This file contains the frequent questions from previous students. The answers are from the previous students plus from the slides. Yellow highlight means a question to ease navigating thru them.

Prepared by: Mosheer

------------------------------------------------------

**Digital Signatures:**These questions are related to asymmetric Encryption cryptography, Digital Signature, and hash/checksum. Be accurate and clear about the key; don’t write just public key or private key but write: Alice’s public/private key or Bob’s public/private key. If Alice wants send a message to Bob: *(From lecture 7)*

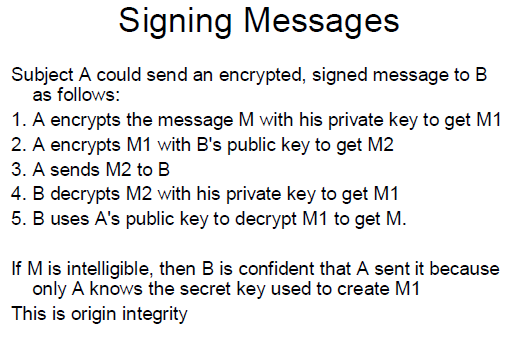
Which key does Alice need to use to digitally sign a document for Bob?

Which key does Alice need to use to encrypt a document for Bob?

Which key does Bob need to use to decrypt a document from Alice?

Is it OK for Alice to share her private key to others? Why? Give brief explanations?

Can I generate hash/checksum of a document using private or public key? Why? Give brief explanation?



------------------------------------------------------------------------------------------------------------------------- **Authentication and Authorization:** Lec#10Explain in short the difference between authentication and authorization?

Authentication is the process of reliably verifying the identity of someone (or something). Another definition: *Authentication* is the binding of an identity to a subject. A subject is a computer entity such as a process. External entities must provide something to confirm their identity. That can be

– Something they know (password)

– Something they have (badge)

– Something they are (fingerprint)

–Where they are (in a locked, guarded room with a computer terminal)

From internet:

* **Authentication** is the process of verifying who you are. When you log on to a PC with a user name and password you are authenticating.
* **Authorization** is the process of verifying that you have access to something. Gaining access to a resource (e.g. directory on a hard disk) because the permissions configured on it allow you access is authorization.

-------------------------------------------------------------------------------------------------------------------------

**Malicious Logic** Lec#12

Write the names any 5 types of the viruses?  
Boot sector infectors, Executable infectors, Multipartite viruses, TSR viruses, Stealth viruses, Encrypted viruses, Polymorphic viruses, Macro viruses

2- What is Hoax? In what ways is like a worm?  
A hoax is an email that contains false information that is meant to cause the recipient to do something like delete a harmless file. Furthermore, the hoax tells the recipient to forward itself to everybody in your address book. A hoax is like a worm since it spreads across a network but a program is not involved, the user is tricked into using the email program to forward the hoax.

3- The textbook gave the following example of a rabbit:  
while true  
 mkdir x (create a directory named x)  
 chdir x (make the newly created directory the current directory)  
done

Would this still be a rabbit if you removed the chdir x? Briefly explain the answer

-------------------------------------------------------------------------------------------------------------------------

**Testing and Buffer overflow** Lec#13

Buffer overflow:

What is the Buffer overflow?  
An example of security vulnerability.   
A buffer overflow, or “buffer overrun” occurs when more data is put into a fixed-length buffer than the buffer can handle. Adjacent memory space becomes overwritten and corrupted. When this occurs – bad things happen. Usually system crashes, but also the opportunity for an attacker to run arbitrary code.

2- How the Java language prevent the Buffer overflow?

Java has array [bounds checking](http://en.wikipedia.org/wiki/Bounds_checking) which will check that data cannot be accessed from area outside of the allocated array. When one tries to access area that is beyond the size of the array, an [ArrayOutOfBounds](http://java.sun.com/javase/6/docs/api/java/lang/ArrayIndexOutOfBoundsException.html) exception will be thrown.

3- Is a Java application which runs on JVM Immune from buffer overflow?  
Java Strings are based on char arrays and Java automatically checks array bounds, However, there can be buffer overflow vulnerabilities in the JVM and JDK. Buffer overflows are only possible in unusual scenarios:

* If you call native code via JNI
* In the JVM itself (usually written in C++)
* The interpreter or JIT compiler does not work correctly (Java bytecode mandated bounds checks)

-------------------------------------------------------------------------------------------------------------------------  
**Auditing and Intrusion Detection**: Lec#14

What are the goals of Intrusion Detection System (at least 3 goals)?  
Detect wide variety of intrusions  
 – Previously known and unknown attacks  
 – Suggests need to learn/adapt to new attacks or changes in behavior  
• Detect intrusions in timely fashion

– May need to be real-time, especially when system responds to intrusion

• Problem: analyzing commands may impact response time of system

– May suffice to report intrusion occurred a few minutes or hours ago

• Present analysis in simple, easy-to-understand format

– Ideally a binary indicator

– Usually more complex, allowing analyst to examine suspected attack

– User interface critical, especially when monitoring many systems

• Be accurate

– Minimize false positives, false negatives

– Minimize time spent verifying attacks, looking for them

What are the three models of the Intrusion detection? Explain each model briefly?

• Anomaly detection: analyzes a set of characteristics of the system, and compares their behavior with expected values; it reports when computed statistics do not match expected statistics

– What is usual, is known

– What is unusual, is bad

• Misuse detection:

– What is bad, is known

– What is not bad, is good

* Determines whether a sequence of instructions being executed is known to violate the site security policy

– Descriptions of known or potential exploits grouped into rule sets

– IDS matches data against rule sets; on success, potential attack found

* Cannot detect attacks unknown to developers of rule sets

– No rules to cover them

• Specification-based detection

– What is good, is known

– What is not good, is bad

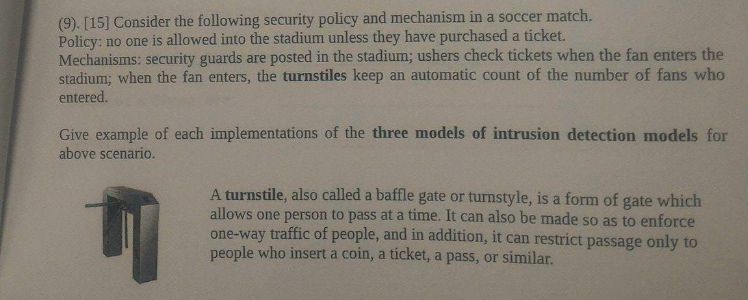
Determines whether execution of sequence of instructions violates specification  
Only need to check programs that alter protection state of system

What are backdoors and how do they differ from Trojan horses? (also in lecture 12)

Trojan horses: Program with an overt purpose (known to user) and a covert purpose (unknown to user). In other words, it is a seemingly innocent program that contains code to perform an unexpected and undesirable function. The intruder must first get the program carrying it to be executed. Could be placed on the Internet, or as an e-mail attachment, or in a directory in the user’s path, etc.  The main characteristic of a Trojan is that first it should be executed by the user.

Backdoor:  
A back door is an undocumented way of accessing a system, bypassing the normal authentication mechanisms. Some back doors are placed in the software by the original programmer and others are placed on systems through a system compromise, such as a virus or worm. Usually, attackers use back doors for easier and continued access to a system after it has been compromised.

A backdoor is a program or a set of related programs that a hacker installs on the victim computer to allow access to the system at a later time. A backdoor’s goal is to remove the evidence of initial entry from the systems log



Maybe you get advantage of this:

That the employee did not violate any security policies regarding access and saving of classified documents. (no misuse)

That the employee only accessed and saved documents that he/she has permission to access. (followed specification)

So the employee is not guilty.  You got full points only if you were able to explain your answer on these lines.

------------------------------------------------------------------------------------------------------------------------- **Network security & DMZ & Data Classes:** Lec#15

Briefly describe the conflict between the principle of economy of mechanism and the principle of psychological acceptability. By conflict I mean that it is sometimes difficult to satisfy both of the principles at the same time. Try to explain it with an example

Principle of Economy of Mechanism

Use small and simple mechanisms wherever possible. Simpler means less can go wrong and when errors occur, they are easier to understand, validate and fix

Principle of Psychological Acceptability:

Security mechanism should not make the resource difficult to access. In other words, don't make a security feature too hard (or too annoying) or else user's will avoid it.

What is the difference?

**DMZ:**

What is DMZ?   
Portion of network separating purely internal network from external network

– Allows control of accesses to some trusted systems inside the corporate perimeter  
– If DMZ systems breached, internal systems still safe  
– Can perform different types of checks at boundary between internal and DMZ networks and between DMZ and Internet network

List the four DMZ servers and briefly describe their primary function and responsibilities in Drib Network?

DMZ Mail Server

• Performs address, content checking on *all* email

• Goal is to hide internal information from outside, but be transparent to inside

• Receives email from Internet, forwards it to internal network

• Receives email from internal network, forwards it to Internet

DMZ Web Server

In DMZ so external customers can access it without going onto internal network

• Accepts, services requests from Internet

• Never contacts servers or information sources in the internal network

DMZ DNS Server

• Supplies DNS information for some hosts to DMZ:

– DMZ mail, web, log hosts

– Internal trusted administrative host

– Inner firewall

– Outer firewall

DMZ Log Server

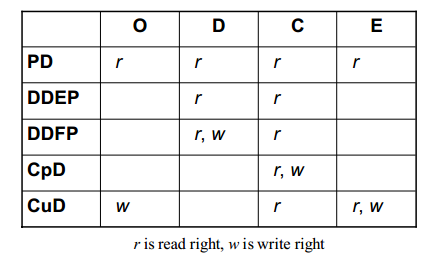
• DMZ systems all log information: Useful in case of problems or attempted attacks

Briefly explain how the principle of least privilege has been followed by each server in the DMZ?

Least privileges says that each component should be allocated sufficient privileges to accomplish its specified functions, but no more. Each of the four servers has the minimum amount of knowledge of the network that is needed to perform their function.

Mail: Email sanitized by removing internal network address  
Web: The Web Server identifies itself as "www.drib.org" and uses the IP address of the outside firewall. Do not keep valuable information online; restrict who can see it.  
DNS: only contains entries needed so that systems in the DMZ can talk to each other. Only has IP addresses needed by machines in the DMZ.  
Log: The use of write-once media in the log server. (Can't alter it and can only destroy it if they have access to the room containing the log server).  
So DMZ servers know only about the inner firewall's address and the trusted administrative host's address.

Complete the following Drib systems ACM. You need to show how the user classes are accessing the Data classes. Fill with r for read, w for write. Answer:



-------------------------------------------------------------------------------------------------------------------------

**Miscellaneous**:  
Cross site scripting:

What is XSS?  
Cross-site scripting (XSS) is a type of [computer security](https://en.wikipedia.org/wiki/Computer_security) [vulnerability](https://en.wikipedia.org/wiki/Vulnerability_(computer_science)). It refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. It occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Give an example of how XSS could happen and what problem it could cause?

Example:

**print** "<html>"   
**print** "<h1>Most recent comment</h1>"

**print** database.latestComment

**print** "</html>"

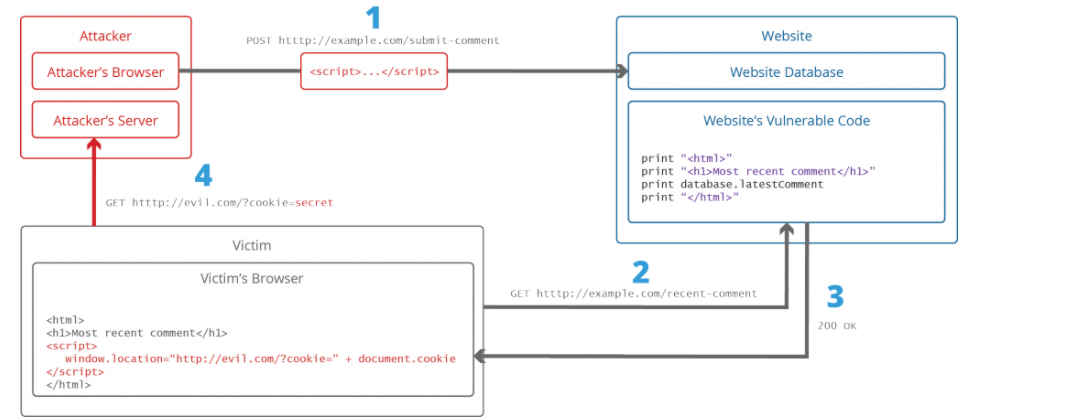
The above script is simply printing out the latest comment from a comments database and printing the contents out to an HTML page, assuming that the comment printed out only consists of text. The above page is vulnerable to XSS because an attacker could submit a comment that contains a malicious payload such as <script>doSomethingEvil();</script>.

Users visiting the web page will get served the following HTML page.

<html> <h1>Most recent comment</h1>

<script>**doSomethingEvil();**</script> </html>

When the page loads in the victim’s browser, the attacker’s malicious script will execute, most often without the user realizing or being able to prevent such an attack.



JavaScript in modern browsers can leverage HTML5 APIs such as accessing a user’s geolocation, webcam, microphone and even the specific files from the user’s file system. So this is real risk.

How to prevent XSS?

There are many types of XSS which requires handling each type. But basically, we prevent by encoding every datum that is given by a user. If data is not given by a user but supplied via the GET parameter, encode these data too. For example, encode these characters: <, >, and “. For example encode < to &lt;

There are many open source libraries that a developer can use to prevent XSS.

-------------------------------------------------------------------------------------------------------------------------  
  
**SCI**:

Explain any 2 of your favorite SCI principles.

Diving principle

Rest and activity