Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques

July 25-29, 2022

Murtuza Jadliwala
murzuja.jadliwala@utsa.edu
What is Cybersecurity?
What is Cybersecurity?

Cybersecurity = Cyber + Security
What is Cyber (a.k.a Internet)?

Evolution of the Internet

![Evolution diagram](image)

What are Cyber Components?

Hardware
Software
Data
Network
Internet Services
Mobile Devices
Online Social Networks
Context-based Service
Cyber-Physical Systems & IoT
What is Cybersecurity?

Cybersecurity = Cyber + Security
Cybersecurity

- Network Security
- The Internet Security
- Mobile-Internet Security
- Mobiles + People + PCs Security
- Internet of Things Security

Hardware Security
Software Security
Data Security
Network Security
Internet Security
Mobile Security
Online Social Networks Security
Context-based Service Security
Cyber-Physical Systems & IoT Security
Computer Security Terminology

Owner

Employ

Countermeasures

Adversary

Minimize

Values

Results in

Have/Are

Vulnerabilities

Give Rise To

Attacks

When Executed

Given Rise To

Threats

Resume

Hardware

Software

Data

Network

Assets

Monday, July 25, 2022
Hardware Security

- Protection against security threats that take advantage of the organizational/architectural vulnerabilities in processing (CPU, ALU, GPU) and memory (SRAM, DRAM) units of a computer system

Software Security

- Protection against security threats due to vulnerable or malicious software (malware)
Data Security

• Protection against security threats to data and information

• Required security properties:
  • Confidentiality
  • Integrity
  • Availability
  • Authenticity
  • Accountability
  • Privacy
Network Security

• Protection against security threats that take advantage of shortcoming in Networking Protocols (TCP, IP, WPA/WEP)
Internet (Web) Security

- Network Security focuses on networking protocols
  - Networking protocols help data move around on the Internet
- Internet or Web Security focuses on Internet or Web applications and services
  - HTTP (Web), Domain Name System (DNS), Web database (SQL) attacks, etc.
Mobile Security

• Protection against security threats to software, hardware and operating system on mobile devices

• Mobile operating systems and security policies seem to be an easier target for hackers
Online Social Network Security

• Privacy is a major concern
  • Know what is visible on your social networking account to the whole world: default settings!
  • How to set good security and privacy policies on who to share our data and information with?
  • Remember anything your put or post on the Internet remains there forever, even if you delete it!

• What else can bad guys do?
  • Create fake accounts (seeming to be someone you know and try to be-friend you)
  • Online stalking and harassment
  • Try to guess your password and break into your account – set strong passwords for your social networking accounts
Cyber-Physical System Security

- All “Physical Systems” are getting enabled with cyber interfaces
- Example, our electricity meters, refrigerators, cars, etc.

- Must secure these systems against cyber attacks.
Different types of Hacking

• Black hat hacking – Hacking for Evil
  • Experts/Advanced
  • Script Kiddies
• White hat hacking – Hacking for Good (Penetration Testing)
Questions?