IT352: Information Assurance and Security

End Semester Examination

2020 - 2021

Name: Chinmayi C. Ramakrishna.

Roll No.: 181IT113

Date: 18th April, 2021.

(6.)

Online shopping system or E-commerce is subject to vulnerabilities, threats and attacks

Vulnerability :-

vulnerability is a weakness in the system that can lead to a threat and exploited by an attacker.

1. Insecure Direct Object Reference (IDOR)

This occurs when an application/website takes input from the user, to retrieve some information from the system without adequate authorization. This poses a threat for the system and attacker can exploit.

2. Javascript card skimming (DOM XSS)

DOM Based XSS is a cross site scripting attack wherein the attack payload is executed as a result of modifying the DOM in the victim's browser, so client code runs in an unexpected manner.

3. Javascript card skimming via included third party scripts)

4. Subdomain takeover.

Proces of registering a non existing domain name to gain control over another domain.

5. Denial of Service (DoS) and Distributed Denial of Service (DDoS)

This threatens the availability of online shopping services.

6. Pharming and Server side masquerading.

This leads client / user to a website that is controlled by attacker.

7. Weak authentication and authorization.

example :- if website/ application does not prohibit multiple password login.

8. SQL injection :-

Here, SQL meta characters are inserted in user input so that attacker can execute their queries by back-end database.

9. Price manipulation :- the pricing of products is manipulated.

10. Buffer overflows : To overload the website with large number of bytes.

Threats.

1. Credit card fraud.
2. Fake online stores.
3. Fooling the customers
4. Non delivery of products or delivering the wrong product.
5. Information shared unencrypted

Attacks.

1. Malware and Ransomware attacks :-

Ransomware is a targeted approach to take control of victim's website or system. Malware is a silent killer in the form of bad bots, phishing etc.

2. Point of Sale attacks
   Spreads via keyloggers, RAM scrapers

3. Session hijacking
4. Dictionary :- gets users passwords.
5. Stealing money through bank account access.

⑦

Network Security	Cyber Security	Data Security
Protects data over network	Protects data residing in devices and servers.	Protects both physical data and digital data.
Subset of cyber security	Subset of information security	Also known as information security
Protects anything in the network realm	Protects anything in the cyber realm	Protects tangible and intangible information.
Deals with protection from DoS attacks.	Deals with protection from cyber attacks.	Deals with physical theft, unauthorized access, natural disasters, power supplies, shredders etc

4.2

Strikes against trojans.	Strikes against cyber crimes and cyber frauds.	strikes against disclosure, destruction.
Includes viruses and worms.	Includes phishing and pre texting.	Includes SQL Injection, Cross-Site Scripting
Ensures to ~~transit~~ protect transit data only.	Ensures to protect entire digital data	Ensures to protect any type of data.
Secures data travelling across the network by terminals.	Deals with protection of rest data.	Protects data for confidentiality, integrity and availability

(8)

RSA algorithm is asymmetric cryptography algorithm. Its asymmetric because it works on two keys - public and private.

RSA algorithm is used so that it is difficult for an attacker to factorise a large number.

The algorithm :-

① Public key consists of two numbers where one number is multiplication of two large numbers which are both prime.

② Private key is also derived from the same two prime numbers.

③ Encryption strength depends on key size
eg :- triple the key size → encryption strength increases exponentially.

$p = 17$ $q = 11$ Plaintext = 88

① p and q private keys.
$p = 17$, $q = 11$.

② $n = p \times q = 17 \times 11 = 187$. → public key

③ $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$

④ e selected randomly, such that
$\gcd(E, \phi(n)) = 1 < E < \phi(n)$
$\Rightarrow E = 7$ as $\gcd(7, 160) = 1$.

⑤ Calculate d, such that $d.e \equiv 1 \pmod{\phi(n)}$
$D \times 7 \equiv 1 \mod 160$

6.
4.

D = 23.

public key {187, 7}
private key {187, 23}

⑥ Encryption, c (code text) $= m^e \bmod n$.

$88^7 \bmod 187 = 11$ = Cipher

⑦ Decryption $m = c^d \bmod n$

$11^{23} \bmod 187 = 88$.

Encryption of plain text 88 = (11)

⑨

Data forensics is defined as the process of preservation, identification, extraction and documentation of computer evidence which can be used by court of law.

This helps the forensics team to analyze, inspect, identify and preserve digital evidence present in various electronic devices.

common scenarios include fraud involving using computers, E-commerce, data theft, industrial spionage, employee internet misuse.

7.

damage assessment etc.

Data present in the cellphone can be handled in following ways :-

① Following appropriate protocols.
② Four phases to be followed :- identification, collection, acquisition and preservation.

(10)

Social engineering is the art of manipulating, influencing or deceiving you in order to gain control over your computer system.

Attacker can use phone, email, snail mail etc.

~~Todo~~ Advantages and limitations

① Phishing

Used to notify customers when unusual activity is detected.

Attackers use this technique to fake these messages and attack client/user's accounts.

e.g :- PayPal notification alarming messages.

② Spear Phishing :-

Expert level fake messages.

Mass phishing to distribute ransomware.

③ CEO Fraud.

eg:- A KnowBe4 customer received an email claiming to be CEO of the company.

④ Social media

fake amounts used to explore users.

⑪

E- commerce

Independent freelancers and small businesses or large businesses can benefit from the ability to sell their goods and services online at scale.

example :-

downdable items like templates, e-books, e-news, courses, Software that must be purchased for use. use of cloud services through online platform.

9.

E- Commerce security importance.

① Privacy
Prevents activities that compromises with customers' data.

② Integrity.
Ensure shared information of customers is unaltered.

③ Authentication
Ensure seller and buyer are real.

④ Non repudiation
a legal principle used to instruct players not to deny their actions in a transaction.

Protocols for security.

① Use multi layer security
② Get secure Server Layer (SSL) certificates.
③ Use solid rock firewalls.
④ Anti malware Software.
⑤ Comply with PCI - DSS requirements

(12)

Importance of OS security.

① Maintain system health.
② To have control over the system.
③ Prevent malware and viruses
④ Efficient functioning of programs in system.

10

OS protection methods.

① Authentication
② One Time Password.
③ Patch updates
④ Firewall installation

(13)

Security policy and procedures of organisation defines steps to be followed and guidelines to abide to for system or data protection.

① A password system can be used.
② A system to use only identified or authorised list of people should be allowed.

(14)

Firewall is a network security that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.

Its purpose is to establish a barrier between your internal network and incoming traffic from external sources.

Firewall approaches.

① Packet filtering firewalls
② Next Generation firewalls (NGFW).
③ Proxy firewalls.
④ Network address translation (NAT) firewalls.
⑤ Stateful multilayer inspection (SMLI) firewalls.

(15)

Piracy is an act of illegal reproduction of copyrighted material such as computer programs, books, music and movies.

Piracy can be considered a marine risk or a war risk depending on terms and conditions of war risk insurances.

If it is a war risk, the P&I covers will be subsidiary to the war risk cover.

Protection and indemnity insurance offers protection against risk of piracy.

P&I insurance has been created in response to the need for owner's third part liabilities coverage, liabilities

that were not recoverable under standard hull policies.

(16)

Public key cryptography.

In this method, Alice in order to send Bob a message she first needs to obtain his public key. Alice obtains his public key, encrypts a message using this key and sends it to Bob. Bob is then able to decrypt the message using the secret part of his own key.

Design Issues.

slow due to the enormous amount of computation involved.

Keys must be long so that hackers cannot decrypt (1024 bits at least).

No proof for that any public key is secure.

Not been around long enough to be tested.

Confidentiality :- The digital signing of keys can be ensure ~~to~~ for confidentiality

Key management :- the key should not be given to anyone.

Authentication :- Digital signing on both sides and a proof system can ensure authentication

Issues with proposed strategy:

① If key is not managed properly, the whole security system collapses.
② Digital signature on both sides can be a little complication.
③ Verification and proof system can be tedious and time consuming.

14.