eCommerce Security

Bob Gehling
Information Systems and Decision Sciences
Auburn University at Montgomery
Montgomery, Alabama 36124-4023
334 244-3482
bgehling@mail.aum.edu

David Stankard
MBA Student
Auburn University at Montgomery
Montgomery, Alabama 36124-4023

ABSTRACT
Internet security has become a consistent and growing problem as new Internet-based technologies and applications are developed. The number of security violation related incidents continues to increase [6]. A reported incident can be as simple as a single computer being compromised or as severe as a complete network compromise involving hundreds of client computers. All Internet content you read, send, and receive carries a risk. The amount of security risks increases at the same time that dependence on information technology grows. This demands the need for a comprehensive security program and makes the job of those persons tasked with network security even harder.

Categories and Subject Descriptors
C.2.0 [**Computer Communications Networks**]: General – *Security and protection*
K.3.2 [**Computers And Education**] - Computer and Information Science Education – *Curriculum, Information systems education.*
K.4.1, .2 & .4 [**Computers And Society**] - .1 Public Policy Issues - *Abuse and crime involving computers, Computer-related health issues, Ethics, Intellectual property rights, Privacy. .2* - Social Issues - *Abuse and crime involving computers.* .4 Electronic Commerce - *Security*
K.6.5 [**Management Of Computing And Information Systems]** - Security and Protection – *Authentication, Invasive software, Unauthorized access.*

General Terms
Management, Performance, Reliability, Security, Human Factors

Keywords
Security awareness, eCommerce, Security

1. INTRODUCTION
Internet security has become a consistent and growing problem as new Internet-based technologies and applications are developed. The number of security violation related incidents continues to increase [6]. A reported incident can be as simple as a single computer being compromised or as severe as a complete network compromise involving hundreds of client computers. All Internet content you read, send, and receive carries a risk. The amount of security risks increases at the same time that dependence on information technology grows. This demands the need for a comprehensive security program and makes the job of those persons tasked with network security even harder.

There are new Internet security vulnerabilities discovered almost daily. These discoveries can be attributed to flaws in software or the result of software configuration errors. These vulnerabilities can be exploited by hackers or other malicious individuals to gain access to the network.

The confidentiality, integrity, and availability of information on the Internet are three basic security concepts [8]. Information that is read or copied by someone not authorized to do so is known as loss of confidentiality. Information that has been classified as confidential is usually private or sensitive and should not be disclosed. Examples of this type of information include credit card applications, medical records, bank records, and corporate business plans. If information is available on an insecure network it can be corrupted. The result is a loss of integrity because the information has been modified in an unexpected way. Unauthorized changes have been made to the information, sometimes by human error or intentional tampering. Integrity of information is important for activities such as electronic funds transfers and air traffic control. The loss of availability is when information is erased or becomes inaccessible. This means that people who are authorized to get information cannot get what they need. Availability is important to service-oriented businesses that depend on information. Availability of the network itself is important to anyone whose business or education relies on a network connection.

1.1 ECommerce Security
Due to the rise of Business-to-Business (B2B) and Business-to-Consumer (B2C) interactions, accurate and secure information exchange is essential for doing business over the Web. Using and understanding ECommerce can give a company a strong advantage over their competitors while providing greater value and comfort to its customers. To make sure access to information is accurate and secure a business should take some precautions.

Many consumers are uncomfortable about giving personal information over the Internet. There are several reasons that contribute to this insecurity: The Internet does not offer much security, eavesdropping and acting under false identity is easy for hackers, and stealing data is undetectable in most cases.

Information Security Curriculum Development (InfoSecCD) Conference '05, September 23-24, 2005, Kennesaw, GA, USA. Copyright 2005 ACM 1-59593-261-5/05/0009…$5.00.

2. CONSUMER AWARENESS

Most users have only vague ideas about the threats and risks related to conducting business over the Internet. They also have a very limited understanding of the technical and legal options for minimizing their risk. As a result, all kinds of misperceptions exist.

For instance, the cardholder's risk in sending their credit card number over the Internet is typically overestimated. Payments over the Internet are treated like mail-order/telephone-order transactions which means the cardholder is not liable at all. All risk is with the merchant. The problem for many users is that there is often no obvious way to check if a transaction is secure. From the web browser, the only generic indication is a small padlock in the corner of the screen that indicates when a SSL connection is active [1].

3. SECURITY IN DEPTH

Security refers to techniques for ensuring that data stored in a computer and transmitted between computers cannot be read or compromised by unauthorized users.

A recent financial services consulting firm's study on the insurance industry's use of the Internet found that insurers have moved too slowly in making a commitment to eBusiness and that their concerns include Internet security [12]. "Bad people do bad things." Jeff Mallett, president of Yahoo!, Inc., made that observation in the aftermath of the recent "hacker attack" that sent the world's largest electronic commerce sites reeling [12]. The following are a list of a few attacks that threatens the security of ECommerce:

- DOS Attacks
- Eavesdroppers
- DNS Attacks
- Input Validation Attacks
- Script Attacks

3.1 Threat Prevention

Many protocols exist for transmitting data securely over the World Wide Web. Security systems are only as strong as their weakest points. ECommerce is composed of security defenses such as firewalls, authentication schemes, and encryption. Some other security issues that occur in ECommerce are authorization, auditing, confidentiality, integrity, availability and non-repudiation.

Business must first understand their business processes and determine the things that are most valuable to them. When that is acknowledged a plan must be put together and implemented. This effort is called security risk management.

3.2 Security risk management

Risk management consists of four phases-assessments, planning, implementation, and monitoring. In the assessment phase of risk management, organizations evaluate their security risks by determining their assets, threats, and vulnerabilities. The second phase, planning, focuses on security policies defining which threats are tolerable and which are not. A threat is tolerable if the cost to safeguard the threat is too high or the risk is too low. In the implementation phase, technology is chosen to prevent high priority threats. The monitoring phase is on going and usually determines if the chosen tactics were successful or not. Some examples of threat prevention are discussed below.

Companies face significant risks due to the behavior of their employees. Many companies do not report incidents caused by employee behavior because of the negative publicity. Employees that compromise the security of the network often do it unknowingly. Accessing offensive or illegal material from a company's network often can leave the organization exposed to litigation. Employees that access web-based e-mail accounts from a corporate intranet increase the risk of damage to data and assets by a virus. Organizations can scan for viruses at its e-mail gateway; employees that download attachments from web-based accounts override this security hole. Some personnel that are upset can download and install hacking software that may allow them to view or steal secure data. Downloaded games can also contain malicious code. Employees using e-mail to forward jokes, chain letters, or hoaxes can compromise productivity. They may also inadvertently send a virus or worm through the network. Employees that have access to privileged information can send it to the press or other companies if they become disgruntled.

Hackers are individuals with a great deal of technical knowledge about computer systems and their security. Hackers or crackers are the most publicized threat to enterprise security [9]. Hackers use their expertise to illegally break into computers and networks. They usually do this by examining source code to discover weaknesses in certain programs. Many source codes are easy to obtain from programmers who make their work freely available on the Internet. The targets of many computer intrusions are organizations that maintain copies of proprietary source code. Once an intruder gains access, they can examine the code to discover weaknesses. Intruders are also targeting the network infrastructure and cloaking their behavior. Intruders are able to use Trojan horses to hide their activity from network administrators by altering authentication and logging programs so they can log in without the activity showing up in the system logs. They have the ability to encrypt output from their activity. Intruders also are beginning to monitor the Internet for new connections. Newly connected systems are often not fully configured from a security perspective and are vulnerable to attacks. Hackers and intruders can also exploit flaws in software or protocol designs. No matter how well a protocol is implemented, if it has fundamental flaw, then it is vulnerable. If the protocol is designed without flaws it is still susceptible to vulnerabilities because of the way it was implemented. This is often the case in a protocol for e-mail. If implemented incorrectly, intruders can connect to the mail port of the victim's machine and trick the machine into performing a task not intended by the service.

There is no standard set of guidelines for addressing security issues. Safeguards need to be specified according to the various needs of the different electronic commerce sites. The safeguards used will depend on a number of things including the services being offered, the types of data being handled and stored, and the types of software and hardware being used. Despite the various

safeguards to be used, an organization must depend on sound risk management to decide their security needs.

There are four phases to risk management: assessment, planning, implementation, and monitoring [5]. During the assessment phase an organization must evaluate their security risks by determining their assets, threats, and vulnerabilities. The evaluation process follows five steps. The first is to establish the organization's objectives. Safeguards should be picked according to an organization's objectives and requirements. Step two is inventory of the assets. An organization needs to itemize the tangible and intangible assets on the network. They should determine the value of these assets. The third step is to delineate threats. Security risks can originate from any person or thing that can use the network to harm an organization's assets. The next step is to identify vulnerabilities. Organizations can use various tools and methods to specify weaknesses in a particular network. The last step of assessment is to quantify the value of each risk. A company can perform a quantitative risk analysis to assign a value to the risk.

The second phase of risk management is planning. The objective is to arrive at a set of security policies that define which threats are tolerable and which are not. The planning phase also involves a series of steps. The first step is to define specific policies. The policy will detail how the safeguard will be instituted, why it is being implemented, when it will be enforced, and who will be responsible. The next step is to establish processes for audit and review. The organization needs to perform regular reviews to determine the effectiveness of the policies. The last step is to establish an incident response team and contingency plan. A network or site is subject to an attack and all attacks require a response. Handling the attacks is the job of the incident response team. The team should monitor public announcements of attacks at other sites and all responses should be outlined in the contingency plan.

The third phase of risk management is implementation. During this time, particular technologies are chosen to counter high-priority threats. The technologies chosen are based on the guidelines established in the planning phase. As a beginning step in the phase, generic types of technology are selected for the high priority threats.

The last phase of risk management is monitoring. Monitoring is a continual process that aides in the determination of which technologies are successful, which are unsuccessful and need modification, whether there are any new threats, if there are any advances or changes in technology, and if any new business needs requires securing. Monitoring is probably one of the most important factors of risk management.

There are a number of security defenses that an organization can use to protect themselves against Internet risks. An organization can ensure that all accounts have passwords and that the passwords are difficult to guess. One-time passwords are more preferable. They can se a strong cryptographic technique to ensure the integrity of system software on a regular basis. An organization should use secure programming techniques when writing software. Changes should be made as vulnerabilities become known and keep systems current with upgrades and patches. System administrators should check on-line security archives for security alerts and technical advice.

3.3 What Do We Mean By Web Application Security?

Business-critical database applications containing custom customer, financial, and other sensitive information are a coveted target for any hacker, so it is not surprising that attacks on web applications and services are the fastest growing area of new attacks. Web applications, which are highly vulnerable to hackers, provide the entry point through which these account details, social security numbers, medical ID numbers, and other sensitive data can be accessed and stolen. This vulnerability is present because current security solutions – including network firewalls, intrusion detection systems, encryption, and manual measures such as aggressive quality assurance and audit procedures – are incapable of preventing attacks at the application layer (and many times incapable also of stopping them at the operating system layer).

Although Web services have the potential to be very powerful for both application developers and users, they also can be a nightmare for security officers and system administrators. Additional security measures need to be in place because the Web services format was designed to bypass existing security measures, to be platform-independent, and to support any application call structure. In the rush to deploy and use Web services technology, companies face the real danger of exposing their systems to costly attacks [5].

The flexibility found in SOAP and other technologies makes communication among applications easy, but it also allows hackers to intercept and manipulate messages more easily. SOAP messages typically are transparent to firewalls, which helps them move more quickly through the network, but this negates an important element of perimeter protection and could expose unforeseen threats [5].

Applications continue to become more functional and flexible, which increases their value to business operations, but it also exposes many potential security problems. Progressive companies that look to take advantage of these emerging technologies may gain a significant competitive advantage, but they must be sure to address the accompanying security issues to avoid costly breeches to their information systems [5].

Applications provide hackers with the opportunity to try things such as SQL injection, to access tables in backend databases, thereby gaining entry to companies' most sensitive data. In addition, viruses such as Nimda and Code Red, both of which infect systems at the application layer, can take down a site for days at a time and do irreparable damage to a company's reputation. Yet a survey on the Security News Portal [3] reveals that:

- "75% of all web servers running MS IIS 5.0 are vulnerable to exploitation."
- "Microsoft issued a security alert on March 17 2003 regarding a buffer overflow vulnerability which allows attackers to execute arbitrary code on Windows 2000 machines. [A recent Netcraft survey] found 767,721 IPs running IIS 5.0 and offering WebDAV and 273,496 IPs running IIS 5.0 with the protocol turned off."

3.4 What Is My Risk Level?

It is a fairly easy task to determine the potential level of risk associated with sensitive information within databases and Web applications if a severe breach or a major system downtime were to occur. The 2002 Computer Security Institute (CSI) Computer Crime and Security Survey revealed that, on a yearly basis, over half of all databases experience some kind of breach and the average breach results in close to $4 million in losses. The survey also noted that Web crime has become commonplace – in fact, six percent of respondents reported financial fraud, up from only three percent in 2000. Web crimes range from cyber-vandalism (e.g., Web-site defacement) at the low end, to theft of proprietary information and financial fraud at the high end [2].

Attacks against web servers succeed because these servers do not maintain deep logs and have stateless protocols, so a skilled attacker will leave no trace. In fact, for the web server to conduct stateful sessions such as password management and shopping carts, it needs to interact closely with the browser. So if an attacker can control the browser, they can access the web server and the back-end databases with confidential information. Hackers today often probe banks and financial firms for weakness by observing web servers and painstakingly trying many different approaches to gain information. Once they understand its vulnerabilities they craft an attack that exploits those vulnerabilities, and manipulate the server to spit the data they are looking for. Serious hackers will patiently try many different ways to trip up the application – they continue to fail but still keep trying. However, it is not the hundreds of foiled attempts that make the headlines but the one that is ultimately successful.

The vast majority of web application attacks are not new innovations, but well known web server or application vulnerabilities that are exploited against an application that has not been patched. However, corporations also need to protect against 'Zero-Day' attacks, which are vulnerabilities exploited before they are announced publicly and patches/fixes become available.

3.5 What Steps Are Required To Secure Web Applications?

The need to secure business-critical applications (many times back-end databases tied into web front-ends) from attack has resulted in solutions from an entire range of vendors, and as usual has resulted in a lot of confusion about what these products do and how they do it.

“To understand how to truly secure a web application, it is first necessary to understand how typical web applications communicate. Most communications consist of a client (web browser) making a request to an application (web server). After the web server receives the request, it processes the request and returns a response to the browser. In many respects, application communications are similar to a conversation between two people [2]. For example:

- The conversation requires a common language (including both vocabulary and sentence structure)
- They are a two-way conversation
- Both expect answers to questions asked
- Both expect answers to be given in a timely manner
- Both expect communications to be in the proper context. In other words, an answer should make sense given the question asked”

“All applications communicate via these types of electronic “conversations”, and any form of web application security must be capable of understanding all these conversations, and be able to distinguish one conversation from another while listening to both sides of every conversation.”

A typical packet inspection firewall will capture and inspect individual IP packets to provide access control to network resources. In addition, with an enhanced ability to deeply inspect and analyze the information within packets, they attempt to detect attacks aimed at applications. Once you realize that IP packets are discrete pieces of information, similar to individual words, you can see that a packet inspection firewall cannot get much meaning from looking at lots of individual packets (words). It is only when these packets (words) are assembled into streams (sentences) that they are able to convey meaning and support a coherent conversation.

Newer firewall technologies allow them to capture complete streams. But what can a firewall do now that it has captured a complete stream? Primarily, they look for certain words or phrases that may appear in the sentence. For example, it can look for attachments to email, and scan them for viruses, or it can look for specific signatures of known attacks. It can also be told to end the conversation if one of those signatures is detected.

Application attacks typically consist of two types: those that prey on known vulnerabilities in commercial software (IIS, Apache, etc.), and those that target custom internally developed web application vulnerabilities that are specific to each enterprise, and the profile of each of these attacks is very different.

Known attacks on commercial software require less sophistication on the part of the hacker, who is mainly taking advantage of hacking tools that are publicly available to exploit known vulnerabilities (the so-called script kiddies). Protection against these attacks can usually be achieved with by ensuring regular application updates, and deployment of existing signature detection technology in the network firewall.

But this does not provide application-level security. Firewalls are designed to stop specific exploits from occurring via signatures, or stopping specific ports from being used, or to track to verify that only conversations initiated from inside the firewall are allowed to go through the firewall. But consider the situation where a user wants to access a banking system. He has a legitimate account with this bank, so he authenticates to the bank and establishes a valid session through the firewall. But now he wants to get information he should not be able to get, and decides to try and convince the backend database he is someone else (perhaps by using a cross-site script attack). The firewall cannot tell he is doing this, because the session-level information it tracks is still valid. Unless he attempts to send a virus/worm/Trojan to the bank, the firewall will not care.

What are some of the limits of current network firewalls?

1. They cannot stop a malicious user who is asking the application to perform an illegal operation, perhaps by using a cross-site script or a command injection.

2. They cannot determine when an application asks a user to submit his phone number, but the user returns his address, a SQL command, or another type of form field manipulation. Because the network firewall was not even aware of the original request it cannot verify whether or not the user's reply is consistent with what the application is expecting.

3. A firewall cannot detect a user asking a question that the application should not answer. For example, a hacker could submit a specially-crafted URL in a request that would access a part of the application that should be off-limits, known as forceful browsing.

4. Firewalls do not follow conversations, and cannot track when cookies are exchanged. Many applications give each user a cookie to use each time they want to communicate. What if an attacker sent someone else's cookie (or modified his own) in an attempt to impersonate that person?

3.6 If Network Firewalls Won't Work, What Should I Do?

Because of these limitations, newer devices called web application security gateways go beyond network firewalls by comprehending electronic conversations. They perform the basic operations of a network firewall – capturing individual words (packets) and forming complete sentences (stream normalization), but unlike firewalls a web application security gateway understands the language in which the conversation is conducted (HTML, XML, SOAP, etc.). The ability to deconstruct conversations based on an understanding of the language, along with the ability to listen to both sides of the conversation, enables an application security gateway to fully protect the application.

Since custom software developed for web applications are typically unique to each organization, the vulnerabilities found in each such application are also unique. Imagine a hacker facing the task of compromising a new Web application. Initially he would know very little about the application and would need to start a reconnaissance effort to learn its structure and find its weak spots. He would begin by taking advantage of the current firewall limitations described above to construct application attacks that relied solely upon well-formed HTTP traffic, hoping to set off no alarms and leave no trail. These application attacks would then target both known vulnerabilities in commercial software and the as-yet unknown vulnerabilities in the custom/internally developed Web application software.

Because much custom web application code is built according to the special needs of each organization, and because the needs of one organization are rarely the same as those of another, each web application has its own set of bugs and flaws that may expose new and unknown security vulnerabilities. An experienced hacker would next move on to uncovering and exploiting these as-yet unknown vulnerabilities. As the hacker learns more about the application and its loopholes, this reconnaissance may become more aggressive and malicious. Finally, the hacker may collect enough information about the application in order to attack using vulnerabilities he has found.

Of course one of the best ways to secure your web applications is by doing a better job of integrating security into the development process. For instance, there are development tools which allow you to proxy the conversation and observe precisely how the application under development responds to staged attacks. "Several studies have indicated that it is cheaper to address security vulnerabilities in software during the development phase versus waiting until the application is released to customers. If a malicious attack is successful on a web application that is already in commercial use or production, companies must face costs associated with removing the application from production, assessing the damage to the application and the data it manages, as well as costs associated with loss of reputation and customer confidence that may result from the attack [3]."

First generation web application security gateways have attempted to protect a portion of the web application farm (web servers) using rule-based firewall techniques. These products attempt to define all allowed web application behaviors and immediately block all behaviors which do not conform to this predefined model. This method, however, has been found to not scale to match the complexity of real world web applications, which are constantly changing. These changes are typically made on a daily basis, without the knowledge of the security team. As a result, a web application firewall policy/profile that works one minute will be out of date and blocking legitimate users the next.

The downside of these web application firewalls is that they require detailed administrator knowledge of the applications being protected, and a large investment in tuning to maintain high levels of security without false positives. Since security managers typically do not have detailed and continuous knowledge of the corporate web application code, most organizations cannot afford to deploy a staff of security administrators for each web application. These "problems", however, are the same ones that surrounded the early deployment of network firewalls. They were seen as high-end devices that only the largest companies could afford, they were difficult to configure and easy to make mis-configuration errors. Yet they were needed, and now almost every company uses one of some kind. The same group of early adopters of network firewalls is also the early web application security appliance adopters – financial institutions, hospitals, and government entities – the places where the most sensitive data (hacker targets) is stored.

4. CONCLUSION

The problem of consumer confidence and trust is one for the business to redress [1]. Implementing a rounded security solution will enable it to explain and justify the measures it has taken to provide the online system and its features [4]. Overall, Ecommerce sites need to be concerned with a variety of security issues including: authentication-verifying the participants involved in the transactions; authorization-verifying the user has permissions to specific data. Firewalls, VPNs and IDNs have been proven useful as tools to ensure a secure ECommerce site.

If the security and privacy problems are addressed, more people would purchase goods and services online and ECommerce will be pushed a huge step forward. It is imperative that security

becomes an integral part of the architecture, design, and implementation of any eCommerce site.

5. REFERENCES

[1] Anonymous (2003) Special Report, 2003, April 17. Computing. Security: Smart Moves to earn Consumer Confidence. Retrieved July 19, 2003 from Lexis Nexis.

[2] Annonymous (2004) “Financial Services”, Teros Corporation, Internal Sales Training Document, Updated April 7, 2004 ,www.teros.com

[3] Annonymous (2004) “About @Stake WebProxy, the Interactive Application Security Testing Tool”, @Stake, Inc., (http://www.atstake.com/products/webproxy/), referenced July 9, 2004.

[4] Anonymous (2003), “Web Defacement Statistics”, Security News Portal, 2 April 2003, (http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanY.dbid=67), referenced July 7, 2004.

[5] Ben-Itzhak, Yuval (2002) “Web Application Security--The Next Evolution”, DevX.com, 9 December 2002, (http://www.devx.com/security/Article/10236), referenced July 7, 2004.

[6] CERT coordination center, CERT advisories and other security information, CERT/CC, Pittsburgh, PA. Available online: http://www.cert.org.

[7] CSI (2002) “2002 Computer Security Institute (CSI) Computer Crime and Security Survey” (conducted with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad), Computer Security Institute, 7 April 2002, (http://www.gocsi.com/press/20020407.jhtml?_requestid=280129), referenced July 6, 2004.

[8] Dekker, M. (1997). The Frolich/Kent Encyclopedia of Telecommunications vol 15. New York. P231.

[9] McCullough, J. (2005) Beyond the Firewall: Using a Layered Security Strategy to Address Internal Security Threats, Accessed June 10, 2005 at http://wp.bitpipe.com/resource/org_978461805_612/surfcontrol.pdf

[10] Morrison, Michael C. 2001 July 13. E-Commerce Trends. Accessed May 12, 2005, at http://www.niacc.cc.ia.us/admin/academic/scroll/trends.html

[11] Turban, E., King, D., Lee, J., Warkentin, M., Chung, H. (2002). Electronic Commerce: A Managerial Perspective 2002. New Jersey:Prentice Hall.

[12] Zinkewiez, Phil, 2000, February 19. Insurance Advocate. Hacker Attackers Raise Troubling questions on eCommerce Security, Developments. Retrieved July 19, 2003 from Business Source Premier.