QA for Students - Chapter 05

3. Give an example of security breaches as they relate to each of the six dimensions of e-commerce security. For instance, what would be a privacy incident?

https://www.youtube.com/watch?v=6p_q_Xp--Rs

There are **six key dimensions** to e-commerce security:

Remember Tip: **(PAANIC)**

1. *Integrity*—ensures that information displayed on a Web site or sent or received via the Internet has not been altered in any way by an unauthorized party.

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transfer into a different account, the integrity of the message has been compromised/altered because the communication no longer represents what the original sender intended.
- US election, if it did happen, is an example of compromising integrity of US national voting system. Unauthorized Russian intelligence have gained access and altered result numbers by intercepting US national voting system.
- If you are an e-commerce business owner, for example, you would want to make sure that whatever you share on your page is never altered/changed. No one but you and your selected web administrators can change any content without your permission.

2. ***Nonrepudiation***—ensures that e-commerce participants do not deny (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

- In an email message, the sender's and recipient's name must be visible to prevent nonrepudiation.
- We need some accountability in place for anything that is free so that we can fight or prevent nonrepudiation. Every participant in a online transaction must not be able to hide his or her identity.
- My Rogaine Bangladesh business. At this moment it's cash on delivery. But better would be using Bkash to take 50% of payment first and then deliver. Why?

3. ***Authenticity***—verifies an individual's or business's identity. 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.

4. ***Confidentiality***—determines whether information shared online, such as through e-mail communication or an order process, can be viewed by anyone other than the intended recipient. Example:

Encryption is one way to provide confidentiality. What encryption in practical world means is this:

- Auhona wants to encourage Zahid Islam for good result in midterm. She types in “Good work, I am sure you can do even better on final” and sends to Zahid using Facebook messenger. Auhona is thinking my message is safe. But Saif Ali is a good hacker who is trying to intercept the message. Saif Ali succeeds to intercept the message, but he cannot read the message. Instead of seeing the original message, Saif sees “ h7s{ hus8 0p M7*gxhgw” . This is what is called a cipher text. This message has been encrypted here and it’s the confidentiality that has been protected.
- CC card reservation print out. CC number not shown. XXXX-XXXX-7830-XXXX

5.***Privacy***—deals with the use of information shared during an online transaction. Consumers want to limit the extent to which their personal information can be divulged to other organizations, while merchants want to protect such information from falling into the wrong hands.

Confidentiality assures Privacy. You are putting in CC numbers in facebook, because you think that facebook security measurements are confidential enough.

Or you on facebook you are making a private picture album with controlling the visibility. You are assured of the confidentiality facebook promises to provide. That is why you are doing it.

6. ***Availability***—determines whether a Web site is accessible and operational at any given moment.

Example: Can I get access to the site? Having an external hard drive to secure your files. For big companies having an extra server to secure all files. The availability is protected.

TABLE 5.3 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?

6. Name the major points of vulnerability in a typical online transaction. Identify the key 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
3. The communications pipeline.

The most common and most damaging forms of security threats to e-commerce sites include:

• ***Malicious code***—viruses, worms, Trojan horses, ransom ware, and bot networks are a threat to a system's integrity and continued operation, often changing how a system functions or altering documents created on the system.

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.

How it is hidden:

- 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

- 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. Someone creating a program that looks like an mp3, but it actually is not an mp3. When you download it, you do not get an mp3. You try another website. But you just installed malware.

Examples:

Virus:

A **virus** is a computer program that has the ability to replicate or make copies of itself, and spread to other files. According to Microsoft, viruses comprised 7.7% of the worldwide malware threats in the fourth quarter of 2011.

Fact: It needs a human action to replicate and spread in the computer.

Worm:

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.

Fact: It does not need a human action to infect. It self replicates.

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.

Trojan Horse:

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.

Fact: Need human action to infect, does not self replicate

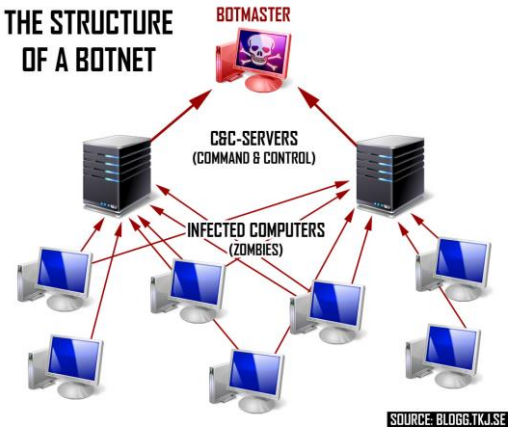
The term *Trojan horse* refers to the huge wooden horse in Homer's *Iliad* that the Greeks gave their opponents, the Trojans—a gift that actually contained hundreds of Greek soldiers. Once the people of Troy let the massive horse within their gates, the soldiers revealed themselves and captured the city. https://www.youtube.com/watch?v=Td1uPq9K--E

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.

Bots: Bots (short for robots) are a type of malicious code that can be covertly (secretly) installed on your computer when attached to the Internet. 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").

Around 90% of the world's spam, and 80% of the world's malware, is delivered by botnets.

Botnets: 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.



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.

https://www.youtube.com/watch?v=afzkoB_lYNk
https://www.youtube.com/watch?v=y8a3QoTg4VQ

• ***Potentially unwanted programs (adware, spyware, etc.)*—**

A kind of security threat that arises when programs are surreptitiously (secretively) installed on your computer or computer network without your consent.

Such programs are increasingly found on social network and user-generated content sites where users are fooled into downloading them. Once installed, these applications are usually exceedingly difficult to remove from the computer.

Adware is typically used to call for pop-up ads to display when the user visits certain sites. While annoying, adware is not typically used for criminal activities.

Adware was found on around 20% of all computers reporting threats to Microsoft in the fourth quarter of 2012.

Spyware, on the other hand, can be used to obtain information such as a user's keystrokes, copies of e-mail and instant messages, and even take screenshots (and thereby capture passwords or other confidential data).

• ***Phishing***:

Any deceptive, online attempt by a third party to obtain confidential information for financial gain.

Phishing attacks typically do not involve malicious code but instead rely on straightforward misrepresentation and fraud, so-called "social engineering" techniques.

Social engineering relies on human curiosity, greed, and gullibility in order to trick people into taking an action that will result in the downloading of malware.

One of the most popular phishing attacks is the e-mail scam letter. The scam begins with an e-mail: a rich former oil minister of Nigeria is seeking a bank account to stash millions of dollars for a short period of time, and requests your bank account number where the money can be deposited. In return, you will receive a million dollars. This type of e-mail scam is popularly known as a "Nigerian letter" scam

Thousands of other phishing attacks use other scams, some pretending to be eBay, PayPal, or Citibank writing to you for "account verification". Click on a link in the e-mail and you will be taken to a Web site controlled by the scammer, and prompted to enter confidential information about your accounts

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

• ***Hacking and cyber vandalism***

Hacking refers to someone intending to gain unauthorized access to a computer system .

Today, hackers have malicious intentions to disrupt, deface, or destroy sites (**cybervandalism**) or to steal personal or corporate information they can use for financial gain (data breach).

A **data breach** occurs whenever organizations lose control over corporate information to outsiders

http://fortune.com/2017/03/09/home-depot-data-breach-banks/
https://www.youtube.com/watch?v=If5EgvU6Zh8
https://www.youtube.com/watch?v=94trvf0wAew

• ***Credit card fraud/theft***

One of the most-feared occurrences and one of the main reasons more consumers do not participate in e-commerce. The most common cause of credit card fraud is a lost or stolen card that is used by someone else, followed by employee theft of customer numbers and stolen identities (criminals applying for credit cards using false identities).

But today, the most frequent cause of stolen cards and card information is the systematic hacking and looting of a corporate server where the information on millions of credit card purchases is stored.

• ***Spoofing***

Spoofing occurs when hackers attempt to hide their true identities or misrepresent themselves by using fake e-mail addresses or masquerading as someone else.

Spoofing involves attempting to hide a true identity by using someone else's e-mail or IP address. For instance, a spoofed e-mail will have a forged sender e-mail address designed to mislead the receiver about who sent the e-mail. IP spoofing involves the creation of TCP/IP packets that use someone else's source IP address, indicating that the packets are coming from a trusted host

• ***Pharming***

Pharming involves redirecting a Web link to an address different from the intended one, with the site masquerading as the intended destination.

Links that are designed to lead to one site can be reset to send users to a totally unrelated site—one that benefits the hacker

• ***Identity fraud***

Identity fraud involves the unauthorized use of another person's personal data, such as social security, driver's license, and/or credit card numbers, as well as user names and passwords, for illegal financial benefit.

Criminals can use such data to obtain loans, purchase merchandise, or obtain other services, such as mobile phone or other utility services.

• Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks

Dos (Denial of Service): Hackers flood a Web site with useless traffic to inundate and overwhelm the network, frequently causing it to shut down and damaging a site's reputation and customer relationships. It involves the use of Bot attacks.

DDos: Distributed Denial of Service (DDoS) attack uses hundreds or even thousands of computers to attack the target network from numerous launch points. DoS and DDoS attacks are threats to a system's operation because they can shut it down indefinitely.

Over 750 separate DDoS attacks were reported to Akamai in 2012, and Akamai anticipates that this number will continue to grow in 2013. During the period from September 2012 through March 2013, many of the attacks were against U.S. banks, as described in the opening case (Akamai, 2013).

Sniffing:

"Sniffs"

A type of eavesdropping (secretly stealing/watching/listening) program that monitors information traveling over a network, enabling hackers to steal proprietary information from anywhere on a network, including e-mail messages, company files, and confidential reports. The threat of sniffing is that confidential or personal information will be made public.

E-mail wiretaps are a variation on the sniffing threat. An e-mail wiretap is a method for recording or journaling e-mail traffic generally at the mail server level from any individual. E-mail wiretaps are used by employers to track employee messages, and by government agencies to survey individuals or groups. E-mail wiretaps can be installed on servers and client computers.

8. Why is adware or spyware considered to be a security threat?

Adware create pop ads to visit unrecognized websites. Security can be compromised if the user is not careful and visit such sites.
Spyware can copy a user's confidential information such as passwords and can cause great harm to a person or business.
That is why both adware and spyware are a definite security threat.

10. Explain some of the modern-day flaws associated with encryption. Why is encryption not as secure today as it was earlier in the century?

Encryption is the process of transforming plain text or data into **cipher text** that cannot be read by anyone other than the sender and the receiver. The purpose of encryption is (a) to secure stored information and (b) to secure information transmission. Encryption can provide four of the six key dimensions of e-commerce security

Example: Saif Ali wants to congratulate Anika Tasnima for good result in midterm. He types in "Good work on Midterm" and sends to Anika using Facebook messenger. Saif is thinking my message is safe. But Farhan is a good hacker who is trying to intercept the message. Farhan succeeds to intercept the message, but he cannot read the message. Instead of seeing " Good Work on midterm", Farhan sees " h7s{ hus8 0p M7*gxhgw" . This message has been encrypted here and it's the confidentiality that has been protected.

• *Message integrity*—provides assurance that the message has not been altered.
• *Nonrepudiation*—prevents the user from denying he or she sent the message.

Instructor: Ahmed Imran Kabir (AIK)

• *Authentication*—provides verification of the identity of the person (or computer)sending the message.
• *Confidentiality*—gives assurance that the message was not read by others.

The possibilities for simple substitution and transposition ciphers are endless, but they all suffer from common flaws.

- First, in the digital age, computers are so powerful and fast that these ancient means of encryption can be broken quickly.
- Second, symmetric key encryption requires that both parties share the same key. In order to share the same key, they must send the key over a presumably *insecure* medium where it could be stolen and used to decipher messages. If the secret key is lost or stolen, the entire encryption system fails.
- Third, in commercial use, where we are not all part of the same team, you would need a secret key for each of the parties with whom you transacted, that is, one key for the bank, another for the department store, and another for the government. In a population of millions of Internet users, thousands of millions of keys would be needed to accommodate all e-commerce customers (estimated at about 156 million in the United States). Clearly this situation would be too unwieldy to work in practice.

13. Is a computer with anti-virus software protected from viruses? Why or why not?

The easiest and least-expensive way to prevent threats to system integrity is to install anti-virus software. Programs by McAfee, Symantec (Norton AntiVirus), and many others provide inexpensive tools to identify and eradicate the most common types of malicious code as they enter a computer, as well as destroy those already lurking on a hard drive. Anti-virus programs can be set up so that e-mail attachments are inspected before you click on them, and the attachments are eliminated if they contain a known virus or worm.

It is not enough, however, to simply install the software once. Since new viruses are developed and released every day, daily routine updates are needed in order to prevent new threats from being loaded. Some premium-level anti-virus software is updated hourly.

So the answers is a computer with an anti-virus software is not protected from viruses, unless the anti virus software is proactive and updated hourly to fight new viruses. Such useful features usually come with a premium level subscription.

14. Identify and discuss the five steps in developing an e-commerce security plan.

The key steps in developing a security plan are:

• ***Perform a risk assessment***

An assessment of the risks and points of vulnerability.

What information is at risk? Is it customer information, proprietary designs, business activities, secret processes, or other internal information, such as price schedules, executive compensation, or payroll? For each

• ***Develop a security policy***

A set of statements prioritizing the information risks, identifying acceptable risk targets, and identifying the mechanisms for achieving these targets.

You will obviously want to start with the information assets that you determined to be the highest priority in your risk assessment. Who generates and controls this information in the firm? What existing security policies are in place to protect the information?

• ***Create an implementation plan***

A plan that determines how you will translate the levels of acceptable risk into a set of tools, technologies, policies, and procedures.

Acceptable Risk: What level of risk are you willing to accept for each of these assets? Are you willing, for instance, to lose customer credit card data once every 10 years?

• ***Create a security team***

The **security organization** educates and trains users, keeps management aware of security threats and breakdowns, and maintains the tools chosen to implement security. the individuals who will be responsible for ongoing maintenance, audits, and improvements.

• ***Perform periodic security audits***

Security audit involves the routine review of access logs (identifying how outsiders are using the site as well as how insiders are accessing the site's assets). A monthly report should be produced that establishes the routine and nonroutine accesses to the systems and identifies unusual patterns of activities.

15. How do biometric devices help improve security? What particular type of security breach do they reduce?

Biometric devices can also be used to verify physical attributes associated with an individual, such as a fingerprint or retina (eye) scan or speech recognition system. (**Biometrics** is the study of measurable biological, or physical, characteristics.) A company could require, for example, that an individual undergo a fingerprint scan before being allowed access to a Web site, or before being allowed to pay for merchandise with a credit card. Biometric devices make it even more difficult for hackers to break into sites or facilities, significantly reducing the opportunity for spoofing.

22. What is Regulation Z, and how does it protect the consumer?

Federal Regulation Z places the risks of the transaction (such as credit card fraud, repudiation of the transaction, or nonpayment) largely on the merchant and credit card issuing bank. Regulation Z limits cardholder liability to $50 for unauthorized transactions that occur before the card issuer is notified. Once a card is reported stolen, consumers are not liable for any subsequent charges