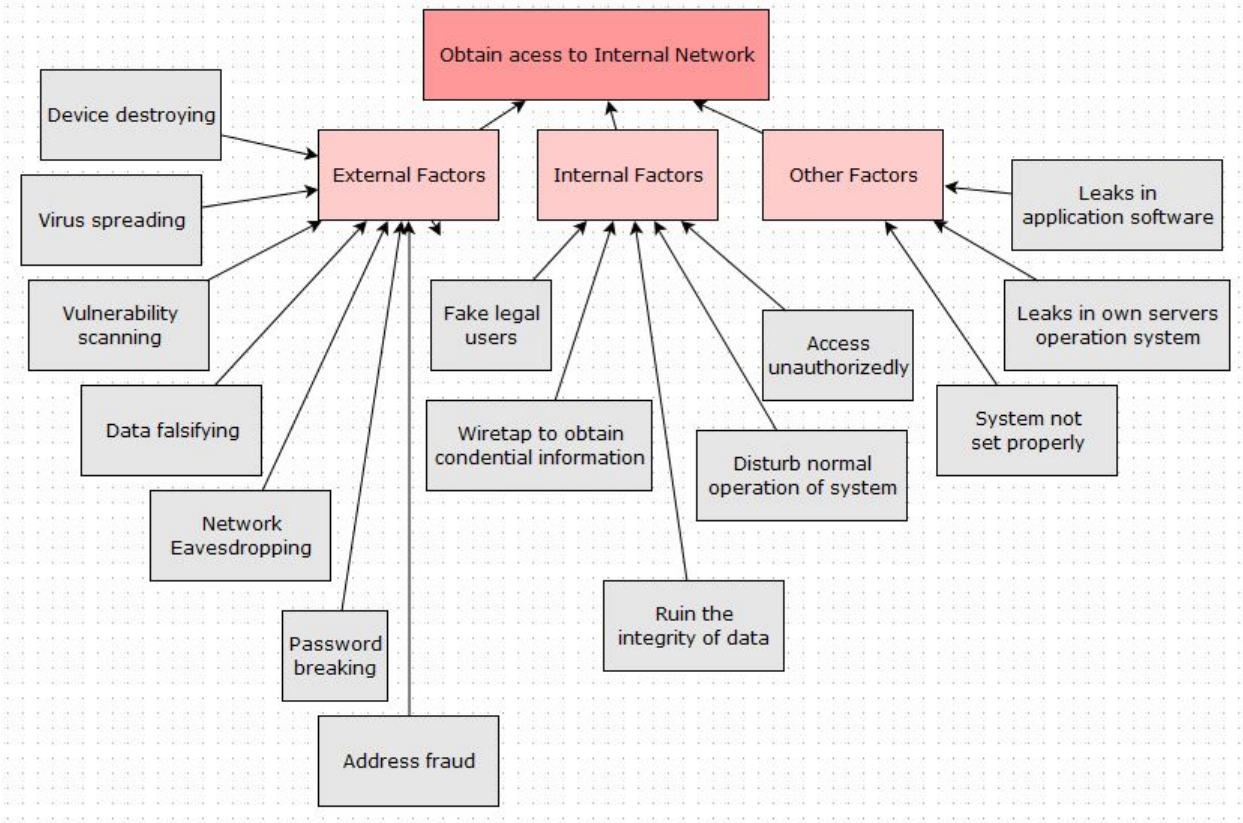
1.1 Threat Tree for the Database



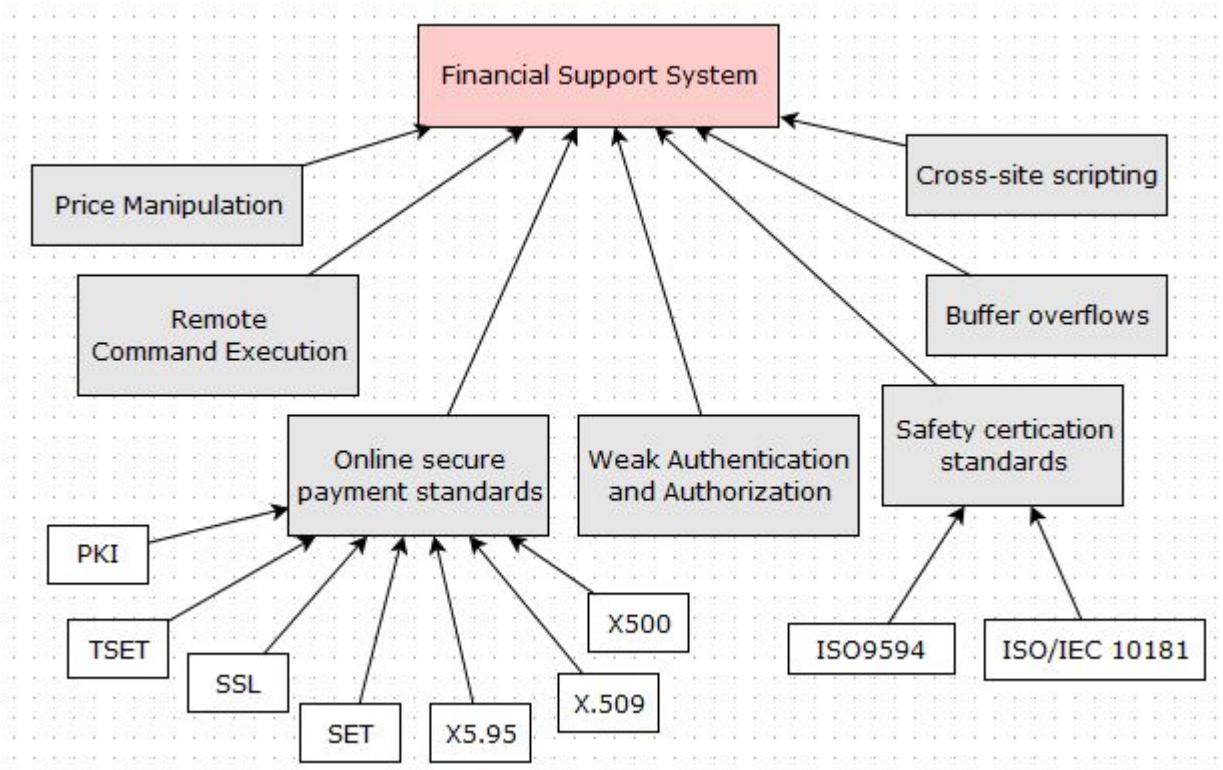
1.2 Threat Tree for the Login Access to E-commerce site



1.3 Threat Tree for the Internal Network



1.4 Threat Tree for the Financial Support System



2 Report

Word count: 1563

2.1 Overview of Techniques and Problems

In this section we perform an overview of techniques and problems from the perspective of a security specialist, constantly considering that the resulting system must be ready for online trading. In the case of an e-commerce site, the communication between client and server happens via the web, thus it is vital to have client-side security, server-side security, and secure transmission of data [1] in consideration, which represent diverse challenges for security [2]. Thus, we focus on addressing the most likely attack points such as the support database, internal network, financial support system and login identities; always referencing current research.

2.2 Security of Support Database

The various components of Database Management System (DBMS) should guarantee data protection. It must provide data confidentiality from its access control mechanism; it should have several well defined authorization states to control access; it should use encryption techniques to ensure data confidentiality when data is transmitted over a network or in the context of outsourced data management; and it should use techniques – such as machine learning techniques – that protect against denial-of-service (DoS) attacks to ensure data availability [3, 4]. The dabase should thus "provide stable storage for security-related data objects" [1], including cryptographic keys, customer transactional data and user information. Furthermore, an e-commerce site will most likely have an ever increasing amount of data to store, thus outsourcing is a real possibility due to its low rate price. The problem with this is that the external server might not be fully trusted. Several solutions were proposed in literature [5, 6, 7] and most agreee that using cryptography is an effective solution to protect data. Thus, by applying these security measures it will make it harder for a possible attacker to access, steal or modify any data [1] from the database.

2.2.1 Access control mechanisms

In terms of access control mechanisms there are mainly two [8] models, namely *i)* Classical Access Control Models, and *ii)* Credential-Based Access Control.

Classical Access Control Models include *i)* Discretionary Access Control (DAC) that bases the decisions on users' identifiy, *ii)* Mandatory Access Control (MAC) that bases the decisions on mandated regulations defined by a central authority and *iii)* Role-Based Access Control (RBAC) that bases the decisions on the roles played by users in the models.

Nonetheless, in an open and dynamic scenario such as an e-commerce site it is not possible to apply classical access control models, thus a better solution is to use *Trust Management* [9] (Credential-Based Access Control). This solution allows for public keys to be bound to authorizations so that credentials have the possibility of being used to illustrate specific delegations of trust among keys. Furthermore, the security level can be increased with the introduction of digital certificates as long as they are certified by a trusted entity.

2.2.2 Encryption techniques

Encryption techniques such as File-System Encryption, DBMS Encryption, Application Encryption and Encryption at the Client are easy but costly to deploy, and they also have performance overheads [4]. Moreover, copyright protection for the database can be provided by using relational database watermarking. This means that even if the attacker manages to copy the watermarked relational data, the content will still be unreadable due to the decryption algorithm necessary for its decoding [1]. Furthermore, steganography can be used so the encrypted watermarked relational database can be hidden in an image.

2.3 Security of Internal Network

In terms of the security of an internal network it is vital to ensure protection from external and internal threats.

External factors to threaten network security include *i)* vulnerability scanning, *ii)* password breaking, *iii)* network eavesdropping, *iv)* data falsifying, *v)* address fraud, *vi)* virus spreading and *vii)* device destroying.

Internal factors to threaten network security include *i)* access unauthorizedly, *ii)* fake legal users, *iii)* ruin the integrity of data, *iv)* disturb normal operation of system, and *v)* wiretap to obtain confidential information.

Other factors such as leaks in our own servers operation system, the fact that the servers system was not set properly, and leaks in application software also pose a huge threat to the security of the internal network. Moreover, the network topology is also an important factor due to the fact that if only one system is connected to the Internet then a potential attack that comes from there will certainly go through that same system. Furthermore, the security for an internal network also has to start in each and every user of this network, if a careless user does not put enough effort into protecting his computer system then a potential threat might spread from there to the other computers in the network [10]. Varian [11] concluded that "the effort of each user (or player) is assumed to be equally important to all other users".

Thus, this system should be equipped with intrusion prevention systems, intrusion detection systems, firewalls and anti-virus [12].

2.4 Security of Financial Support System

The security of the financial system for an e-commerce site is divided into two categories, *i)* online secure payment standards such as "PKI, SSL, SET

[1, 13], X5.95 (Account Digital Signature Standard), X.509 (Certificate E-Commerce Payment standards) and X500 (Electronic publication directory standard)" [13], and *ii)* safety certification standards such as "ISO9594 (Key identification criteria) and ISO/IEC 10181 (Security frameworks for open systems)" [13].

SET is one of the most common standard security protocols for online transactions [14, 15, 16, 17] and its goal is to "ensure the safety of the information flow between the various entities in the security flow" [13]. Thus, it ensures the protection of information confidentiality, data integrity and authentication.

Nonetheless, an improved protocol named TSET (Token based Secure Electronic Transaction) was suggested by Borgohain et al. [18]. The TSET protocol aims to provide end-to-end security, together with a trust evaluation mechanism, and a grading mechanism. Their aim is to make the trustworthiness of merchants known and improve the quality of service, features that SET does not possess [19, 20].

2.5 Security of Login Identities

Two-way certificate authentication should be used to ensure the legitimacy of a user which allows the service to only give access when the user is validated. In terms of authentication it is important to encrypt and salt the password, this means that the password should be converted into a cipher and that a random string of characters should be attached to it before hashing [1]. When the password is changed it is important to also change the salt.

It is also important that the data transmitted between the e-commerce site and the user is encrypted through the whole period that the user is connected to the system, so that it is very difficult for the attacker to obtain the message from the network. This can be achieved by randomly generating an encryption key for each user session [1].

2.5.1 User Privacy Protection

Bertino et al. [3] argue that "data should be used only for the purposes sanctioned by the user and not misused for other purposes". Thus, the Secure Electronic Transaction (SET) protocol should be used to protect user privacy. Moreover, if dual digital signature technology [13] is used it will enable for encrypted transmissions of data and allow two different receivers to be independently connected to two pieces of information.

2.6 Discussion & Recommendation

Typically, problems in security are often associated with "unauthorized data observation, incorrect data modification, and data unavailability" [3]. In simple terms, unauthorized data observation is a result of an exposure to information to which users are not supposed to have access; incorrect data modification may or may not be intentional and it can result in an incorrect database state; finally, data unavailability happens when data is not accessible when needed. Thus, to assure that the e-commerce solution is secure all the previous problems need to be addressed. So the following requirements must be met *i)* data privacy, *ii)* data integrity, *iii)* availability, *iv)* authentication of sender and recipient, and *iv)* authorization of legitimate users to information [3, 1].

The Internet is known as a constant source of new threats and attacks [21, 18, 22], thus an e-commerce site should be released as a whole because it is part of a complex system of advanced technologies coordinated with a consciousness of protection mechanisms [23]. As an example, users can be affected both in terms of privacy and integrity by computer viruses, loss of machine, and line taps, among other threats. The network can suffer from sniffing, theft of data, tapping or message alteration; and the server can experience DoS attacks, hacking, and theft of data, among many other issues; the database can also suffer from sniffing attacks, and many other attacks that can result in the theft, copying and/or alteration of data [1].

Possible recommendations include *i)* taking advantage of software and hardware equipment such as routers and firewalls in order to create several barriers between clients and servers to ensure network security, *ii)* improving operating system security by using some simple strategies, such as shutting off the OS default sharing, deleting non-essential network protocol and service, enabling security strategies, enabling account management, eliminating pagefiles, eliminating dump files, updating the system frequently and implementing account lock mechanism; *iii)* improving the network protocol by restricting users from opening multiple accounts, setting restrictions on the length and complexity of user accounts opened, checking journals in order to keep up-to-date with suspicious incidents, shutting off irrelevant ports and services, deleting Internet service supervisors and preventing illegal intrusion by applying IP rules; *iv)* finally, it is crucial to educate the people responsible for network management and programmers because they do not understand enough about network security to protect it against threats and attacks.

Bibliography

[1] P.B. Rane, BB Meshram, G.S. Kumar, P.P. Reddy, M.S. Swamy, S. Gupta, EM Srinivasan, K. Ramar, A. Suruliandi, M. Grs, et al. Application-level and database security for e-commerce application. *International Journal of Computer Applications*, 41(18):1–5, 2012.

[2] T.E. Lindquist. Security considerations for distributed web-based e-commerce applications in java. In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, pages 5–pp. IEEE, 2002.

[3] E. Bertino and R. Sandhu. Database security-concepts, approaches, and challenges. *Dependable and Secure Computing, IEEE Transactions on*, 2(1):2–19, 2005.

[4] E. Shmueli, R. Vaisenberg, Y. Elovici, and C. Glezer. Database encryption: an overview of contemporary challenges and design considerations. *ACM SIGMOD Record*, 38(3):29–34, 2010.

[5] K.P. Birman. *Reliable Distributed Systems: Technologies, Web Services, and Applications*. Springer-Verlag New York Inc, 2005.

[6] G. Orlando. Reliable elliptic curve cryptography computation, June 22 2010. US Patent 7,742,596.

[7] S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, and M. Blaze. One-way cryptography. *Security Protocols XIX*, pages 336–340, 2011.

[8] M. Gertz and S. Jajodia. *Handbook of database security: applications and trends*. Springer-Verlag New York Inc, 2008.

[9] W. Lee and D. Xiang. Information-theoretic measures for anomaly detection. In *Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on*, pages 130–143. IEEE, 2001.

[10] L. Jiang, V. Anantharam, and J. Walrand. How bad are selfish investments in network security? *IEEE/ACM Transactions on Networking (TON)*, 19(2):549–560, 2011.

[11] H. Varian. System reliability and free riding. *Economics of Information Security*, pages 1–15, 2004.

[12] W. Peng. Analysis and exploration of related issues on the computer network security based on firewall and anti-virus software. In *Advanced Technology in Teaching-Proceedings of the 2009 3rd International Conference on Teaching and Computational Science (WTCS 2009)*, pages 45–49. Springer, 2012.

[13] S. Devaraj, M. Fan, and R. Kohli. Antecedents of b2c channel satisfaction and preference: validating e-commerce metrics. *Information Systems Research*, 13(3):316–333, 2002.

[14] A. Tiwari, S. Sanyal, A. Abraham, S.J. Knapskog, and S. Sanyal. A multi-factor security protocol for wireless payment-secure web authentication using mobile devices. *Arxiv preprint arXiv:1111.3010*, 2011.

[15] J. Mangler, C. Witzany, O. Jorns, E. Schikuta, H. Wanek, and I. Ul Haq. Mobile gsetsecure business workflows for mobile-grid clients. *Concurrency and Computation: Practice and Experience*, 22(14):2036–2051, 2010.

[16] Y. ZHAO, Y. MA, Y. DENG, and Y. LI. A secure electronic transaction protocol based on cpk. *Communications*, page 08, 2010.

[17] N. Boudriga. *Security of mobile communications*. Auerbach Publications, 2010.

[18] R. Borgohain, M.T. Singh, C. Sakharwade, and S. Sanyal. Tset: Token based secure electronic transaction. *Arxiv preprint arXiv:1203.5960*, 2012.

[19] Jun-feng Zhang Xiaodong Ma Xun-yi Ren, Li-li Wei. The improvement of set protocol based on security mobile payment. *Journal of Convergence Information Technology*, 2011.

[20] S. Sanyal, A. Tiwari, and S. Sanyal. A multifactor secure authentication system for wireless payment. *Emergent Web Intelligence: Advanced Information Retrieval*, pages 341–369, 2010.

[21] M. Jensen, N. Gruschka, and R. Herkenhöner. A survey of attacks on web services. *Computer Science-Research and Development*, 24(4):185–197, 2009.

[22] T. Holz, S. Marechal, and F. Raynal. New threats and attacks on the world wide web. *Security & Privacy, IEEE*, 4(2):72–75, 2006.

[23] Y. Zhang, Y. Mian, and L. Bin. Strategies and practice of the small and medium-sized enterprise network security. *Energy Procedia*, 13:9625–9631, 2011.