## 

## [3413ICT Network Security](file:///E:\Courses_2003\6216INT_03\6216inthome.html)

### **Workshop 5B**

**Part 1 – Reviewing the lecture notes, answer the following questions**

**Section A:**

1. List and discuss some examples of Web security threats, to explain why Internet & Web are vulnerable.

SQL injections: Attacker can change SQL statements by taking advantage of input fields that are fed into SQL queries that are no sanitized correctly. This allows the attacker to change the behavior of the SQL statements as well as possibly gain access to the site.  
  
JavaScript injections: Changing client side variables by using JavaScript console. Could potentially send data back to server and affect server side privileges.  
  
XSS (cross site scripting): Allows the attacker to inject client side scripts into a web server   
  
DoS (Denial of Service/Distributed Denial of Service (DDos)): An attempt to use up all available resources flooding all available data channels so others are unable to get access to a service. Distributed denial is split amongst more than one computer.

1. What is SSL? Explain the protocols that comprise SSL.

SSL (Secure Socket Layer) is a transport layer security service that was originally developed by Netscape. It has become the Internet standard known as TLS (Transport Layer Security). SSL is composed of two layers of protocols:  
  
SSL Record Protocol: basic security services to various higher-layer protocols (in particular HTTP which can operate on top of SSL)

Handshake protocol:  
Change Cipher Spec Protocol:  
Alert Protocol: warning message

1. Explain SSL connection and SSL session and the differences between them.

SSL Connection: A connection is a transport that provides a suitable type of service. Every connection is associated with one session that is transient.  
SSL Session: Association between a client and server. Sessions are created by the Handshake Protocol and are defined by a set of cryptographic security parameters that are shared amongst multiple connections. Sessions are used to avoid expensive negotiations and maintaining security parameters with a single session.

1. Explain the security services provided by the SSL Record Protocol.

**Confidentiality: Defines a shared secret key that is used for conventional encryption of the SSL payloads.  
Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).**

1. Explain what a digital envelope is, and how a digital envelope is produced.   
   A digital envelope is used to encrypt the contents of dual signature. It is called a envelope because it must it must first be decrypted before the contents can be viewed (i.e an envelop must be opened before the contents can be seen). It is created bt encrypting a session key with a gateway’s public key which produces a digital envelope.
2. Discuss what information is protected by using the scheme of dual signature in SET.

In SET the merchant does not need to know the customer’s credit card number, and the bank does not need to know the details of the customers order. The customer is afforded extra protection in terms of privacy by keeping these two items separate.

1. Compare SET and “3D-secure” mechanisms.

SET: Uses dual signatures and envelopes to send transaction information.  
3-D Secure: Allows you to use a password with you credit card to make online purchases. Redirects you to a central login service. Created in response to circumvent card not present fraud.

**Section B:**

1. List and explain three classes of intruders.

**Masquerader: Unauthorized intruder.  
Misfeasor: Legitimate user making unauthorized attempts to access data, programs, resources ,etc.  
Clandestine User: Out/Insider seizing root privileges**

1. Explain the two useful techniques for password file protection.

Access control: only select users have access to view or modify sensitive files  
One way function: Storing hash values instead of the actual password. Comparing the results of entered password with the stored hashed value will verify if the password is correct or not.

1. On what fundamental assumption do intrusion detection systems work?

IDS operate on the assumption that an intruder behaves differently from a legitimate user.

1. List and explain some benefits of intrusion detection, as a second line of defence for security.

* By detecting intrusions, we can
  + block an intrusion, if it is detected quickly
  + have a deterrent, so reducing or preventing intrusions
  + collect information to improve intrusion prevention facility

1. Explain the two commonly used approaches to intrusion detection.

**Statistical intrusion detection: Analysing and comparing user behaviours of legitimate users over a period of time to determine whether the behaviour is legitimate or not.  
-Threshold detection:** **defining thresholds, independent of user, for the frequency of occurrence of various events  
-Profile Based:** **Developing a profile of past behavior of users, detecting significant deviations from this (Profile is usually multi-parameter)   
  
Rule based detection:  
Defining a set of rules that can be used to decide that a given behavior is that of an intruder  
-Anomaly detection: rules are developed to detect deviation from previous usage patterns  
-Penetration identification:** **an expert system approach that searches for suspicious behavior**

1. List and explain some metrics for behaviour measurement used by profile-based intrusion detection.   
     
   Counter:  
   Examples include: the *number of logins* by a single user during an interval of time, the *number of times a command is executed* during a single user session, and the *number of password failures* during an interval of time  
     
   Gauge:  
   Examples include: the *number of logical connections* assigned to a user application, and the *number of outgoing messages* queued for a user process   
     
   Interval Timer:  
   The length of time between two related events, e.g., the length of time between successive logins  
     
   Resource Utilization: Examples include: the number of pages printed during a user session.
2. What is a honeypot?  
   A honeypot is a sandbox designed to attract attackers to target a decoy system in order to study how they launch an attack. This is useful in gaining data about the attack in order to secure the real system after examining what techniques were used during the attack.

1. What is “salt” in the context of UNIX password management? How does it increase security for password authentication?

A salt is fed into a hash function with a password. The result is stored and compared when authorizing passwords. If a user get access to the password list it requires them not only to guess the correct password but the correct salt as well which is difficult to do.

**Part 2 – Challenge Exercises**

**Exercise 1:**

Review the procedures for dual signature generation and verification.

**Dual signature generation:** The cardholder, say, C, creates two message digests, message digest for the *order information* (OI) and message digest for the *payment information* (PI), making use of a hash function, H, based on secure hash algorithm, that is,

* OIMD = H(OI)
* PIMD = H(PI)

where OIMD denotes the message digest for the order information, and PIMD stands for the message digest for the payment information.

Two message digests are then concatenated, H(PI) || H(OI); and then the hash of the concatenated message digests is taken, that is, H(H(PI) || H(OI)).

Finally, the cardholder C encrypts the hash value with his/her private key, *KRc,* creating the dual signature as:

DS = E( *KRc,* H(H(PI) || H(OI)) ).

The cardholder sends the following two messages to the merchants: One of them (which is for the merchant) consists of:

* OI
* PIMD, and
* DS.

Another one (which is for the bank) is the ciphertext of:

* PI
* OIMD, and
* DS

that have been encrypted by a session key, *Ks.* The session key *Ks* is encrypted by using the bank’s public key; and the encrypted session key is to be forwarded to the bank along with the information above.

After receiving the two messages, the merchant will forward the second message and the encrypted session key to the bank, and verify the dual signature using the first message.

**Dual signature verification by the merchant:** Using OI, PIMD and DS, the merchant operates the following: First computes H(OI). The PIMD and H(OI) are then concatenated, PIMD || H(OI). Next, the merchant computes the hash code

H( PIMD || H(OI)).

Then the merchant decrypts DS, using the public key of the cardholder, *KUc*,

D(*KUc*, DS).

Finally, the merchant compares the following two values

H(PIMD || H(OI)) and D(*KUc*, DS).

If they are equal, the dual signature is valid.

Answer the following questions:

1. The cardholder actually sends both the message for the merchant and the message for the bank to the merchant. Explain how the dual signature technique can prevent the merchant from reading the payment information and obtaining the credit information (such as card number and account detail).

The merchant only receives a hash of the payment information. The hash alone isn’t enough to reverse and get card information or order information.

1. For the merchant to verify the dual signature, why does the following equality H(PIMD || H(OI)) = D(*KUc*, DS) show the validness of the dual signature?   
     
   The decryption process will reveal the session key, which can be used to decrypt the CONCATENATED hash of the order information and the purchase information. If the hashes are the same the dual signature is valid.
2. Given the cipher text of the following information: PI, OIMD, and DS. Explain how the bank verifies the dual signature.

* Bank computes H(PI), and then H(PI) || OIMD
* Bank then computes H( H(PI) || OIMD)
* Bank decrypts DS, that is, computes
* D(*KUc*, DS)
* Bank compares the following two values. If they are equal, the signature is valid

H(H(PI) || OIMD) and D(*KUc*, DS)

**Exercise 2:**

Identify one of the recent articles on password selection/ management techniques and summarise it in your own words (100 – 150 words). You should be able to discuss your findings in the class.

Correct password selection can be viewed as art. Select the wrong password, and someone could have access to your e-mail account if you don’t have 2 step-verification on your e-mail account. Choose one that is overly complicated, you are quite likely to forget it. The trick for selecting a good password is to select one that does not include any bad criteria and contains good criteria.   
  
Criteria for a bad password:  
-Short in length 6 or less characters  
-Dictionary words  
-Contains a predictable stream of characters (123, abc, qwerty)  
-Name of a relative, someone you know, loved one  
-1337 substitution

Criteria for a good password:

- Come up with a good secret substitution: for example for every vowel replace it with a period.  
- Every letter o is replaced with 2 zeros 00  
  
Many websites do not contain 2 step verification logins, so it’s important to pick strong passwords.  
could be quite disastrous if someone does gain access to an e-mail account. Blackmailing, lead to other account password resets.