Security and Password

Introduction

Security is the state of being free from danger or threat. There are 3 main types of security in computing:

**1. Physical Security:** Using physical barriers to prevent unauthorized access to data (like locking the door of the server room).  
**2. Software Security:** Fixing flaws in your application that could grant attackers unwanted levels of access to your systems.  
**3. Network Security:** Security of networked services (websites, [databases](https://lms.clarusway.com/mod/lesson/view.php?id=995), etc).

The computer is like a castle with walls, inside and outside are very different. The bad guy cannot just access the bytes outside the computer but inside the computer at will. The bad guy needs to work at it.

A couple of bad guy strategies:

* obtain a password allowing access
* trick the computer into running bad guy code

| **https://docs.google.com/uc?id=11EtqcaHoaZSZdleIMbyyXeoTQkyA5RBZ** |
| --- |
| *Bad guy will want to access your castle from open doors (network)* |

Access Control

Access Control is a framework for controlling who has access to what resources on a system. There are many ways to implement Access Control, but the three basic principles of Access Control are **Identification**, **Authentication**, and **Authorization**.

* **Identification:** Who is this person?
* **Authentication:** Is this the person who he claims to be?
* **Authorization:** Is this person allowed to perform this action?

Passwords

Passwords are the de facto form of Authentication for computers, but they aren’t a perfect solution. Passwords are hard to remember and surprisingly easy for computers to guess.

There are some problems for passwords:

* People use same passwords for different accounts,
* People use simple passwords that are easy to guess,
* Passwords are hard to remember.

Solutions to these problems:

* Using a password manager,
* Changing passwords regularly,
* Using multi-step authentication.

## Cyber Attacks

### Phishing

**Phishing** is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website that matches the look and feel of the legitimate site.

| **https://docs.google.com/uc?id=1h81YXIuk_5nljcPCklSONNbWh_Hgjbj2** |
| --- |
| Phishing web site acting like Paypal's official website |

Phishing is an example of social engineering techniques being used to deceive users. Users are often lured by communications purporting to be from trusted parties such as social web sites, auction sites, banks, online payment processors or IT administrators. The above screenshot belongs to a phishing site, not the genuine PayPal site. If you type your username and password at this fake site, your credentials will be sent to the bad guy and then he will gain access to your account.

Q: Explain Phishing and how to prevent it.  
A: Phishing is a Cyberattack in which a hacker disguises as a trustworthy person or business and attempt to steal sensitive financial or personal information through fraudulent email or instant message.  
You can prevent Phishing attacks by using the following practices:

Q: Explain Phishing and how to prevent it.  
A: Phishing is a Cyberattack in which a hacker disguises as a trustworthy person or business and attempt to steal sensitive financial or personal information through fraudulent email or instant message.  
You can prevent Phishing attacks by using the following practices:

* Don’t enter sensitive information in the webpages that you don’t trust
* Verify the site’s security
* Use Firewalls
* Use AntiVirus Software that has Internet Security
* Use Anti-Phishing Toolbar

 - Interview Q&A

* Don’t enter sensitive information in the webpages that you don’t trust
* Verify the site’s security
* Use Firewalls
* Use AntiVirus Software that has Internet Security
* Use Anti-Phishing Toolbar

 - Interview Q&A

### Malware

The term **malware** is a contraction of **mal**icious soft**ware**. Put simply, malware is any piece of software that was written with the intent of damaging devices, stealing data, and generally causing a mess. Viruses, trojans, spyware, and ransomware are among the different kinds of malware.

A **computer virus** is a type of malicious code or program written to alter the way a computer operates and is designed to **spread** from one computer to another.

A Trojan horse or **Trojan** is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems.

**Spyware** is a type of malware that's hard to detect. It collects information about your surfing habits, browsing history, or personal information (such as credit card numbers), and often uses the Internet to pass this information along to third parties without you knowing.

**Ransomware Trojan** is a type of cyberware that is designed to extort money from a victim. Often, ransomware will demand a payment in order to undo changes that the Trojan virus has made to the victim’s computer.

| **https://docs.google.com/uc?id=1xX--vKdQJosSf4pgrhqQ1hiMH0vtF22n** |
| --- |
| Bad guy |

Q: Define Spyware.  
A: Spyware is a malware that aims to steal data about the organization or person. This malware can damage the organization's computer system.

 - Interview Q&A

Q: Define Spyware.  
A: Spyware is a malware that aims to steal data about the organization or person. This malware can damage the organization's computer system.

 - Interview Q&A

### SQL Injection-XSS-CSRF

**SQL injection** is a code injection technique that might destroy your database. This type of attack usually occurs when you ask a user for input, like their user-name/user-id, and instead of a name/id, the user (bad guy) gives you an SQL statement that you will unknowingly run on your database.

**Cross-Site Scripting (XSS)** attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end-user.

**Cross-site Request Forgery (CSRF)** is a very common vulnerability. It's an attack that forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

| **https://docs.google.com/uc?id=1q2lyqohBacXZWaKmahdQio-Xo7CCc-YI** |
| --- |
| Injecting SQL query to web site form |

Q: Explain SQL Injection and how to prevent it.  
A: SQL Injection (SQLi) is a code injection attack where an attacker manipulates the data being sent to the server to execute malicious SQL statements to control a web application’s database server, thereby accessing, modifying and deleting unauthorized data. This attack is mainly used to take over database [servers](https://lms.clarusway.com/mod/lesson/view.php?id=1015).  
You can prevent SQL Injection attacks by using the following practices:

* Use prepared statements
* Use Stored Procedures
* Validate user input

 - Interview Q&A

Q: Explain SQL Injection and how to prevent it.  
A: SQL Injection (SQLi) is a code injection attack where an attacker manipulates the data being sent to the server to execute malicious SQL statements to control a web application’s database server, thereby accessing, modifying and deleting unauthorized data. This attack is mainly used to take over database [servers](https://lms.clarusway.com/mod/lesson/view.php?id=1015).  
You can prevent SQL Injection attacks by using the following practices:

* Use prepared statements
* Use Stored Procedures
* Validate user input

 - Interview Q&A

## Encryption/Decryption

### Encryption

**Encryption** is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting **plaintext** (the original bytes (text, image, etc.)) to **ciphertext** (encrypted text). In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of an **encryption key** that is a set of mathematical values known only by the sender and the recipient of the encrypted message know.



Q: What is ciphertext?  
A: When the message is encrypted into a state which is totally incomprehensible and indecipherable, this is known as the ciphertext. So, to illustrate all of this, with the previous example, when the sending party creates the written message of “I LOVE YOU”, this is the plaintext or the cleartext. Once this message is encrypted into the format of “UYO I VEOL” and while it is in transit, it becomes known as the ciphertext. Then, once the receiving party gets this ciphertext and then decrypts it into a comprehensible and understandable form of “I LOVE YOU,” this message then becomes the plaintext or the cleartext again.

 - Interview Q&A

Q: What is plaintext or cleartext?  
A: The decrypted message, when it is returned back into its plain or original state of context which is comprehensible and decipherable, is also known as cleartext or plaintext.

 - Interview Q&A

Q: What is ciphertext?  
A: When the message is encrypted into a state which is totally incomprehensible and indecipherable, this is known as the ciphertext. So, to illustrate all of this, with the previous example, when the sending party creates the written message of “I LOVE YOU”, this is the plaintext or the cleartext. Once this message is encrypted into the format of “UYO I VEOL” and while it is in transit, it becomes known as the ciphertext. Then, once the receiving party gets this ciphertext and then decrypts it into a comprehensible and understandable form of “I LOVE YOU,” this message then becomes the plaintext or the cleartext again.

 - Interview Q&A

Q: What is ciphertext?  
A: When the message is encrypted into a state which is totally incomprehensible and indecipherable, this is known as the ciphertext. So, to illustrate all of this, with the previous example, when the sending party creates the written message of “I LOVE YOU”, this is the plaintext or the cleartext. Once this message is encrypted into the format of “UYO I VEOL” and while it is in transit, it becomes known as the ciphertext. Then, once the receiving party gets this ciphertext and then decrypts it into a comprehensible and understandable form of “I LOVE YOU,” this message then becomes the plaintext or the cleartext again.

 - Interview Q&A

Decryption

**Decryption** is a process of converting encoded/encrypted data (ciphertext) in a form that is readable and understood by a human or a computer. This method is performed by un-encrypting the text manually or by using keys that were used to encrypt the original data.

| **https://docs.google.com/uc?id=1TWp9M2gU1jPPvrhgPWC10hbSc9OMsfYK** |
| --- |
| *Decryption example* |

Q: What exactly are encryption and decryption?  
A: The terms “scrambling” and “descrambling” are commonly known as “encryption” and “decryption.”  
For example: when the written message “I LOVE YOU” is scrambled by the sending party, it becomes what is known as the “encrypted message.” This means that the written message has been disguised in such a manner that it would be totally meaningless, or in the terms of cryptography, it would be undecipherable.  
Encryption can also be described as the conversion of information from a readable state to apparent nonsense. When the receiving party receives this encrypted written message, it must be unscrambled into an understandable and comprehensible state of the context. This process of unscrambling is also known as decryption

 - Interview Q&A

Q: What exactly are encryption and decryption?  
A: The terms “scrambling” and “descrambling” are commonly known as “encryption” and “decryption.”  
For example: when the written message “I LOVE YOU” is scrambled by the sending party, it becomes what is known as the “encrypted message.” This means that the written message has been disguised in such a manner that it would be totally meaningless, or in the terms of cryptography, it would be undecipherable.  
Encryption can also be described as the conversion of information from a readable state to apparent nonsense. When the receiving party receives this encrypted written message, it must be unscrambled into an understandable and comprehensible state of the context. This process of unscrambling is also known as decryption

 - Interview Q&A

Hashing

Hashing is the process of converting a given key to another value. A **hash function** is used to generate the new value according to a mathematical algorithm. The result of a hash function is known as a **hash value** or simply, a **hash**.

Hashing is also used in data encryption (we will learn in the following lessons). Passwords can be stored in the form of their hashes so that even if a database is breached, plaintext passwords are not accessible. **MD5**, **SHA-1** and **SHA-2** are popular cryptographic hashes.

| **https://docs.google.com/uc?id=1SBmIKZN8PzETVCKBWcq4HSpSxhDqI2C7** |
| --- |
| *Hashing Example* |

Q: What is the hashing function?  
A: The hashing function is a one-way mathematical function. This means that it can be used to encode data, but it cannot decode data. Its primary purpose is not to encrypt the ciphertext; rather, its primary purpose is to prove that the message in the ciphertext has not changed in any way, shape or form. This is also referred to as “message integrity.” If the mathematical function has changed in any way, the message has then changed.

Q: What is the hashing function?  
A: The hashing function is a one-way mathematical function. This means that it can be used to encode data, but it cannot decode data. Its primary purpose is not to encrypt the ciphertext; rather, its primary purpose is to prove that the message in the ciphertext has not changed in any way, shape or form. This is also referred to as “message integrity.” If the mathematical function has changed in any way, the message has then changed.

 - Interview Q&A

 - Interview Q&A

Cryptocurrency

**Cryptocurrency** is an internet-based medium of exchange which uses cryptographical functions to conduct financial transactions. Cryptocurrencies leverage blockchain technology to gain decentralization, transparency, and immutability.

**Blockchain** is the technology that enables the existence of cryptocurrency. **Bitcoin** is the name of the best-known cryptocurrency, the one for which blockchain technology was invented. A cryptocurrency is a medium of exchange, such as the US dollar, but it is digital and uses encryption techniques to control the creation of monetary units and to verify the transfer of funds.

| **https://docs.google.com/uc?id=1t-_RT7tIxMZYDrYPFaxwzDM3hitLDmGA** |
| --- |
| *Cryptocurrency* |

Formun Üstü