

IG CS Topic 5.4-5.5 Digital Currency and Cyber Security

Created by HardyWen

IG CS Topic 5.4-5.5 Digital Currency and Cyber Security

Digital Currency

How they are used

Cryptocurrency

Blockchain

Process of Blockchain

Cyber Security

Brute-force attack

Data interception

DDoS attack

Procedure

Aim

Solution

Hacking

Aim

Solution

Malware

Aim

Solution

Pharming

Aim

Solution

Phishing

Aim

Solution

Social Engineering

Aim

Solution

Digital Currency

- **Digital currency** is a currency that **only exists electronically**
 - they are exchanged digitally using computers
- they are used in credits cards and digital payments (AliPay)

How they are used

- when the data about the payment with the digital currency is sent from one computer to another, it is encrypted using the **HTTPS protocol**
- the payment details can be stored in a **persistent cookie**

Cryptocurrency

- **Cryptocurrency** is a type of digital currency that uses **encryption procedures**
 - for example, the **Bitcoins**

Digital Currency	Cryptocurrency
regulated by a central authority	decentralized and unregulated
needs strong passwords to protect digital wallets, banking apps, credit, debit cards	are secured by encryption
stable and globally accepted	highly volatile, not widely accepted
transactions are only known to the sender, receiver, and the bank	transactions are publicly available on a decentralized ledger

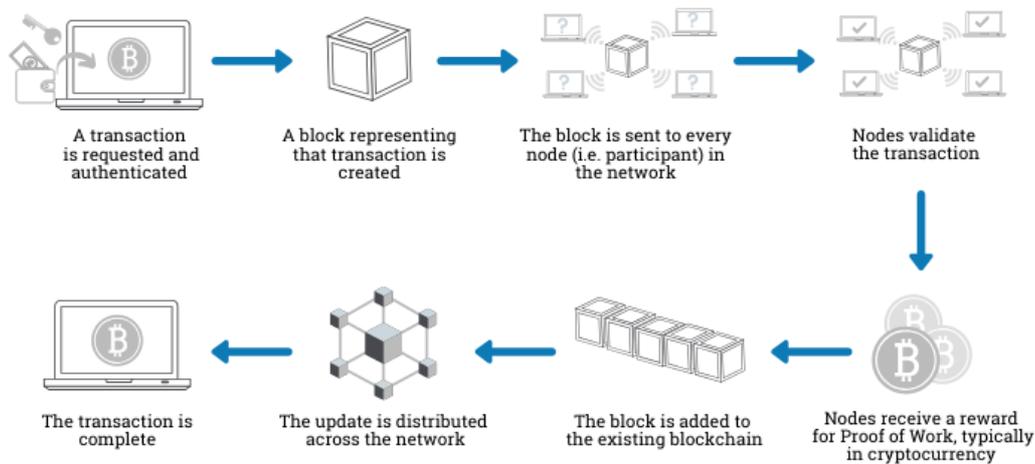
Blockchain

- **Blockchain** is a **digital ledger** that **is a time-stamped series of records that cannot be altered**
 - it is used to maintain **secure** and **decentralized** record of data

Process of Blockchain

1. a transaction is initiated
2. this action creates a **block** that represents that specific transaction or data
3. the **block** is sent to **every computer node** in the network
4. **authorized nodes** verify the transaction and add the block to the existing **blockchain**
5. the verified block is **time-stamped** with **cryptographic hash** and has a reference to the previous block's hash
 - every block in the block chain contains its own hash and its previous block's hash
6. the unit of value moves from the sender's account to the receiver's account. The update is distributed across the network, which finalizes the transaction.
 - once a transaction is completed, it **cannot** be **deleted** or **altered**

How does a transaction get into the blockchain?



© Euromoney Learning 2020

Cyber Security

- You need to describe the process involved, the aim of carrying out, and the solutions to the cybersecurity threats listed below

Brute-force attack

- Most networked terminals rely on a **password** to restrict access and **encryption** to ensure secure communications
 - they are both vulnerable to brute-force attacks
- A brute force attack goes through **every possible combination of a password or encryption key**
 - 暴力试每一个可能的密码看看能不能猜到
- **Aim:** to steal your personal data or to use your account to buy things online
- Can be solved through **Authentication measures**
 1. strong username and password
 2. biometrics
 - fingerprint scanner
 - face id
 - biometrics are **unique** to you so cannot be brutally attacked
 3. two-step verification
 - takes two tasks in authorization (e.g. SMS + password)
 4. limiting times of password inputted

Data interception

- packages containing personal information are transmitted throughout the network to reach their destined receiver
- so, hackers might try to get this private information by **intercepting data packets** as they are transmitted across the network

- they use a **packet sniffer** to examine the data packets
 - the software would report packets that contain useful data
- **Aim:** to steal your personal data for criminal activity such as fraud
- Can be solved through **Data encryption**
 - data is encrypted through the **SSL protocol**
 - secure socket layer
 - SSL encrypts the data, so anyone who intercepts it would just see a piece of meaningless letters

DDoS attack

- the webserver can only handle a limited amount of requests at once, so it may collapse when too many requests are made at once
- so, hackers carry out **Distributed Denial of Service (DDoS attack)**, a type of cyber threat that targets a web server to cause it to crash and prevent access to the webpage that it stores

Procedure

1. a perpetrator will send **malware** to many computers to try and control them
 - the controlled computers are called **bots**
 - if the bots are not being used, they are called as **zombies**
2. when many computers are controlled, they form a **botnet**
3. the perpetrator would ask all the bots in the botnet to **send requests** to a certain web server at the same time
 - the webserver can only deal with a limited number of requests at once, so may crash

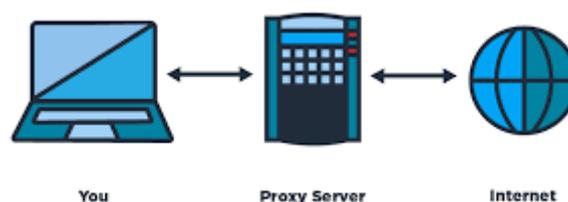
Aim

- to cause the webserver to crash, for revenging purpose or demanding for money

Solution

1. Proxy server

- a server that acts as an **intermediary** between a server and a requestor



- the proxy server examines the requests and decides which to forward to the server
 - so when DDoS occurs that attacks the proxy, the proxy can forward the requests at a slower rate to the webserver, so the server wouldn't be overwhelmed by too many requests at a time
- the proxy server can also **ban** an IP if that IP requests constantly
 - this method is called **catching**

2. Anti-malware

- a type of software that scans a computer or device with the purpose of finding and removing malware
- so your computer won't become a **bot** due to the malware sent by the perpetrator

Hacking

- **Hacking** is the act to **gain unauthorized access to data**
- they are able to hack you through
 1. brute-force attacks
 2. exploiting vulnerabilities
 - such as there may be vulnerabilities linked with the software you've downloaded

Aim

- to steal, corrupt, or leak your data for criminal activity

Solution

1. Firewall

- a cyber security method that is used to **examine incoming and outgoing traffic** from a computer network
- the firewall sets up **rules** for which data to be passed into the computer system

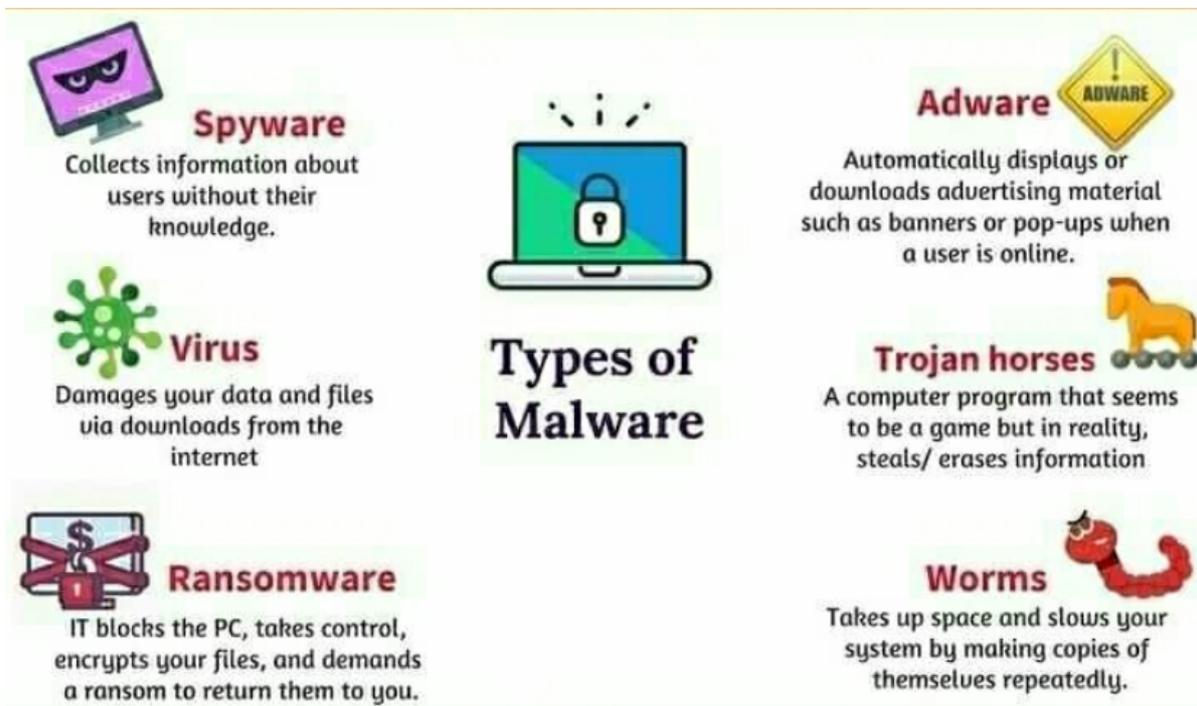
2. Automatic software updates

- so that the software with vulnerabilities will be updated automatically when a safe release is issued, and hence the vulnerabilities would disappear

3. Solutions against brute-force attacks as mentioned above

Malware

- a term used to describe any **malicious software** that is designed to disrupt your computer or data
- Make sure that you remember the different types of malware below



Aim

- to corrupt your data, gain access to your data, or damage your hardware

Solution

1. Anti-malware software

- anti-virus and anti-spyware
- they scan every file on your computer to see if any of them are known to be a virus
 - they compare the file with a given list of known viruses

2. Firewall

- prevent malware from being downloaded into your computer

3. Exercising caution when downloading software and creating a backup of data

Pharming

- Malicious software is downloaded onto your hard drive that will **redirect** you to a **fake page** when you input the genuine URL

Aim

- to get your personal data to commit criminal activity such as stealing your money, identity theft or fraud

Solution

1. Anti-malware software

- to prevent the malicious software from being downloaded

2. Checking the URL attacked to a link

- since the malware will direct you to a fake page, the URL of the webpage wouldn't be the genuine one, so please check the URL

3. Only downloading the data from trusted sources

Phishing

- a type of cyber threat that involves sending the user a **fake email** that is designed to look genuine
 - it will encourage the user to provide their personal data either by clicking a link to a fake website, or by responding to the email

Aim

- to get your personal data

Solution

- **Checking the spelling and tone of communications**
 - the spelling of phishing emails tends to contain errors as if they would harm the copyright if they use the correct spelling
 - many companies would not ask you to provide personal details over responding to an email, and therefore you should check the tone of communications to see whether the email is deemed or is seemed to be sent from an authority

Social Engineering

- **hacking without code**
 - a cyber threat that involves **manipulating** or **deceiving** people into providing confidential personal data
 - 就像冒充客服要你身份证号才能给你退货啥的
 - Phishing & pharming are types of social engineering
 - "social" -> 与人打交道, 欺骗

Aim

- to get data to commit criminal activity, such as stealing your money, hacking into a computer network and identity theft or fraud

Solution

1. Access level

- employees are given a **different level of access** to the data in the company
 - employees will only have access to the data that they use on a daily basis
 - only seniors can access more confidential data
- so when a perpetrator logs into the account which he/she has stolen, he/she can only access a limited amount of data

2. Awareness of how social engineering is conducted