MODUL PERKULIAHAN ELEARNING
MATA KULIAH - MCM 205 – ECOMMERCE (3 SKS)

PERTEMUAN 13 – *ELEARNING*

Berbagai aspek yang berhubungan dengan keamanan eCommerce

Dosen
H. Andri Budiwidodo, S.Si., M.I.Kom.
(ID 7715)

Sumber penulisan modul:

Kenneth C. Laudon and Carol Guercio Traver. 2014. e-Commerce Business Technology Society. 10th Edition. New Jersey: Pearson. Halaman 244-295.

Introduction: eCommerce Security

There are several steps you can take to protect your business Web sites, your mobile devices, and your personal information from routine security attacks. Reading this chapter, you should also start thinking about how your business could survive in the event of a large-scale “outage” of the Internet.

In this chapter, we will examine e-commerce security. First, we will identify the major security risks and their costs, and describe the variety of solutions currently available. **Table 1** highlights some of the major trends in online security in 2013–2014.

Table 1	**What’s New in E-commerce Security 2013–2014**
• Mobile malware presents a tangible threat as smartphones and other mobile devices become more common targets of cybercriminals. • Politically motivated, targeted attacks by hacktivist groups continue, in some cases merging with financially motivated cybercriminals to target financial systems with advanced persistent threats. • Hackers and cybercriminals continue to focus their efforts on social network sites to exploit potential victims. • Nations continue to engage in cyberwarfare and cyberespionage. • Large-scale data breaches continue to expose data about individuals to	

hackers and other cybercriminals.
- Certificate authorities and the digital encryption regime that provides a basis for trust within the Internet infrastructure tighten standards in an attempt to prevent further attacks after several high-profile hacks.
- Malicious attacks targeting Mac computers increase.
- The amount of spam continues to decrease as a result of the demise of Rustock, the largest spam sending botnet in the world and better detection techniques by e-mail providers.

The E-commerce Security Environment

For most law-abiding citizens, the Internet holds the promise of a huge and convenient global marketplace, providing access to people, goods, services, and businesses worldwide, all at a bargain price. For criminals, the Internet has created entirely new—and lucrative—ways to steal from the more than 1 billion Internet consumers worldwide in 2013. From products and services to cash to information, it's all there for the taking on the Internet.

It's also less risky to steal online. Rather than rob a bank in person, the Internet makes it possible to rob people remotely and almost anonymously. Rather than steal a CD at a local record store, you can download the same music for free and almost without risk from the Internet. The potential for anonymity on the Internet cloaks many criminals in legitimate-looking identities, allowing them to place fraudulent orders with online merchants, steal information by intercepting e-mail, or simply shut down e-commerce sites by using software viruses and swarm attacks. The Internet was never designed to be a global marketplace with a billion users, and lacks many basic security features found in older networks such as the telephone system or broadcast television networks. By comparison, the Internet is an open, vulnerable-design network. The actions of cybercriminals are costly for both businesses and consumers, who are then subjected to higher prices and additional security measures. However, the overall security environment is strengthening as business managers and government officials make significant investments in security equipment and business procedures.

The Scope of the Problem

Cybercrime is becoming a more significant problem for both organizations and consumers. Bot networks, DDoS attacks, Trojans, phishing, data theft, identity fraud, credit card fraud, and spyware are just some of the threats that are making daily headlines. Social networks also have had security breaches. But despite the increasing attention being paid to cybercrime, it is difficult to accurately estimate the actual amount of such crime, in part because many companies are hesitant to report it due to the fear of losing the trust of their customers, and because even if crime

is reported, it may be difficult to quantify the actual dollar amount of the loss.

One source of information is a survey conducted by Ponemon Institute of 56 representative U.S. companies in various industries. The 2012 survey found that the average annualized cost of cybercrime for the organizations in the study was $8.9 million per year, representing a 6% increase over 2011, and a 38% increase over 2010. The average cost per attack was around $600,000, an over 40% increase from the previous year. The number of cyberattacks also increased, by over 40%. The most costly cybercrimes were those caused by denial of service, malicious insiders, and Web-based attacks. The most prevalent types of attacks were viruses, worms, and Trojans, experienced by 100% of the companies surveyed, followed by malware (95%), botnets (71%), and Web-based attacks (64%) (Ponemon Institute, 2012).

Reports issued by security product providers, such as Symantec, are another source of data. Symantec issues a semi-annual Internet Security Threat Report, based on 69 million sensors monitoring Internet activity in more than 150 countries. Advances in technology have greatly reduced the entry costs and skills required to enter the cybercrime business. According to Symantec, low-cost and readily available Web attack kits, which enable hackers to create malware without having to write software from scratch, are responsible for more than 60% of all malicious activity. In addition, there has been a surge in polymorphic malware, which enables attackers to generate a unique version of the malware for each victim, making it much more difficult for pattern- matching software used by security firms to detect. Other findings indicate that targeted attacks are increasing (by 40% in 2012); social networks are helping criminals identify individual targets; and mobile platforms and applications are increasingly vulnerable. According to Symantec, mobile malware presented a tangible and significant threat, with a 58% increase in the number of mobile malware families identified compared to 2011 (Symantec, 2013a). However, Symantec does not attempt to quantify actual crimes and/or losses related to these threats.

Online credit card fraud and phishing attacks are perhaps the most high-profile form of e-commerce crimes. Although the average amount of credit card fraud loss experienced by any one individual is typically relatively small, the overall amount is substantial. The research firm CyberSource estimates online credit card fraud in the United States amounted to about $3.5 billion in 2012. Online fraud peaked in 2008 at $4 billion, suggesting that merchants are managing their credit card payment risks much better than in the past (CyberSource, 2013). The overall rate of online credit card fraud is estimated to be about 0.8% of all online card transactions. As a percentage of all e-commerce revenues, credit card fraud is declining as merchants and credit companies expand security systems to prevent the most common types of low-level fraud. But the nature of credit card fraud has changed greatly from the theft of a single

credit card number and efforts to purchase goods at a few sites, to the simultaneous theft of millions of credit card numbers and their distributions to thousands of criminals operating as gangs of thieves. The emergence of identity fraud, described in detail later in this chapter, as a major online/offline type of fraud may well increase markedly the incidence and amount of credit card fraud, since identity fraud often includes the use of stolen credit card information and the creation of phony credit card accounts.

The Underground Economy Marketplace: The Value of Stolen Information

Criminals who steal information on the Internet do not always use this information themselves, but instead derive value by selling the information to others on so-called underground economy servers. For example, in 2013, Vladislav Horohorin (alias "BadB") was sentenced to over 7 years in federal prison for using online criminal forums to sell stolen credit and debit card information (referred to as "dumps"). At the time of his arrest, Horohorin possessed over 2.5 million stolen credit and debit card numbers. There are several thousand known underground economy servers around the world that sell stolen information (about half of these are in the United States). **Table 2** lists some recently observed prices, which typically vary depending on the quantity being purchased. Experts believe the cost of stolen information has fallen as the tools of harvesting have increased the supply. On the demand side, the same efficiencies and opportunities provided by new technology have increased the number of people who want to use stolen information. It's a robust marketplace.

Table 2 The Cyber Black Market for Stolen Data

Credit card	$2–$90
A full identity (U.S. bank account, credit card, date of birth, social security, etc.)	$3–$20
Bank account	$80–$700
Online accounts (PayPal, eBay, Facebook, Twitter, etc)	$10–$1500
E-mail accounts	$5–$12
Botnet rental	$15
A single compromised computer	$6–$20
Social security number	$5–$7
Attack toolkits	$120 per month
1,000 fake Instagram "followers"	$15

SOURCES: Based on data from Finkle, 2013; PandaSecurity, 2012; Danchev, 2011; Symantec, Inc., 2011, 2010.

Finding these servers is difficult for the average user (and for law enforcement agencies), and you need to be vetted by other criminals before gaining access. This vetting process takes place through e-mail exchanges of information, money, and reputation. Criminals have fairly good, personalized security!

Not every cybercriminal is necessarily after money. In some cases, such criminals aim to just deface, vandalize, and/or disrupt a Web site, rather than actually steal goods or services. The cost of such an attack includes not only the time and effort to make repairs to the site but also damage done to the site's reputation and image, as well as revenues lost as a result of the attack. Ponemon Institute estimates that the average loss to corporations for a breach of data security in 2012 was $5.4 million (Ponemon Institute, 2013).

So, what can we can conclude about the overall size of cybercrime? Cybercrime against e-commerce sites is dynamic and changing all the time, with new risks appearing often. The amount of losses to businesses appears to be significant but stable, and may represent a declining percentage of overall sales because firms have invested in security measures to protect against the simplest crimes. Individuals face new risks of fraud, many of which (unlike credit cards where federal law limits the loss to $50 for individuals) involve substantial uninsured losses involving debit cards and bank accounts. The managers of e-commerce sites must prepare for an ever-changing variety of criminal assaults, and keep current in the latest security techniques.

What is Good E-commerce Security?

What is a secure commercial transaction? Anytime you go into a marketplace you take risks, including the loss of privacy (information about what you purchased). Your prime risk as a consumer is that you do not get what you paid for. As a merchant in the market, your risk is that you don't get paid for what you sell. Thieves take merchandise and then either walk off without paying anything, or pay you with a fraudulent instrument, stolen credit card, or forged currency.

E-commerce merchants and consumers face many of the same risks as participants in traditional commerce, albeit in a new digital environment. Theft is theft, regardless of whether it is digital theft or traditional theft. Burglary, breaking and entering, embezzlement, trespass, malicious destruction, vandalism—all crimes in a traditional commercial environment—are also present in e-commerce. However, reducing risks in e-commerce is a complex process that involves new technologies, organizational policies and procedures, and new laws and industry standards that empower law enforcement officials to investigate and prosecute offenders. **Figure 1** illustrates the multi-layered nature of e-commerce security.

To achieve the highest degree of security possible, new technologies are available and should be used. But these technologies by

themselves do not solve the problem. Organizational policies and procedures are required to ensure the technologies are not subverted. Finally, industry standards and government laws are required to enforce payment mechanisms, as well as to investigate and prosecute violators of laws designed to protect the transfer of property in commercial transactions.

Figure 1	**THE E-COMMERCE SECURITY ENVIRONMENT**

E-commerce security is multi-layered, and must take into account new technology, policies and procedures, and laws and industry standards

The history of security in commercial transactions teaches that any security system can be broken if enough resources are put against it. Security is not absolute. In addition, perfect security of every item is not needed forever, especially in the information age. There is a time value to information—just as there is to money. Sometimes it is sufficient to protect a message for a few hours, days, or years. Also, because security is costly, we always have to weigh the cost against the potential loss. Finally, we have also learned that security is a chain that breaks most often at the weakest link. Our locks are often much stronger than our management of the keys.

We can conclude then that good e-commerce security requires a set of laws, procedures, policies, and technologies that, to the extent feasible, protect individuals and organizations from unexpected behavior in the e-commerce marketplace.

Dimensions of E-commerce Security

There are **six key dimensions to e-commerce security**: (1) integrity, (2) nonrepudiation, (3) authenticity, (4) confidentiality, (5) privacy, and (6) availability.

Integrity refers to the ability to ensure that information being displayed on a Web site, or transmitted or received over the Internet, has not been altered in any way by an unauthorized party. For example, if an unauthorized person intercepts and changes the contents of an online communication, such as by redirecting a bank wire transfer into a different account, the integrity of the message has been compromised because the communication no longer represents what the original sender intended.

Integrity the ability to ensure that information being displayed on a Web site or transmitted or received over the Internet has not been altered in any way by an unauthorized party

Nonrepudiation refers to the ability to ensure that e-commerce participants do not deny (i.e., repudiate) their online actions. For instance, the availability of free e-mail accounts with alias names makes it easy for a person to post comments or send a message and perhaps later deny doing so. Even when a customer uses a real name and e-mail address, it is easy for that customer to order merchandise online and then later deny doing so. In most cases, because merchants typically do not obtain a physical copy of a signature, the credit card issuer will side with the customer because the merchant has no legally valid proof that the customer ordered the merchandise.

Nonrepudiation the ability to ensure that e-commerce participants do not deny (i.e., repudiate) their online actions

Authenticity refers to the ability to identify the identity of a person or entity with whom you are dealing on the Internet. How does the customer know that the Web site operator is who it claims to be? How can the merchant be assured that the customer is really who she says she is? Someone who claims to be someone he is not is “spoofing” or misrepresenting himself.

Authenticity the ability to identify the identity of a person or entity with whom you are dealing on the Internet

Confidentiality refers to the ability to ensure that messages and data are available only to those who are authorized to view them. Confidentiality is sometimes confused with **privacy**, which refers to the ability to control the use of information a customer provides about himself or herself to an e-commerce merchant.

Confidentiality the ability to ensure that messages and data are available only to those who are authorized to view them

Privacy the ability to control the use of information about oneself

E-commerce merchants have two concerns related to privacy. They must establish internal policies that govern their own use of customer information, and they must protect that information from illegitimate or unauthorized use. For example, if hackers break into an e-commerce site and gain access to credit card or other information, this violates not only the confidentiality of the data, but also the privacy of the individuals who supplied the information.

Availability refers to the ability to ensure that an e-commerce site continues to function as intended.

Availability the ability to ensure that an e-commerce site continues to function as intended

Table 3 **CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY**

DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmitted or received been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

Table 3 *summarizes these dimensions from both the merchants' and customers' perspectives. E-commerce security is designed to protect these six dimensions. When any one of them is compromised, overall security suffers*

The Tension Between Security and Other Values

Can there be too much security? The answer is yes. Contrary to what some may believe, security is not an unmitigated good. Computer security adds overhead and expense to business operations, and also gives criminals new opportunities to hide their intentions and their crimes.

Ease of Use

There are inevitable tensions between security and ease of use. When traditional merchants are so fearful of robbers that they do business in shops locked behind security gates, ordinary customers are discouraged from walking in. The same can be true with respect to e commerce. In general, the more security measures added to an e-commerce site, the more difficult it is to use and the slower the site becomes.

As you will discover reading this chapter, digital security is purchased at the price of slowing down processors and adding significantly to data storage demands on storage devices. Security is a technological and business overhead that can detract from doing business. Too much security can harm profitability, while not enough security can potentially put you out of business.

Public Safety and the Criminal Uses of the Internet

There is also an inevitable tension between the desires of individuals to act anonymously (to hide their identity) and the needs of public officials to maintain public safety that can be threatened by criminals or terrorists. This is not a new problem, or even new to the electronic era. The U.S. government began informal tapping of telegraph wires during the Civil War in the mid-1860s in order to trap conspirators and terrorists, and the first police wiretaps of local telephone systems were in place by the 1890s—20 years after the invention of the phone (Schwartz, 2001). No nation-state has ever permitted a technological haven to exist where criminals can plan crimes or threaten the nation-state without fear of official surveillance or investigation. In this sense, the Internet is no different from any other communication system. Drug cartels make extensive use of voice, fax, the Internet, and encrypted e-mail; a number of large international organized crime groups steal information from commercial Web sites and resell it to other criminals who use it for financial fraud. Over the years, the U.S. government has successfully pursued various “carding forums” (Web sites that facilitate the sale of stolen credit card and debit card numbers), such as Shadowcrew, Carderplanet, and Cardersmarket resulting in the arrest and prosecution of a number of their members and the closing of the sites. However, other criminal organizations have emerged to take their place.

Terrorists are also fond users of the Internet and have been for many years. Encrypted files sent via e-mail were used by Ramzi Yousef—a member of the terrorist group responsible for bombing the World Trade

Center in 1993—to hide plans for bombing 11 U.S. airliners. The Internet was also used to plan and coordinate the subsequent attacks on the World Trade Center on September 11, 2001. The case of Umar Farouk Abdulmutallab further illustrates how terrorists make effective use of the Internet to radicalize, recruit, train, and coordinate youthful terrorists. Abdulmutallab allegedly attempted to blow up an American airliner in Detroit on Christmas Day 2009. He was identified, contacted, recruited, and trained, all within six weeks, according to a Pentagon counterterrorism official. In an effort to combat such terrorism, the U.S. government has significantly ramped up its surveillance of communications deliveredvia the Internet over the past several years. The extent of that surveillance has created a major controversy with National Security Administration contractor Edward Snowden's release of classified NSA documents that revealed that the NSA had obtained access to the servers of major Internet companies such as Facebook, Google, Apple, Microsoft, and others, as well as that NSA analysts have been searching e-mail, online chats, and browsing histories of U.S. citizens without any court approval. The proper balance between public safety and privacy in the effort against terrorism has proven to be a very thorny problem for the U.S. government.

Security Threats in the E-commerce Environment

From a technology perspective, there are **three key points** of vulnerability when dealing with e-commerce: (1) the client, (2) the server, and (3) the communications pipeline. **Figure 2** illustrates a typical e-commerce transaction with a consumer using a credit card to purchase a product. **Figure 3** illustrates some of the things that can go wrong at each major vulnerability point in the transaction—over Internet communications channels, at the server level, and at the client level.

In this section, we describe a number of the most common and most damaging forms of security threats to e-commerce consumers and site operators: malicious code, potentially unwanted programs, phishing, hacking and cybervandalism, credit card fraud/theft, spoofing, pharming, and spam (junk) Web sites (link farms), identity fraud, Denial of Service (DoS) and DDoS attacks, sniffing, insider attacks, poorly designed server and client software, social network security issues, mobile platform security issues, and finally, cloud security issues.

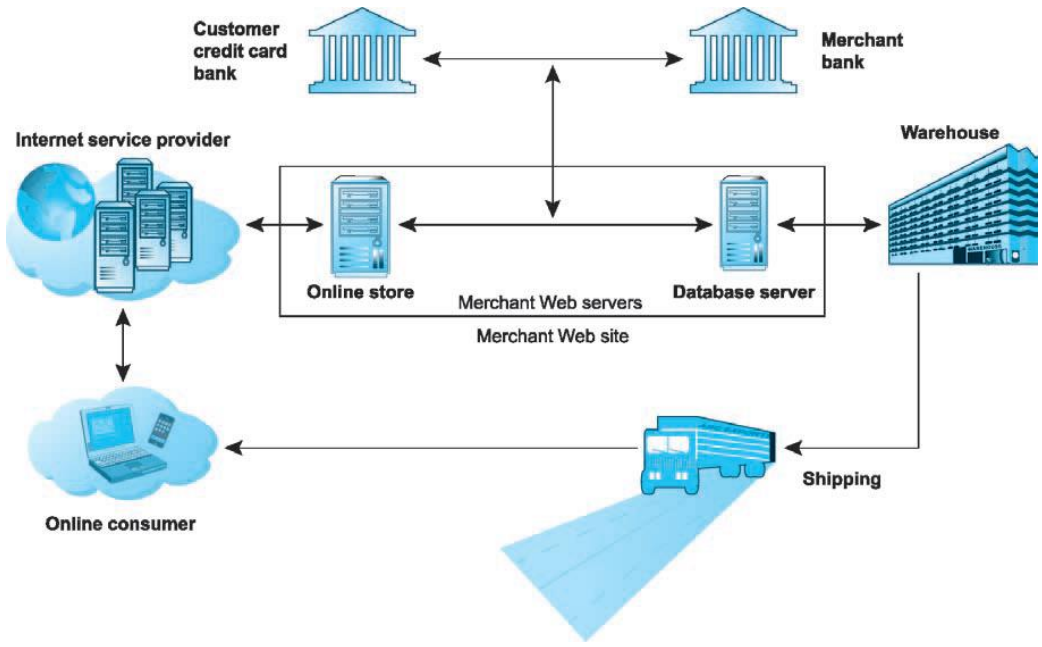
Malicious Code

Malicious code (sometimes referred to as "**malware**") includes a variety of threats such as viruses, worms, Trojan horses, ransomware, and bots. Some malicious code, sometimes referred to as an exploit, is designed to take advantage of software vulnerabilities in a computer's operating system, Web browser, applications, or other software components. For example, Microsoft reported that the Blackhole exploit kit available for purchase or rent from various hacker forums was the most commonly detected exploit family in the second half of 2012. Java exploits,

those that affected Adobe products, and those aimed at the Windows operating system were also quite common. Overall, according to Microsoft, exploits comprised 14.5% of the worldwide malware threats in the fourth quarter of 2012 (Microsoft, 2013). According to Panda Security, 27 million new strains of malware were created in 2012, an average of about 74,000 every day (PandaLabs, 2013). In the past, malicious code was often intended to simply impair computers, and was often authored by a lone hacker, but increasingly the intent is to steal e-mail addresses, logon credentials, personal data, and financial information. Malicious code is also used to develop integrated malware networks that organize the theft of information and money.

malicious code (malware) includes a variety of threats such as viruses, worms, Trojan horses, and bots

Figure 2 A TYPICAL E-COMMERCE TRANSACTION



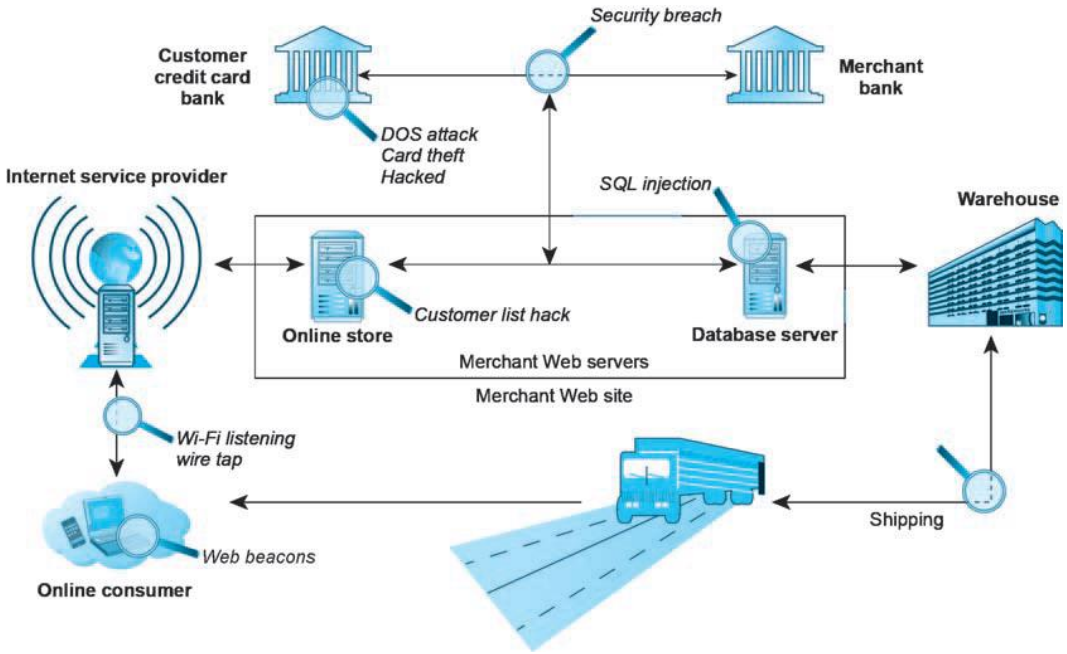
In a typical e-commerce transaction, the customer uses a credit card and the existing credit payment system

One of the latest innovations in malicious code distribution is to embed it in the online advertising chain, including in Google and other ad networks. As the ad network chain becomes more complicated, it becomes more and more difficult for Web sites to vet ads placed on their sites to ensure they are malware-free. Favorite targets are social media sites and large government agencies. In fact, according to Cisco's 2013 Annual Security Report, online advertisements are the second most likely origin of malicious content online, comprising about 16% of total Web

malware encounters (Cisco, 2013). More than 1.5 million malicious ads are served every day, including “drive-by downloads” and fake anti-virus campaigns. A **drive-by download** is malware that comes with a downloaded file that a user intentionally or unintentionally requests. Drive-by is now one of the most common methods of infecting computers. For instance, Web sites as disparate as eWeek.com (a technology site) to MLB.com (Major League Baseball) to AmericanIdol.com have experienced instances where ads placed on their sites either had malicious code embedded or directed clickers to malicious sites. Malicious code embedded in PDF files also is common. Malware authors are also increasingly using links embedded within e-mail instead of the more traditional file attachments to infect computers. The links lead directly to a malicious code download or Web sites that include malicious JavaScript code. Equally important, there has been a major shift in the writers of malware from amateur hackers and adventurers to organized criminal efforts to defraud companies and individuals. In other words, it’s now more about the money than ever before.

drive-by download malware that comes with a downloaded file that a user requests

Figure 3	**VULNERABLE POINTS IN AN E-COMMERCE TRANSACTION**



There are three major vulnerable points in e-commerce transactions: Internet communications, servers, and clients

A **virus** is a computer program that has the ability to replicate or make copies of itself, and spread to other files. In addition to the ability to replicate, most computer viruses deliver a "payload." The payload may be relatively benign, such as the display of a message or image, or it may be highly destructive—destroying files, reformatting the computer's hard drive, or causing programs to run improperly. According to Microsoft, viruses comprised 7.7% of the worldwide malware threats in the fourth quarter of 2011.

Virus a computer program that has the ability to replicate or make copies of itself, and spread to other files

Viruses are often combined with a worm. Instead of just spreading from file to file, a **worm** is designed to spread from computer to computer. A worm does not necessarily need to be activated by a user or program in order for it to replicate itself. The Slammer worm is one of the most notorious. Slammer targeted a known vulnerability in Microsoft's SQL Server database software, infected more than 90% of vulnerable computers worldwide within 10 minutes of its release on the Internet; crashed Bank of America cash machines, especially in the southwestern part of the United States; affected cash registers at supermarkets such as the Publix chain in Atlanta, where staff could not dispense cash to frustrated buyers; and took down most Internet connections in South Korea, causing a dip in the stock market there. The Conficker worm, which first appeared in November 2008, is the most significant worm since Slammer, and reportedly infected 9 to 15 million computers worldwide (Symantec, 2010). In the fourth quarter of 2012, worms accounted for 17.6% of the worldwide malware threats, according to Microsoft.

Worm malware that is designed to spread from computer to computer

Ransomware (scareware) is a type of malware (often a worm) that locks your computer or files to stop you from accessing them. Ransomware will often display a notice that says an authority such as the FBI, Department of Justice, or IRS has detected illegal activity on your computer and demands that you pay a fine in order to unlock the computer and avoid prosecution.

Ransomware (scareware) malware that prevents you from accessing your computer or files and demands that you pay a fine

A **Trojan horse** appears to be benign, but then does something other than expected. The Trojan horse is not itself a virus because it does not replicate, but is often a way for viruses or other malicious code such as bots or rootkits (a program whose aim is to subvert control of the computer's operating system) to be introduced into a computer system.

The term Trojan horse refers to the huge wooden horse in Homer's Iliad that the Greeks gave their opponents, the Trojans—a gift that actually contained hundreds of Greek soldiers. Once the people of Troy let the massive horse within their gates, the soldiers revealed themselves and captured the city. In today's world, a Trojan horse may masquerade as a game, but actually hide a program to steal your passwords and e-mail them to another person. Miscellaneous Trojans and Trojan downloaders and droppers (Trojans that install malicious files to a computer they have infected by either downloading them from a remote computer or from a copy contained in their own code) were found on almost 45% of computers around the world reporting malware threats to Microsoft in the fourth quarter of 2012. According to PandaLabs, Trojans accounted for over 75% of all malware created in 2012, and over 75% of all malware infections. In May 2011, Sony experienced the largest data breach in history when a Trojan horse took over the administrative computers of Sony's Play-Station game center and downloaded personal and credit card information involving 77 million registered users (Wakabayashi, 2011). Zeus is another example of a Trojan horse. Zeus steals information from users by keystroke logging. It is distributed through the Zeus botnet, which has millions of slave computers, and utilizes drive-by downloads and phishing tactics to persuade users to download files with the Trojan horse.

Trojan horse appears to be benign, but then does something other than expected. Often a way for viruses or other malicious code to be introduced into a computer system

A **backdoor** is a feature of viruses, worms, and Trojans that allows an attacker to remotely access a compromised computer. Downadup is an example of a worm with a backdoor, while Virut, a virus that infects various file types, also includes a backdoor that can be used to download and install additional threats. According to GData Security Labs, the number of backdoors increased steadily in 2012 (GData SecurityLabs, 2013).

Backdoor feature of viruses, worms and Trojans that allows an attacker to remotely access a compromised computer

Bots (short for **robots**) are a type of malicious code that can be covertly installed on your computer when attached to the Internet. Around 90% of the world's spam, and 80% of the world's malware, is delivered by botnets. Once installed, the bot responds to external commands sent by the attacker; your computer becomes a "zombie" and is able to be controlled by an external third party (the "bot-herder"). **Botnets** are collections of captured computers used for malicious activities such as sending spam, participating in a DDoS attack, stealing information from computers, and storing network traffic for later analysis. The number of

botnets operating worldwide is not known but is estimated to be well into the thousands. Bots and bot networks are an important threat to the Internet and e-commerce because they can be used to launch very large-scale attacks using many different techniques. In March 2011, federal marshals accompanied members of Microsoft's digital crimes unit in raids designed to disable the Rustock botnet, the leading source of spam in the world with nearly 500,000 slave PCs under the control of its command and control servers located at six Internet hosting services in the United States. Officials confiscated the Rustock control servers at the hosting sites, which claimed they had no idea what the Rustock servers were doing. The actual spam e-mails were sent by the slave PCs under the command of the Rustock servers (Wingfield, 2011). In 2013, Microsoft and the FBI engaged in another aggressive botnet operation, targeting 1,400 of Zeus-derived Citadel botnets, which had been used in 2012 to raid bank accounts at major banks around the world, netting over $500 million (Chirgwin, 2013). However, illustrating the difficulty of the task, new Citadel botnets resurfaced within several months, once again stealing banking credentials, this time from Japanese banks (Muncaster, 2013).

Bot type of malicious code that can be covertly installed on a computer when connected to the Internet. Once installed, the bot responds to external commands sent by the attacker

Botnet collection of captured bot computers

Malicious code is a threat at both the client and the server levels, although servers generally engage in much more thorough anti-virus activities than do consumers. At the server level, malicious code can bring down an entire Web site, preventing millions of people from using the site. Such incidents are infrequent. Much more frequent malicious code attacks occur at the client level, and the damage can quickly spread to millions of other computers connected to the Internet.