Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques

June 24-28, 2024

Murtuza Jadliwala

murtuza.jadliwala@utsa.edu

SPrITE LAB

UTSA

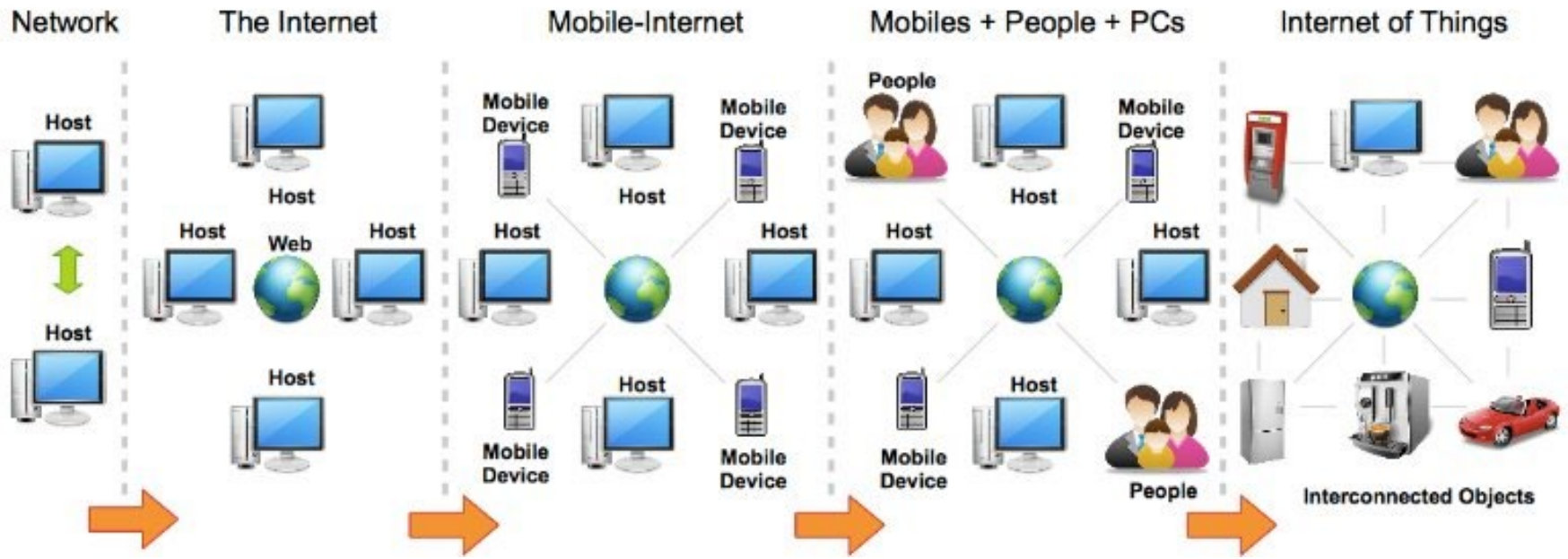
NSF

What is Cybersecurity?

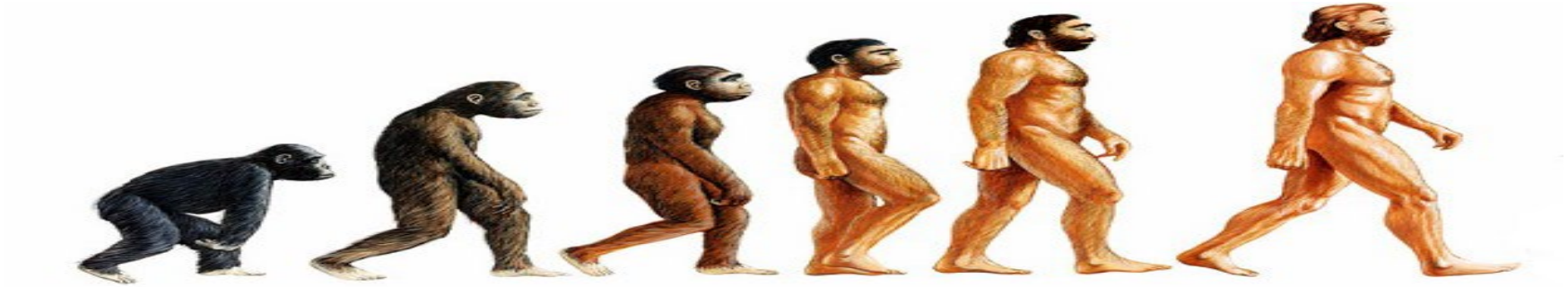
What is Cybersecurity?

Cybersecurity = Cyber + Security

What is Cyber (a.k.a Internet)?

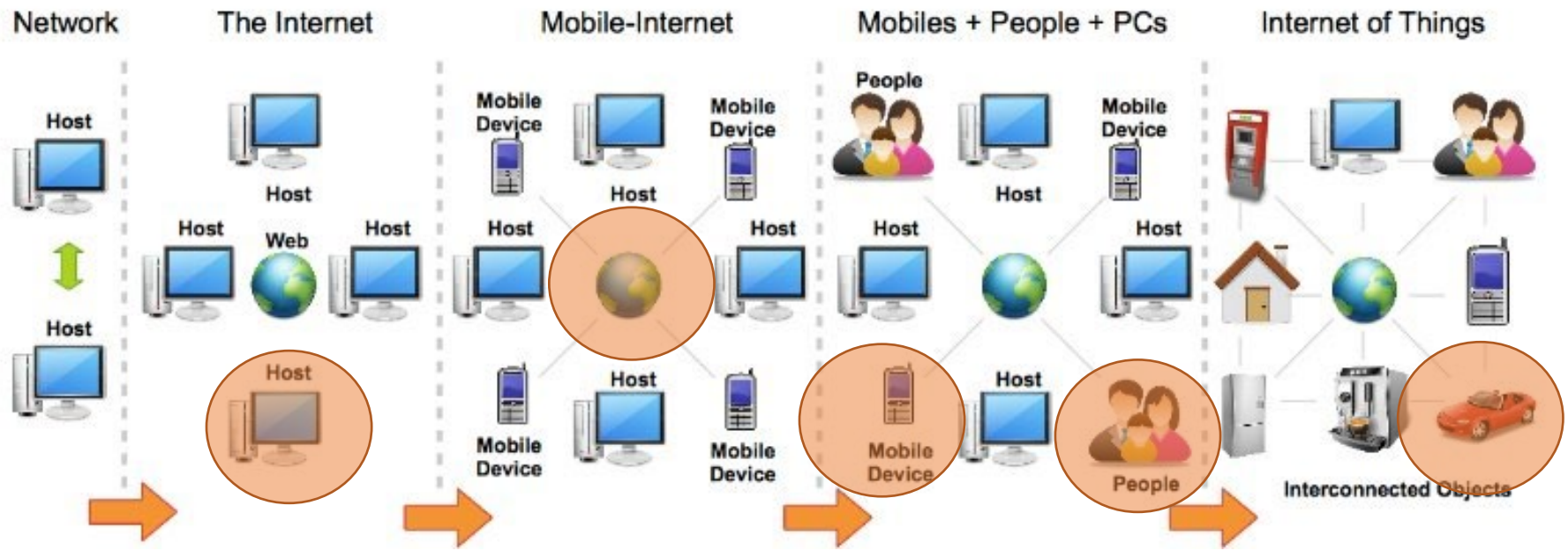


Evolution of the Internet[1]



[1] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey," in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 414-454, First Quarter 2014.

What are Cyber Components?



Hardware

Software

Data

Network

Internet Services

Mobile Devices

Online Social Networks

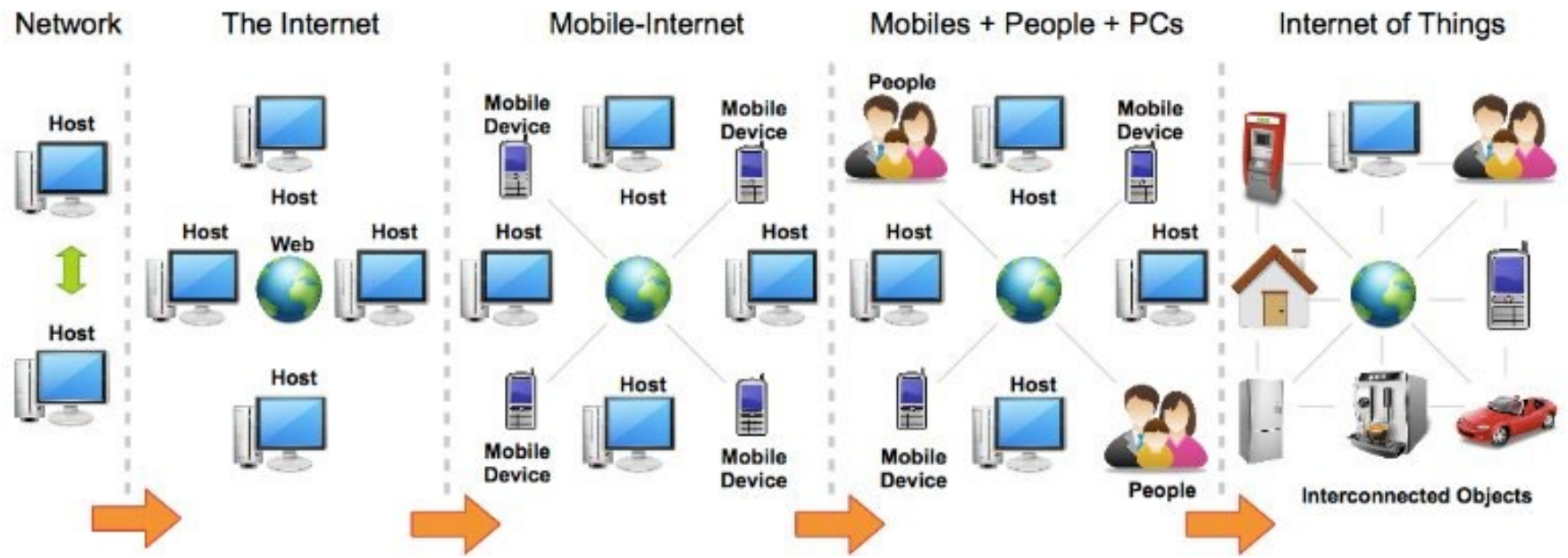
Context-based Service

Cyber-Physical Systems & IoT

What is Cybersecurity?

Cybersecurity = Cyber + Security

Cybersecurity



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

Abuse/Damage

Give Rise To

Results in

Have/Are

When Executed

Give Rise To

Hardware

Software

Data

Network

Assets

Risks

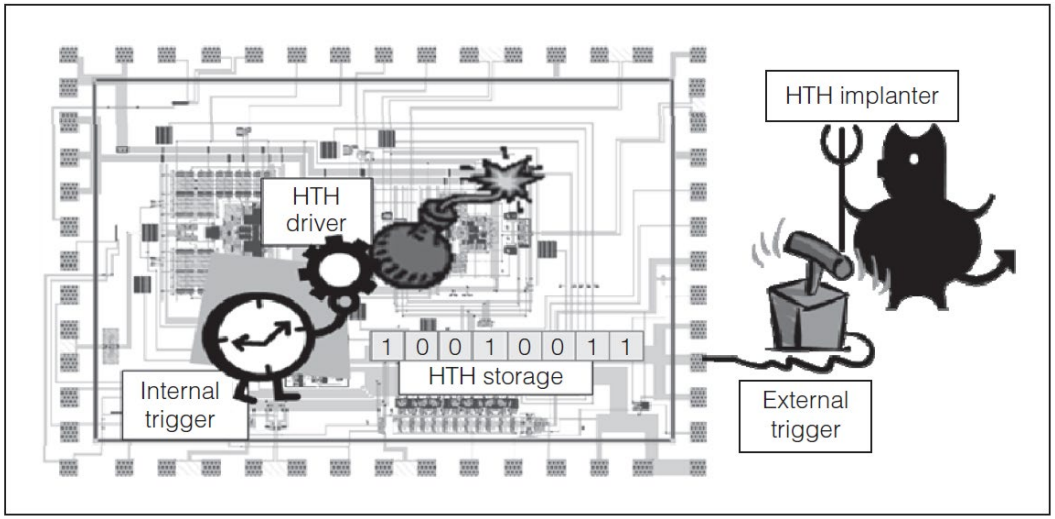
Vulnerabilities

Attacks

Threats

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



Hardware Trojan

Source: Y. Alkabani and F. Koushanfar, "Extended Abstract: Designer's Hardware Trojan Horse," Proc. IEEE Int'l Workshop Hardware-Oriented Security and Trust (HOST 08), IEEE CS Press, 2008, pp. 82-83

Software Security

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

Data Security

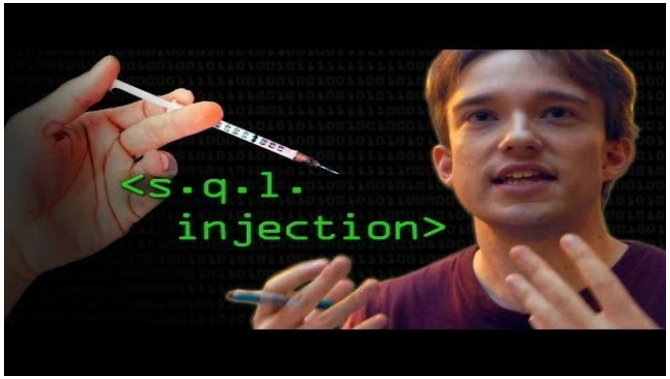
- Protection against security threats to data and information
- Required security properties:
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity
  - Accountability
  - Privacy

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.

Machine Learning/AI Security

- Artificial Intelligence (or AI): Tools and techniques that enable computers/machines to simulate human intelligence and problem-solving capabilities
- Machine Learning (or ML): An AI technique that can observe and learn (some functionality) from data and its statistical features and generalize (the same functionality) to unseen data!
- Machine Learning algorithms have several security and privacy challenges:
  - Is it possible to fool ML algorithms in executing an incorrect functionality, say by subtly modifying the data you feed it?
  - Is it possible to leak the (private) data on which ML algorithms have learnt their functionality (or have been trained) on?
  - It is possible to use ML algorithms and techniques for nefarious purposes, for example, fake images and fake audio? And how to protect against it?

Different types of Hacking

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

Questions?