Introduction to Cyber Security

greatlearning
Power Ahead

Introduction to Cyber Security

- What is Cyber Security?
- Key Concept of Cyber Security
- Popular Attacks
- Security goals and Its Implementation
- Design a basic Security System

What is Cyber Security?

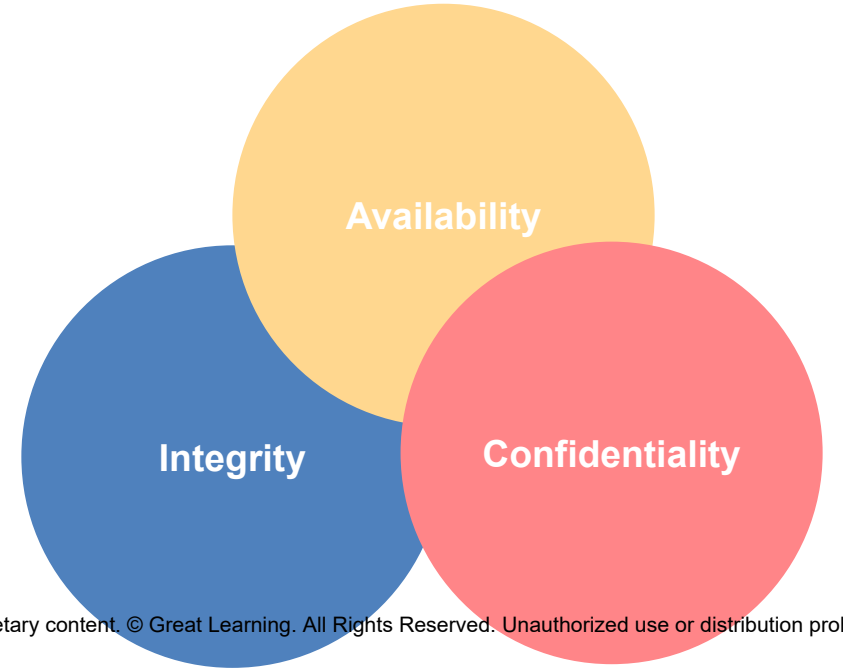
What is Cyber Security?

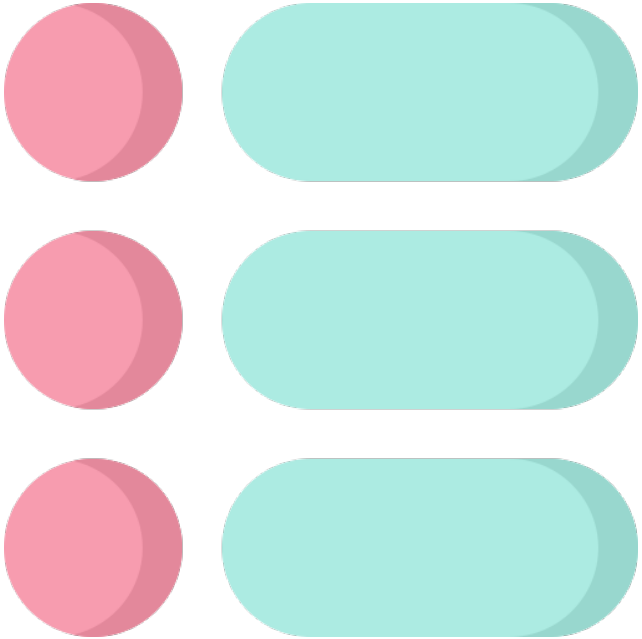
CyberSecurity is the protection of inter-connected systems, including hardware, software and data, from cyber attacks.

Key Concepts of Cyber Security

Key Concepts of Cyber Security

The Cyber Security on a whole is a very broad term but is based on three fundamental concepts known as “The CIA Triad”.

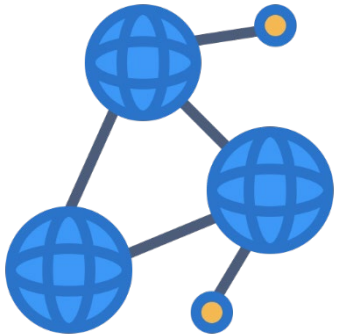




Pre-requisites

Pre-requisites

Basics Computer Skills



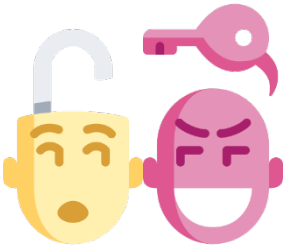
Basics of Networking

Popular Attacks

Popular Attacks

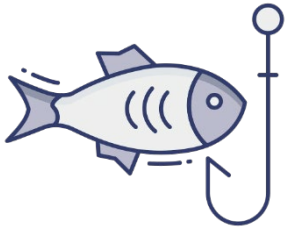
Ransomware

Botnet Attacks



Social Engineering Attacks

Cryptocurrency Hijacking



Phishing

Ransomware

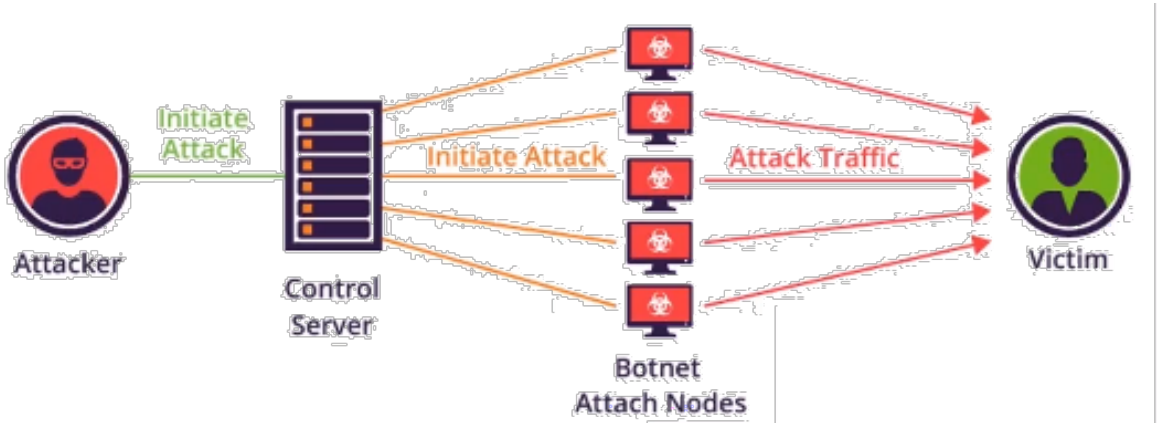
Ransomware

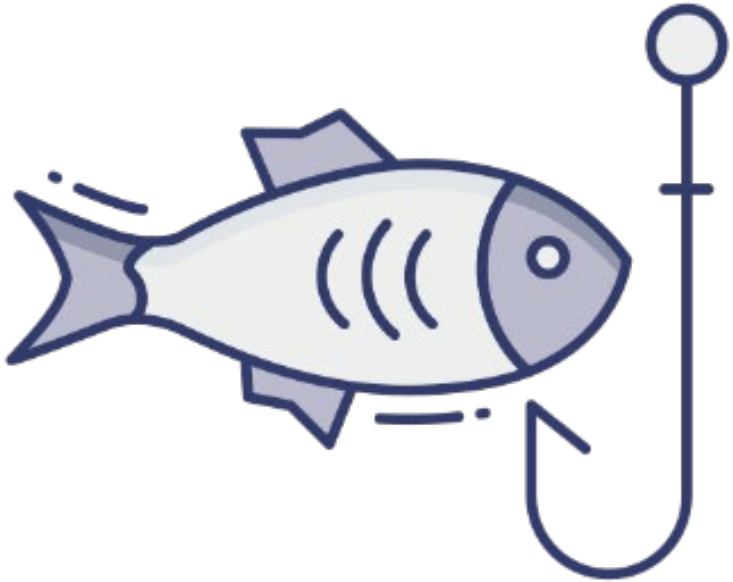
The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cyrptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

Botnet Attacks

Botnet Attacks

Mirai is a malware that turns networked devices running linux into remotely controlled bots that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers.

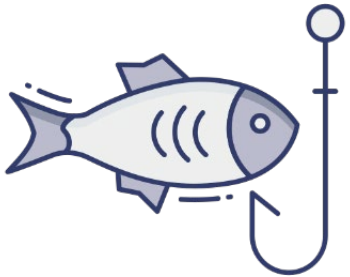




Phishing

Phishing

The Ukrainian Power Grid Attack – The December 2015 Ukrainian power grid attack was a history-making event for a number of reasons. It was the second time that malicious firmware was developed specifically for the purpose of destroying physical machinery – the first being stuxnet , used by U.S. and Israel to shut down Iranian nuclear centrifuges in 2009. But unlike Stuxnet, the Ukrainian malicious firmware attack used email phishing as its originating attack vector.



Security goals and Its Implementation

Security goals and Its Implementation

Authentication: It is the process of giving individuals access to system objects based on their identity.

Authorization: It is the function of specifying access rights/privileges to resources.

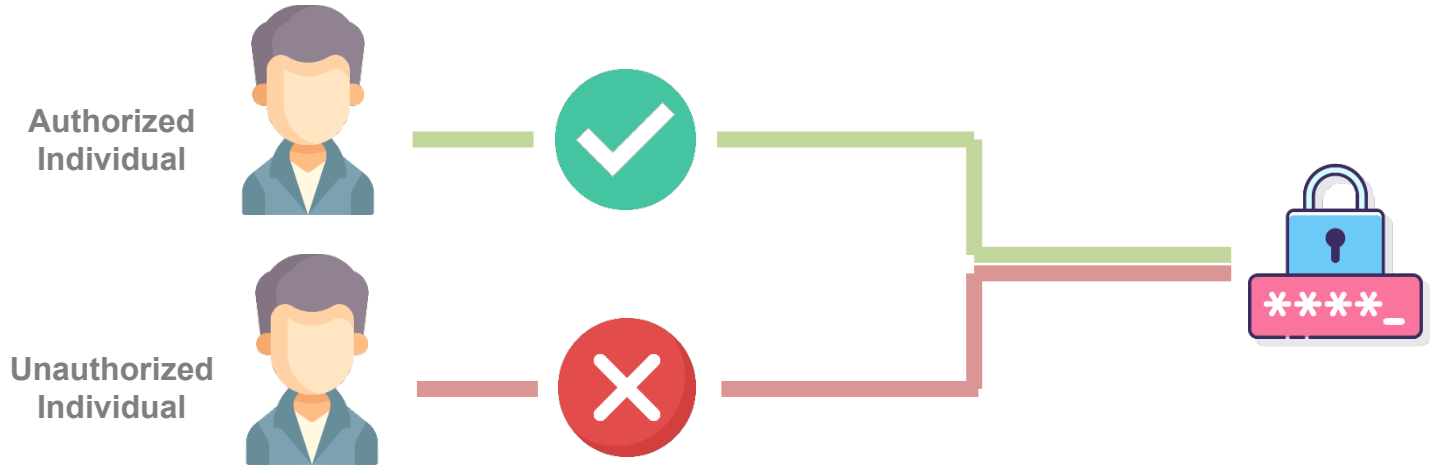
Authentication – Who you are

Authorization – What you can do

Security goals and Its Implementation

Confidentiality: IT refers to protecting information from being accessed by unauthorized parties.

Accountability: It means that every individual who works with a system should have specific responsibilities for information assurance.



Security goals and Its Implementation

Transfer $10 to B

I never requested to transfer to B

Design a Security System

Understanding threats:

- ID & Mitigate Threads
- Threat Modeling

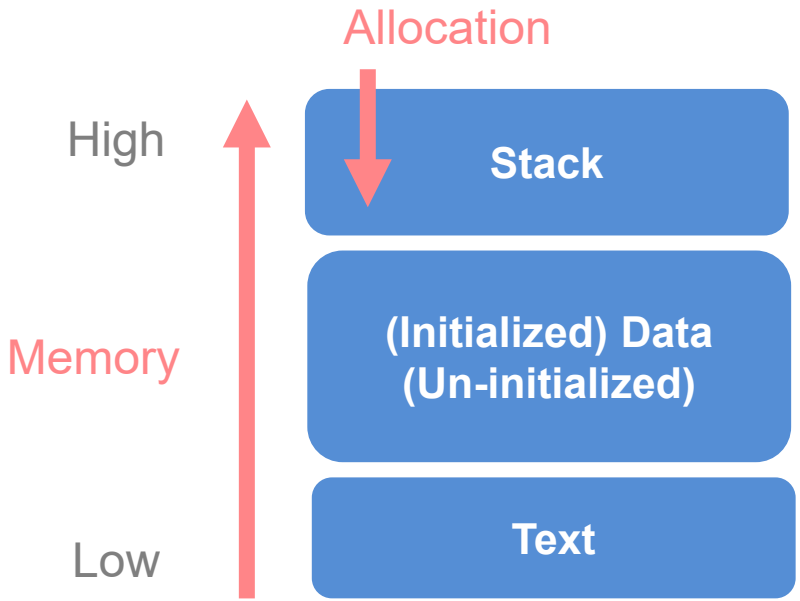
Application Type	Most Significant Threat?
White House web site Political party web site	Defacement
Electronic Commerce Financial Institute	Denial of service Compromise
Military	Infiltration

Design a Security System

- Security in Software Requirements
- Robust, consistent error handling
- Share requirements w/ QA team
- Handle internal errors securely
- Use of “defensive programming”
- Validation and fraud checks
- “Security or Bust Policy”

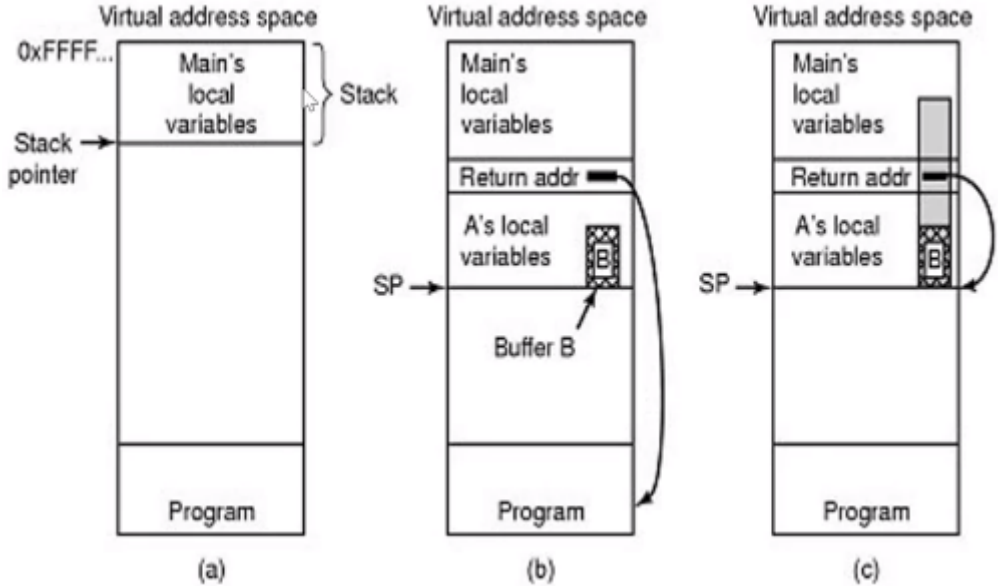
Buffer Overflow and its vulnerabilities

A Buffer Overflow, or buffer overrun, is a common software coding mistake that attacker could exploit to gain access to your system.



Buffer Overflow and its vulnerabilities

A Buffer Overflow, or buffer overrun, is a common software coding mistake that attacker could exploit to gain access to your system.



Stimulation of the main program is running and how program is called. Buffer overflow is shown in the gray (c).

CASE STUDY: WhatsApp

CASE STUDY: WhatsApp

```
if ( packet_length_field <= length_argument )
{
  v18 = (void (__fastcall *)(int, int *, unsigned int, int, unsigned int))v5[4650];
  if ( v18 )
  {
    v19 = v5[4648];
    v20 = sub_D6ADAD08(v8[1]);
    v18(v19, v8, length_argument, v13, v20);
    sub_D69175B4(v8, length_argument, &v23);
    v21 = 12;
    if ( !v13 )
      v21 = 5;
    sub_D692C2DC(v5, v21, &v23, 4);
  }
  else if ( length_argument <= 0x5C8 && a5 && (v11 & 0xFE00) == 51200 )
  {
    qmemcpy(v5 + 32137, v8, length_argument);
    v5[32507] = length_argument;
  }
}
else if ( sub_D6AD6160() >= 2 )
{
  sub_D6AD6620((int)"wa_transport.cc", "RTCP payload length overflow %d, skip", packet_length_field);
}
```