E-Commerce Security Issues

Randy C. Marchany
Virginia Tech
Computing Center
Blacksburg, VA USA 24061
marchany@vt.edu

Joseph G. Tront
Electrical & Computer Engineering
Virginia Tech
Blacksburg, VA 24061-0111
jgtront@vt.edu

Abstract

Without trust, most prudent business operators and clients may decide to forgo use of the Internet and revert back to traditional methods of doing business. To counter this trend, the issues of network security at the e-commerce and customer sites must be constantly reviewed and appropriate countermeasures devised. These security measures must be implemented so that they do not inhibit or dissuade the intended e-commerce operation. This paper will discuss pertinent network and computer security issues and will present some of the threats to e-commerce and customer privacy. These threats originate from both hackers as well as the e-commerce site itself.

A straightforward comparison could be made of the security weaknesses in the postal system vs. security weaknesses on the Net. The vulnerable spots in both cases are at the endpoints – the customer's computer/network and the business' servers/network. Information flowing in the conduit (trucks/planes and wires) is relatively immune to everyday break-ins. Privacy issues are amongst the major drivers for improved network security along with the elimination of theft, fraud and vandalism. Two major threats to customer privacy and confidence come from sources both hostile to the environment as well as sources seemingly friendly. Coordinated attacks on Yahoo, eBay, ZDNet, Buy.com (on their IPO day) and amazon.com generated a huge amount of publicity and a federal government response. A brief description of these attacks will be given in this paper. Another threat may originate at ostensibly friendly companies such as DoubleClick, MemberWorks and similar firms that collect customer information and route it to other firms. Much of this transaction information is able to be associated with a specific person making these seemingly friendly actions potential threats to consumer privacy.

Many of the issues and countermeasure discussed here come from experiences derived with consulting with clients on how to maintain secure e-commerce facilities. These methods and techniques can be useful in a variety of client and server environments, also serving to alert e-commerce users of potential threats.

1. Introduction

The eradication of trust in Internet commerce applications may cause prudent business operators and clients to forgo use of the Internet for now and revert back to traditional methods of doing business. This loss of trust is being fueled by continued stories of hacker attacks on e-commerce sites and consumer data privacy abuse. Hackers demanding a ransom from an e-commerce site for not publishing customer credit card information have increased the visibility of the network security weaknesses in most business institutions. The conflict between convenience and ease-of-use vs. security has always been resolved in favor of convenience. However, recent virus attacks against Microsoft Outlook (The NIMDA, Code Red worms, the "ILOVEYOU", "Resume" and KAK viruses) have demonstrated that convenience allows the rapid proliferation of viruses and worms throughout the Internet. Microsoft released a patch that disabled the feature that allows the "ILOVEYOU" virus to work. This is the first time a software vendor has released a patch that *restricted* a feature. Further, the success of the Distributed Denial of Service (DDOS) attacks against major e-commerce sites pointed out the importance of maintaining adequate security at sites not even remotely associated with the targeted e-commerce sites.

0-7695-1435-9/02 $17.00 (c) 2002 IEEE

Not all of this is bad news. The majority of security breaches on the Internet occur at the endpoints, i.e., the local network, rather than the main "backbone" of the Internet. This situation allows us to make a comparison of the security weaknesses in the postal system and the Internet. The most vulnerable spots of the postal infrastructure are at the endpoints: the mailboxes at the sender and recipient sites. An example of abuse in the postal system was reported in a Roanoke Times newspaper reprint of a Los Angeles Times article that describes a thief stealing postal mail from mailboxes [7]. The thieves were stealing bills, paychecks and other consumer identity related mail from the victim's home mailboxes or from the postal system's street mailboxes. This type of security breach happens much more often than one in which a thief steals directly from inside a post office. Security standards, controls and practices have been developed within the main trunks of the postal infrastructure to monitor and hopefully prevent mail interception or tampering when the letter is in the system. Similar controls are in place at the equivalent Internet network level. Controls at the endpoints on the other hand vary widely from very good (usually at the originating business) to non-existent (usually at the home computer).

Consumer privacy is becoming the most publicized security issue replacing theft and fraud as top concerns in e-commerce. The DDOS attacks demonstrated that business sites did not maintain adequate security protection and intrusion detection measures. Some of the sites did not detect the compromise, which occurred months before the DDOS attacks. The hackers who penetrated these sites had the ability to deliver a data integrity attack on the compromised business for the same amount of time. Businesses were spared simply because the hackers chose not to attack them in that manner. The recent NIMDA and Code Red worms succeeded in penetrating systems because sysadmins *failed to installed vendor patches*. No customer will want to use a business that distributes sensitive customer data such as credit card information, SSN information or credit limits without the knowledge or permission of the customer. Is this situation different from similar abuse in the phone or mail order business model? Not really but the major difference has to do with the speed of access to and dissemination of the sensitive data.

User and system administrator awareness is becoming more important in the effort to counter e-commerce attacks. Consumers are slowly becoming aware of some security features such as encrypted WEB transactions, privacy statements by companies, etc. Internet service providers are becoming more responsive to complaints about Internet abuse originating from their sites.

E-commerce security needs to be addressed not only at the business site with its servers/network but also on the client side, which includes direct connected home computers. It is this group of computers that are the most vulnerable to attack because the level of user security training or awareness is not high at all.

2. The Threats to E-Commerce

The standard client server model has three components: the server system, the network and the client system. In the past, server systems were typically mainframes running operating systems such as MVS, VM, VMS or Unix. Window NT and Windows 2000 (W2K) are now making inroads into this arena. The network component includes the internal business network, the path between the business and the customer through various ISPs and the customer's internal network. Client systems are usually PC or Macintosh systems running their respective Window 9x, NT, W2K or MacOs operating systems although Unix systems do serve as client systems.

2.1. E-commerce Security Components

E-commerce security strategies deal with two issues: protecting the integrity of the business network and its internal systems; and with accomplishing transaction security between the customer and the business. The main tool businesses use to protect their internal network is the firewall. A firewall is a hardware and software system that allows only those external users with specific characteristics to access a protected network [8]. The original design was supposed to allow only specific services (e.g., email, web access) between the Internet and the internal network. The firewall has now become the main point of defense in the business security architecture. However, firewalls should a small part of the business security infrastructure. There are hacker tools such as SMTPTunnel and ICMPTunnel [12] that allow hackers to pass information through the allowed ports. The "ILOVEYOU" virus successfully penetrated firewalled networks because inbound and outbound email is allowed to pass through the firewall. The Code Red and NIMDA worms passed through firewalls because they accessed systems through the standard WEB server ports.

Transaction security is critical to bolstering consumer confidence in a particular e-commerce site. Transaction security depends on the organization's ability to ensure privacy, authenticity, integrity, availability and the blocking of unwanted intrusions [8]. Transaction privacy can be threatened by unauthorized network monitoring by software devices called sniffer programs. These programs are most likely found at the endpoints of the network connection. There are a number of defenses against this threat such as encryption and switched network topologies. Transaction confidentiality requires the removal of any trace of the actual transaction data from intermediate sites. Records of its passage are a different thing and are required to verify the transaction actually took place. Intermediate nodes that handle the transaction data must not retain it except during the actual relaying of the data. Encryption is the most common method of ensuring confidentiality. Transaction integrity requires methods that prevent the transactions from being modified in any way while it is in transit to or from the customer. Error checking codes are an example of such a method.

Encryption techniques such as secret-key, public-key and digital signatures are the most common method of ensuring transaction privacy, confidentiality and integrity. The common weakness of these techniques is that they depend on the security of the endpoint systems to protect the keys from modification or misuse. The following paragraphs will discuss the vulnerabilities of this client-server model.

Early hacker attacks were directed at the server systems because that's where the access or data lived. As server system administrators became more experienced, it became harder for hackers to successfully penetrate the servers. The hackers then shifted their focus to the network feeding into the server. They were able to continue subverting the servers by intercepting the cleartext traffic flowing in and out the server. Encrypting network traffic, converting the network to a switched topology and filtering unknown access were some of the countermeasures to this "sniffer" attack. In response to this, the hackers simply shifted to the client side and this is where most network security architectures collapse. Why? Looking at the OS architectures prevalent in the client side, we observe: an OS used in a server is also used on the client system or the PC/Macintosh OS is used on the client. If the client OS is the same as the server, then the same server defense mechanisms can be used on the client system. However, if the client OS architecture is based on Windows 9x or MacOs then there is no effective defense available. These OS platforms have no built-in security designed into them and allow anyone with access to the system to be able to gain control of it. These OS architectures will continue to be susceptible to virus and Trojan horse program attacks.

The two main threats to the e-commerce client-server model are viruses and Trojan horse programs. Viruses are simply disruptive in nature but the Trojan horse programs are the more serious threat because they not only facilitate breaking into another system, they also permit data integrity attacks.

2.2. Viruses

Viruses are the most publicized threat to client systems. They are effective because of the built-in insecurity of client systems (PC/Mac). Subverting a PC/Mac system requires access to the system and no special privilege is needed to write code or data into sensitive system areas. This operating system design issue is evident in older versions of Windows 9x or MacOs 8.x. Operating systems such as Windows NT, Windows 2000, while still vulnerable to this type of attack, do have the capability of restricting who can activate the virus. The more publicized viruses such as Melissa, ILOVEYOU, Resume, KAK and IROK have no effect on Unix systems. Viruses need "system privilege" in order to be effective. In general, the multiple privilege access schemes present in Unix, VMS and other multi-user operating systems prevents a "virus" from damaging the entire system. It will only damage a specific user's files.

2.3. Trojan Horses

The **BackOrifice**, **Netbus**, **BO2K** hacker tools allow a remote user to control, examine, monitor any information on the target PC. What makes them especially beguiling is that they are also capable of using the target PC to send information to the net *as if the legitimate user had done so.* There are commercial tools like CUCme, VNCviewer that perform the same function. There are numerous hacker exploit web sites such as www.portwolf.com/trojans.htm, www.cultdeadcow.com, www.rootshell.com, http://thc.pimmel.com and www.insecure.org where anyone can download a copy of the abovementioned Trojan horse programs. The good side of the Force allows system administrators to use these tools to remote manage large numbers of workstations. This is the typical sysadmin support tool since there are many more machines than sysadmins. However, the dark side of the Force allows a malicious user to install these tools for nefarious purposes such as forgery, data modification and eavesdropping.

Figures 1 and 2 are screen shots of an actual remote control program that was installed on an unsuspecting victim's computer. The victim had a mini-cam attached to his PC and the hacker can see what's going on inside his room. The reason why the person has a stunned look on his face is shown in Figure 2. There you can see the victim’s desktop with the icons blacked out for illustrative purposes. The Yahoo Messenger window is revealing to the victim that his machine has been taken over by someone else. The message was sent in a humorous tone but the implied threat is quite real. *The hacker has full control of the victim's computer*. The hacker can move the mouse and run any program, modify any file or delete any file from the victim’s system. In addition, the hacker can see everything that the victim does on his computer. These types of programs become more dangerous to e-commerce than viruses as more direct connect households enter the Internet with little or no protection from this type of attack. Thus the purveyors of e-commerce must find ways to provide the tools and change the culture of personal computing in order to tighten security at the client endpoints.

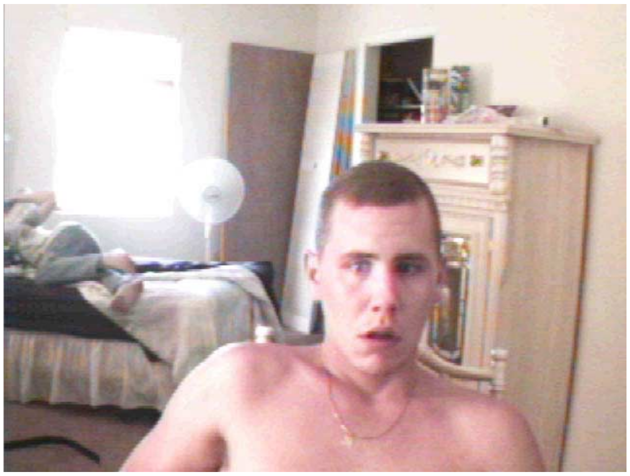
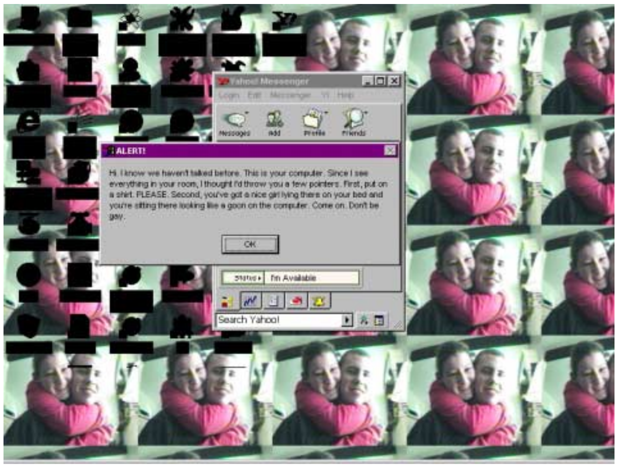


Figure 1: The Hacker’s View: A Victim looking at his Monitor

These hacking tools are easiest to install on PC or Mac systems and the preferred method of delivery is by email attachment. The author presented a paper in 1996 at the SANS Institute's Network Security Conference describing how a keystroke recorder program could be sent and installed on client systems via email attachments [1]. The ease of constructing such an attack still frightens the author. No real computer knowledge other than how to use a web browser is needed. These types of monitoring programs can easily subvert any encryption system in place since they will capture the data *before* it gets encrypted. Designing filters to detect these tools will be difficult since source code is provided with each of the tools. Defense mechanisms in this case are reduced to being reactive instead of proactive.

The main difference between an attack aimed at PC or Mac and one aimed at a Unix or NT systems is the former is system wide in scope while the latter is user-centric. The exception in this case is if the admin or root user of the NT or Unix system is targeted. These types of tools pose a threat to the data integrity and confidentiality aspect of e-commerce.


[redacted]

Hi, I know we haven't talked before. This is your computer. Since I see everything in your room, I thought I'd throw you a few pointers. First, put on a shirt. PLEASE. Second, you've got a nice girl lying there on your bed and you're sitting there looking like a goon on the computer. Come on. Don't be gay.

Figure 2: What the Victim is Reading on <u>his</u> screen

2.4. Which is the Bigger Threat to E-commerce?

Viruses are a nuisance threat in the e-commerce world. They only disrupt e-commerce operations and should be classified as a Denial of Service (DoS) tool. The Trojan horse remote control programs and their commercial equivalents are the most serious threat to e-commerce. Trojan horse programs allow data integrity and fraud attacks to originate from a seemingly valid client system and can be extremely difficult to resolve. A hacker could initiate fraudulent orders from a victim system and the e-commerce server wouldn’t know the order was fake or real. Password protection, encrypted client-server communication, public-private key encryption schemes are all negated by the simple fact that the Trojan horse program allows the hacker to see all cleartext before it gets encrypted. The reader need only look at Figure 2 to be reminded of the danger.

3. Privacy Issues

The abuse of consumer privacy is becoming a concern at the consumer, business and government level. There will be resistance to participating in certain types of e-commerce transactions if the assurance of privacy is low or non-existent.

3.1. Abusing Customer Privacy

The government (Big Brother) isn't the biggest threat to privacy anymore. Businesses are!
US Bankcorp was sued for deceptive practices in 1999. The bank supplied a telemarketer, MemberWorks, with sensitive customer data such as name, phone #, bank account and credit card numbers, SSN, account balances and credit limits. MemberWorks used these customer lists to sell dental plans, videogames, and services. US Bankcorp settled out of court. Well Fargo, Bank of America and other financial institutions announced they were *discontinuing the practice* after the US Bankcorp settlement was announced. Many banks still deal with MemberWorks today. Jane Bryant Quinn's essay on Privacy Issues [3] lists a couple of items of concern:

1. No Federal law shields "transaction and experience" information.
2. Social Security Number information is periodically disclosed either intentionally or not.
3. Self-regulation by business doesn't work.

Obviously, not all businesses are dens of information disclosure. However, most businesses do not treat the information security cycle as a high priority until an event happens. They consider a firewall to be the best line of defense and pay not enough attention to securing the internal net.

3.2. 1984 or Lord of the Flies?

Firms like the Internet advertising firm DoubleClick collect customer information and route it to other firms for use in creating customer profiles. Doubleclick recently acquired a direct marketing company, Abacus, Inc., is an effort to link anonymous hits on Web sites with actual names and addresses of Web surfers. The firm backed off this effort after the Federal Trade Commission launched an investigation. In another example of a consumer privacy threat, grocery store chains offer discount cards to its customers. Swipe the card through their reader and the customer gets discounts on food items. This service allows the business to determine the buying habits of the customer and perhaps better stock the store with the items the customers buys frequently. The store is free to sell this data to marketing firms without notifying the customer. This Personal Service vs. anonymity conundrum represents the major issue with E-commerce privacy. If the majority of businesses are not considered to be secure, the confidentiality and integrity of the customer information is suspect. This may be a bold statement to make about most business network security but the DDOS attacks, the results of the Internet Audit Project shown in Table 2 and the Top Ten Vulnerabilities list compiled by SANS demonstrated this lack of security at thousands of sites. This lack of security is the biggest threat to consumer privacy from external sources. Selling consumer data without the customer knowledge or permission is the major internal threat to consumer privacy.

Consumer information integrity is the clearly a problem if sites fail to secure the customer data at the server or the client. It is just as easy to modify customer data, as it is to publish it. This ability to instantly rewrite a consumer's history with a particular business is quite possible and certainly easy to do with the BO2K style Trojan horse programs installed on an unsuspecting client.

The US Federal Trade Commission is urging the US Congress to pass legislation to bolster online privacy because it has doubts about whether companies can or will self-regulate. The FTC conducted a survey of 335 commercial Websites and 91 of the 100 most popular sites to determine their information gathering practices. Almost all the sites in both groups collected email address information from visitors but only 88% of the 335 sites had posted privacy policies. Twenty percent of these sites had policies "that reflect the fair information principles of notice, choice and access security" [6]. The FTC lists four types of privacy protection that it considers essential:

1. a notice defining privacy policies
2. a choice of how the user information collected by the site is used
3. access to that data by the individual
4. assurances that the data is secure

The same FTC survey found that 42% of the most popular web sites and only 20% of the 335 sites offer consumers the above types of protection. The same Computerworld article made the observation that "the FTC applied very easy grades to the Web sites it investigated…. For instance, if a Web site offered any type of access, such as allowing consumers to update their email addresses, the survey scored the Web site as having access. 'And the majority of them still flunked' ". A recent commentary by William Safire [9] pointed out that e-commerce is "an industry busily compiling dossiers on every American." These sites collect information about web browsers by using web "cookies" to track your movements around their web site. One can certainly see the merits of this action; however, it's not quite apparent why the organization is allowed to sell that data to other businesses.

Appendix 1 shows some of the user data that can be gleaned from a simple access to a web site. One of the authors visited www.anonymizer.com to generate the figure. The information shown in the appendix is accurate. Even more detail can be obtained from the www server logs. One of the issues raised at www.glr.com is that a composite profile can be constructed about a user from seemingly disparate databases. For example, one can look up a person at www.switchboard.com to get the address and phone number of an individual. Accessing www.mapquest.com and entering the address from the previous query to get a map and driving directions to the person's address could pose a threat to the individual's privacy. Access the person's personal web page and you most likely can get a photograph of the individual. This is an example of data residing in completely different and geographically separate sites being used to build a composite about a person. The danger is that the access security is different at the sites and is not coordinated at all.

E-commerce sites have the capability of assembling an incredible amount of information about consumers and disseminating this information with or without the individual's permission. The absence of privacy regulations will continue until a major privacy failure happens. The failure of a site to maintain adequate security allows someone to rewrite the consumer history of an individual with very little mechanisms for verifying the accuracy of the information.

4. The Distributed Denial of Service Attacks (DDOS)

Businesses that rely on web-based transactions are and will continue to be vulnerable to Denial of Service (DoS) attacks. DoS attack scripts are the most common, effective and easiest to implement attacks available on the WEB. No actual damage is done to the victim site. The access paths to it are simply overwhelmed with incoming packets. It would be every businessman's dream to be in this situation if the incoming packets were legitimate customer orders. However, it can be their worst nightmare if they are the targets of a DoS attack. Early DoS attacks were triggered by one internal machine against another. The Distributed Denial of Service (DDOS) attacks are the latest evolution of DoS attacks and their success depends on the inability of intermediate sites to detect, contain and eradicate the penetration of their network. The more intermediate sites are compromised, the more sites are available to launch a DDOS attack against a victim site. The 1999 DDOS attack against the University of Minnesota generated over 2 billion packets sent from under 300 systems in 10 minutes.

The DoS attack is diabolically simple. Every packet transmitted on the Internet contains a source and destination address. The simplest example is that of a ICMP ping transaction. The basic transaction is:

1. source system sends a "ping" packet to the target. This is an ICMP_ECHO_REQUEST packet containing the source address of the sender and the target address of the receiver.
2. If the target system is able to respond, it sends a response back to the source address listed in the "ping" packet. This is an ICMP_ECHO_REQUEST_REPLY packet.

A ping packet is used to determine if a target site is online. The original attack was called Smurf and simply replaced the source address of the ICMP_ECHO_REQUEST packet with the address of a host other than the original sender. This new and unaware source site would receive the REPLY packet and ignore it. This process does consume some processing time. The DoS occurs when the source site receives hundreds of thousands of these packets.

DDOS took the original Smurf attack one step further. Entire networks were compromised and slave daemons were installed on the individual machines. These slave daemons can launch an ICMP, SYN, UDP or smurf flood attack but do so only at the command of master systems that were also compromised. The hacker sends the attack command to the masters, each of which relays the command to the slave daemons. It is quite possible to have tens of thousands of machines launching the attack against a single site. The success of a DDOS depends on the failure of the compromised networks to detect and eradicate the master and slave programs. This failure could be caused by a number of reasons: lack of system administrator experience, lack of base security standards for each machine, lack of intrusion detection software to notify the admins or a management decision to not get involved. The DDOS programs are called TFN, Trinoo, Win-trinoo, Stacheldracht among others. There are numerous variants of these original programs but the concept is the same. The most dangerous of these is the Windows 9x variant called win-trinoo because there are millions more Windows systems than servers.

4.1. The Reason why DDOS attacks worked

4.1.1 Are Sites Vulnerable?

Internet sites are vulnerable if site managers did not perform standard patch maintenance and did not monitor their systems regularly with any intrusion detection tools. In 1998, a group of hackers probed as many Internet hosts as they could find[11]. The probe checked these sites for common, well-known vulnerabilities on their systems. The results are shown in Table 2. All of the vulnerabilities could be fixed by having installed vendor-supplied patches. A successful exploit of any of these weaknesses would grant a hacker full control of the machine. The table clearly showed that standard system security maintenance was not done on a large number of machines. This lack of preparedness set the stage for the recent DDOS attacks. The SANS Institute released a “Top 10 Vulnerabilities”[10] document that lists the 10 vulnerabilities that have resulted in over 80% of the network break-ins in the last 3 years. The list closely supports the data in Table 2.

Vulnerability	**%**
webdist	0.77
imap	15.5
qpopper	12.4
innd(News)	0.52
tooltalk	26.1
rpc_mountd	10.8
nameserver	18.1
www	12

Table 2: Internet Audit Project Findings of Common Vulnerabilities Found. A total of 735065 hosts were checked for well known vulnerabilities.

Table 1 lists the top four operating system platforms that were compromised during the period of 8/99 to 5/00. The full data is available at www.attrition.org. and contains data from sites who were willing to admit the compromises happened. The interesting point about the table is that Microsoft Windows NT servers were compromised almost four times more than the next OS. The statistics may reflect the dominance of Windows NT but the underlying fact is that most of the NT compromises were the result of a failure to install vendor security patches. This is certainly true with the other line items in the table. However, the NT systems are new in the server arena and so are its system administrators. Each of these compromised systems could have been used in a DDOS attack.

Operating System	Count	Percent
Window -NT	2252	59.5
Linus	544	14.37
Solaris	411	10.86
BSDI	117	3.33

Table 1: OS Compromise Counts from 8/99-5/00 (www.attrition.org)

4.1.2 Key Factors

The Consensus Roadmap for Defeating Distributed Denial of Service Attacks[4] lists the following trends that allow attacks against e-commerce sites to succeed:

1. Defensive strategies tend to be reactive rather than proactive. The antivirus strategy is a prime example. It works only for what it knows. The 1999 Melissa virus caught the Internet community by surprise with the speed of its propagation. Standard antivirus filters have practically eliminated the Melissa virus as a threat but they did not eliminate the class of virus. This became evident when the ILOVEYOU virus successfully penetrated institutions that had firewalls installed. Later ILU attacks were repulsed by the firewalls once a filter was created to look for that particular flavor of virus. The new filters failed to stop newer viruses like the Resume virus and the reactive antiviral strategy continues.
2. There are tens of thousands, possibly millions of systems with weak security connected to the Internet. A hacker group conducted an "audit" of as many sites as they could probe for common, well known vulnerabilities. They probed over 730,000 sites and the results were astonishing. They are shown in table 2. Attacker are building attack networks and triggering them at a later date. The number of directly connected homes, schools and other venues with little or no system administration or security staff is increasing rapidly. These always-on, rarely protected systems allow attackers to add these systems to their captured list.
3. Increasingly complex software is being written by programmers who have had no training in writing secure code. They are working for organizations that are sacrificing the safety of their clients for speed to market.

4. User demand for new software features instead of safety, coupled with industry response to that demand, has resulted in software that is increasingly supportive of subversion, computer viruses, data theft and other malicious acts.
5. The explosion in use of the Internet is straining the already scarce technical talent pool. Over 2 million new Internet hosts are added every month and there are not 2 million properly trained system administrators to manage these machines. The average level of system administrator technical competence has decreased dramatically in the last five years as non-technical people are drafted into service as system administrators. These people are typically not given the training resources they need to adequately fulfill their job functions.
6. Attack technology and tool deployment is international in scope. Solutions must transcend national boundaries.
7. The difficulty of cybercrime investigation, apprehension and prosecution means that successful prosecution in unlikely and won't be an effective deterrent. The ILOVEYOU virus case is an example of this difficulty.

4.2. The E-commerce Site’s Security Responsibility

DDOS attacks worked because sites failed to detect the initial compromise of their systems. The compromises could have been prevented if standard system maintenance had been performed. Had the sites detected the compromises, they would have eliminated themselves as unwitting accomplices in the attack. Proper system administration training is the easiest method of countering this and other types of attacks. The security of a site depends on the security of the internal systems *and the security of external networks*.

E-commerce sites need to tailor their security architecture to meet the demands of ensuring consumer data privacy and that company resources are not used to attack other Internet sites. A business can certainly survive the publicity generated if their network is used to attack another site. It most certainly wouldn't survive if word gets out that customer credit, purchase, or personal data is stolen or copied without their knowledge or permission. For example, a hacker broke into an Internet music store, CD Universe, and published 300,000 customer credit card numbers when the store refused to meet his extortion demands [13]. This action prompted major credit card companies to issue replacement cards for the customers affected by the attack. The e-commerce industry suffered a major setback in its effort to allay consumer fears about security when it was revealed that CD Universe's site was open to hackers for a few hours before the attack was discovered [13]. It suffered another blow when the security investigation revealed that the security hole was well known and that a vendor patch was available to close the hole. The hacker could have easily mounted a data integrity attack on CD Universe's customer database instead of demanding a ransom. The company was spared only by the whim of the hacker.

Jim Seymour stated in a recent article at The.Street.com that the "last-inch" problem entails a horrendous cost if the e-commerce site is *always* up and available. He claims e-commerce won't be crippled by the DDOS attacks. E-commerce as an overall business factor won't be crippled but individual e-commerce sites will be affected.

Software developers need to design software that is engineered for safety and security. It is still possible to add ease-of-use features but they should be initially turned off. Automated security updates are another feature that could be used to help limit the scope of these attacks. Microsoft released a patch that disabled some of the features of its Outlook/Exchange tool. This was most certainly due to the negative publicity the company was getting about their product but it demonstrated the power of that negative publicity.

Proper training programs for the system administrators are the easiest and most effective way to prevent major security compromises. The Audit group needs to review the security methods to ensure their compliance with company policy and general Internet security standards.

4.3. The Client Responsibility

Cable modems, DSL connections and other high speed direct connect mechanisms for connecting to the Internet create an entirely different set of security issues. The migration of DDOS attack tools to the Windows OS now allows a hacker to use these direct connect systems as another base of operation. The ISP’s responsibility to maintain network integrity and create a model for containing any attack with their domain is paramount.
There are a number of documents available to these ISPs that provide guidelines for securing their networks [14].

The estimated number of systems used in the original DDOS attacks of early 2000 is thought to be less than 1000. There are certainly orders of magnitude more direct connect systems with minimal security tools installed. Certainly, the system administration expertise of these systems is not very high.

The client's main responsibility deals with requiring e-commerce sites acknowledge the right of the customer to examine their credit history and to be provided with information about who gets that information. E-commerce businesses should develop orientation programs for their customers that teach about basic security practices. This certainly helps ensure confidence in the business' ability to secure and protect the customer information.

5. Conclusions

The e-commerce industry is slowly addressing security issues on their internal networks. There are guidelines for securing systems and networks available for the e-commerce systems personnel to read and implement. Educating the consumer on security issues is still in the infancy stage but will prove to be the most critical element of the e-commerce security architecture.

Trojan horse programs launched against client systems pose the greatest threat to e-commerce because they can bypass or subvert most of the authentication and authorization mechanisms used in an e-commerce transaction. These programs can be installed on a remote computer by the simplest of means: email attachments.

Training programs, orientation programs will become more critical in order to increase the general populace's awareness of security on the Internet.

IT and financial control/audit groups within the e-commerce site should form an alliance to overcome the general resistance to implementing security practices at the business level.

Industry self-regulation of consumer privacy appears to be ineffective. The FTC privacy survey and its recommendations to Congress may result in the introduction of legislation on privacy issues.

6. References

1. Randy C. Marchany, Tom Wilson. A Keystroke Recorder Attack on a Client/Server Infrastructure. Proceedings of the Network Security '96 Conference, SANS Institute
2. Peter Keen. Ensuring E-Trust. ComputerWorld, 3/13/00 issue
3. Jane Bryant Quinn. The Spies in Your Pocket". Newsweek, 8/16/99
4. Northcutt, Cheswick, Kent, Cooper, Marchany et al. Consensus Roadmap for Defeating Distributed Denial of Service Attacks. www.sans.org/ddos_roadmap.html
5. "Distributed System Intruder Tools - Trinoo and Tribe Flood Network", Computer Incident Advisory Capability, Lawrence Livermore National Laboratory, CIAC 00.040, 12/21/99
6. Patrick Thibodeau. Privacy Concerns Rankle Industry – In Blow to sites, FTC pushes for regulation. Computerworld, 5/29/00, Vol 34.no 22.
7. “Lucrative mail theft on the rise”, RoanokeTimes reprint of LA Times article, 6/1/00
8. Ravi Kalakota, Andrew B. Whinston. Electronic Commerce: A Manager’s Guide, Addison-Wesley, ISBN: 0-201-88067-9
9. William Safire. The Phantom of the Internet. New York Times Service, article appeared in 6/4/00 issue of the Roanoke Times.
10. The SANS Institute, www.sans.org/topten.htm
11. The Internet Audit Project, http://www.securityfocus.com/templates/forum_message.html?forum=2&head-32&id=32
12. www.detached.net
13. www.usatoday.com/life/cyber/tech/cth186.htm
14. www.sans.org/dosstep/index.htm