OKAN UNIVERSITY

INSTITUTE OF SOCIAL SCIENCES

ELECTRONIC COMMERCE SECURITY

Gökhan ÇAKIL

THESIS

FOR THE DEGREE OF

MASTER OF BUSINESS ADMINISTRATION

ADVISOR

Prof. Dr. Gonca TELLI YAMAMOTO

ISTANBUL, May 2014

OKAN UNIVERSITY

INSTITUTE OF SOCIAL SCIENCES

ELECTRONIC COMMERCE SECURITY

Gökhan ÇAKIL

THESIS

FOR THE DEGREE OF

MASTER OF BUSINESS ADMINISTRATION

The Date of Delivery of The Thesis to The Institute	**: 3 June 2014**
The Date of The Thesis Defense	**: 26 May 2014**

Advisor : Prof. Dr. Gonca TELLI YAMAMOTO

Jury members : Dr. Özgür ŞEKEROĞLU

Yrd.Doç. Dr. İbrahim GÖNEN

ISTANBUL, May 2014

FOREWORD

Electronic commerce, with another discourse e-commerce, is the trading products or services over electronic systems such as the Internet. Regardless of which one is the trading methods or option a merchant prefers, there are a lot of key issues to be considered regarding the security of sensitive cardholder data. Because I wanted to investigate this issue e-commerce continues to develop rapidly, including lots of different technologies, methods, tools and options. With the any unceasingly evolving technology, their corresponding security risks increases such as in e-commerce.

I wrote this thesis has been formed six parts. The first part includes the definition of e-commerce security and fundamentals of e-commerce security. The second part includes the e-commerce security threats and I tried to explain common security attacks and methods. Third part explains methods of securing e-commerce from these threats. The fourth part defines advanced security concerns including disaster recovery and business continuity. The fifth part includes more details about e-commerce implementations and their corresponding security compliance. The sixth parts explains about e-commerce security and data breaches with examples.

This work is my Master’s MBA thesis at Okan University. I would like to thank Prof. Dr. Gonca Telli Yamamoto for her opinions and suggestions during my study.

May, 2014 Gökhan ÇAKIL

CONTENTS

LIST OF FIGURES

PAGE NO

PREFACE

It is becoming increasingly common for attackers to gain access to an e-commerce site not to steal products or services, but rather the customers’ credit card information and other personal information. The fact that a theft was able to occur typically means that the access controls on that information were not sufficient to address the potential threat or the thief was somehow able to circumvent the access control mechanisms.

My purpose for writing this thesis, detection of security vulnerabilities in electronic commerce and related security controls is provided. Because nowadays almost everything is bought and sold in the electronic media. And with emerging technologies, security breach incidents are increasing with each passing day. Due to this inevitably increase shoppers' security concerns have reached a level that will determine their market share.

E-commerce is an important factor that providing a major contribution to the economies of the developed countries will become even greater significance with integrity of secure online commerce element and gain much more confidence of the people.

CHAPTER I

INTRODUCTION TO E-COMMERCE SECURITY

1.1 E-COMMERCE SECURITY OVERVIEW

Web e-commerce applications that handle payments (online banking, electronic transactions or using debit cards, credit cards, PayPal or other tokens) have more compliance problems, are at increased risk from being targeted than other websites and there are greater consequences if there is data loss or alteration. Banking services are highly regulated, but even the smallest electronic retailer is affected by the Payment Card Industry Data Security Standard (PCI DSS). Currently both Visa and MasterCard require Merchants and Service Providers to be validated according to the PCI DSS. Smaller merchants and service providers are not required to explicitly validate compliance with each of the controls prescribed by the PCI DSS although these organizations must still implement all controls in order to maintain safe harbour and avoid potential liability in the event of fraud associated with theft of cardholder data (WEB_1 , 2014). Nowadays, this has become more widely known due to increased publicity and enforcement to clarify and add requirements. Web applications, user protection for protection of the paying system requires a combination of administrative, technological and physical controls. All e-commerce service providers whether it is small or not must be required to be validated and controlled by the government agencies for the general body and standards.

Sensitive information security is a highly critical measure for online transactions including shopping and banking applications and steadily growing in importance year after year. The value of reputation is directly interconnect with confidentiality and it is very hard to gain confidence after disaster. E-commerce websites and online businesses regardless of the products and services they are promoting need to provide customers and users with a safe and secure online shopping portal. These growing security issues are very important to explain and understand e-commerce security. E-commerce security is a crucial necessity to mitigate the risk of exposing sensitive information. I try to conduct a literature review of the written materials of e-commerce security issues.

Companies faces a lot of threats for their e-commerce applications. For example according to a survey conducted with 1320 companies in the United States in 1996, 78% of companies that lose money due to the inability to provide security,63% of companies that suffer losses due to virus and in 20 companies stated that they loss of at least $ 1 million. (Singh and Frolick, 2000:58).

In Turkey companies and the public are also facing this kind of threats. There is a growing potential of Internet and smartphone usage in Turkey however less shopping rates from internet which means a lot of people face with this kind of threats or there is a mistrust of e-commerce. Research in Turkey shows that internet shopping levels are very low. According to a survey of 1000 users who do not shopping from the internet is 85 percent while the 3 percent of the remaining 15 percent do shopping 1 or 2 times in a month. (WEB_2 , 2013).

In recent years, innovations like a widely used payment on delivery, the virtual card provide internet users with a safer shopping (Telli Yamamoto, 2011). For example some payment systems which is developed by banks and in conjunction with the leading companies of the world that makes internet shopping is fast, easy and enjoyable. Card holders do shopping without share their card information on the internet safely.

Accordingly one of the most important obstacles in front of e-commerce is security. If security problem of business is solved, it is certain to increase the volume of e-commerce.

1.2 FUNDAMENTALS OF E-COMMERCE SECURITY

Creating a thriving e-commerce business, e-retailers need to inspire trust and confidence in their customers by minimising the various risks that they are faced with online. With fraudulent e-commerce scams and hackers becoming evermore sophisticated and commonplace, it's vital that all e-retailers and budding e-retailers learn about the basics of e-commerce security.There are four fundamentals of E-commerce security and these are; Customer Privacy and Confidentiality, Integrity of Information, Authentication of Identify, Non-Repudiation.

1.2.1 The 4 Fundamentals of E-commerce Security

Before any e-commerce website or online business can consider itself secure, it first needs to fulfil these four fundamentals of e-commerce security:

Customer Privacy and Confidentiality- All customer information (especially sensitive information such as payment details and delivery details) needs to be stored in a safe and secure way which is inaccessible to unauthorised parties.

The growing expanse of e-commerce and the widespread availability of online databases raise many fears regarding loss of privacy and many statistical challenges. Even with encryption and other nominal forms of protection for individual databases, we still need to protect against the violation of privacy through linkages across multiple databases. These issues parallel those that have arisen and received some attention in the context of homeland security (WEB_3, 2014).

Confidentiality is the property of nondisclosure to unauthorized parties. Attacks against confidentiality are by far the most prevalent today because information can be sold or exploited for profit in a huge variety of (mostly criminal) manners. The network, as the carrier of almost all digital information within the enterprise, provides an attractive target to bypass access control measures on the assets using the network and access information while it is in transit. Among the information that can be acquired is not just the payload information, but also credentials, such as passwords.

Social capital has been one of the important building blocks for developed countries on the road to development. Then social capital is the name of an overall system of work in coordination and dynamics is the element of "trust". In other words, social capital is a leading ability if you dominate the sense of confidence in a society or some of its parts (Fukuyama, Bugdayci (Trans.) , 2001).

Integrity of Information - Any communication and transactions between the e-commerce website and the customer must be tamper proof and maintain the integrity of the original communication.

Authentication of Identify - During the communication process both the e-commerce website and the customer need to prove that they are who they say they are.

Non-Repudiation- is a service that ensures the sender cannot deny a message was sent and the integrity of the message is intact. Even though ecommerce security is by nature a complex subject, e-retailers don't need to find complex solutions to fulfil the four fundamentals. The basic requirements of ecommerce security can be easily met by e-retailers using the following solutions:

Encryption - The role of cryptography in e-commerce continues to be as an enabler of trust between business entities and between consumer and business. Data encryption plays a central role in securing online transactions. Encryption ensures transaction privacy to prevent unauthorized access to confidential transactions. During encryption a message "key" such as a PKI (Public Key Infrastructure) is used to scramble the information sent in a transaction into an unreadable and unintelligible format. The information is only capable of being unscrambled by the intended recipient of the transaction who holds a matching "private key". Encryption is the first step towards meeting the fundamentals of ecommerce security

Digital Signatures - The purpose of a digital signature is to provide the same level of accountability for electronic transactions where a handwritten signature is not possible. A digital signature will provide assurance that the message does indeed come from the person who claims to have sent it, it has not been altered, both parties have a copy of the same document, and the person sending the document cannot claim that he did not send it. A digital signature will usually include a date and time of the signature, as well as a method for a third party to verify the signature.

SSL Digital Certificates - SSL (Secure Socket Layer) digital certificates act as digital ID and can be used to fulfil the authentication requirements of ecommerce security. Digital certificates are used by e-retailers to prove their authenticity and identify them as genuine online merchants. Digital certificates are issued by certification authorities such as Verisign, and provide e-retailers with a completely unique digital identity.

CHAPTER II

E-COMMERCE SECURITY THREATS

2.1 SOCIAL ENGINEERING

Social engineering stands for techniques using social interaction, typically with the organization’s employees, suppliers, and contractors, to gather enough information to be able to penetrate the organization’s physical premises or systems. Such techniques could include posing as a representative of the IT department’s help desk and asking users to disclose their user account and password information, posing as an employee and gaining physical access to restricted areas that may house sensitive information.

According to Ross (2008), the term "social engineering" as an act of psychological manipulation is also connected with the social sciences, but its usage has caught on among computer and information security professionals.

2.1.1 SOCIAL ENGINEERING TECHNIQUES

In social engineering attackers can exploit human nature and good will to claim illicit legitimacy, for instance, by claiming to belong to a certain company or social group., some of which are listed here:

Pretexting , also known in the UK as blagging or bohoing, is the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances. An elaborate lie, it most often involves some prior research or setup and the use of this information for impersonation (e.g., date of birth, Social Security number, last bill amount) to establish legitimacy in the mind of the target **(** Federal Trade Commission , 2006**).**

Diversion theft, also known as the "Corner Game" or "Round the Corner Game", originated in the East End of London.

In brief, diversion theft is a "con" exercised by professional thieves, normally against a transport or courier company. The objective is to persuade the persons responsible for a legitimate delivery that the consignment is requested elsewhere — hence, "round the corner" (WEB_4 , 2013).

Phishing is unadulterated social engineering or deception. However, some recent phishing attacks have associated technical aspects, such as the creation of unframed browser windows in order to overlay areas in the browser frame and recreate “browser chrome,” such as the padlock symbol denoting a site certificate and authentication/encryption via the SSL protocol.

Phishing attempts to get the user to provide information that will be useful for identity theft-type frauds. Although phishing messages frequently use Web sites and try to confuse the origin and ownership of those sites, very little programming, malicious or otherwise, may be involved.

Phone phishing: If a user were to receive a phone call from a “system administrator” asking for their password, users should be aware of social engineering threats and ask that the system administrator come to their office to discuss the problems in a face-to-face format. Even if the user is 100% sure that the person on the phone is the system administrator and the phone line could not be tampered with, it is almost impossible to imagine a situation under which a user should give a password to anyone else, particularly using the phone lines.

Baiting is like the real-world Trojan Horse that uses physical media and relies on the curiosity or greed of the victim (WEB_5 , 2010). Baiting attacks could be akin to phishing attacks, however, instead of using email as the delivery method of the attack we use different ways of physical media which relies on the curiosity or sometimes even greed of the victims. After gathering a list of full names, working address and position for all of the associates of an organization, attackers carefully analyzed this list and decided to target a certain number of employees per location. After having decided on the targets, the next step was to choose which attack method we were going to be using for that specific case. Attackers decided on trying to impersonate users (most of them part of sales team) with a custom message requesting users to update their local Anti-Virus software. Its really old school, but you would be surprised on how effective this is. The physical medias have been delivered by postal service to each one of the targets along with a letter with details about the (fake) antivirus update and instructions on how to install either the CD-ROM or USB pen-drive that was also included in the packages.

Quid pro, Quid pro quo means something for something:

An attacker calls random numbers at a company, claiming to be calling back from technical support. Eventually this person will hit someone with a legal problem, grateful that someone is calling back to help them. The attacker will "help" solve the problem and, in the process, have the user type commands that give the attacker access or launch malware. In a 2003 information security survey, 90% of office workers gave researchers what they claimed was their password in answer to a survey question in exchange for a cheap pen (Leyden, 2003). Similar surveys in later years obtained similar results using chocolates and other cheap lures, although they made no attempt to validate the passwords.

Tailgating: A common and frustrating loophole in an otherwise secure access control systems can be the ability of an unauthorized person to follow through a checkpoint behind an authorized person, called “piggybacking or “tailgating. One solution is an airlock-style arrangement called a mantrap, in which a person opens one door and waits for it to close before the next door will open. Another system that is available is a turnstile, which can be used as a supplemental control to assist a guard or receptionist while controlling access into a protected area.

Other types: Social engineering is the oldest form of attack used to bypass access controls and commit theft or fraud. Social engineering is the practice of misdirection to obtain information through social contact. Social engineering can take many forms, ranging from telephone calls to e-mail to face-to-face interaction. Additionally, the degree of personal interaction needed is variable.

A very recent type of social engineering technique includes spoofing or cracking IDs of people having popular e-mail IDs such as Yahoo!, GMail, Hotmail, etc. Among the many motivations for deception are (WEB_6, 2013):

- Phishing credit-card account numbers and their passwords.
- E-mail can be a powerful persuasion device for attackers and chat records, and manipulating them by using common editing techniques before using them to extort money and creating distrust among individuals.
- Cracking websites include impacts in the public space and the reputation of the organization.
- Hoaxes use an odd kind of social engineering, relying on people’s desire to communicate, and on a sense of urgency and importance

Countermeasures

Organizations reduce their security risks by (WEB_6, 2013) :

- Establishing frameworks of trust on an employee/personnel level (i.e., specify and train personnel when/where/why/how sensitive information should be handled)
- Backup tapes, off-site storage, password files, and many other types of sensitive information need to be protected from disclosure or undetected alteration and evaluating its exposure to social engineering
- Preparing and implementing security protocols, policies, and procedures to protect sensitive information.
- Training employees provides guidance surrounding the performance of particular security or risk management functions, as well as providing information surrounding the security and risk management functions in general.
- Performing unannounced, periodic tests (penetration tests or vulnerability scanning) to ensure that the application and network infrastructure meet its security requirements and specifications
- Reviewing the above steps regularly: no solutions to information integrity are perfect.
- Using a waste management service that has dumpsters with locks on them, with keys to them limited only to the waste management company and the cleaning staff. Locating the dumpster either in view of employees such that trying to access it carries a risk of being seen or caught or behind a locked gate or fence where the person must trespass before they can attempt to access the dumpster.

2.2 DICTIONARY AND BRUTE FORCE ATTACKS

Dictionary attack is a method used to break security systems, specifically password-based security systems, in which the attacker systematically tests all possible passwords beginning with words that have a higher possibility of being used, such as names and places. The word "dictionary" refers to the attacker exhausting all of the words in a dictionary in an attempt to discover the password. Dictionary attacks are typically done with software instead of an individual manually trying each password (WEB_7, 2013)

A brute force attack can manifest itself in many different ways, but primarily consists in an attacker configuring predetermined values, making requests to a server using those values, and then analyzing the response. For the sake of efficiency, an attacker may use a dictionary attack (with or without mutations) or a traditional brute-force attack (with given classes of characters e.g.: alphanumerical, special, case (in)sensitive). Considering a given method, number of tries, efficiency of the system which conducts the attack, and estimated efficiency of the system which is attacked the attacker is able to calculate approximately how long it will take to submit all chosen predetermined values.

2.3 OWASP TOP 10 ATTACKS

OWASP has several guides available for web application development including code review guide, testing guide , OWASP Mobile. The Open Web Application Security Project (OWASP) is a nonprofit focused on improving the security of software. OWASP develops numerous free and useful products of interest to the security architect including (F. Tipton , 2013) :

OWASP Top 10 Project: Provides OWASP’s opinion of the top ten web-based application security flaws and how to mitigate them.

OWASP Guide Project: Aimed at architects this is a comprehensive manual for designing secure web applications and services.

OWASP Software Assurance Maturity Model (SAMM): SAMM is a framework used to design software which is secure and tailored to an organization’s specific risks.

OWASP Mobile Project: Provides a resource for developers and architects to develop and maintain secure mobile applications.

The OWASP Top 10 - 2013 is as follows (WEB_8, 2014)**:**

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Components with Known Vulnerabilities
- A10 Unvalidated Redirects and Forwards

2.4 MAN IN THE MIDDLE / MAN IN THE BROWSER ATTACKS

Both types of spoofing are forms of a common security violation known as a man in the middle (MITM) attack. In these attacks, a malicious party intercepts a legitimate communication between two friendly parties. The malicious host then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either the original sender or the recipient.

If the communication parties have no public key certificates and no shared secret, the negotiation is vulnerable to a man-in-the-middle attack. In other words, no party can be sure that the messages sent by another party have not been intercepted and modified. The best defense against session hijacking and man-in-the-middle (MITM) attacks is unique and random identifiers present a challenge for the attacker to guess what the next identifier may be. A man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other — it is an attack on mutual authentication (or lack thereof). Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, SSL can authenticate one or both parties using a mutually trusted certification authority.

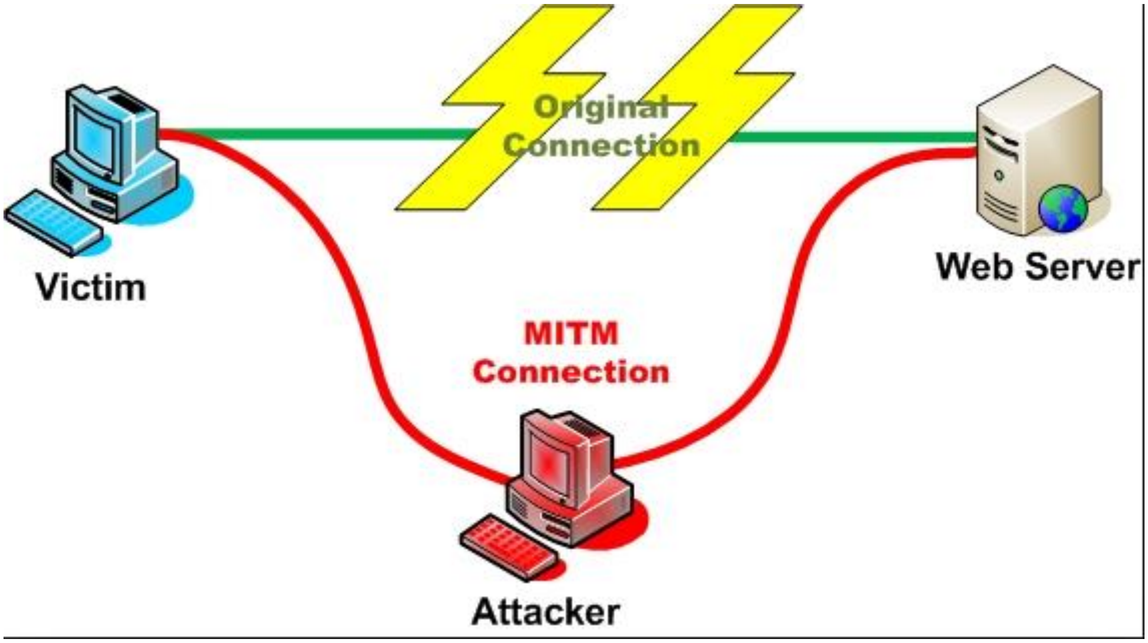


Figure 2.1 - Man in the Middle Attack **(**https://www.owasp.org/index.php/Man-in-the-middle_attack**)**

Man-in-the-browser , a kind of threat according to man-in-the-middle (MITM), is a proxy Trojan horse that use an internet browser via vulnerabilities in web browser security to edit web sources, change transaction data or add other transactions, but all of these transactions are entirely within covert channels and so unnoticeable for both the customer and host web application. A MitB attack will be successful irrespective of whether security mechanisms such as SSL/PKI and/or two or three-factor Authentication solutions are in place. A MitB attack may be countered by utilising out-of-band transaction verification, although SMS verification can be defeated by man-in-the-mobile (MitMo) malware infection on the mobile phone. Trojans may be detected and removed by antivirus software with a 23% success rate against Zeus in 2009, and still low rates in 2011 (WEB_9 , 2013). The browser verifies the validity of the signature and asks the user to make a judgment on whether or not the developer is trustworthy. Unfortunately, most end users do not have the security or technical knowledge to make an informed decision in such a circumstance, and most simply bypass the code and allow the control to execute.

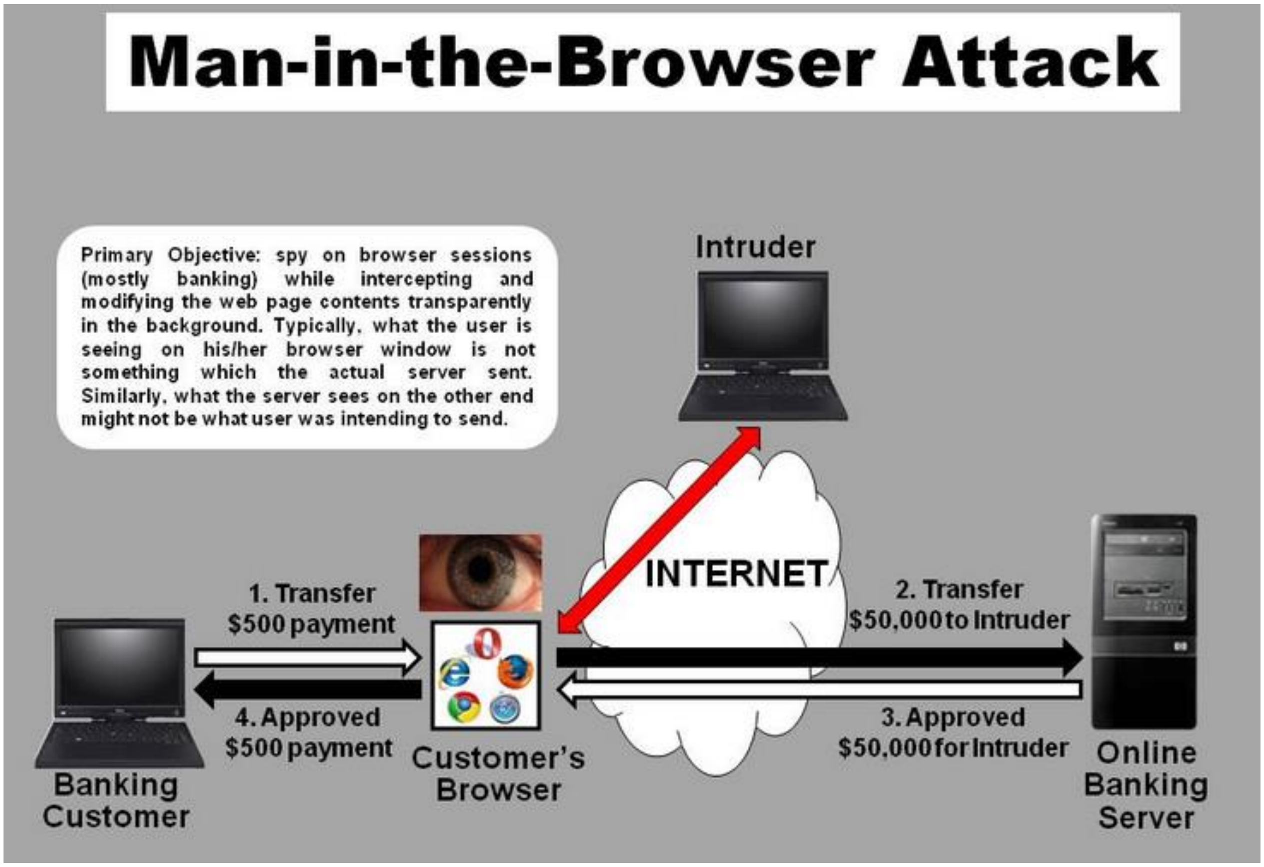

Man-in-the-Browser Attack
Primary Objective: spy on browser sessions (mostly banking) while intercepting and modifying the web page contents transparently in the background. Typically, what the user is seeing on his/her browser window is not something which the actual server sent. Similarly, what the server sees on the other end might not be what user was intending to send.
Intruder
INTERNET
1. Transfer $500 payment
2. Transfer $50,000 to Intruder
3. Approved $50,000 for Intruder
4. Approved $500 payment
Banking Customer
Customer's Browser
Online Banking Server

Figure 2.2 - Man in the Browser Attack (http://www.nutech.net/history.htm)

A standard browser security manager will disallow most operations when they are requested by untrusted code, and will allow trusted code to perform all of its operations. It is the responsibility of the security manager to make all final decisions as to whether a particular operation is permitted or rejected. A MitB Trojan works by utilising common facilities provided to enhance browser capabilities such as Browser Helper Objects (a feature limited to Internet Explorer), browser extensions and user scripts (for example in JavaScript) etc. Antivirus software can detect some of these methods. In a nutshell example exchange between user and host, e.g. an Internet banking transaction such as a funds transfer, the customer will always be shown, via confirmation screens, the exact payment information as keyed into the browser. The bank, however, will receive a transaction with materially altered instructions, i.e. a different destination account number and possibly amount. The use of strong authentication tools simply creates an increased level of misplaced confidence on the part of both customer and bank that the transaction is secure. Authentication, by definition, is concerned with the validation of identity credentials. This should not be confused with transaction verification (WEB_10 , 2013).

2.5 DOS & DDOS ATTACKS

Distributed denial-of-service attack: Using a network of remote-controlled hosts known as “botnets” (typically workstations that have been compromised by a virus or other form of “malware”), the target is subjected to traffic from a wide range of sources that are very hard to block. The downside of this type of attack to both the attacker and network service provider is that the attack may already throttle upstream network channels, taking out more than just its intended target (Tipton , 2013).

In the late 1990s and into the twenty-first century, distributed denial of service (DDoS), became a significant threat to operations. Rather than attack a server from a single location (and risk being detected and blocked), DDoS attacks target a server from hundreds or thousands of locations. Attackers build vast networks of commandeered systems (also known as botnets) by infecting vulnerable machines with software agents known as zombies. The zombies react to commands relayed typically over IRC channels from the “

botherder" and, when instructed, simultaneously make numerous requests to a single system or application, such as a Web site. The zombie systems make millions of requests to the Web site at once, completely flooding the target system to the point where others cannot access it, or until it simply fails and shuts down.

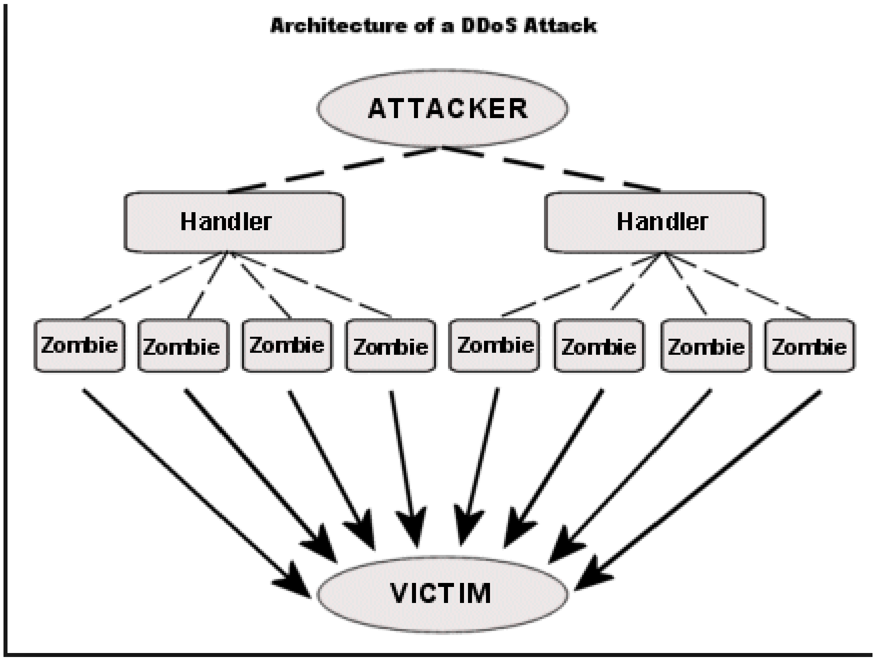


Figure 2.3 - DDoS Attack (http://www.betterhostreview.com/ddos-attack-protected-hosting.html)

2.6 KNOWN VULNERABILITIES

When seeking to determine the security position of an organization, the security professional will eventually turn to a vulnerability assessment to help identify specific areas of weakness that need to be addressed. A vulnerability assessment is the use of various tools and analysis methodologies to determine where a particular system or process may be susceptible to attack or misuse. Most vulnerability assessments concentrate on technical vulnerabilities in systems or applications, but the assessment process is equally as effective when examining physical or administrative business processes. To begin the vulnerability assessment process, assessor must have a good understanding of the business, its mission and the system or application to be assessed. While it is possible to simply run an automated tool against the target system to produce a list of potential problems, understanding first what the system does and its relationship to the overall business process will assist the analyst in determining the overall risk of any discovered vulnerabilities. Using automated tools, a vulnerability scan of the target system or application should be performed. In addition to the logical vulnerabilities, administrative and physical weaknesses should be reviewed as well. Questions such as the following should be considered:

Is the organization financially weak?

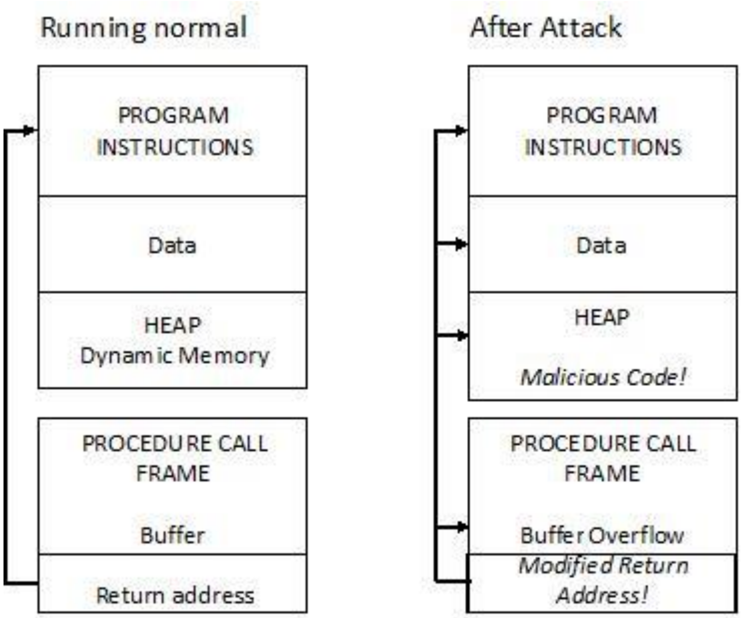
Does the organization leadership have rapid turnover?

Is there backup administration for the system?

Is the datacenter located in a flood zone or an area prone to weather disasters?

2.7 BUFFER OVERFLOW

The buffer overflow problem is one of the oldest and most common problems in software development and programming, dating back to the introduction of interactive computing. It can result when a program fills up the assigned buffer of memory with more data than its buffer can hold. When the program begins to write beyond the end of the buffer, the program's execution path can be changed, or data can be written into areas used by the operating system itself. This can lead to the insertion of malicious code that can be used to gain administrative privileges on the program or system. Buffer overflows can be created or exploited in a wide variety of ways, but the following is a general example of how a buffer overflow works. A program that is the target of an attack is provided with more data than the application was intended to handle. This can be done by diverse means such as entering too much text into a dialog box, submitting a Web address that is far too long, or creating a network packet much larger than is necessary. The attacked program (target) overruns the memory allocated for input data and writes the excess data into the system memory. The excess data can contain machine language instructions so that when the next step is executed, the attack code, like a Trojan horse or other type of malicious code, is run. (Frequently, the early part of the excess data contains characters that are read by the CPU as "perform no operation," forming a "no-op sled."The malicious code is usually at the end of the excess data.)



Attacker plants code that overflows buffer and corrupts the return address. Instead of returning to the appropriate calling procedure, the modified return address returns control to malicious code, located elsewhere in process memory.

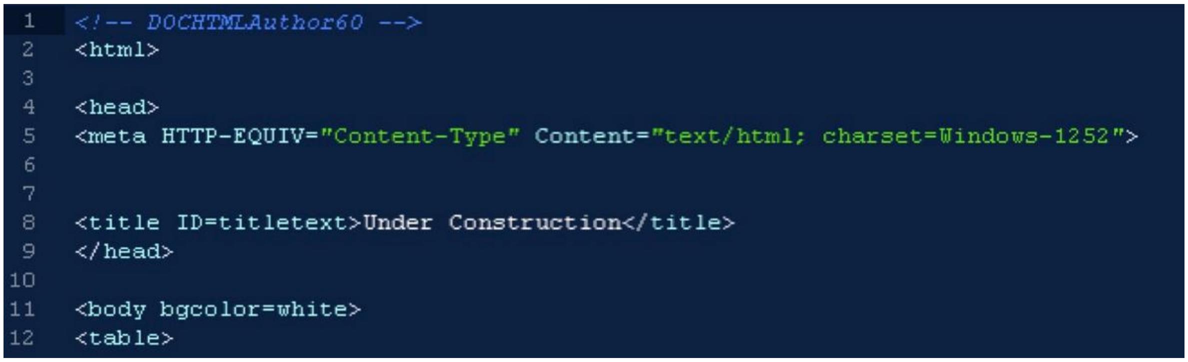
Figure 2.4 - Buffer Overflow (http://cis1.towson.edu/~cssecinj/modules/cs2/buffer-overflow-cs2-java/)

2.8 HTML CODES

Generally most of the web sites contains HTML documents. In this part I would like to explain how the attackers use sensitive information in the HTML code, and how they could use SSI commands to control the web server. Also this part includes the disadvantages of embedding unknown applets into a web site.

2.8.1 Information Disclosure

Shoppers can analys HTML codes on the client side which means that if HTML codes have critical information, an attacker might use it. For example if you use firefox browser, attackers can identify codes as in the example by viewing and selecting source, or pressing Ctrl and u. It is possible to gather sensitive information about the web application such as usernames, passwords and sensitive file locations.



```
<!-- DOCHTMLAuthor60 -->
<html>

<head>
<meta HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">


<title ID=titletext>Under Construction</title>
</head>

<body bgcolor=white>
<table>
```

Figure 2.5 - Target HTML code for attacker (http://blog.accuvant.com/dgriffinaccuvant/anatomy-of-a-targeted-attack/)

2.8.2 Server Side Scripting

Server-side scripting is the term that is used to describe the technology that allows a user to send a request, which is then verified by running a script directly on a web server. The technology provides interactive websites that interface with other databases. Server Side Includes are useful for including a common piece of code throughout a site, such as a page header, a page footer and a navigation menu. Conditional navigation menus can be conditionally included using control directives.

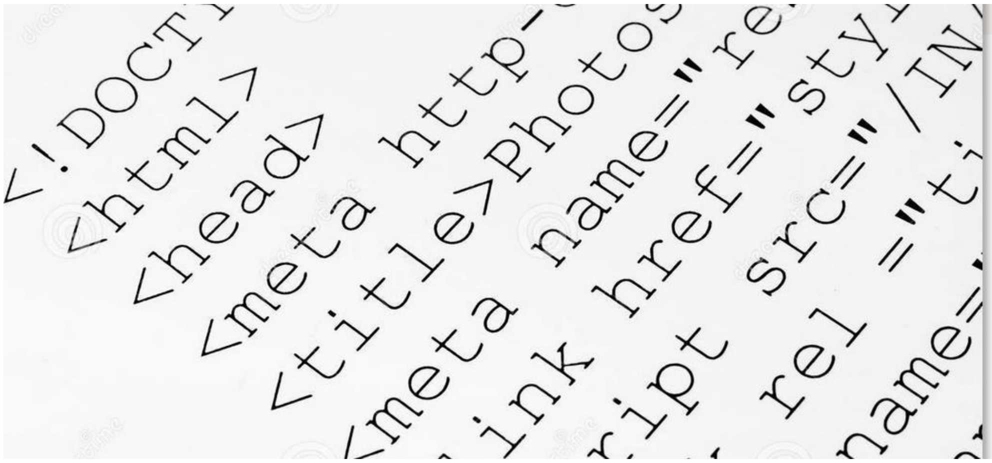


Figure 2.6 - Target HTML code for attacker (http://www.dreamstime.com/royalty-free-stock-photos-printed-internet-html-code-computer-technology-background-image36150358)

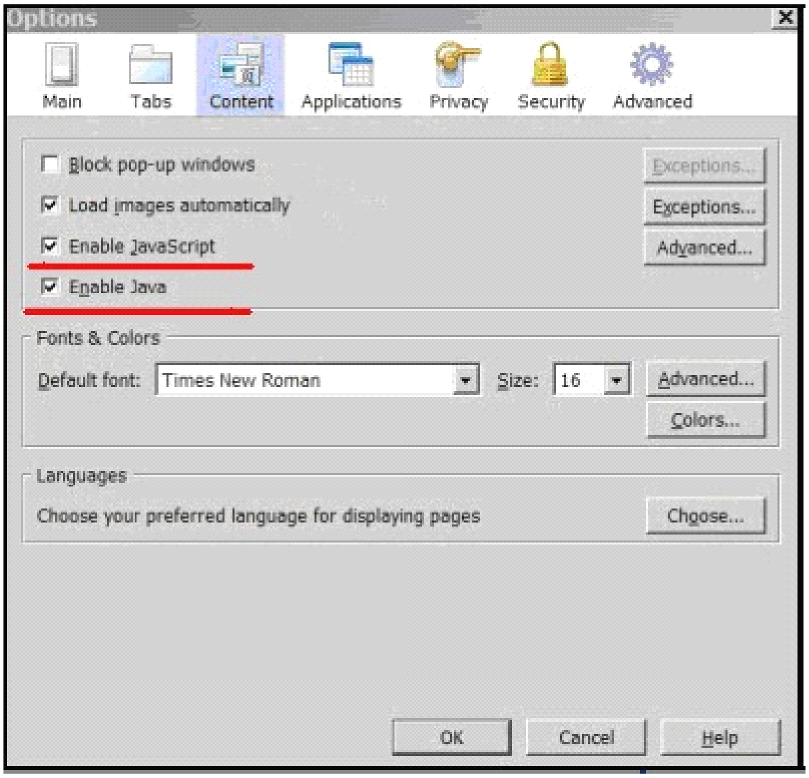
The sign (#) indicates to the web server that the following code is the SSI command. For Example , "echo" is the command, which requires that a web server prints certain data to the client browser. The element "var=" is used to indicate that the phrase is a variable of some kind—most likely in the context of showing an example value, other example is DATE_LOCAL so the web server will print current local time to client browser. By changing the variable, the attackers may utilize the echo command to print the information they need. The attackers can edit the variable of example to DOCUMENT_URI, which is other common variable in SSI, and DOCUMENT_URI displays to the attackers current document names and path. Other example the "include" command tells the web server to invoke another file into the HTML documents, so that shoppers will see the text or pictures from the another file. If an administrator does not set proper permission of sensitive documents, an attacker will use the "include" instruction to discover the content of the documents, which may include the shoppers' sensitive information. The instruction "exec" runs the program on the system or r the shell scripts' file. If a web site does not need this command, its administrator could disable it by selecting "IncludesNOEXEC" option. In the case of HTML, code is elements, attribute names, entities, comments. Data is everything else. Data must be escaped to avoid being mistaken for code. In case of URLs, code is the scheme, the host name, the path, the mechanism of the query string (?, &, =, #). Data is everything in the query string: parameter names and values. They must be escaped to avoid being mistaken for code.

2.8.3 Activex, Java And Javascript

Java provides examples of a number of other points related to the security of software and development. At the time the bytecode is interpreted, Java checks the use of variables and memory by the application. This check can be a good thing for security, or a bad thing. In general it is good, since programs use memory properly, and do not exceed set bounds. However, overreliance on such functions if developers do not use additional security checks in their code may result in sloppy practices that lead to other security problems. ActiveX work quite similarly to Java applets; it is embedded in HTML documents and runs applets after the shoppers have downloaded them into their computers' memory. For example, Java is usually held to be very good at garbage collection, the automatic review of memory locations, and the de-allocation of memory areas that are no longer required. This is good in that it ensures the program does not fill all available memory and then run into problems.

The difference between Java and ActiveX is that Java can be run on virtually any OS such as Windows, Linux, and Macintosh, whereas ActiveX components are distributed as compiled binaries, so they will only work on the operating system for which they were programmed (Forristal, 2001).

JavaScript is a language most commonly used in Web pages. However, it is not Java and has no relation to Java. It was originally named LiveScript and was renamed as a marketing strategy. It is interpreted by the user’s Web browser and allows control over most of the features of the Web browser. It has access to most of the contents of the Hypertext Markup Language (HTML) document and has full interaction with the displayed content. Depending upon the browser, it may have significant access to the system itself. As opposed to Java, which has sandbox restrictions for applets and an extensive security model, security management in JavaScript is minimal; it is either enabled or disabled. This feature of JavaScript is convenient for the shoppers. But JavaScript may contain malicious codes as well, especially, the codes written by unknown parties. Is it possible to reduce this kind of rogue applets? The answer is positive. First of all, programmers need to read the code of each applet before they apply it in the HTML code. Programmers need to recognize the entire codes of the applets and ensure that the code can be trusted. In the contrary, programmers should not use those applets without testing. On the other hand, traders can use applets and ActiveX components, which are formed by well-known companies. For example, Microsoft publishes many code samples on the web site, which programmers could use these codes while they design the e-commerce web site. The shoppers need to read those information boxes, which ask them to install the ActiveX control. Users can turn off the functions of ActiveX ,Java and JavaScript, and from the browsers’ menu. Figure 2.7 shows how to turn off JavaScript and Java in the Firefox browser.



☐ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

Fonts & Colors

Default font: Times New Roman Size: 16

Languages

Choose your preferred language for displaying pages

Figure 2.7 - Firefox Options to enable/disable JavaScript and Java
(http://www.alanwood.net/demos/enabling-javascript.html)

2.9 COMMON SECURITY VULNERABILITIES IN E-COMMERCE SYSTEMS

E-commerce has a lot of advantages, on the other hand we should consider about risks and responsibilities. Testing web applications and managing vulnerabilities are most important issues to build secure environment against data breaches. Because of that it is vital for traders considering security issues while they provide secure e-commerce applications.

According to the Open Web Application Security Project (OWASP):

“Insecure software is already undermining our financial, healthcare, defense, energy, and other critical infrastructure. “ OWASP provides an accessible and thorough framework with processes for web application security. The information security professional should be familiar with the “top ten” web application vulnerabilities and also how to mitigate them. Traders or merchants purchase e-commerce applications should evaluate according to PA-

DSS. Also data encryption plays a central role in securing online transactions. Encryption ensures transaction privacy to prevent unauthorized access to confidential transactions. Authentication protocols allow each party to an online transaction to verify each other’ s identity. Often this is accomplished using digital certificates or username/password across an encrypted transport such as SSL. To ensure that transactions have not been modified in transit by a third party, cryptographic hashing is used. Digital signatures are sometimes used to prevent a party from denying they ever received or sent a particular message or transaction, or nonrepudiation.

2.9.1 Vulnerabilities Caused By Insecure Coding Practices

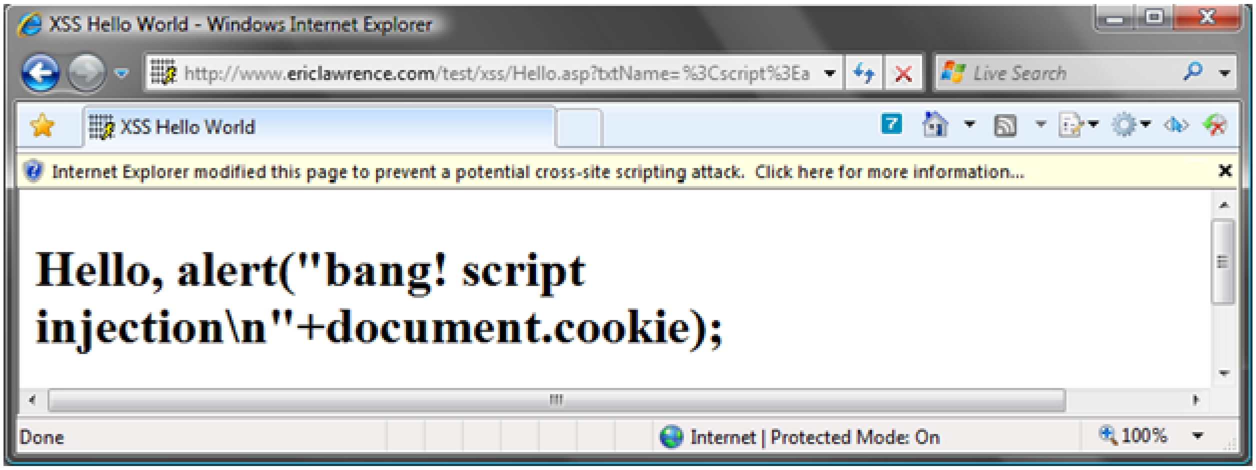
Some common vulnerabilities in web applications (such as e-commerce shopping carts) can be categorized as following sections.

2.9.1.1 Injection Flaws

Injection flaws allow attackers to relay malicious code through a web application to another system. These attacks include calls to the operating system via system calls, the use of external programs via shell commands, as well as calls to backend databases via SQL (i.e., SQL injection). Whole scripts written in perl, python, and other languages can be injected into poorly designed web applications and executed. Any time a web application uses an interpreter of any type there is a danger of an injection attack.

2.9.1.2 Cross-Site Scripting (Xss)

XSS is one of the most common application-layer web attacks. XSS commonly targets scripts embedded in a page which are executed on the client-side (in the user’s web browser as in the example) rather than on the server-side. XSS in itself is a threat which is brought about by the internet security weaknesses of client-side scripting languages, with HTML and JavaScript (others being VBScript, ActiveX, HTML, or Flash) as the prime culprits for this exploit. The concept of XSS is to manipulate client-side scripts of a web application to execute in the manner desired by the malicious user.


XSS Hello World - Windows Internet Explorer
http://www.ericlawrence.com/test/xss/Hello.asp?txtName=%3Cscript%3Ea
Live Search
XSS Hello World
Done
Internet | Protected Mode: On
100%

Internet Explorer modified this page to prevent a potential cross-site scripting attack. Click here for more information...

Hello, alert("bang! script injection\n"+document.cookie);

Figure 2.8 - XSS Attacks (http://www.zdnet.com/blog/security/anti-malware-blocker-cross-site-scripting-protections-coming-in-ie-8/1396**)**

2.9.1.3 Cross-Site Request Forgery (CSRF)

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user (WEB_11 , 2013).

2.9.1.4 Buffer Overflows

The most effective defense against a buffer overflow attack is bounds checking. A buffer is a portion of system memory that is used to temporarily store information for processing. Buffers are essential to computer operations for managing data input and output at all levels of system interaction. Buffer overflows can also be used to inject malicious software for processing on behalf of the attacker. Buffer overflows are typically the result of poor application or system memory management. Buffer overflows are one of the oldest and most common forms of system exploit in use today.

2.9.1.5 Weak Authentication And/Or Session Credentials

Weak authentication not only makes it easier for an attacker to take control of an account with no accountability but also allows users to blame weak authentication on account abuses. Strong authentication such as biometrics helps ensure non-repudiation by strongly associating something only one individual has to an account.

2.9.2 Security Misconfigurations

Lots of security configuration baselines can be used to determine and secure the infrastructure of an application stack or network, for example operating systems, servers, databases, or piece of codes. Software developers and administrators should work together to ensure that the application or network infrastructure is configured properly. Some of scanners or patch management systems should be used to manage missing patches, misconfigurations, built-in default accounts, insecure or useless services, etc. Especially security configuration areas addressed in PCI DSS include:

- Secure configuration of the DMZ to limit inbound traffic to only those components intended to provide authorized, publicly accessible services, and to prohibit unauthorized outbound traffic (PCI DSS Requirements 1.3.1 and 1.3.4)

- Secure system configuration and changing vendor-supplied default passwords and settings (PCI DSS Requirement 2)

- Using secure encryption mechanisms when transmitting data over the Internet (PCI DSS Requirement 4)

- Protecting e-commerce components from known malware (PCI DSS Requirement 5)

- Keeping all software and network components up to date with vendor-supplied patches (PCI DSS Requirement 6.1)

- Using secure software development and coding practices for websites (PCI DSS Requirements 6.3 – 6.5)

- Implementing a process to address new security vulnerabilities (PCI DSS Requirements 6.1, 6.2, 6.6 and 11.2)

- Limiting access to only those users with a need to know and requiring strong authentication credentials for those with access (PCI DSS Requirements 7 and 8)
- Logging and monitoring (PCI DSS Requirements 10 and 11)

2.10 REPLAY ATTACKS

This attack is meant to disrupt and damage processing by the attacker sending repeated files to the host. If there are no checks or sequence verification codes in the receiving software, the system might process duplicate files (Tipton, 2013).

- Why replay attacks?
  - To gain access to resources by replaying an authentication message
  - In a denial-of-service attack, to confuse the destination host

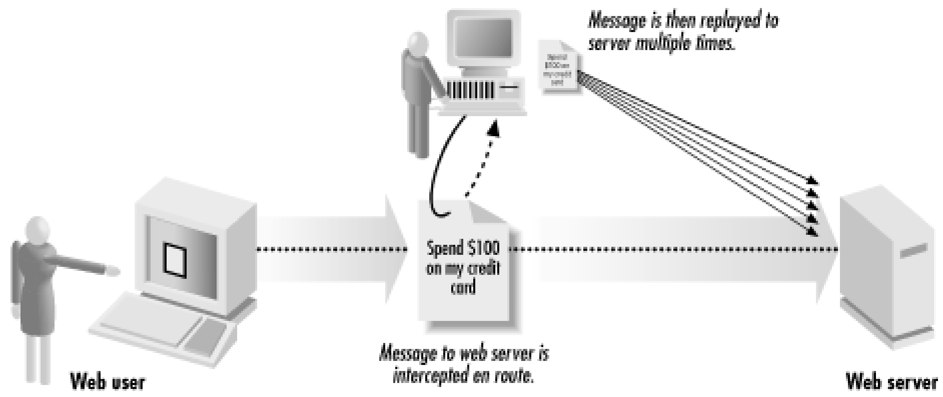

Message is then replayed to server multiple times.
Spend $100 on my credit card
Message to web server is intercepted en route.
Web user
Web server

Figure 2.9 - Replay Attack (http://flylib.com/books/en/2.513.1.29/1/)

2.10.1 Thwarting Replay Attacks

- Put a time stamp in each message to ensure that the message is "fresh"
  - Do not accept a message that is too old

- Place a sequence number in each message
  - Do not accept a duplicated message

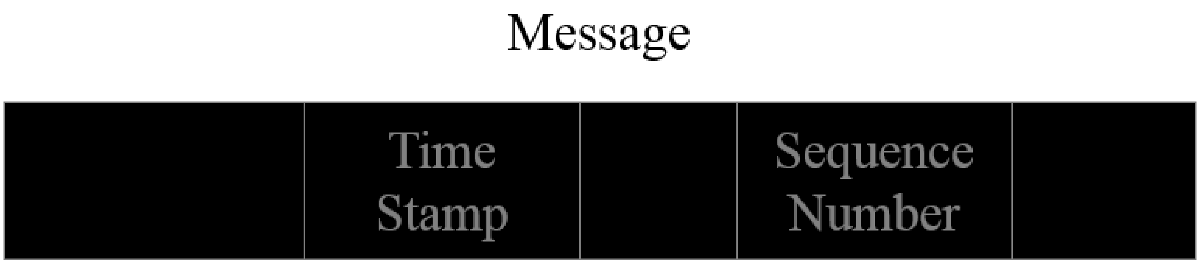


Figure 2.10 - Message

- In request-response applications,
  - Sender of request generates a nonce (random number)
  - Places the nonce in the request
  - Server places the nonce in the response
  - Neither party accepts duplicate nonces

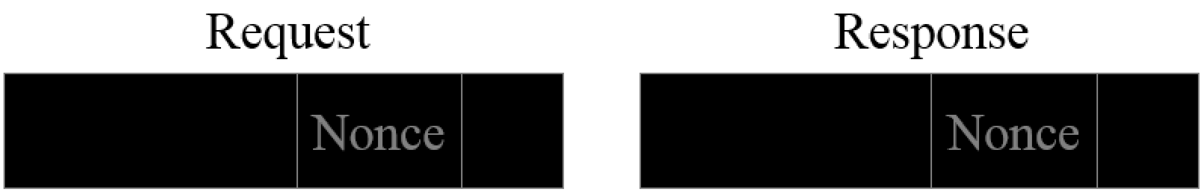
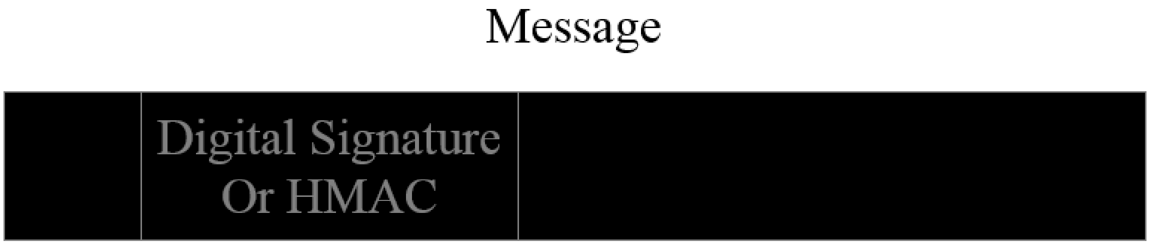


Figure 2.11 – Response-Request

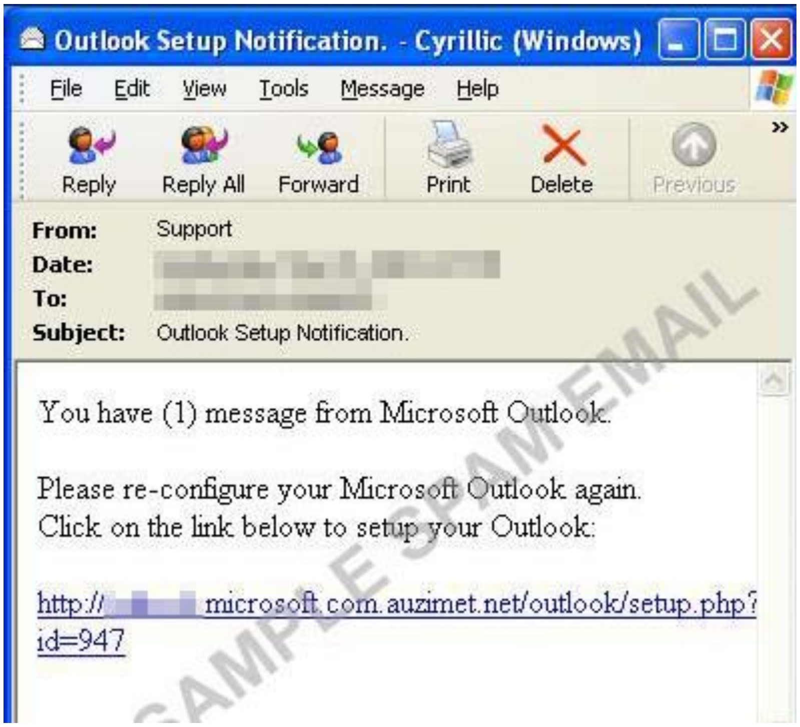
- To prevent changes in the message being replayed
  - Message integrity is needed
  - Requires a digital signature or equivalent

- See HMAC under IPsec



2.11 PHISHING ATTACKS

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication (Merwe, A J, Dabrowski, 2005). Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include flegislation, user training, public awareness, and technical security measures.



From: Support
Date: [redacted]
To: [redacted]
Subject: Outlook Setup Notification.

You have (1) message from Microsoft Outlook.

Please re-configure your Microsoft Outlook again.
Click on the link below to setup your Outlook:

http://[redacted]microsoft.com.auzimet.net/outlook/setup.php?id=947

Figure 2.12 – Phishing Attack (http://blog.trendmicro.com/trendlabs-security-intelligence/phishing-attack-targets-microsoft-outlook-users/)

2.11.1 Phishing Techniques

Email / Spam : Phishers may send the same email to millions of users, requesting them to fill in personal details.

Web Based Delivery : The phisher traces details during a transaction between the legitimate website and the user. As the user continues to pass information, it is gathered by the phishers, without the user knowing about it.

Instant Messaging : Instant messaging is the method in which the user receives a message with a link directing them to a fake phishing website which has the same look and feel as the legitimate website.

Trojan Hosts : Trojan hosts are invisible hackers trying to log into your user account to collect credentials through the local machine. The acquired information is then transmitted to phishers.

Link Manipulation : Link manipulation is the technique in which the phisher sends a link to a website. When the user clicks on the deceptive link, it opens up the phisher's website instead of the website mentioned in the link. One of the anti-phishing techniques used to prevent link manipulation is to move the mouse over the link to view the actual address.

Key Loggers : Key loggers refer to the malware used to identify inputs from the keyboard.

Session Hacking : In session hacking, the phisher exploits the web session control mechanism to steal information from the user. In a simple session hacking procedure known as session sniffing, the phisher can use a sniffer to intercept relevant information so that he or she can access the Web server illegally.

System Reconfiguration : Phishers may send a message whereby the user is asked to reconfigure the settings of the computer. The message may come from a web address which resembles a reliable source.

Content Injection : Content injection is the technique where the phisher changes a part of the content on the page of a reliable website. This is done to mislead the user to go to a page outside the legitimate website where the user is asked to enter personal information.

Phishing through Search Engines : Spammers and hackers manipulate search engines to direct web users to fake websites, gather their personal details and swindle them before absconding. Most times it is very difficult to track them back as they make use of fake identities and dynamic addresses. Hackers make their websites popular by blog spamming, forum spamming, keyword stuffing, and adding backlinks to their websites on reputable sites. Keywords, link popularity, traffic derivation etc all play a crucial part in deciding the fate of the website. Search engine algorithms make use of these factors to index websites and rank them accordingly. Hackers have embedded corrupted links on several forums and blogs. A click on the link establishes a connection with automated programs that aids the hackers in accessing the particular work station from which the click was generated.

Phone Phishing : In phone phishing, the phisher makes phone **calls** to the user and asks the user to dial a number. The purpose is to get personal information of the bank account through the phone. Phone phishing is mostly done with a fake caller ID

Malware Phishing : Phishing scams involving malware require it to be run on the user's computer. The malware is usually attached to the email sent to the user by the phishers. Once you click on the link, the malware will start functioning. Sometimes, the malware may also be attached to downloadable files.

2.12 MALICIOUS CODE ATTACKS

Weak controls on software can subject a system to compromise through the introduction of backdoors and malicious code such as Trojan horses, viruses, and worms. Software, particularly malicious software, has traditionally been seen in terms of a tool for the attacker. The only value that has been seen in the study of such software is in regard to protection against malicious code. However, experience in the virus research field, and more recent studies in detecting plagiarism, indicates that evidence of intention can be gained, and cultural and individual identity, from the examination of software itself.

2.13 PHARMING ATTACKS

Pharming is the evil cousin of phishing which doesn't rely on sending e-mails to thousands of online users in order to trap them. What makes pharming dangerous is that the attack is unrecognizable to even an alert user. Pharming leverages malicious code such as viruses, worms, trojans and spyware to carry out sophisticated attacks such as hosts file modification, DNS cache poisoning etc. Pharmers can even hijack domains or spoof static domain names in order to fool users by redirecting them to malicious websites.

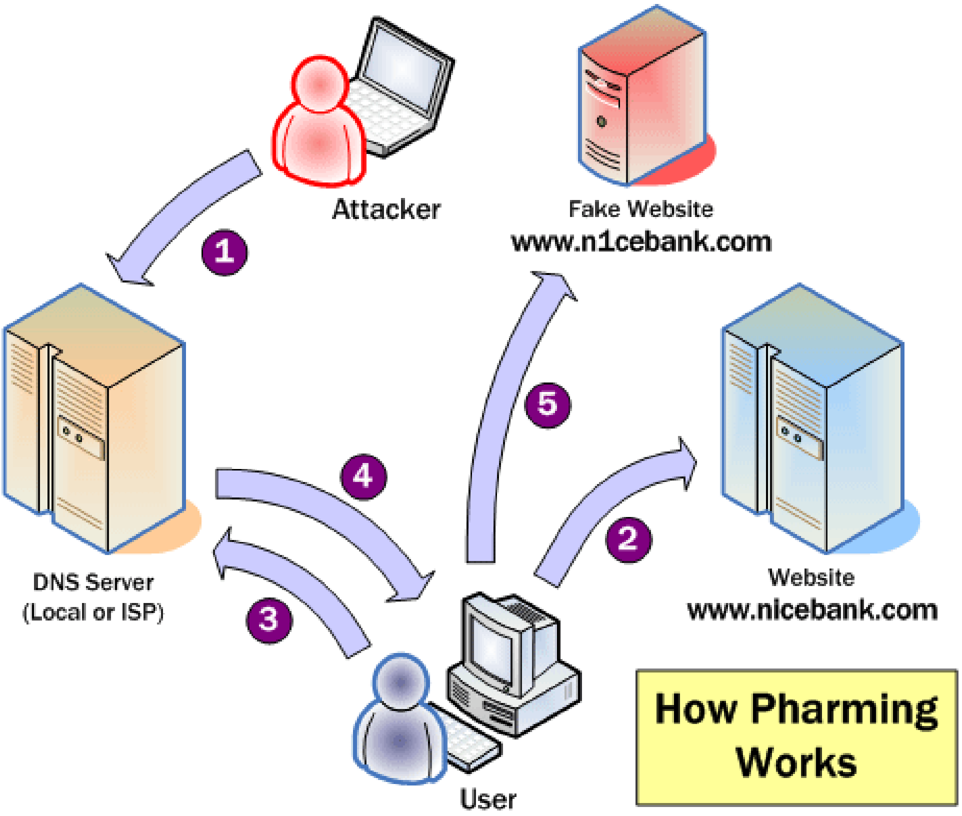


Figure 2.13 - Pharming Attack (http://palizine.plynt.com/issues/2006Mar/pharming/)

2.13.1 Pharming Techniques

Pharming, as mentioned earlier, relies on changing the DNS entries of the organization's website. There are multiple ways to accomplish this; (SANS Institute, (2007))

Hosts file modification: Most OS store files locally which consist of a mapping between the domain name and the corresponding IP address e.g. www.xyzbank.com maps to say 210.10.10.3 Phishers can benefit from this OS vulnerability by modifying these host lookup files with malicious mapping e.g. they can map www.xyzbank.com to say 230.10.10.3 which is actually the IP address of the malicious website.

DNS cache poisoning : DNS servers, for a limited amount of time, cache the queries made by the users. Caching is done to speed up the user response times for frequently used domains in order to enhance the user experience. Phishers can poison the DNS cache itself, which contains the alias to IP address mapping, by inserting malicious content to lead users to fake where they are asked to update their personal information, such as passwords and credit cards, social security and bank account numbers.

Usage of Malwares :

Usage of malwares have become very common with pharmers deploying Viruses and Trojans on the user's system which intercept user requests to visit a particular site or webpage, such as xyzbank.com, and redirects him/her to the site the pharmer has set up.

Domain Hijacking :

The pharmer may hijack or steal an organization's website, by techniques like Domain Slamming and Domain Expiration, which allow them to redirect all legitimate Internet traffic to an illegitimate site. In Domain slamming a pharmer can submit domain transfer requests and switch a domain from one registrar to another. The account holder at the new registrar can then alter routing instructions to point to a different, illegitimate server. In Domain expiration the domain names are leased for fixed periods and failure to manage the leasing process properly could result in a legitimate ownership transfer possibly to a pharmer.

Static domain name spoofing: The pharmer may attempt to take advantage of slight misspellings in domain names to trick users into accidentally visiting the malicious website e.g. a pharmer may redirect a user to xyzbnk.com instead of xyzbank.com, the site the user actually wanted to access.

2.14 TROJAN HORSES

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer. A Trojan often acts as a backdoor, contacting a controller which can then have unauthorized access to the affected computer. The Trojan and backdoors are not themselves easily detectable, but if they carry out significant computing or communications activity may cause the computer to run noticeably slowly. Some of Trojan types are:

Password stealers, Destructive Trojans(Ransom Trojan, security software disabler), Remote Access Trojan (DoS attack, Trojan Clicker, Proxy Trojan), Mailfinder Trojans, Trojan FakeAV, Trojan Spy, Trojan-ArcBomb, Trojan SMS, e-banking Trojans etc…

Famous computer Trojans are Beast, which made the client-server model very popular. The server being on the infected computer and the client on the operator. Its many features and the ease of use for the client made it very popular. Another Backdoor that was very popular and well-known is Sub7. Zeus on the other hand started as a banker Trojan, originally aimed at a limited group of people, but years later the various Zeus' botnets are estimated to include millions of compromised computers. A more recent giant is the ZeroAccess Rootkit, held responsible for a botnet spread estimated to have been present on millions systems.

Below is an example of E-banking Trojan trying to bypass online banking security ;

(1.) The user is infected by a Trojan when visiting a compromised website. The site scans the user's computer for vulnerabilities and, when it finds one, it injects a Trojan.

(2.) By monitoring all the user's online activity, the Trojan collects and transmits login credentials, phone numbers and other sensitive data to the attacker.

(3.) The attacker sends a phishing SMS to the victim's cell phone using the number stolen at Step 2. The message is intended to persuade the user to click on a link

(4.) Upload a mobile Trojan to the user's cell phone.

(5.) The attacker performs an unauthorized funds transfer using the stolen login credentials.

(6.) The bank sends an SMS with confirmation code to the compromised cell phone.

(7.) The cell phone silently sends this code to the attacker, which is then used to confirm the transaction

(8.) Steps 5-8 can be repeated many times, because the Trojan masks true funds amount and displays only the online banking page the user expects to see.

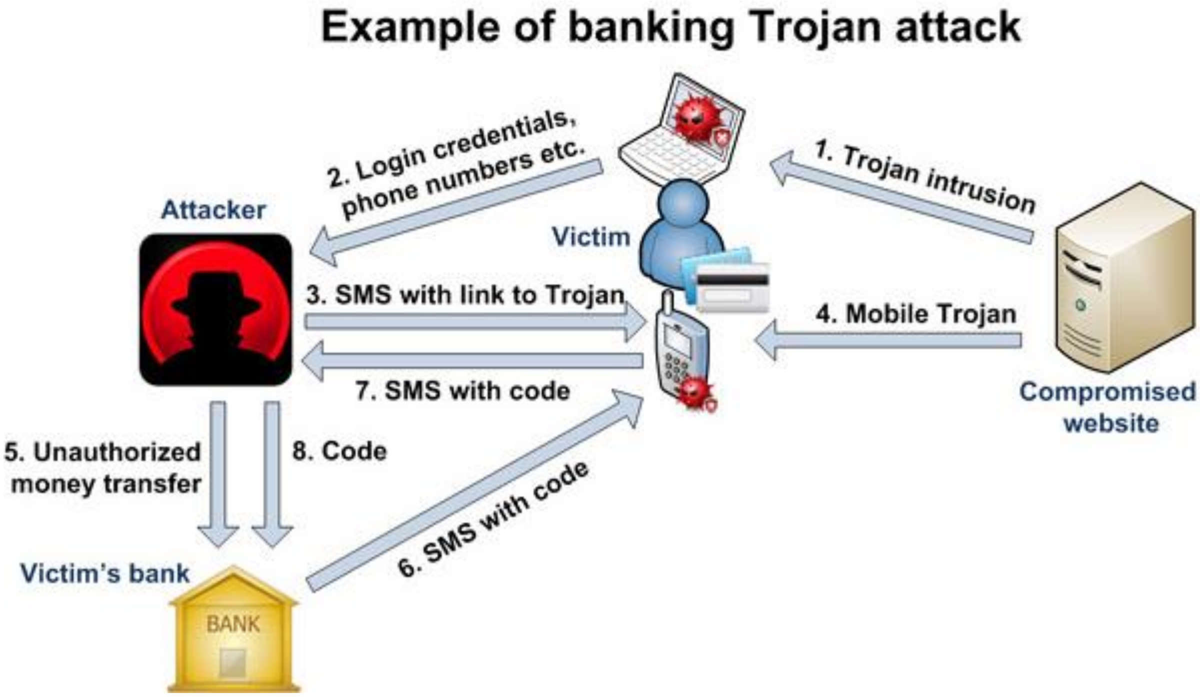

Example of banking Trojan attack
1. Trojan intrusion
2. Login credentials, phone numbers etc.
Attacker
Victim
3. SMS with link to Trojan
4. Mobile Trojan
7. SMS with code
Compromised website
5. Unauthorized money transfer
8. Code
6. SMS with code
Victim's bank
BANK

Figure 2.14 - E-banking Trojan (http://www.safensoft.com/Online_Banking_Security/)

CHAPTER III

METHODS OF SECURING E-COMMERCE

3.1 E-COMMERCE SECURITY POLICIES AND TRAINING

When an organization is concerned about protecting its e-commerce assets, they should have a security policy in place. A security policy is a written statement describing which assets to protect and why they are being protected, who is responsible for that protection, and which behaviors are acceptable and which are not. The policy must address physical security, network security, access authorizations, virus protection,and disaster recovery. Policies form the foundation of an organization's expectations for its employees. Information security policy is crucial in ensuring an organization conveys the significance of information security and also is able to enforce information security should the need arise. The first step an organization must take in creating a security policy is to determine which assets to protect from which threats; a company that stores its customers' credit card numbers might decide that those numbers are an asset that must be protected from eavesdroppers; then the organization must determine who should have access to various parts of the system; next, the organization determines what resources are available to protect the assets identified. Using the information it has acquired, the organization develops a written security policy. Finally, the organization commits to resources to building software, hardware, and physical barriers that implement the security policy.

A comprehensive plan for security should protect a system's privacy, integrity, and availability, and authenticate users.

* Secrecy-Prevent unauthorized persons from reading messages and business plans, obtaining credit card numbers or deriving other confidential information.

* Integrity-Enclose info in a digital envelope so that the computer can automatically detect messages that have been altered in transit.

* Availability-Provide delivery assurance for each message segment so that messages or message segments cannot be lost undetectably.

* Key management-Provide secure distribution and management of keys needed to provide secure communications.

* Formally define a policy creation and policy maintenance practice: A clearly defined process for initiating, creating, reviewing, recommending, approving, and distributing policies communicates the roles and responsibilities of all parties.

*Employees should acknowledge policies: All users should sign an acknowledgement that they have read and understand the policies. While this does not ensure that they have read or understand the policies, it will help to protect the organization if a user' s behavior violates the policy. Typically this may be part of an information security awareness or training program.

3.1.1 Authentication Data Security

Equally as important as the access control system is to an organization are the controls that protect the authentication data itself. The authentication data include user identities, passwords, biometric information, access capabilities, and a host of other sensitive information which if obtained by an attacker, would provide a roadmap for infiltrating and navigating around an organization's information systems. The protections around the authentication database should be researched and tested before the system is implemented. Data encryption should be in place, system and file-level access controls should be present, and strong authentication for administrative functions should be investigated.

3.1.2 Social Engineering Tricks

The best method of preventing social engineering is to make users aware of the threat and give them the proper procedures for handling unusual or what may seem usual requests for information. For example, if a user were to receive a phone call from a “system administrator” asking for their password, users should be aware of social engineering threats and ask that the system administrator come to their office to discuss the problems in a face-to-face format.

3.2 SETTING STRONG PASSWORD

Here is a review of tactics to use when choosing a password (WEB_12, 2009) :

-Don't use passwords that are based on personal information that can be easily accessed or guessed.
-Don't use words that can be found in any dictionary of any language.
-Develop a mnemonic for remembering complex passwords.
-Use both lowercase and capital letters.
-Use a combination of letters, numbers, and special characters.
-Use passphrases when you can.
-Use different passwords on different systems

3.3 COOKIE MANAGEMENT

When shoppers open an account in a web shop, they may use a cookie to store their passwords, Email addresses, account numbers and so on, so shoppers do not need to enter this information again when they login to the web site again. Basically, websites also use cookies to manage shopping carts and authenticate users (Schrenk, 2007). The feature of cookies provides convenient service to shoppers, but it also provides a chance for an attacker to steal information. Once shoppers apply cookies, the certain information shoppers enter into the web site will be recorded into the shoppers' disk or hard drive. When attackers compromise the victims' device, they try to get the cookies and the sensitive user session informations. Because of that security issues users should configure their browsers depends on the security best practice for example to turn off or disable cookies.

A banking or e-commerce site may restrict their cookies to only SSL, while a blog or news aggregator may want to leave things more open. Cookies remain the basic method of identify tracking on most websites and keeping them secure is a vital part to keeping applications as a whole locked down and secure. In this article we went over four methods for protecting cookies on a general level.

When using cookies its important to remember to:

-Limit the amount of sensitive information stored in the cookie.

-Limit the subdomains and paths to prevent interception by another application.

-Enforce SSL so the cookie isn’t sent in cleartext.

-Make the cookie HttpOnly so its not accessible to javascript.

3.4 HOST BASED FIREWALL

A host-based firewall is a piece of software running on a single host that can restrict incoming and outgoing network activity for that host only. They can prevent a host from becoming infectedand stop infected hosts from spreading malware to other hosts. While firewalls and IPS are normally associated with network partitioning and the enforcement of security zones of control, they are also frequently used to protect individual hosts from attack. Software or hardware-based firewalls can be implemented within individual hosts to control traffic to and from a particular system. Unlike network firewalls, many personal firewalls are able to control network traffic allowed to programs on the firewalled computer. When an application attempts an outbound connection, the firewall may block it if blacklisted, or ask the user whether to blacklist it if it is not yet known. This protects against malware implemented as an executable program. Personal firewalls may also provide some level of intrusion detection, allowing the software to terminate or block connectivity where it suspects an intrusion is being attempted.

3.5 ENCRYPTION AND DECRYPTION ALGORITHM

3.5.1 Cryptography

Several common methods of cryptography exist including stream-based and block ciphers. The information security professional must have a basic understanding of both to ensure further understanding of encryption implementations (F. Tipton, 2013).

-Stream-Based Ciphers

There are two primary methods of encrypting data: the stream and block methods. When a cryptosystem performs its encryption on a bit-by-bit basis, it is called a streambased cipher. This is the method most commonly associated with streaming applications, such as voice or video transmission. Wired Equivalent Privacy (WEP), uses a streaming cipher, RC4, but is not considered secure due to a number of weaknesses that expose the encryption key to an attacker, weak key size and other vulnerabilities in WEP implementation. Newer wireless cryptography implements block ciphers such as Advanced Encryption Standard (AES), which provides stronger security. The cryptographic operation for a stream-based cipher is to mix the plaintext with a keystream that is generated by the cryptosystem. The mixing operation is usually an exclusive-or (XOR) operation‒a very fast mathematical operation.

-Block Ciphers

A block cipher operates on blocks or chunks of text. As plaintext is fed into the cryptosystem, it is divided into blocks of a preset size‒often a multiple of the ASCII character size‒64, 128, 192 bits, etc. Most block ciphers use a combination of substitution and transposition to perform their operations. This makes a block cipher relatively stronger than most stream-based ciphers, but more computationally intensive and usually more expensive to implement. This is also why many stream-based ciphers are implemented in hardware, whereas a block-based cipher is implemented in software.

Block chipher encryption modes are Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter (CTR) modes. (J.S. , 2004)

-Initialization Vectors (IV)—Why Needed

Because messages may be of any length, and because encrypting the same plaintext using the same key always produces the same ciphertext as described below, several “modes of operation” have been invented, which allow block ciphers to provide confidentiality for messages of arbitrary length (See Table 3.1 for block cipher mode descriptions). The use of various modes answers the need for unpredictability into the keystream such that even if the same key is used to encrypt the same message the ciphertext will still be different each time.

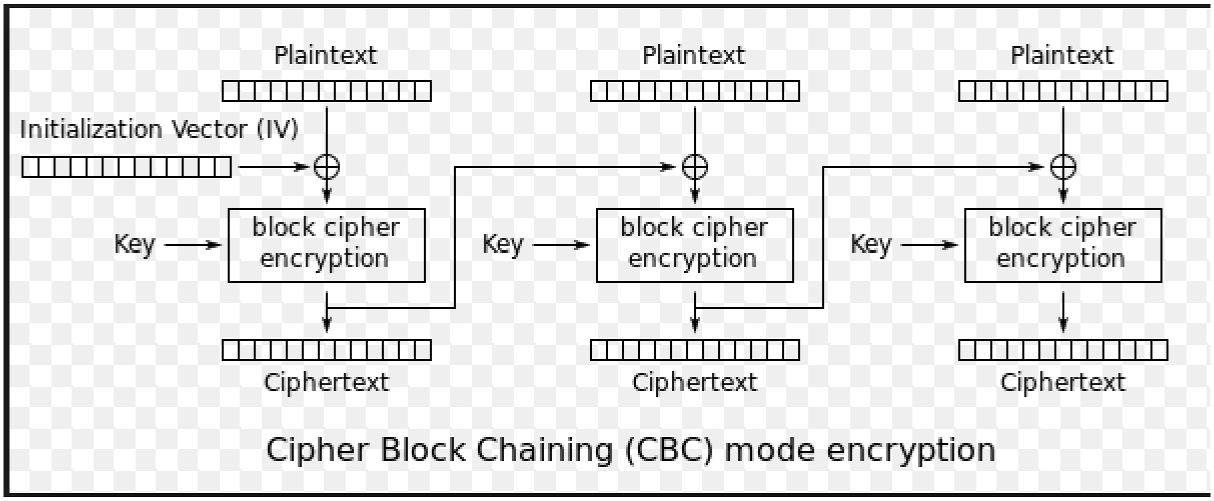


Figure 3.1 - Initializing vector (http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation)

3.5.2 Encryption

The role of cryptography in e-commerce continues to be as an enabler of trust between business entities and between consumer and business. Encryption is the process of converting the message from its plaintext to ciphertext. Encryption is becoming more a generic technology, Integrated into an ever increasing number of applications and products. Voice and data are increasingly converging onto a single, Internet Protocol (IP) based transport network. Technology has reached the point where voice/data can be transmitted via Internet telephony, encrypted mobile phones, or stored on computers using disk encryption. The wide use of encryption technology can be seen in many news reports about terrorist attacks and serious domestic crimes includes findings that these technologies have been employed in perpetrating crime. The main technologic methods for lawful access to private data are key escrow, where a third party, possibly a government entity or service provider, holds a copy of the cryptographic keys, and brute force, where massive computer resources attack the key.

3.6 DIGITAL SIGNATURES

A digital signature is intended to be comparable to a handwritten signature on an important document such as a contract. It is important to note that a digital signature is a mathematical representation and conveys specific meaning in binary data, and is not the same as a “digitized signature.” A digitized signature is a representation of a handwritten personal signature as can be created using a scanner or fax machine (Tipton , 2013).

3.7 DIGITAL CERTIFICATE

A Digital Certificate is an electronic document that contains the name of an organization or individual, the business address, the digital signature of the certificate authority issuing the certificate, the certificate holder’s public key, a serial number, and the expiration date. The certificate is used to identify the certificate holder when conducting electronic transactions. Certificate Authority (CA) is an entity trusted by one or more users as an authority in a network that issues, revokes, and manages digital certificates. The most common use of PKE for e-commerce involves the use of so-called Digital Certificates issued by "trusted" third parties. Here's how this one works. Say you are a customer of Big Safe Bank and you would like to communicate with your bank. If you sent the bank some information (for instance, "please wire the contents of my savings account to a new account in Switzerland"), you might worry that the information could get intercepted en route but you might also worry that the bank would not know it was you who sent the information. You and Big Safe Bank agree to use a trusted third party to help you communicate in an encrypted manner to one another over the Internet. The bank contracts with VeriSign or another provider of a Digital Certificates. When you send a message to the bank, you send your message about wiring funds encrypted twice: once with your own private key, and once with the bank's public key, along with a certificate, encrypted using the institution's private key. Once the bank gets your message, they use the institution's private key to decrypt the certificate, which in turn gives the bank your public key (WEB_13, 2014).

3.8 SSL AND TLS

-Secure Sockets Layer Protocol

SSL is one of the most common protocols used to protect Internet traffic. It encrypts the messages using symmetric algorithms, such as IDEA, DES, 3DES, and Fortezza, and also calculates the MAC for the message using MD5 or SHA-1. The MAC is appended to the message and encrypted along with the message data. The exchange of the symmetric keys is accomplished through various versions of Diffie-Hellmann or RSA. According to the Internet Draft of the SSL Protocol, the point of the protocol “is to provide privacy and reliability between two communicating applications. The protocol release further explains that three points combine to provide connection security (WEB_14, 2014). These points are:

· Privacy - connection through encryption

· Identity authentication – identification through certificates

· Reliability –dependable maintenance of a secure connection through message integrity checking.

The SSL version 3.0 is released by Netscape in 1999. The Internet Engineering Task Force (IETF) has created a similar protocol in an attempt to standardize SSL within the Internet community. This protocol, the Transport Layer Security (TLS) protocol.

-Transport Layer Security (TLS) protocol

TLS is the Internet standard based on SSLv3. TLSv1 is backward compatible with SSLv3. It uses the same algorithms as SSLv3; however, it computes an HMAC instead of a MAC along with other enhancements to improve security.The Transport Layer Security

(TLS) protocol was released in January 1999 to create a standard for private communications. The protocol "allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering or message forgery (SANS Institute, 2003).

3.9 SERVER FIREWALL

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.

Basically, a firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination. Features include logging and reporting, automatic alarms at given thresholds of attack, and a graphical user interface for controlling the firewall. Firewalls provide network level security so it can not detect traffic details for ports 80(http) and 443(https).

3.9.1 Dmz Network

The hosts most vulnerable to attack are those that provide services to users outside of the local area network, such as e-mail, web and Domain Name System (DNS) servers. Because of the increased potential of these hosts suffering an attack, they are placed into this specific sub-network in order to protect the rest of the network if an intruder were to successfully compromise any of them. E-commerce just happens to be the first application to demand the same degree of security behind the firewall as is traditionally applied to the DMZ (Demilitarized Zone). Web servers that communicate with an internal database require access to a database server, which may not be publicly accessible and may contain sensitive information. The web servers can communicate with database servers either directly or through an application firewall for security reasons (Maiwald. 2003).

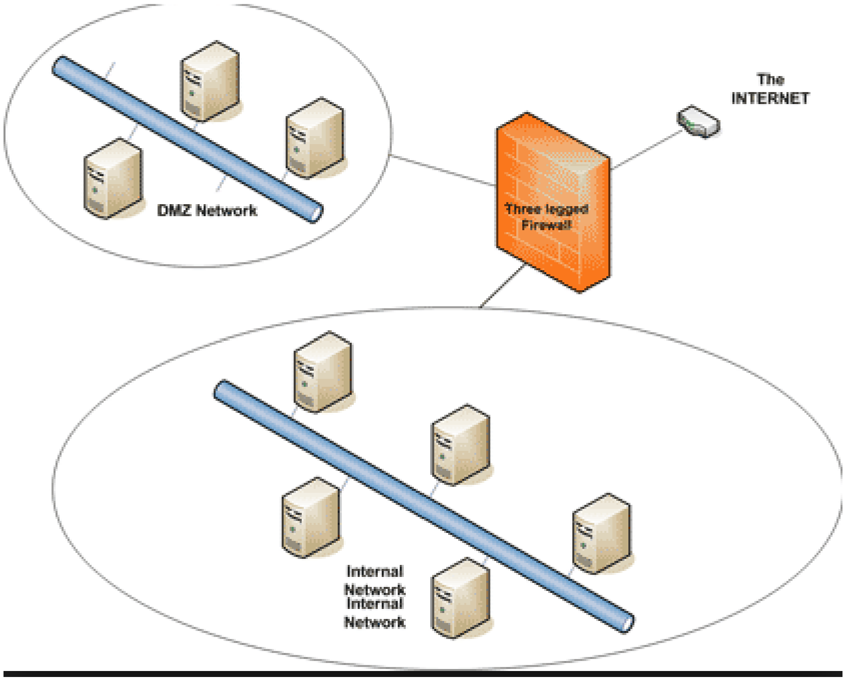


Figure 3.2 - DMZ Network (http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/)

3.9.2 Honeypot

A Honey Pot system is setup to be easier prey for intruders than true production systems but with minor system modifications so that their activity can be logged of traced. The general thought is that once an intruder breaks into a system, they will come back for subsequent visits. During these subsequent visits, additional information can be gathered and additional attempts at file, security and system access on the Honey can be monitored and saved.

Generally, there are two popular reasons or goals behind setting up a Honey Pot:

1. Learn how intruders probe and attempt to gain access to your systems. The general idea is that since a record of the intruder’s activities is kept, you can gain insight into attack methodologies to better protect your real production systems.

2. Gather forensic information required to aid in the apprehension or prosecution of intruders. This is the sort of information often needed to provide law enforcement officials with the details needed to prosecute.

The common line of thought in setting up Honey Pot systems is that it is acceptable to use lies or deception when dealing with intruders. What this means to you when setting up a Honey Pot is that certain goals have to be considered.

3.10 DOS TYPES AND MITIGATION

Denial-of-Service (DoS) attacks represent one of the leading threats to the secure operation of an organization’s technology infrastructure. DoS attacks can range from the consumption of specific system resources, preventing useful processing, and interruption of network resources to preventing communication, rendering a system service or application unusable, or a complete system outage. Any deliberate effort to cut off your web site or network from its intended users qualifies as a DoS attack. Such attacks have been successfully deployed against major online businesses including Visa and Mastercard, Twitter, and WordPress. Some of DDoS mitigation techniques are SYN proxy , connection limiting, aggressive aging ,source rate limiting ,dynamic filtering , anomaly recognition ,granular rate limiting ,white-list, black-list. Generally DDoS attacks are two kinds which is direct and reflected attacks. Reflective attacks are those which employ intermediate hosts for their attacks. From the below figure, the difference between Direct and the Reflective attacks could be well understood. In the direct attack, the attacking system sends out packets directly to the victim but hides its original IP address. It adopts the IP address of some other host which is R in this below diagram. The victim would have its further correspondence with host R assuming it was the source. But in the reflective attacks, the attacker floods millions of reflectors with its source address spoofed with the victim’s. Thus all the reflectors would reply victim flooding its bandwidth (Chang, 2002).

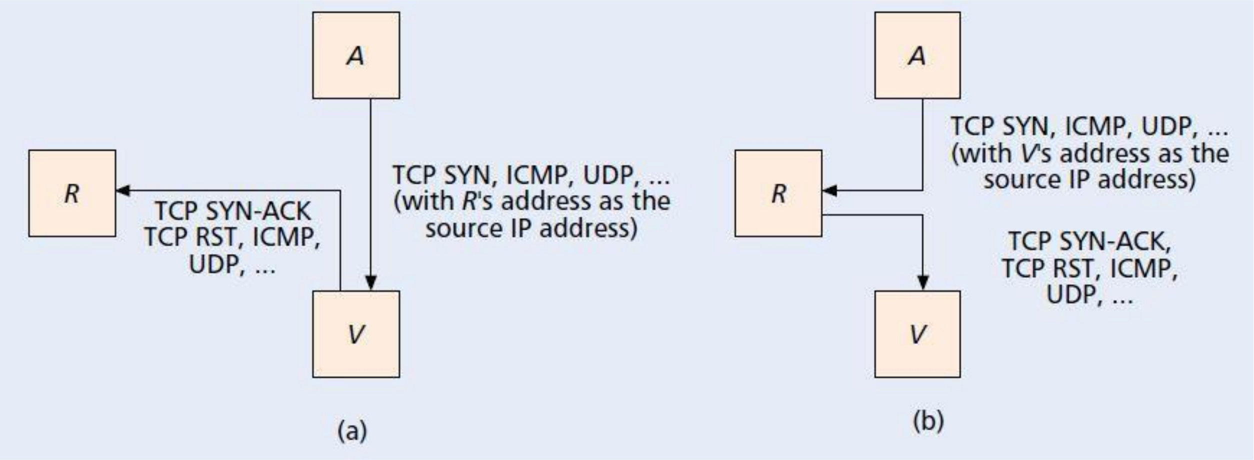


Figure 3.3 - (a) Direct Denial of Service attack (b) Reflective Denial of Service attack
(http://www.sans.org/reading-room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi-33764**)**

3.11 PATCH MANAGEMENT

A key part of configuration and change management involves the deployment of software updates, which is also known as patch management. Flaws in vendor products are continuously discovered. The development and distribution of vendor patches results in a never-ending cycle of required updates to production systems. Managing these updates is not a trivial task for any organization. The patch management process must be formalized through change and configuration management to ensure that changes to existing configurations are carefully controlled. Security-related patches will typically be issued following the discovery or disclosure of a security vulnerability. Vendors will frequently fix security problems in software or firmware through version updates.

3.12 SECURITY LOGS INVESTIGATION

The access information can come from a variety of sources including system logs, file access logs, error logs and security logs to name a few. To ensure successful access audit trails:

-Do not overwrite the security or access logs of a system. Often system administrators will configure log files to overwrite after a certain size is reached. This often removes useful information from historical access events. Determine an appropriate retention period per regulation and business need and ensure the system can support it.

-When a log file is full, ensure it is archived off the system it was created.

-Consider using a SIEM to collect log information for review and access.

-Classify information and know where the most valuable information is processed, stored and transmitted.

-Conform to standard user profiles as much as possible for access as this creates expected access log results including unauthorized behavior, malicious hacks and denials of service (DoS), anomalies and trend analysis. It is the first step in an incident response process.

3.13 INTRUSION PREVENTION AND DETECTION SYTEMS

Intrusion Prevention System (IPS) best provides in constructing a continuous monitoring system, numerous feeds from several systems must be correlated and analyzed. Security perimeters may also include proxies and devices, such as an intrusion detection system (IDS), to warn of suspicious traffic. The defensive perimeter extends out from these first protective devices, to include proactive defense such as boundary routers, which can provide early warning of upstream attacks and threat activities.

IPS and IDS originally were designed to address requirements lacking in most legacy firewalls and traditional perimeter defense systems. IDS solutions are typically used to monitor potential intrusions after the fact, and IPS solutions are focused on identifying and blocking attack traffic. IPS's inherited from their IDS predecessors both a reliance on reactive signatures to detect attacks and an orientation for perimeter security. While both systems play a critical role in preventing external attacks, neither is prepared to completely protect an organization from internal threats (WEB_15, 2014).

3.14 INCIDENT RESPONSE TEAM (IRT)

Keeping organizational information assets secure in today's interconnected computing environment is a true challenge that becomes more difficult with each new "e" product and each new intruder tool. Most organizations realize that there is no one solution or panacea for securing systems and data; instead a multi-layered security strategy is required. One of the layers that many organizations are including in their strategy today is the creation of a Computer Security Incident Response Team, generally called a CSIRT.

CHAPTER IV

ADVANCED SECURITY AND CONTINUITY CONCERNS

4.1 IMPLEMENTING SECURITY POLICIES

The primary and most basic security tool of any organization is security policy. The security policy is the backbone of the entire operation because it defines the rules by which business is conducted (Ryan, Brent, 2000).

4.1.1 Password Policies

In addition to overall user management, it is necessary to define policies, procedures, and controls regarding passwords. The use of passwords is a common practice for validating a user's identity during the authentication process. Given that, in most traditional authentication solutions, the password is the only secret in the transaction, great care should be considered in how passwords are created and managed by users and systems. A process governing user password should consider the following:

-Users should be required to sign a statement agreeing to keep their passwords safe and confidential and to not share, distribute, or write down their passwords.

-All temporary passwords should be permitted to be used only once–to reset the user's password to something that only he or she knows.

- Passwords should never be stored unprotected and in clear text.

-Passwords should have a minimum and maximum length and require the use of various characters and formats to increase their complexity and reduce their susceptibility to brute force and guessing attacks.

-Passwords should be changed regularly.

4.1.2 Types of Policies

A comprehensive security policy is actually made up of several individual policies, each of which target unique lateral aspects of the site's business processes.

Organizational or program policy: This policy is issued by a senior management individual or group, who creates the authority and scope for the security program. The purpose of the program is described, and the assigned responsibility is defined for carrying out the information security mission.

Functional, issue-specific policies: While the organizational security policies are broad in scope, the functional or issue-specific policies address areas of particular security concern requiring clarification. The issue-specific policies may be focused on the different domains of security and address areas such as access control, contingency planning, segregation of duties (SOD), principles, and so forth.

System-specific policies: Areas where it is desired to have clearer direction or greater control for a specific technical or operational area may have more detailed policies. These policies may be targeted for a specific application or platform.

Typically, high-level organizational security policies are broad statements, establish corporate security philosophy, and can survive for several years, while those focused on the use of technology will change much more frequently as technology matures and new technology is added to the environment.

4.1.3 Compliance & Security Considerations

Organizations must operate in environments where laws, regulations and compliance requirements must be met. Information security professionals must understand the laws and regulations of the country and industry they are working in. An organization’s governance and risk management processes must take into account these requirements from an implementation and a risk perspective. These laws and regulations often offer specific actions which must be met for compliance, or in some cases, what must be met for a “safe harbor” provision. A safe harbor is typically a set of “good faith” conditions which if met, may temporarily or indefinitely protect the organization from the penalties of a new law or regulation. Potentially new policies, standards and procedures to support compliance with any laws, regulations and requirements that the organization will need to be aware of. IT auditors determine whether users, owners, custodians, systems, and networks are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements placed on systems. The auditors provide independent assurance to the management on the appropriateness of the security controls. The auditor examines the information systems and determines whether they are designed, configured, implemented, operated, and managed in a way ensuring that the organizational objectives are being achieved. The auditors provide top company management with an independent view of the controls and their effectiveness. The security administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.

Ultimately, the route an organization takes to meet the requirements of PCI-DSS is a business decision and should be evaluated carefully. Each approach has benefits and downfalls to consider. 96% of businesses in 2012 that were subject to PCI DSS and suffered a breach were not in compliance (WEB_16, 2012).

4.1.4 Emergency Plan

The bulk of security-related advice is based upon preventing break-ins, hacks, and attacks, but responsible e-commerce developers and administrators know that it's just as important to have created an emergency plan well before trouble occurs.

There are clear goals for an emergency plan (WEB_17, 2014):

- Find the cause of the trouble
- Fix the cause to prevent future problems
- Minimize the fallout
- Repair the damage

One of the hardest, and most important of these goals identifying and fixing the cause of the problem. Actually, fixing the problem shouldn't be that hard, once you've found it, that is. If there's a hole in software you wrote, you should be able to close it. If there's a hole in some other server software, such as the Web server application, upgrading to the most recent version or applying a patch should take care of that. But question is how you find the cause in the first place. The first part of your emergency plan, then, is to log all the key incoming traffic. By reviewing the logs, hopefully you can pinpoint the vulnerability. You may want to also use notifications for particular connections. For example, I normally have my servers email me when anyone logs in or connects via FTP. Knowing who accessed the computer when is invaluable with respect to your site’s and server’s security.

4.1.5 IT Security Awareness

A well-structured and repeated security awareness program is generally accepted as a baseline for ensuring security staff and users understand consequences and acceptable behaviors for the critical applications security. For example users need to be trained and have a basic awareness of the penalties for misuse of accounts, information and systems. Informed users are less likely to intentionally or unintentionally abuse accounts, access or information if they are aware of the consequences. In Turkey the big problem about security is unable to understand the perspective of security awareness and training, selecting the right staff for the right position. IT security is generally divided into two section. One of them operations security and the other security operations. In my view operations security is primarily concerned with the protection and control of information processing assets in centralized and distributed environments. Security operations are primarily concerned with the daily tasks required to keep security services operating reliably and efficiently. In Turkey generally these two concepts are not intercepted truly by the companies or managers who decided to hire security staff and specify the qualities of staff or requirements of the security related jobs. So if you don’t understand and distinguish these differences you can not select the right staff and security solutions so not being successfull to manage your security systems safely and effectively. All over that problems we have another issue that companies and security managers are facing to handle is funds. All over the world especially developed countries fund for the security staff and advanced security solutions and devices. All I mentioned above about is awareness of the unseen enemy that is security breaches and you are the target all time especially if you earn money by e-commerce applications.

4.2 CHOOSING INFRASTRUCTURE COMPONENTS AND INTERNET CONNECTION

It often happens that shoppers see a slow, unreachable, or not fully functional web site. What might cause that? One of the possibilities is that the network components do not handle sufficient volumes of network traffic. We should discuss how merchants can use suitable components to work together and provide a stable working web site for shoppers.

4.2.1 Handling with Overloaded Device

E-commerce application infrastructure has lots of components like web and database servers, DNS etc. Some of these devices are over their capacity, the e-commerce application may not work properly. The system is in general use throughout the organization. The activities involve monitoring the performance of the system and ensuring continuity of operations. This includes detecting defects or weaknesses, managing and preventing system problems, recovering from system problems, and implementing system changes. The operating security activities during this phase include testing backup and recovery procedures, ensuring proper controls for data and report handling, and ensuring the effectiveness of security processes.

4.2.2 Managing Bandwidth

Bandwidth usage can be defined as any visit to a website that causes data to be transferred to a visitor (be it a customer, search engine, security scanning device, etc.). Anytime someone or something visits any website, it uses a certain amount of bandwidth (as you can see in the Multi Router Traffic Grapher-MRTG example) is always good to find enough site bandwidth for customers, and the merchants do not need to pay much. The worst situation is having a problem with your website and not being able to get a hold of anyone to report the problem to or help you troubleshoot through it. The best hosting companies will provide 24/7 technical support and be able to fix problems and answer questions quickly and accurately.

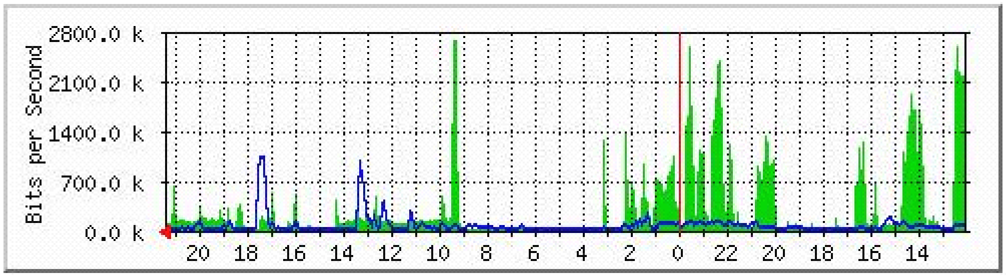


Figure 4.1 - A sample MRTG bandwidth graph
(http://en.wikipedia.org/wiki/Multi_Router_Traffic_Grapher)

4.3 DISASTER RECOVERY PLAN

Disaster recovery is the process of restoring services from a contingency state. DR is typically performed and described in several areas including response, personnel, communications, assessment, restoration, and training. The process must be documented. During adverse events personnel should rely on documented plans and not on ad hoc solutions as judgment may be impaired during stressful events such as natural disasters (Tipton , 2013).

If a site administrator configures a secure firewall, updates the latest patch for OS, uses secure software, and manages the whole network according to security policies, what should the administrator do if one of the servers is still down? How can the administrator find lost data from an unfixable server? A good disaster recovery plan may help the merchant to decrease that risk. The business continuity planning (BCP) and Disaster Recovery Planning (DRP) domain addresses the preparation, processes, and practices required to ensure the preservation of the organization in the face of major disruptions to normal organization operations.

4.3.1 Implement Backup Strategy

It is vital that the data that is stored offsite include not only the application data but also the application source code, hardware and software images for the servers and end user desktops, utility software, license keys, etc. Most organizations, no matter what strategy they employ for storing data offsite, start by performing full backups of all their data followed by periodic incremental backups. Incremental backups take copies of only the files that have changed since the last full or incremental backup was taken and then set the archive bit to “0.”

The other common option is to take a differential backup. A differential backup copies only the files that have had their data change since the last full backup and does not change the archive bit value. It is vital that the data that is stored offsite include not only the application data but also the application source code, hardware and software images for the servers and end user desktops, utility software, license keys, etc. Most organizations, no matter what strategy they employ for storing data offsite, start by performing full backups of all their data followed by periodic incremental backups. Incremental backups take copies of only the files that have changed since the last full or incremental backup was taken and then set the archive bit to “0.” The other common option is to take a differential backup. A differential backup copies only the files that have had their data change since the last full backup and does not change the archive bit value.

4.3.2 Off-Site Data Protection

Off-site data protection, or vaulting, is the strategy of sending critical data out of the main location (off the main site) as part of adisaster recovery plan. Data is usually transported off-site using removable storage media such as magnetic tape or optical storage. Data can also be sent electronically via a remote backup service, which is known as electronic vaulting or e-vaulting. Sending backups off-site ensures systems and servers can be reloaded with the latest data in the event of a disaster, accidental error, or system crash. Sending backups off-site also ensures that there is a copy of pertinent data that isn’t stored on-site. Off-site backup services are convenient for companies that backup pertinent data on a daily basis (classified and unclassified) (WEB_18, 2014).

Although some organizations manage and store their own off-site backups, many choose to have their backups managed and stored by third parties who specialize in the commercial protection of off-site data.

4.3.3 Redundancy And Fault Tolerance

Redundant items are said to provide fault tolerance within a system. This means that a system can continue to operate in the event of a component failure. This can involve the use of spare components, leveraging redundant servers or networks, and / or redundant data storage.

In soft real-time systems it is more important to economically detect a fault as soon as possible rather than to mask a fault. Examples of soft real-time systems are all kind of airline reservation, banking, and e-commerce applications. Fault tolerance system is to be kept running despite the failure of some of its parts, it must have spare capacity to begin.

There are two ways to make a system more resistant to faults (Kumar, 2008).

-Hardware: this technique relies on adding extra redundant hardware to a system to make it fault-tolerant.

-Software: this technique relies on duplicating the code, process, or even messages, depending on the context.

CHAPTER V

E-COMMERCE IMPLEMENTATIONS

5.1 MERCHANT-MANAGED E-COMMERCE IMPLEMENTATIONS

This kind of e-commerce environments are being developed generally by merchants and use their own application or by other third party software firms develop the payment application, or in other words they use a commercial applications.

Merchants which they responsible for their own e-commerce applications should test and develop according to the Payment Application Data Security Standard (**PA-DSS**). And ensure that the software are being tested securely and with PCI DSS compliance.

The e-commerce payment systems which are compliant with PA-DSS are more secure for cardholder sensitive data.

5.2 SHARED-MANAGEMENT E-COMMERCE IMPLEMENTATIONS

When we consider about shared management e-commerce environments the merchants should be responsible for some of e-commerce application components.

For instance, when e-commerce applications needs an implementation or piece of code for the merchant’s site or to deliver it to the customers, but always the merchant is the responsible for secure transaction over their environment and develop codes considering the whole e-commerce software.

Allowing to develop the shared management applications to third party while merchants considering about PCI DSS compliance being with or without belonging to self-assessment questionnaire (SAQ). Because of these shared implementations, security risk always should be evaluated for the merchant and weaknesses detected on the merchant’s website that enable attackers to steal the transaction data.

5.3 WHOLLY-OUTSOURCED E-COMMERCE IMPLEMENTATIONS

Merchants may prefer to handle their PCI DSS compliance while all their data is stored and processed by third party. In this instance, merchants should request a solution from the third parties which is completely responsibility of the third party. When considering about the solution that could include of third parties environment which consist with e-commerce application, hardware and software infrastructure. It is obligation to provide the merchants the access from their sites to the third party environment to handle with the storage and customers. It is vital getting access to the e-commerce application components to provide compliance and evaluate customer needs. In this scenario, the merchant may be eligible for the PCI DSS Self-Assessment Questionnaire (SAQ) A. SAQ A reduces the number of applicable PCI DSS requirements for merchants that outsource all storing, processing, and transmitting of cardholder data to an e-commerce payment processor (WEB_19, 2013).

5.4 OUTSOURCED E-COMMERCE IMPLEMENTATIONS AND SAQ A

Merchant is proper to use SAQ as a PCI DSS compliance requirements and their e-commerce components wholly outsourced including storage, processing data and transmission to compliant third parties, the merchant may be eligible to complete SAQ A which reduces the number of applicable PCI DSS requirements for the merchant. Merchants should consult with their acquirer(s) or the payment brands about individual PCI DSS compliance validation requirements and whether they are eligible to use an SAQ as a validation tool (WEB_20, 2010).

Some merchants which have not been qualified when considering customer sensitive data, data storage and processing could not use SAQ A. In that case merchants which have PCI DSS scope should record the payment data by manually instead of using the SAQ A. If these merchants try to minimize the scope of e-commerce application and components should think about segmenting the workstations that used to record payment data manually. All these merchants should evaluate with their SAQs to check if they are appropriate for an SAQ and if so, to determine which SAQ is applicable.

CHAPTER VI

SECURITY BREACHES

6.1 DATA BREACHES AND E-COMMERCE

Despite the recent economic crisis, lagging unemployment and lingering consumer doubts about the economy, one bright spot has persisted in the retail landscape: e-commerce has continued to grow as a major force in global retail. Online retail sales are expected to reach nearly $250 billion by 2014, with annual growth rates of 10 percent, despite the lagging economy (Forrester Research, 2010). Javelin Research predicts growth for e-commerce in 2010 to be 13 percent, again, despite the challenging economy. This compares with slower overall retail growth rates of 2.5 percent or less.

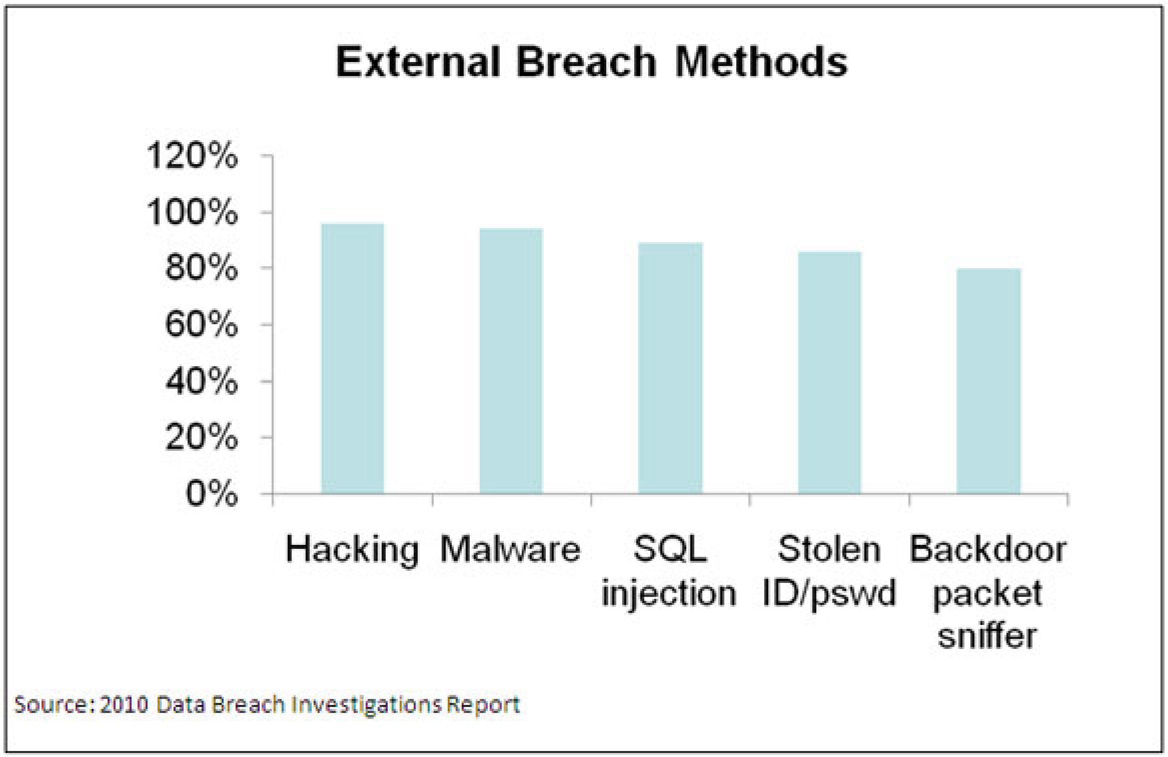
As a result, e-commerce sales are expected to account for 8 percent of total U.S. retail sales by 2014. In certain industries, including consumer electronics, books and office supplies, online sales account for 25 percent to 50 percent of total sales.

E-Commerce growth comes with downsides as well. Perhaps the most noteworthy area of concern is the growth in online security breaches, fraud and other forms of electronic malfeasance. Direct e-commerce fraud rates have decreased significantly over the last several years, in part due to major investments in security and fraud prevention.

However, fraud still costs e-commerce merchants billions in losses. Loss estimates vary, but conservative estimates puts e-commerce fraud losses at $3 billion. Most of these losses have their origin in compromised card data, either through data breaches (online and offline) or other forms of cardholder data theft.

In spite of online security investments, e-commerce merchants remain vulnerable to fraud committed using stolen information compromised in data breaches, highlighting a unique challenge to tighten security both in the physical and electronic environments. This becomes even more important given the nascent mobile commerce industry, which introduces additional security challenges. Some analysts fear that total fraud losses across channels – card-not-present (CNP) and card present – could exceed the current level estimated to be as high as $100 billion (WEB_21 , 2009).

These security problems come with significant hard dollar costs, as well as harder-to-quantify costs to consumer confidence and brand reputation. So it’s crucial to discuss existing data breach problems and financial implications of recent data breaches, as well as some solutions to these security and data breach situations. As you see in the chart below over 70 percent of data breaches because of external attacks. Many potential solutions are being proposed by both security players and traditional payment players. We should focus on a handful of solutions that aim to address a broad range of security problems with minimal cost to players in the payments ecosystem.



Source: 2010 Data Breach Investigations Report

Figure 6.1 - Over 70 percent of these breaches the result of external attacks
(http://www.pymnts.com/company-profile/2011/data-breaches-and-ecommerce-is-there-promise-in-new-prevention-options/#.U3MhWvl_uGo)

6.1.1 Potential Solutions

Due to a range of data breaches in the mid 2000s, including the aforementioned attacks at T.J. Maxx, DSW and others, the U.S. financial services industry focused most data security efforts on supporting a huge push by the card networks – Visa and MasterCard – to get commitment to PCI compliance. However, following the massive data breach experienced by Heartland Payments back in 2008, it became clear to many that PCI efforts alone were not enough to prevent costly security breaches. Nearly 20 percent of recent breaches, including some of the largest, took place against PCI compliant entities (Verizon Business Risk Team, 2009). Deeper investigation continues to suggest that the PCI compliance recommendations are the critical first line of defense in preventing attacks, but it is clear that other safeguards and measures are needed.

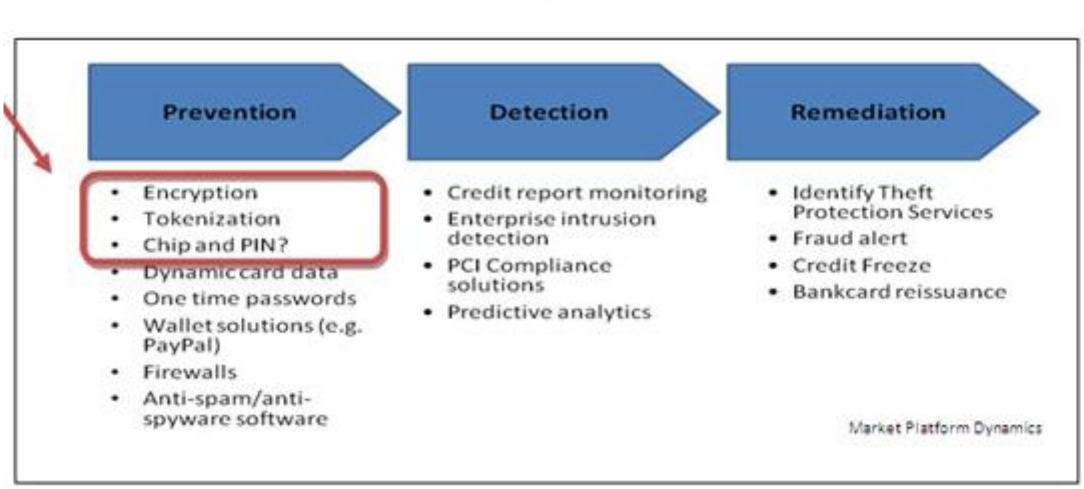


Figure 6.2 - Potential Solutions (http://www.pymnts.com/company-profile/2011/data-breaches-and-ecommerce-is-there-promise-in-new-prevention-options/#.U3MkHfl_uGo)

6.1.1.1 Encryption

Encryption is protecting the transmission of the signal by employing a data-encryption standard that applies a specific algorithm to alter the appearance of the data. For high security areas such as data centers, which fall into the category of controlled access areas, the encryption standard should be a strong and validated format, such as one that complies with the National Institute for Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 140-2. Systems protecting all other assets should meet UL 1076 Section 64A1 line security standards. In Turkey in common there is no encryption standard especially for e-commerce including e-banking.

BDDK (banking regulation and supervision of institutions) and TUBITAK (The Scientific and Technological Research Council of Turkey) should specify together a standard about the encryption especially for the e-commerce transactions. Although these merchant encryption solutions vary, they each help avoid some of the data breach problems experienced in high-profile data breach cases, eliminating the ability to intercept card data in transit and also protecting card data at rest. Particularly for physical POS retailers, this eliminates major data vulnerabilities. Since e-commerce merchants have been using SSL encryption for years now, this added layer of security may not be as pivotal to them.

6.1.1.2 Tokenization

Tokenization solutions reduce the security challenges of dealing with card data by replacing sensitive card information with a token value that can be used by the merchant for receiving payment but cannot be used by anyone else for fraudulent purchases. Essentially, the token takes card data out of the merchant environment, eliminating the need for merchants to store that sensitive data, potentially also reducing downstream costs of securing that data.

One of the most powerful attributes of tokenization is that it effectively eliminates the need for merchants to focus on card security in its operations, from payment authorization and settlement, through fulfillment and customer service. As a result, data are protected in all states – in transit, at rest and at work.

6.1.1.3 Emv/Chip & Pin

Most pundits believe that low fraud and high electronic authorization rates limit the need for this technology in the United States. Yet in 2010, key players began to reconsider EMV/chip & PIN as a prevention measure for the United States. The EMV/chip & PIN protocol in place in Europe, Canada and elsewhere is designed to minimize the vulnerabilities of magnetic stripe cards, which can be easily reproduced. Magnetic stripe cards can been recreated through magnetic stripes that use legitimate cardholder data “skimmed” from legitimate magnetic stripe cards or from cardholder data accessed through a data breach. In theory, chip & PIN card technology should reduce the incidence of card data theft, since it is harder to create counterfeit cards.

Even the theoretical security benefits of chip & PIN have proven vulnerable to simple attacks. A recent University of Cambridge paper highlights problems with chip & PIN, including a material increase in CNP fraud following EMV implementation (Murdoch, Drimer, Anderson, Bond, 2010). Since most CNP fraud costs are borne by merchants, banks did not have a direct stake in the fraud losses in CNP channels. In addition, the paper highlights a simple failure in the EMV protocol itself that made it possible for Cambridge researchers to “trick” a chip & PIN terminal into accepting cards without valid PINs using a £20 device (WEB_22, 2010).

Figure 6.3 - EMV Chip (http://blog.gemalto.com/blog/2012/02/01/mastercard-joins-visa-with-emv-roadmap-in-us/)

6.2 EXAMPLES OF SECURITY BREACHES

Clearly, data vulnerabilities affect all parts of an enterprise that captures and stores personally identifiable, sensitive information about their customers, vendors or partners. The following figure shows a representative view of areas in which a corporation may have data vulnerabilities.

Many companies, particularly e-commerce companies, leverage payment information as a convenient customer ID used for marketing, customer service and operations/order management. This practice leaves those enterprises vulnerable to data attacks, not only on data in transit, but also data at rest or at work.

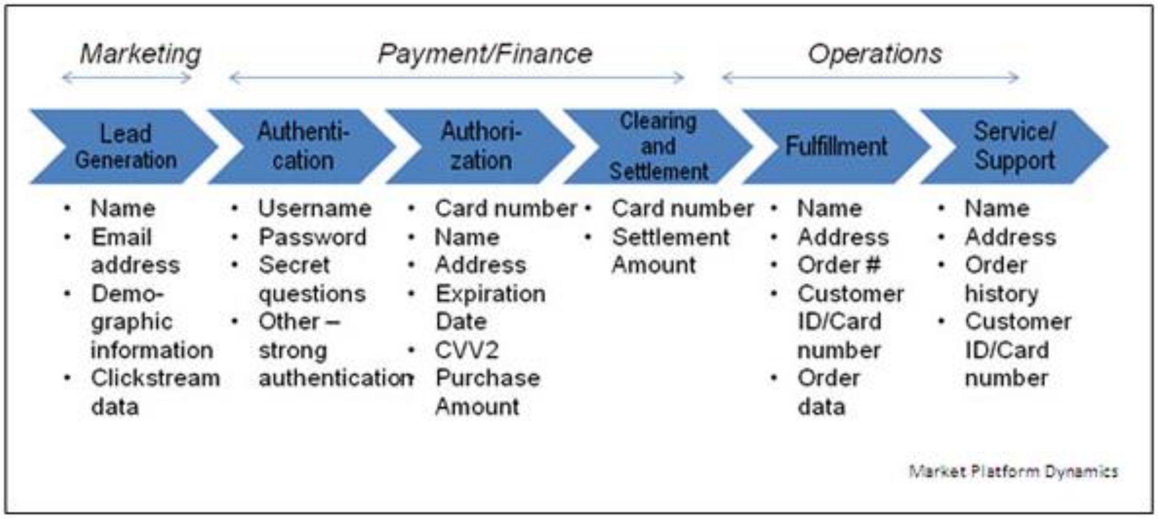

Marketing
Payment/Finance
Operations
Lead Generation
Authenti-cation
Authori-zation
Clearing and Settlement
Fulfillment
Service/ Support
• Name • Email address • Demo-graphic information • Clickstream data
• Username • Password • Secret questions • Other – strong authentication
• Card number • Name • Address • Expiration Date • CVV2 Purchase Amount
• Card number • Settlement Amount
• Name • Address • Order # • Customer ID/Card number • Order data
• Name • Address • Order history • Customer ID/Card number
Market Platform Dynamics

Figure 6.4 - Data Vulnerabilties (http://www.pymnts.com/company-profile/2011/data-breaches-and-ecommerce-is-there-promise-in-new-prevention-options/#.U3MlqPl_uGp)

6.2.1 Target Company Security Breach

The Target Corporation is an American retailing company, founded in 1902 and headquartered in Minneapolis, Minnesota. It is the second-largest discount retailer in the United States which is hacked on Nov 2013.

Target said that the thieves who stole massive amounts of credit and debit card information during the holiday season also swept up names, addresses and phone numbers of 70 million customers, information that could put victims at greater risk for identity theft.Every bit of added data helps criminals develop more sophisticated tactics for either impersonating victims or luring them to give up more sensitive information, according to security experts (WEB_23, 2013).

An investigation by security journalist Brian Krebs indicates that the malware used to breach point of sale (POS) systems in the epic Target breach that compromised some 110 million customers has been available for sale on the black market. The memory-scraping malicious agent known as “Reedum” has been available on underground criminal forums under the name of “BlackPOS” since at least the middle of last year for a fee of $1,800 for the basic version and $2,300 for the full version. This type of malicious software uses a technique that parses data stored briefly in the memory banks of specific POS devices; in doing so, the malware captures the data stored on the card’s magnetic stripe in the instant after it has been swiped at the terminal and is still in the system’s memory. Armed with this information, thieves can create cloned copies of the cards and use them to shop in stores for high-priced merchandise. Earlier this month, U.S. Cert issued a detailed analysis of several common memory scraping malware variants.

The Target breach already ranks as one of the worst ever. During the peak of holiday shopping last month, Target said that up to 40 million customers’ credit and debit card information had been stolen from people who shopped in stores from Nov. 27 to Dec. 15. On Friday, the company said a new group of 70 million customers — some of whom might also have had their card data stolen — have had their personal information compromised, as well.

Affected customers will be sent an e-mail providing them with general security tips, said Target, adding that no personal information would be requested in the e-mail. The Minneapolis-based retailer is also offering one year of free credit monitoring and identity theft protection to all shoppers. Customers are not liable for any fraudulent charges made to their cards as a result of the breach, according to Target, which has also put a list of tips for shoppers on its Web site. “I know that it is frustrating for our guests to learn that this information was taken, and we are truly sorry they are having to endure this," Gregg Steinhafel, Target's chairman, president and chief executive, said in a statement. "I also want our guests to know that understanding and sharing the facts related to this incident is important to me and the entire Target team." (WEB_23, 2013).

Friday's announcement is the result of an ongoing investigation into the security breach, Target said. The company is working with the Secret Service and the Department of Justice to determine who was behind the attack. Spokesmen at the Secret Service and the Justice Department declined to comment on the investigation. Analysts said that Target's problems reflect a crisis in how customer data is protected (WEB_23, 2013).

Target has tried to win back consumers. After news of the attack broke last month, the company offered 10 percent off all in-store purchases after the attack. But it wasn't enough to stave off a drop in sales, which the company said Friday were "meaningfully weaker-than-expected."

Target noted that sales had improved in the past several days, though that was before the latest announcement. On Friday, the company's stock dropped more than 1 percent.

6.2.2 76 Turkish Government Websites Have Been Hacked

Unauthorized access to the 76 Turkish government website were made by the hacker group which name is HacKingZCrew on February 2013. The members of HacKingZCrew prefer to upload page bearing his name and did not interfere the hacked home pages of the web sites. The index pages of the government web sites have not been changed by the hackers instead of that they have upload different defacement webpage for all of web sites. According to the news by Cyber News all the sites affected by the hacking incident hosted on the same server (Windows Server). This situation explains how to perform attacks easily at the same time to all web sites.

The majority of hacked web sites are belonging to hospitals and other health institutions. Batman Maternity and Child Health Hospital, Fatsa State Hospital, Menemen State Hospital are some of the hospitals that their web sites get unauthorized accessed.

6.2.3 E-Commerce Site (Salesgate.Com) Breached By Credit Card Thieves

On March 2000, The site, called SalesGate.com, is an example of an online business being hit by a security breach. The attacks are raising concern among consumers, industry executives and law-enforcement authorities. About 2,000 records were taken at SalesGate, including credit card numbers and other personal information, Chris Keller, one of SalesGate's founders, told. "We regretfully inform you that SalesGate has suffered a security breach in our customer database," the company said in a memo to customers. "Among the data accessed illegally from our system and posted to the Internet are credit card numbers of some of our customers."We have been working closely with the Secret Service in the United States to catch the hacker responsible for the breaking into our system."

SalesGate, owned by Buffalo, N.Y.-based Internet Management Services, is a marketplace where small businesses come to sell their products and services in a central location. SalesGate guarantees the security of transactions and has a message posted on its Web site promising to refund any charges linked to cards stolen from the site.

CONCLUSION

Electronic commerce has entered into every area of our lives and in parallel with the rapidly developing technology of security measures that should be located on the upper level. Gaining the trust of customers and uninterrupted service has become inevitable. The creation of security policies including their implementation and periodic security checks to ensure risk mitigation and compliance are very important. E-commerce security issues are related to different technical fields, so maintaining a secure environment is not only work deal with technical staff at the same time with merchants, providers, customers and everyone who take part in e-commerce. In a disaster scenario for example being hacked or denial of service will be crucial for financial sense and of course damage to reputation and confidence which are very difficult to gain again. During the study I would like to explain e-commerce security threats and their corresponding preventions that all have crucial impacts on online business volume. And I hope the study has been informative and comprehensive material for security researchers, security specialists who deal especially with e-commerce security.

REFERENCES

Anderson, Ross J. (2008). Security engineering: a guide to building dependable distributed systems (2nd ed.). Indianapolis, IN: Wiley. p. 1040. ISBN 978-0-470-06852-6. Chapter 2, page17

Akash Kumar, (2008 , ”Scheduling for Fault-Tolerant Distributed Embedded Systems”,IEEE Computer 2008.

Chang, R.K.C. , (2002), "Defending against flooding-based distributed denial-of-service attacks: a tutorial," Communications Magazine, IEEE , vol.40, no.10, pp. 42- 51, Oct 2002 doi: 10.1109/MCOM.2002.1039856

Eric Maiwald. (2003) Network Security: A Beginner's Guide. Second Edition. McGraw-Hill/Osborne, 2003

Fukuyama, F. (2001) Güven:Sosyal Erdemler ve Refahın Yaratılması, Çev: Buğdaycı, A. , Türkiye İş Bankası Yayınları, 2. baskı, İstanbul, 2001

Harold F. Tipton , (2013) Official (ISC)2® Guide to the CISSP® CBK®, Third Edition, EditorISBN: 978-1-4665-6976-8 p.366

Harold F. Tipton, (2013), Official (ISC)2® Guide to the CISSP® CBK®, Third Edition, EditorISBN: 978-1-4665-6976-8 p.684

Harold F. Tipton, (2013), Official (ISC)2® Guide to the CISSP® CBK®, Third Edition, EditorISBN: 978-1-4665-6976-8 p.620

Harold F. Tipton , (2013) , Official (ISC)2® Guide to the CISSP® CBK®, Third Edition, EditorISBN: 978-1-4665-6976-8 p.678

Harold F. Tipton , (2013) ,Official (ISC)2® Guide to the CISSP® CBK®, Third Edition, EditorISBN: 978-1-4665-6976-8 p.886

Jeff Forristal ,(2001) ,Hack Proofing Your Web Applications, , ISBN: 1-928994-31-8 p.105

Leyden, John (2003-04-18) "Office workers give away passwords". Theregister.co.uk. Retrieved 2012-04-11.

Russell, Ryan (Contributor); Huston, L. Brent (Editor). 2000. Hack Proofing Your E-commerce Site: The Only Way to Stop a Hacker Is to Think Like One. Rockland, MA, USA: Syngress Publishing, p 220.

Schrenk, Michael. 2007. Webbots, Spiders, and Screen Scrapers. San Francisco, CA,USA: No Starch Press, Incorporated, p 47.

Singh and Frolick, 2000, p.58 cited "Muammer Z. , Esen Ş. , (2013) , The Impact on Electronic Commerce Activities of SMEs"

S. Murdoch, S. Drimer, R. Anderson, M. Bond, (2010) , "Chip and PIN is Broken," 2010 IEEE Symposium on Security and Privacy. University of Cambridge, pp. 433 – 443.

Telli Yamamoto, G. (Prof. Dr.) , (2011), E-commerce Concepts, Evolution and Applications, Istanbul, p 102.

Tiller, J.S. (2004), Message authentication, in Information Security Management Handbook, 5th ed., Tipton, H.F. and Krause, M., Eds., Auerbach Publications, New York, 2004

Van der Merwe, A J, Loock, M, Dabrowski, M. (2005), Characteristics and Responsibilities involved in a Phishing Attack, Winter International Symposium on Information and Communication Technologies, Cape Town, January 2005.

WEB_1, 2014, wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

WEB_2 , 2013, http://www.ecommercetimes.com/story/3440.html

WEB_3, 2014, Privacy and Confidentiality in an e-Commerce World, http://www.citeulike.org/user/imrchen/article/2634677

WEB_4, 2013 , Social engineering , http://blinkcoding.blogspot.com.tr/2013/04/social-engineering-hacking.html

WEB_5, 2010 , "Internet Archive Wayback Machine". Web.archive.org. 2010-06-22. Archived from the original on 2010-06-22. Retrieved 2012-08-09.

WEB_6, 2013,Social engineering (security), http://en.wikipedia.org/wiki/Social_engineering_(security)

WEB_7, 2014, http://www.webopedia.com/TERM/D/dictionary_attack.html

WEB_8, 2014, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

WEB_9 , 2013 , Man-in-the-browser , http://en.wikipedia.org/wiki/Man-in-the-browser

WEB_10, 2012 , Quarri Technologies, Inc. "Web Browsers: Your Weak Link in Achieving PCI Compliance" www.quarri.com/files/Quarri_PCI_Brief.pdf. Retrieved 2012-02-05.

WEB_11, 2013, Cross Site Request Forgery, http://projects.webappsec.org/w/page/13246919/Cross%20Site%20Request%20Forgery

WEB_12, 2009 ,http://www.us-cert.gov/ncas/tips/ST04-002 Choosing and Protecting Passwords. US CERT. Retrieved June 20, 2009.

WEB_13, 2014 , http://cyber.law.harvard.edu/ecommerce/encrypt.html . Security and the Basics of Encryption in E-Commerce. Retrieved 2014-03-25 .

WEB_14, 2014 , http://sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029. SSL and TLS: A Beginners Guide. Retrieved 2014-02-01 .

WEB_15,2014,http://www.checkpoint.com/securitycafe/readingroom/internal_security/ips_ids_internal_security.html . What is the Difference Between IPS, IDS and Internal Security? Retrieved 2014-02-12 .

WEB_16, 2012, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_ xg.pdf?__ct_return=1

WEB_17, 2014, http://www.peachpit.com/blogs/blog.aspx?uk=Have-a-Emergency-Plan-Five-Critical-E-Commerce-Security-Tips-in-Five-Days

WEB_18, 2014 , http://en.wikipedia.org/wiki/Off-site_data_protection

WEB_19,2013,http://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf. PCI DSS E-commerce Guidelines. Retrieved 2013-10-23 .

WEB_20, 2010,PCI DSSE-commerce Guidelines ,https://www.pcisecuritystandards.org/

WEB_21, 2009 LexisNexis True Cost of Fraud Study. Cited in the article, “Fighting Fraud with Chase Paymentech,” at the Direct Response Forum, and posted on www.directresponseform.org ,2009

WEB_22, 2010 , “Cambridge Researchers Under Fire,” Top Tech Reviews website. www.toptechnews.net, 2010

WEB_23, 2013,http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html . Target says up to 70 million more customers were hit by December data breach . Retrieved 2014-02-23

Federal Trade Commission , 2006 , "Pretexting: Your Personal Information Revealed"

Forrester Research, March 2010.

SANS Institute, 2003, sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029

© SANS Institute, (2007) , sans.org/reading-room/whitepapers/privacy

Verizon Business Risk Team , 2009, Data Breach Investigations Report,

CURRICULUM VITAE

Gökhan ÇAKIL
IT Security Specialist
/ ISTANBUL
gokhancakil@gmail.com

PERSONAL INFORMATION

Date of birth,place: 01.01.1984, TURKEY

Nationality: Turkish

Interests : Reading, Traveling, Swimming

EDUCATION

2012-2014
Okan University , Social Sciences Institute
MBA

2003-2007
Yildiz Technical University, Electric-Electronics Faculty Electronics and Communication Engineering Department

EMPLOYMENT HISTORY

4+ years hands-on network security architecture and implementation experience

2+ years technical leadership in a consulting and professional services organizations, lead network and application security design, implementation, and configuration projects

JOB SKILSS

FOREIGN LANGUAGES:

ENGLISH (Advanced Level, Yildiz Technical University, Foreign Languages Academy)

TOEIC score: 830

COMPUTER LITERATURE : **MS Windows**
Linux (Ubuntu, RedHat, Debian),

C++, Python, ASP, Java

TRAININGS AND CERTIFICATIONS

- **CEH v8 (Certified Ethical Hacker) (March 2014)**
- **Checkpoint Certified Security Expert (CCSE certificate –August 2012)**
- **Checkpoint Certified Security Administration (CCSA certificate-May 2012)**
- **CCNA Certification (Cisco ICND1-ICND2), BT Eğitim ---144 hours (Certificate**

  November,2012) (Cisco ID: CSCO11514215)
- **IBM ISS Site Protector v2 sp 8.1 and NIPS certificate (December 2011)**

PROJECTS

- **Checkpoint Provider-1 SecurePlatform Gaia upgrade project**
- **500+ client local and wireless 802.1x and ssl-vpn project**
- **Firewall migration and compliance management project**
- **500-1000 client endpoint security project**
- **HQ and remote offices web and network penetration and verifications-remediations**