E-COMMERCE SYSTEMS SECURITY FOR SMALL BUSINESSES

Syed (Shawon) M. Rahman, Ph.D.[1] and Robert Lackey[2]

[1]Computer Science Faculty, University of Hawaii-Hilo, Hilo, USA
and Adjunct Faculty, Capella University, Minneapolis, USA
SRahman@Hawaii.edu
[2]School of Business & Technology Capella University, Minneapolis, MN 55402
rlackey4@gmail.com, rlackey1@capellauniversity.edu

ABSTRACT

Small business e-commerce websites make an excellent target for malicious attacks. Small businesses do not have the resources needed to effectively deal with attacks. Large and some mid-size organization have teams that are dedicated to dealing with security incidents and preventing future attacks. Most small businesses do not have the capabilities of dealing with incidents the way large organizations do. Security of e-commerce websites is essential for compliance with laws and regulations as well as gaining and maintaining the trust of consumers, partners and stakeholders. Many security standards have been established by various organizations to help guide security of small business servers, however, many of those standards or guidelines are too costly or time consuming. This paper[1] will discuss how attacks are carried-out and how a small business can effectively secure their networks with minimum cost.

KEYWORDS:

e-commerce systems security, small business security, server security, information security.

1.0 INTRODUCTION

Many businesses have come to the realization that, in order to compete in the market, key business processes need to be part of the Internet. E-commerce has become a popular adaptation for businesses, which has been a major transformation for many businesses. The popularity of the Internet has transformed traditional commerce into e-commerce, which has proven to be a successful platform for many businesses. Small businesses provide an easy target for attackers because they typically have limited funds and do not have dedicated personnel to monitor, update and defend their systems. The attacks on small businesses continue to rise each year (figure 1).

[1] This work is partially supported by EPSCoR award EPS-0903833 from the National Science Foundation (NSF) to the University of Hawaii, USA

2.0 BACKGROUND STUDY

Since the advent of the Internet, people have been looking for new ways of improving it, doing business, making money and committing crimes. "In 1990, a researcher named Tim Berners-Lee, proposed a hypertext-based web of information that a user could navigate using a simple interface called a browser. In 1994, Netscape 1.0's released included an important security protocol known as Secure Socket Layer, which could send and receive encrypted messages. Also in 1994, the first third-party services for processing online credit card sales began to appear" (Roos, n.d.). With the ability to accept credit cards online, businesses were no longer forced to traditional brick and mortar sales. This is where e-commerce began. It can be challenging to gain trust, maintain trust and build relationships with partners, customers, clients and suppliers. The relationships and trust that can take a long time to acquire can quickly be destroyed with a breach in security.

2.1 E-commerce Challenges

The challenge with e-commerce has been to successfully integrate effective security measures and mechanisms to protect the business from being compromised by attackers. Effective security is important for the continuity of business, trust of clients, and compliance with industry-specific laws and regulations. One breach in security can cost a business a lot of money, even shut it down.

Security is not just a "set and forget" kind of issue. Effective security involves a thorough analysis, implementation, updating and monitoring. The constant involvement with security can be a deterrent for some people. Some people do not want to take on the task of dealing with security. It is a major task, and it is also a very necessary task.

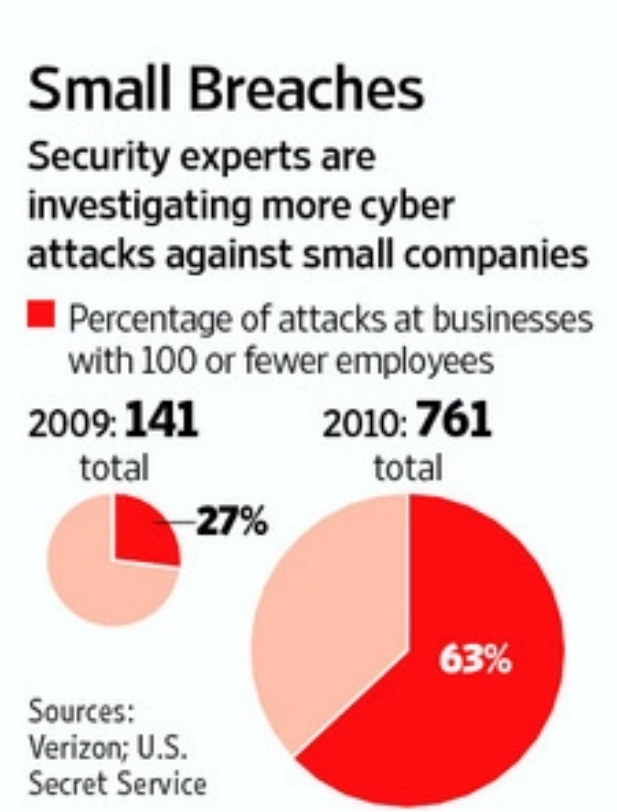

Figure 1. 2009-2010 Small Business Breaches. (2011).

2.2 Ethical Issues with E-commerce

Companies using the internet to do business should adhere to the same ethical standards online as they do offline. If they do not follow the same ethical standards, they face the same consequences. A damaged reputation and a long-term loss of trust can result from not following ethical standards.

Protecting consumer information should be a major concern for businesses. The costs can seem high and the benefits seem low, which is why some businesses do not feel the need to properly secure their e-commerce websites. When making purchases online, consumers should have a general sense of security. While there is no way to completely secure consumer information, businesses should take as many precautions as possible, while still allowing for usability.

Technology has revolutionized the way society operates and does business. Technology is constantly changing, criminals are constantly finding new methods of attack, and it is the responsibility of users and administrators of various technologies to use it in a way that is ethical and complies with all laws and regulations. Businesses need to ensure their e-commerce infrastructures are up-to-date with the latest updates and security necessities.

2.3 Threats to Business

Businesses are exposed to the following risks with e-commerce:

Direct Financial Loss:

- Fines or other legal repercussions could occur due to a violation of contracts, laws, or other regulations.

Indirect Loss:

- Loss of Credibility: People will lose trust in a business that has security issues, even if the security issues didn't cause any loss or damage.
- Loss in Productivity: The unavailability of e-commerce systems could result in loss of productivity because employees will not be able to work during downtime.
- Disclosure of confidential information: Business secrets could be stolen as well as employee and customer information.
- Blackmail: Malicious attackers could take over a system and demand compensation to restore the server to the control of the business.

Technical Issues:

- Damage to files or system: Security compromises could result in damage to files or the system as a whole. Files could be lost and the server could even be ruined by a malicious attack.

- Errors in configuration: Some malicious attacks could reconfigure the system to perform in ways that are different than normal.
- Errors in applications: Applications on the server could have errors and not perform properly.

3.0 ATTACKS AND VULNERABILITIES

Every day, different types of technology crimes are being committed, which can cause many problems for the victims. Technology crimes happen all around us, but are less visible and less personal than other crimes. It is less likely for the criminal to get caught because they do not have to risk a neighbor seeing them or an audible alarm going off. The anonymity and availability of the internet has made it easy for malicious hackers to commit crimes and not get caught.

Technology crimes also have bigger payouts most of the time than traditional crimes. "Sophisticated and ingenious techniques have allowed these modern-day crooks to use thousands of stolen identities to drain billions from banks and other financial institutions. Meanwhile, the average stickup guy gets about $7,200 in a bank heist" (Segal, A., & Thorne, J., 2006). It is important to understand attack methods in order to effectively know and understand how to protect against them. Attack methods are constantly changing, so it is important to stay abreast of the latest tools and techniques malicious hackers are using to penetrate network defenses as well as the latest protection necessities.

3.1 Web Server Threats

Web server software is designed to deliver web pages by responding to HTTP requests. Web server software is typically designed for usability and convenience, instead of security. "The more complex the software, the greater the probability that it contains coding errors or security weaknesses" (Schneider, 2009). The more lines of code, the greater chance there are going to be errors. "A common estimate used in the industry is that there are between 5-50 bugs per 1,000 lines of code. So an estimate would be that Windows 7 has approximately 1,200,000 bugs" (Eagle, Harper, Harris, Ness, & Williams, 2011).

Web servers can be compromised by an attacker obtaining the user name and password of one of the users. Once the attacker has the user name and password, he can then gain access and escalate privileges so he can have unlimited access to the server. The attacker can then install a backdoor so he can gain access in the future.

Web servers are also subject to physical attacks. A person could gain access to the room where the server is located and cause damage to it. Once a person has physical control over a server, he is capable of doing almost anything with it.

3.2 Database Threats

Electronic Commerce Systems store user data and retrieve product information from databases connected to a web server. Databases also contain valuable information that is a great target for

an attack. Trojan horses can change access rights or remove access controls to give users unlimited access.

3.3 Reconnaissance

Acquiring as much information about the target network is important to carry out an effective attack. You will need to know what type of operating system the machine is running on, what ports are open and the vulnerabilities of the target system. Knowing all of that information will make it easier to execute an attack.

3.4 Social Engineering

Social engineering is a form of deceit where a person pretends to be someone he or she is not and tries to infiltrate a facility or gain information. Social engineering can be the easiest way to gain access to an account, system or facility and does not require much technical knowledge. "It's a common hacker trick to telephone unsuspecting employees and pretend to be a network system administrator or security manager. If the hacker knows enough about the company's network to sound convincing, he can get passwords, account names, and other sensitive information (Schneier, B., 2004). This could also be done in-person or over the phone and a hacker could gain access to and account or a secure area in a facility.

3.5 Port Scanning

After all of the information about the system has been retrieved through social engineering or other means, port scanning is used to determine ports that are open on the system. Each TCP/IP protocol has several thousands of ports, which help with communication to the internet. Open ports are like open doors or windows to your home. A port scanner is used to scan the ports of a system and generate a report to the user on the status of the ports. The port scanner sends a message to the computer requesting access to each port. The port then sends a signal back to the port scanner and the scanner is able to determine the status of those ports with that message. This is similar to a criminal checking all of the doors or windows to your home in an effort to find one that is unlocked so he or she can gain access to your house.

3.6 Vulnerability Scanning

Vulnerability scanning is an important part of an attack because it shows the different weaknesses of the target system. "Once a series of accessible network "listeners" (ports) has been identified for a set of target systems and any associated application information, the next 'step' in the execution of an attack is usually to embark on the process of identifying specific operating system and application vulnerabilities" (Young, S., 2004). Computer programs are built with the usability in mind and the focus goes away from security. Every program has several vulnerabilities that make it susceptible to an attack. Once a weakness is determined, a hacker can take advantage and modify it, which could cause damage to the program or the system.

3.7 Ecommerce Server Attacks

Now that all of the information has been gather, the actual attack can take place. The attacker should plan his or her attack based on the skills, tools, and knowledge he or she has. Hackers have many different motives for attacking a network and not all are malicious. Some hackers attack a network to exploit the weaknesses and then fix that weakness for compensation. Other hackers attack networks to test their skills, while others want to steal information.

3.8 Physical Attacks

Physical attacks do not require much technical knowledge but can be just as damaging as other attacks. Physical attacks require physical access to the network, which is usually done by an insider or a social engineer. Once a person gains physical access to a server, he or she can have full control over that system. Preventing a person from gaining physical access to a server is probably the most important, but almost impossible. Malicious hackers might also be employees that have a grudge against a company and want to harm that company; they could even be network or security administrators.

3.9 Malware

Malware programs, also known as malicious software, are built to secretly infect a target computer upon opening the program. Malware includes viruses, Trojan horses, worms, and rootkits and any other software with a malicious intent. Malware programs can be disguised as legitimate software but may cause harm after installation.

Computer viruses and worm are the most common type of malware. Viruses are programs that infect executable software and spreads to other executable software when the program is ran. “Traditionally, a computer worm was considered an application that could replicate itself via a permanent or a dial-up network connection. Unlike a virus, which seeds itself within the computer’s hard disk or file system, a worm is a self-supporting program (Brenton, C., 2003).

Trojan horses and rootkits are nondestructive software, which allows a hacker remote access and administrative privileges. Trojan horses allow a user continual access to a system but only allow the hacker user privileges. Rootkits allows a hacker to have continual access to a target system and administrative privileges. Trojan horses and rootkits are used for denial of service attacks, data theft, modifying files, key logging or computer monitoring. They are also used to make a computer a zombie, which is used to attack other computers.

3.10 Denial of Service

Many companies run and rely on their networks for their business needs. Some companies use their network to send files and others use it to sell products. In a denial of service (DOS) attack, a hacker floods a network with so much information that it causes an overload and shuts down the system. The name of the attack says it all and explains what the purpose of a DOS attack is; to shut down a company’s services.

4.0 PROTECTION METHODS

Computer and information security is essential for businesses, families and individuals to stay protected from malicious hackers, scam artists, and online predators. With all of the crimes that are possible, network security should be a major concern for everybody, regardless of status.
If information is accidentally or maliciously deleted, modified or stolen, it could put that business out of service for an extended period of time or even indefinitely. Maintaining confidentiality, integrity and availability (CIA) are the main goals of network security. Different types of security are needed to accomplish the goal of CIA and provide a well-rounded protection system. Those methods might be costly but could be worth it depending on the risk of attack. While it is impossible to create patches for complete program protection, it is still necessary to apply the latest updates and install patches to make it more difficult for hackers to implement an attack.

4.1 E-Commerce Security Standards

Businesses, small and large, are required to comply with certain laws and regulations related to their activities. The concern for security has led to the development of standards and regulations to safeguard valuable data.

4.2 ISO 17799

ISO adopted standards originally published by the British Standard Institute (BSI). The BSI issued BS7799 in 1998 and was later adopted by the ISO as 17799. ISO 17799 provides recommendations for the following:

- Asset Classification and Control- All information assets should be accounted for and have security classifications to indicate the need and priorities for protection.
- Personnel security- Personnel should be provided appropriate security education and be aware of the incident reporting procedures.
- Physical and Environmental Security
- Network Security
- Access Control

4.3 Security Policies

Any organization concerned with protecting its electronic commerce assets should have a security policy in place. The security policies should describe which assets to protect and why, who is responsible for their protection, and what is acceptable and what is not. Security policies act as a guide for employees so they know what to do before, during and after an incident. The employees should all be aware of the policies, and tests can be conducted to ensure their competency. Tests can be in a variety of forms, such as written, oral and scenario-based tests. The tests should be designed so that employees are comfortable with the information in the policies and are comfortable responding to a variety of situations.

4.4 Physical Security

Physical security should be the first type of security that is implemented. It doesn't make sense to secure your computer and leave your place unsecure; that is almost the same as locking the doors to your home but leaving the windows open. Physical security can even be in the form of video monitoring systems and access control devices. While there is no way to be completely secure, it is best to limit the chances of being a victim.

4.5 Access Control

Controlling access to a facility or regions in the facility is an important part of security. Security guards should be used for roving patrols and ID verification of employees. The problem with security guards is that they are human and social engineering can be used to manipulate them. Because of the social engineering concerns, locks, biometrics scanners, and passwords should also be considered for access control.

4.6 Monitoring

Monitoring is very important because a hacker could sneak in without a company knowing and cause a lot of damage. The facility and the network need to be monitored to prevent a hacker from penetrating defenses and causing irreversible damage. With constant monitoring, security will be able to detect an attack and stop it before damage occurs. It is better to take measures to prevent something from happening than to try to repair the damage later. Some things may be damaged beyond repair and important information could be lost forever.

4.7 Authentication

Different methods of verification are used by different agencies to prevent unauthorized users from accessing their facilities, systems, and services.

4.8 Biometrics

Biometrics uses a person's body for access verification. Retinal scans, finger and palm print readers, and other body scanners are used for access control to verify a person's identity. Biometrics is good because it uses parts of the body that are unique to that individual. The problem with biometrics comes when a person damages their part of the body that is used for verification. If a person damages the body part used for verification, it will require extra work and the administrator will have to use a different means to allow that person access.

4.9 Usernames and Passwords

Usernames and passwords are user chosen credentials, which usually have certain requirements that are set by administrators. Requirements have to be set because people will use passwords that are common and hackers can break them. "The most secure passwords are at least 8 characters long with a mixture of upper and lower case letters and symbols and numbers. The longer the password length, and the more random the selection of characters and numbers, the

stronger the password is" (Failor, D., 2009). The problem with passwords and usernames is that people either forget them or they write them down and put them in a place where people can find them.

4.10 Smartcards

Smartcards are used in many facilities to control access to a certain area, system, or service. Smartcards allow a person access without having to remembering a password. The problem with many smartcards is that people lose them and other people might be able to use them.

4.11 Wireless Security

The days of connecting computers with wires are gone; now businesses use wireless connections to send, received and access information. Sending and receiving information wirelessly makes it susceptible to being apprehended. Systems can send and receive information via a wireless router that is connected to a modem which is connected to the Internet. The computers send out packets to the wireless router, which then transfers that to the modem and through the Internet.

4.12 802.1X Standard

802.11 provides wireless access to wired networks. "The overall framework for providing access control for networks is what's referred to as a port-based authentication system, which some people refer to as 802.1X" (Geier, 2008). Because of its enhanced security, 802.1x is the recommended wireless standard. "The strongest type of wireless authentication currently available, IEEE 802.1x authentication provides the most robust authentication for a WPA2 Enterprise model WLAN" (Ciampa, 2009). 802.1x provides access control features such as MAC Address filtering, a WPA2 access encryption key, and the ability to turn off SSID broadcast. Although 802.1x is the recommended wireless standard because of security, the problem with 802.1x is the cost to implement and maintain.

4.13 Cryptography

Cryptography is used to turn plaintext into an algorithm known as ciphertext, which is a complex mathematical sequence unreadable to anybody without the code to decipher it. Once data is encrypted into ciphertext, it is given a password and that password is needed to decrypt the data and turn it back into plaintext. That data can be sent to another person as long as that person has the password to decrypt the information. The type of algorithm determines the strength of the encryption and can make it more or less difficult to decrypt without the proper key. Cryptography is also used to create signatures for documents, which help to determine originality of that document.

4.14 Hashing

Hashing is a way of creating a unique signature for a document to prove that the document is the original document. This is important to prevent a person from copying a document. If a person

does copy the document, the same hash from the original will not be on the copy. Hashing is used to compare to the document to ensure it is the original. The most secure type of hash is the Secure Hash Algorithm (SHA), which uses a 160 bit encryption.

4.15 Symmetric

Symmetric encryption uses a single key to encrypt and decrypt data and replaces each letter and number in the document with another in a random order so it is almost impossible to decode without the key. The Advanced Encryption Standard (AES) is the most current and most secure symmetric encryption on the market. "After a lengthy process that required the cooperation of the U.S. government, industry, and higher education, five finalists were chosen, with the ultimate winner being an algorithm known as Rinjdael, which is more often referred to as AES" (Ciampa, M., 2009). The problem with symmetric encryption is that it uses a single key, which is passed around and expected to be kept secure.

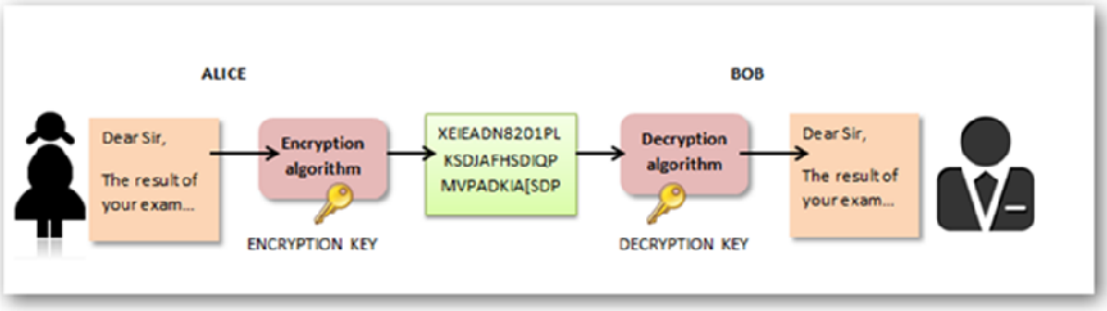

Figure 2. Symmetric Encryption (n.d.).

4.16 Asymmetric

Although both are still used today, asymmetric cryptography is much more secure than symmetric cryptography. "Asymmetric ciphers are much more mathematically complex than symmetric ciphers" (Dent, A., Mitchell, C., 2005). Unlike symmetric cryptography, asymmetric cryptography has more than one key, which are known as the public and private key. The multiple keys are good for security reasons but it can get confusing on which one to use.

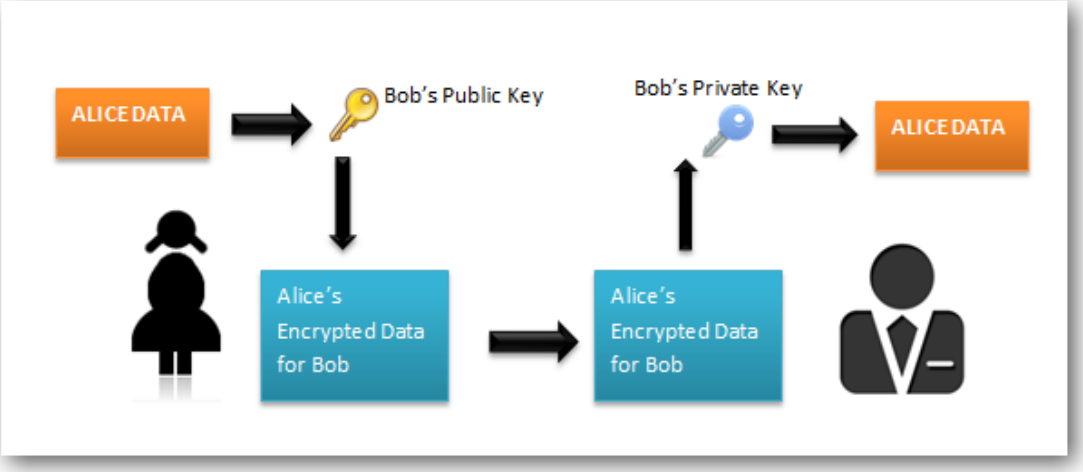

Figure 3. Asymmetric Encryption (n.d.).

4.17 EAP-TLS (Transport Layer Security)

EAP-TLS is generally regarded as the strongest available and the most expensive to deploy. It provides mutual certificate authentication between client and server, using the standard TLS protocol (a descendant of the SSL protocol used to secure most Web transactions). "It is a client/server protocol that is stacked on top of a reliable transport layer protocol, such as TCP in the case of TCP/IP and consists of the same two layer and protocols as SSL" (Oppliger, R., 2009). The server uses TLS to demonstrate that it holds a digital certificate and requests the same from the client. The client uses its certificate to prove its identity and keying material is exchanged. The TLS tunnel ends once authentication has been completed. The keys delivered by EAP-TLS can be used to encrypt data with the Advanced Encryption Standard (AES), Temporal Key Integration Protocol (TKIP) or Wired Equivalent Privacy (WEP). EAP-TLS is a good fit in WLANs where clients already have digital certificates or where high security needs justify investment in a public key infrastructure to manage those certificates.

4.18 EAP-TTLS (Tunneled TLS)

This EAP type balances security vs. deployment cost by replacing client-side certificates with legacy password authentication methods like PAP, CHAP and MSCHAPv2. EAP-TTLS requires the server to authenticate itself by certificate and establish a TLS tunnel through which to challenge the client. The TLS tunnel is used to protect less secure inner authentication methods. Even when a clear text password is returned, the TLS tunnel obscures the client's response. To avoid exposing the client's name, EAP-TTLS should be configured to send an "anonymous" identity when 802.1X starts, then send the actual identity through the TLS tunnel. That tunnel ends when authentication is completed and keys are delivered. "EAP-TTLS has been widely deployed, and it is likely to be encountered in many enterprise WLANS. While EAP-TTLS is almost identical to EAP-PEAP, it doesn't enjoy the native support for the Windows operating systems, which has resulted in relatively much less market penetration" (Wescott, D., 2010).

4.19 PEAP (Protected EAP)

PEAP is very similar to EAP-TTLS but uses different client authentication protocols. Like EAP-TTLS, PEAP establishes a TLS tunnel through server-side certificates. Although the same user credentials can be used with EAP-TTLS, a PEAP authentication server must be able to parse both EAP and the contained legacy authentication protocols. Today, PEAP is more broadly supported than EAP-TTLS because it is considered highly secure. The best choice for your network depends on the kinds of clients used in your WLAN and your budget.

4.20 WPA2 AES Passphrase

Pre-shared Key mode (PSK) doesn't require the complexity of an 802.1x authentication server. Each wireless network device encrypts the network traffic using a 256-bit key. This key may be entered either as a string of 64 hex digits, or as a passphrase of 8 to 63 ASCII characters. “In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively” (Mcbrewster, Miller, & Vandome, 2009). The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES).

4.21 Digital Certificates

The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate (IBM, n.d.). The digital certificates are used to communicate across the Internet using secure protocols like HTTPS.

4.22 Firewalls

A firewall is a software or hardware configuration. The primary purpose of firewalls is to control inbound and outbound internal network traffic. It is supposed to grant or deny access to a private network. Firewalls can be used to restrict the system from only providing a small set of services. Three types of firewalls exist:

- Packet-filtering firewalls- These inspect the source and destination addresses of packets. They ensure the packets received from the outside are in response to the ones sent.
- Proxy gateway firewalls- These act as a gateway for the outside users connecting to the network. Outside users must first connect to the gateway firewall before being able to connect to the network.
- Application proxy firewall- These inspect a user's request to connect to the application server. They ensure that the user's request conforms to that of the application's protocol.

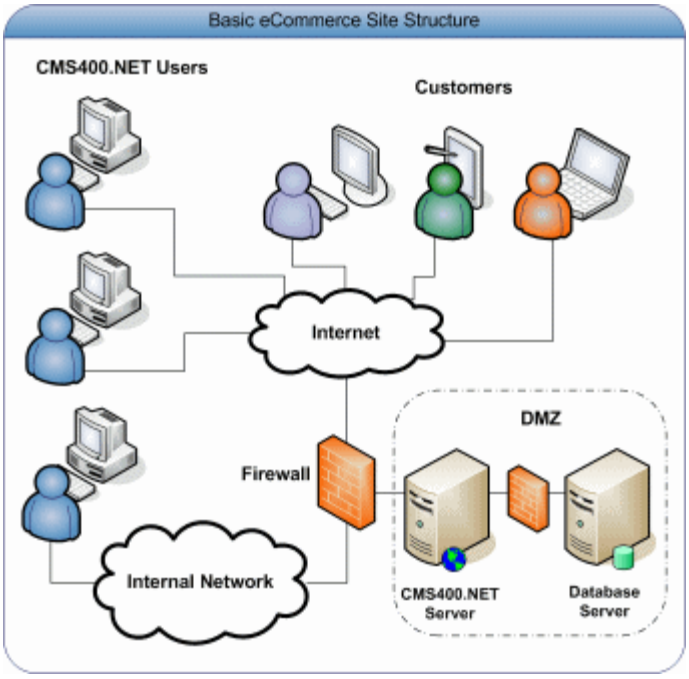

Figure 4. Basic eCommerce Site Structure. (n.d.).

The components of an e-commerce system should be configured to allow systems or servers on the internal network to initiate a connection with the network. The firewalls can be used to restrict the servers or systems on a network from initiating connections to an internal network.

4.23 Computer Intrusion Detection and Prevention Systems

Computer Intrusion Detection and Prevention Systems are similar to having a motion detector on the building and locks on the doors and windows. The Computer Intrusion Detection (IDS) System, similar to the motion detector, is meant to detect potential attackers and alert someone to take action. The Intrusion Prevention System (IPS), similar to the locks on the doors and windows, is meant to keep the attacker out. The names of the two systems sums up exactly what they are meant for. To have a good security program, you need both protection systems in place; one for detection and the other for prevention of malicious activity. Many systems these days incorporate both detection and prevention into one system and are known as Intrusion Detection and Prevention Systems (IDPS).

4.24 Intrusion Detection Systems

IDS's monitor a network for possible malicious activity and then report that activity to the administrator so he or she can make a decision on what to do with that threat. There are many different types of IDS's, which use different protocols for detection of threats such as network-based, wireless, behavior analysis, and host-based detection systems. Some threats reported by the IDS might not actually be malicious and the administrator will have to decide what to do with

the possible threat. Ideally, e-commerce systems should deploy both network and host-based IDS's, however the cost might be too much for some small businesses.

4.25 Host-Based IDS.

The functionality of host-based IDS's are similar to a virus scanner tool. The software is automated and runs in the background of the host system to detect any suspicious activities. It can be configured to take specific actions when an issue is detected. For example, it can be configured to automatically quarantine the suspicious activity or simply notify the administrator of the issue.

4.26 Network-Based IDS.

Network-Based IDS's examine the type and content of network packets. Network IDS's are less expensive than host-based IDS's, but it cannot monitor activities on individual host systems. It can protect the network as a whole but cannot protect individual systems. When choosing the IDS, it needs to be compatible with the firewall that is being used. The network-based IDS should be deployed between the incoming connections and the firewall. It should also be installed under two network interfaces, one for analyzing and one for reporting information to the IDS console.

4.27 Intrusion Prevention System

IPS's use a certain protocol of identifying threats and preventing them from accessing a network so they do not have a chance to harm the system. IPS's monitor the network traffic for malicious activity, log the activity, attempt to prevent it from accessing the network, and then report the activity to the administrator so he or she can follow-up with an action. Just like the IDS, the IPS may detect activity that is not malicious and the administrator will have to decide what to do with it.

4.28 Operating System Hardening

In e-commerce systems, it is important to reduce the attack possibilities by reducing or eliminating as many vulnerabilities as possible. This is accomplished by incorporating IDS's, installing anti-virus systems, removing all unnecessary programs, closing all ports and configuring it to protect against unauthorized access. "In many instances, an operating system provides a gateway into a computer system because of the large number of open ports and services running. These paths are a potential source of attack to Web commerce systems" (Nahari, & Krutz, 2011).

4.29 Automating Security

For most small businesses, there are not enough people to effectively manage an e-commerce system. Many small business owners, outsource or contract the management of their e-commerce systems. Many companies offer the option to host e-commerce systems for small businesses, but it might be important for some business owners to have everything in-house. If small business

owners want to have and manage their own servers and e-commerce systems, it is important to set-up security that is ran primarily by the software. Many types security software can be configured to detect and automatically handle suspected incidents. It is important to look for software that has low false-positives because it could potentially hurt business if it is blocking transactions from occurring instead of blocking attempted attacks. Also, it is important to find the software that has a good team and offers continuous updates. Threats are constantly evolving and it is important for software companies to stay up-to-date with the latest threats to their software. It will be important to continually check for updates and patches so vulnerabilities in the software are fixed before an attack occurs.

5.0 CONCLUSION

E-commerce is an effective way to do business. It allows businesses to provide products and services to a wider population than they could with traditional brick and mortar operations. However, e-commerce also comes with a wide variety of risks that need to be mitigated to operate securely. Small businesses provide an easy target for attackers because they typically have limited funding and do not have dedicated network professionals to monitor and protect their network. Hackers have a wide variety of tools that allow them to attack networks even with little technical knowledge. Hackers use a system along with their tools to attack systems. They first need to gather as much information as possible about the target system, scan for open ports, scan for vulnerabilities and then conduct their attack. Along with technical attacks, some attackers might try physical attacks through social engineering and gain access to the business servers by pretending to be someone they are not.

Small businesses need to take as many precautions as possible to protect their systems, even if it means spending extra money to do so. There is really no way of completely securing a network, but there are ways to minimize the chances of becoming a victim. Limiting the chances of becoming a victim is better than trying to repair the damages after an attack, which may not be repairable. Attacks come in many forms, so it is imperative to ensure that as many security measures are put in place as possible. The implementation of various security measures is important for the protection of family, business continuity and national security. With the possible outcomes of an attack on a network, businesses should take network security very seriously and properly protect their systems.

REFERENCES

[1] Brenton, C. (2003). Mastering Network Security. 2nd ed. Alameda, CA: Sybex,
[2] Center of Excellence Defence Against Terrorism (2008). Responses to Cyber Terrorism. Amsterdam, NLD: IOS Press.
[3] Ciampa, M. (2009). CompTIA Security+ 2008 In Depth. Boston, MA: Course Technology.
[4] Dent, A., Mitchell, C. (2005). User's Guide to Cryptography and Standards. Norwood, MA: Artech House, Incorporated.
[5] Department of Homeland Security (2003). The National Strategy to Secure Cyberspace. Retrieved March 01, 2011 from: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf
[6] DevCenter (n.d.). INFO: Understanding PCI Compliance. Retrieved from: http://dev.ektron.com/kb_article.aspx?id=26304

[7] Failor, D. (2009). InsidersChoice to CompTIA? Security+ Certification Exam SY0-201 and Exam BRO-001. Friendswood, TX: TotalRecall Publications, Incorporated
[8] Fowler, G. & Worthen, B. (2011). Hackers Shift Attacks to Small Firms. Retrieved from: http://online.wsj.com/article/SB10001424052702304567604576454173706460768.html#articleTabs%3Darticle
[9] IBM (n.d.). Installing GUI Certificates. Retrieved from: http://www-01.ibm.com/support/docview.wss?uid=swg21516057
[10] Mcbewster, J., Miller, F., & Vandome, J. (2009). Advanced Encryption Standard. Alphascript Publishing.
[11] Nahari, H., & Krutz, R. (2011). Web Commerce Security: Implementation and Design. Wiley Publishing
[12] Oppliger, R. (2009). SSL and TLS: Theory and Practice. Artech House.
[13] Roos, D. (n.d.). The History of E-Commerce. Retrieved from: http://money.howstuffworks.com/history-e-commerce1.htm
[14] Segal, A. & Thorne, J. (2006). Identity Theft: The New Way to Rob Banks. Retrieved from: http://articles.cnn.com/2006-05-18/us/identity.theft_1_identity-theft-bank-employee-bank-heist?_s=PM:US
[15] Strebe, M. (2004). Network Security Foundations. Alameda, CA: Sybex, Incorporated.
[16] Wescott, D. (2010). CWSP Certified Wireless Security Professional Official Study Guide. Sybex Publishing.
[17] Young, S. (2004). Hacker's Handbook: The Strategy Behind Breaking Into and Defending Networks. Boca Raton, FL: Auerbach Publications
[18] Fowler & Worthen, (2011). Hackers Shift Attacks to Small Firms. Retrieved from: http://online.wsj.com/article/SB10001424052702304567604576454173706460768.html
[19] How to Geek (n.d.). Symmetric Encryption. Retrieved from: http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
[20] How to Geek (n.d.). Asymmetric Encryption. Retrieved from: http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
[21] DevCenter, (n.d.).Retrieved from: http://dev.ektron.com/kb_article.aspx?id=26304
[22] Henderson, James and Rahman, Syed (Shawon); " Working Virtually and Challenges that must be overcome in today's Economic Downturn"; International Journal of Managing Information Technology (IJMIT); ISSN : 0975-5586 (Online) ;0975-5926 (Print)
[23] Dreelin, S., Gregory and Rahman, Syed (Shawon);" Enterprise Security Risk Plan for Small Business"; International Journal of Computer Networks & Communications (IJCNC), ISSN : 0974 – 9322 [Online] ; 0975- 2293 [Print])
[24] Donahue, Kimmarie and Rahman, Syed (Shawon); "Healthcare IT: Is your Information at Risk?"; International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.5, September 2012, ISSN:0974-9330(online); 0975-
[25] Rice, Lee and Rahman, Syed (Shawon); "Non-Profit Organizations' need to Address Security for Effective Government Contracting"; International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.4, July 2012
[26] Neal, David and Rahman, Syed (Shawon); "Video Surveillance in the Cloud?"; The International Journal of Cryptography and Information Security (IJCIS), Vol.2, No.3, September 2012
[27] Lai, Robert and Rahman, Syed (Shawon); "Analytic of China Cyberattack"; The International Journal of Multimedia & Its Applications (IJMA), June 2012, Volume 4, Number 3
[28] Halton, Michael and Rahman, Syed (Shawon); "The Top 10 Best Cloud-Security Practices in Next-Generation Networking"; International Journal of Communication Networks and Distributed Systems (IJCNDS); Special Issue on: "Recent Advances in Next-Generation and Resource-Constrained Converged Networks", Vol. 8, Nos. ½, 2012, Pages:70-84, ISSN: 1754-3916
[29] Amin, Syed; Pathan, Al-Sakib, and Rahman, Syed (Shawon);" Special Issue on Recent Advances in Next-Generation and Resource-Constrained Converged Networks" , International Journal of Communication Networks and Distributed Systems (IJCNDS)

[30] Mohr, Stephen and Rahman, Syed (Shawon);"IT Security Issues within the Video Game Industry"; International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 5, Oct 2011, ISSN:0975-3826

[31] Dees, Kyle and Rahman, Syed (Shawon);"Enhancing Infrastructure Security in Real Estate"; International Journal of Computer Networks & Communications (IJCNC), Vol.3, No.6, November 2011

[32] Hood, David and Rahman, Syed (Shawon);"IT Security Plan for Flight Simulation Program"; International Journal of Computer Science, Engineering and Applications (IJCSEA), Vol.1, No.5, October 2011

[33] Schuett, Maria and Rahman, Syed (Shawon); "Information Security Synthesis in Online Universities"; International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011

[34] Jungck, Kathleen and Rahman, Syed (Shawon); " Cloud Computing Avoids Downfall of Application Service Providers";International Journal of Information Technology Convergence and services (IJITCS), Vol.1, No.3, June 2011

[35] Slaughter, Jason and Rahman, Syed (Shawon); " Information Security Plan for Flight Simulator Applications"; International Journal of Computer Science & Information Technology (IJCSIT), Vol. 3, No 3, June 2011

[36] Benson, Karen and Rahman, Syed (Shawon); "Security Risks in Mechanical Engineering Industries", International Journal of Computer Science and Engineering Survey (IJCSES), Vol.2, No.3, August 2011

[37] Bisong, Anthony and Rahman, Syed (Shawon); "An Overview of the Security Concerns in Enterprise Cloud Computing "; International journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011

[38] Mullikin, Arwen and Rahman, Syed (Shawon); "The Ethical Dilemma of the USA Government Wiretapping"; International Journal of Managing Information Technology (IJMIT); Vol.2, No.4, November 2010

[39] Rahman, Syed (Shawon) and Donahue, Shannon; "Convergence of Corporate and Information Security"; International Journal of Computer Science and Information Security (IJCSIS), Vol. 7, No. 1, 2010

[40] Hailu, Alemayehu and Rahman, Syed (Shawon); "Protection, Motivation, and Deterrence: Key Drivers and Barriers of Organizational Adoption of Security Practices" ; IEEE the 7th International Conference on Electrical and Computer Engineering (ICECE) December 20-22, 2012, Dhaka, Bangladesh

[41] Hailu, Alemayehu and Rahman, Syed (Shawon); "Security Concerns for Web-based Research Survey" IEEE the 7th International Conference on Electrical and Computer Engineering (ICECE), December 20-22, 2012, Dhaka, Bangladesh

[42] Neal, David and Rahman, Syed (Shawon); "Consider video surveillance in the cloud-computing"; IEEE the 7th International Conference on Electrical and Computer Engineering (ICECE), December 20-22, 2012, Dhaka, Bangladesh

[43] Neal, David and Rahman, Syed (Shawon); "Securing Systems after Deployment"; The Third International Conference on Communications Security & Information Assurance (CSIA 2012), May 25-27, 2012, Delhi, India

[44] Johnson, Mazie and Rahman, Syed (Shawon); "Healthcare System's Operational Security"; IEEE 2011 14th International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh, December 22-24, 2011

[45] Rahman, Syed (Shawon) "System Security Specifications for a Multi-disciplinary Research Project",7th International Workshop on Software Engineering for Secure Systems conjunction with The 33rd IEEE/ACM International Conference on Software Engineering (ICSE 2011), May 21-28, 2011, Honolulu, Hawaii.

[46] Rahman, Syed (Shawon) and Donahue, Shannon; "Converging Physical and Information Security Risk Management", Executive Action Series, The Conference Board, Inc. 845 Third Avenue, New York, New York 10022-6679, United States
[47] Rahman, Syed (Shawon) and Peterson, Mike; "Security Specifications for a Multi-disciplinary Research Project"; The 2011 International Conference on Software Engineering Research and Practice (SERP'11), Las Vegas, Nevada, USA July 18-21, 2011
[48] Jungck, Kathleen and Rahman, Syed (Shawon); " Information Security Policy Concerns as Case Law Shifts toward Balance between Employer Security and Employee Privacy"; The 2011 International Conference on Security and Management (SAM 2011), Las Vegas, Nevada, USA July 18-21, 2011

Authors Bio:

Dr. Syed (Shawon) M. Rahman is an assistant professor in the Department of Computer Science and Engineering at the University of Hawaii-Hilo and an adjunct faculty of School of Business and Information Technology at the Capella University. Dr. Rahman's research interests include software engineering education, data visualization, information assurance and security, web accessibility, software testing and quality assurance. He has published more than 80 peer-reviewed papers. He is a member of many professional organizations including ACM, ASEE, ASQ, IEEE, and UPE.

Robert Lackey is a United States Army veteran who has been in the IT security industry for over six years. He holds various IT certifications, a Bachelor's degree in Criminal Justice Computer Crime from Kaplan University and a Master's degree in Information Assurance and Security from Capella University.