Topic 1: An Introduction

Introduction to course unit and cybersecurity

- **Main textbook: Computer Security,** 4th Edition by William Stallings and Lawrie Brown, ISBN-13: 9780134794105, Pearson, 2018.
- Supplementary textbooks:
  - Effective Cybersecurity: A Guide to Using Best Practices and Standards, Williams Stallings, ISBN-13: 9780134772806, Addison-Wesley, 2019.
  - Computer Security: Art and Science, 2nd Edition, Matt Bishop.
- In addition, there are lots of on-line resources.

Overview

- Introduction to the Course Unit
- What is Cybersecurity
- Cybersecurity Domains
- Security: past and now
- Scope of the Course Unit
- Course Unit Roadmap

Home Reading: Main textbook, Chapter 1

Introduction to the Course Unit

- Course Unit Leader
  - Ning Zhang
  - ning.zhang@manchester.ac.uk

Introduction to the Course Unit

- Reading materials
  - **Main textbook:** Computer Security, 4th Edition by William Stallings and Lawrie Brown, ISBN-13: 9780134794105, Pearson, 2018.
  - There is a lot of useful resources on the Internet, e.g. www.cert.org and www.nist.gov. Search for relevant materials using key words, e.g. use materials covered in the lecture handouts to scope/guide your reading.
- Will also supplement the textbooks with other literature materials.
- Lecture Handouts are hosted in the Blackboard.

Introduction to the Course Unit

- New materials are structured into topics
  - There is a main handout per topic.
  - Exercise questions are set.
    - Exercise questions for enhancing understanding of lecture materials and development of key skills.

- Assessment
  - 100% written exam

What is Cybersecurity?

- Cybersecurity = cyberspace + security;
- Cyberspace consists of physical infrastructure, critical infrastructure and cyber infrastructure (i.e. the Internet).

What is Cyberspace?

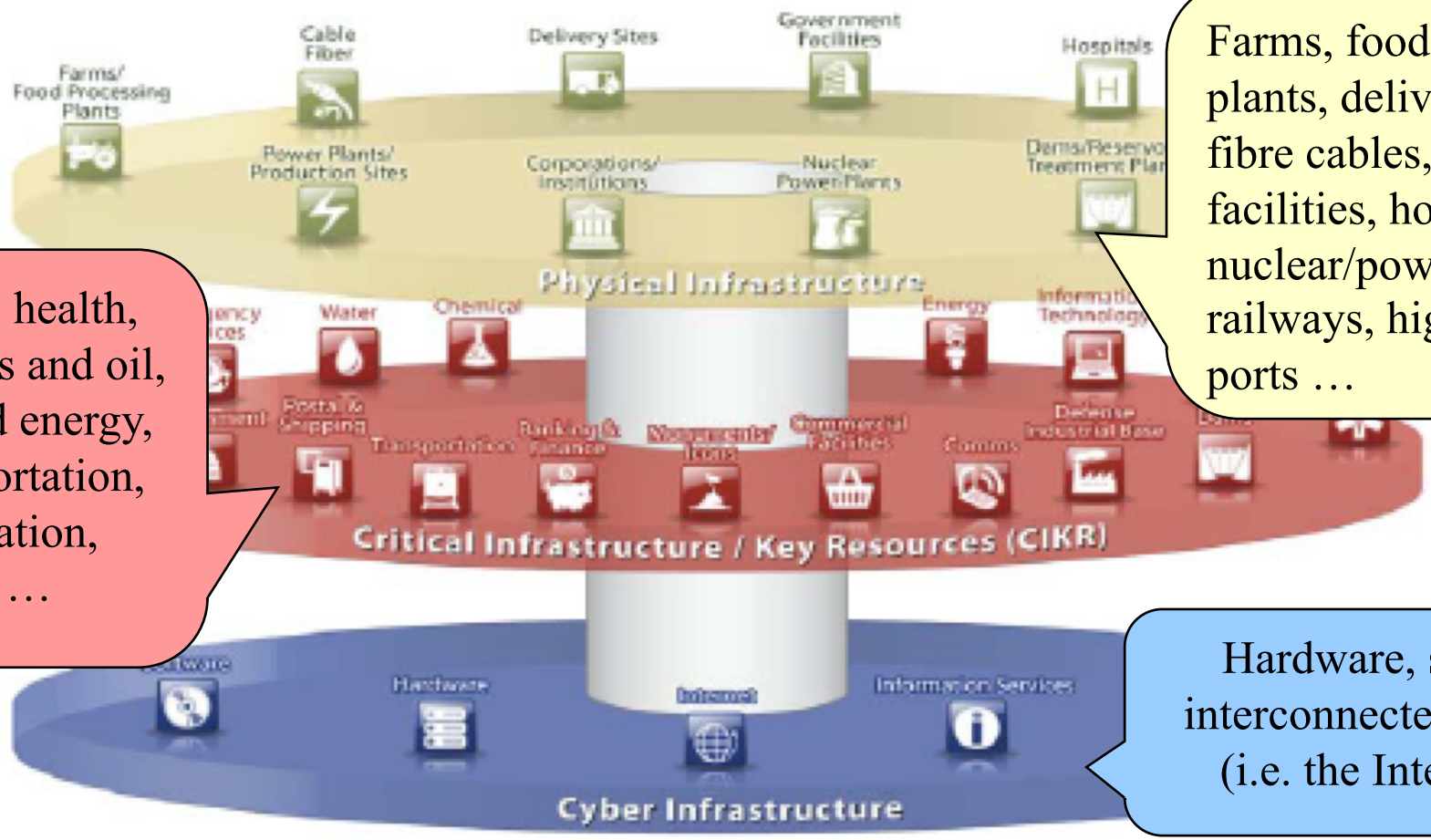


Figure 2-3. Infrastructure relationships in cyberspace[10]

Farms, food processing plants, delivery site, fibre cables, gov facilities, hospitals, nuclear/power plants, railways, highways, ports …

Government, health, emergency, gas and oil, electricity and energy, water, transportation, communication, banking …

Hardware, software, interconnected networks (i.e. the Internet), …

Source: DHS, "Securing the Nation's Critical Cyber Infrastructure

What is Security?

Information hiding

eCommerce/transaction security

Entity authentication

Digital Right Management

Privacy

Malicious code

Trust

Digital signatures

Integrity

eGovernment

Threats/vulnerabilities

Access control

Fraud

Encryption

Key management

POLICY MAKING

Computer forensics

Biometrics

Information security

Anonymity

Network security

Cryptographic Algorithms & Protocols

Risk assessment

Huge list of attacks

What is Cybersecurity?

- From different perspective, the definitions are different, e.g.
- According to NCSC (the UK National Cyber Security Centre) [https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security], "*Cyber security is how individuals and organisations reduce the risk of cyber attack. Cyber security's core function is to protect the* ***devices*** *we all use (smartphones, laptops, tablets and computers), and the* ***services*** *we access - both online and at work - from theft or damage. It's also about preventing unauthorised access to the vast amounts of* ***personal information*** *we store on these devices, and online*."
- According to IBM [https://www.ibm.com/topics/cybersecurity], "*Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks*."

What is Cybersecurity?

- From our (IT managers, system analysts, system developers, …) perspective, "Cybersecurity is the **process** and **techniques** involved in protecting sensitive data, computer systems, networks, and software applications from cyber (network-based, digital) attacks".

Cybersecurity Domains

- **Critical infrastructure security -** protecting devices, computer systems, networks, and other assets that society relies upon.
- **Network/Internet security** - protecting a computer network from intruders.
- **Application security** - protecting applications operating on-premises and in the Cloud, handling data, user authentication, authorisation, etc, securely.
- **Cloud security** – protecting data at rest, in transit and in use to support customer privacy, business requirements and regulatory compliance standards.

Cybersecurity Domains

- **Information security** - securing sensitive data from unauthorized access, exposure, or theft.
- **End-user education** - building security awareness across the organization to strengthen endpoint security.
- **Disaster recovery/business continuity planning** - tools and procedures for responding to unplanned events, such as natural disasters, power outages, or cybersecurity incidents, with minimal disruption to key operations.

Cybersecurity Domains

- Securing a system involves
  - use of cryptographic methods/tools and design of protocols (design)
  - secure programming (implementation)
  - interacting with, and educating, people
  - defining policy, procedures
  - physical security
  - monitoring what you have designed/implemented

Cybersecurity Domains

- Many parties are involved, e.g.
  - System developers
  - Companies/organisations deploying the system – multi-level roles/people
  - End users
  - Adversaries (external and internal - insider threats)

- Different parties have different interests and goals
  - System developers and companies may wish to cut costs
  - End users are concerned about security, privacy, and usability
  - The relationship between these goals may be complex or conflicting, e.g. a higher level of security/privacy often means a higher level of development cost and a lower level of usability.

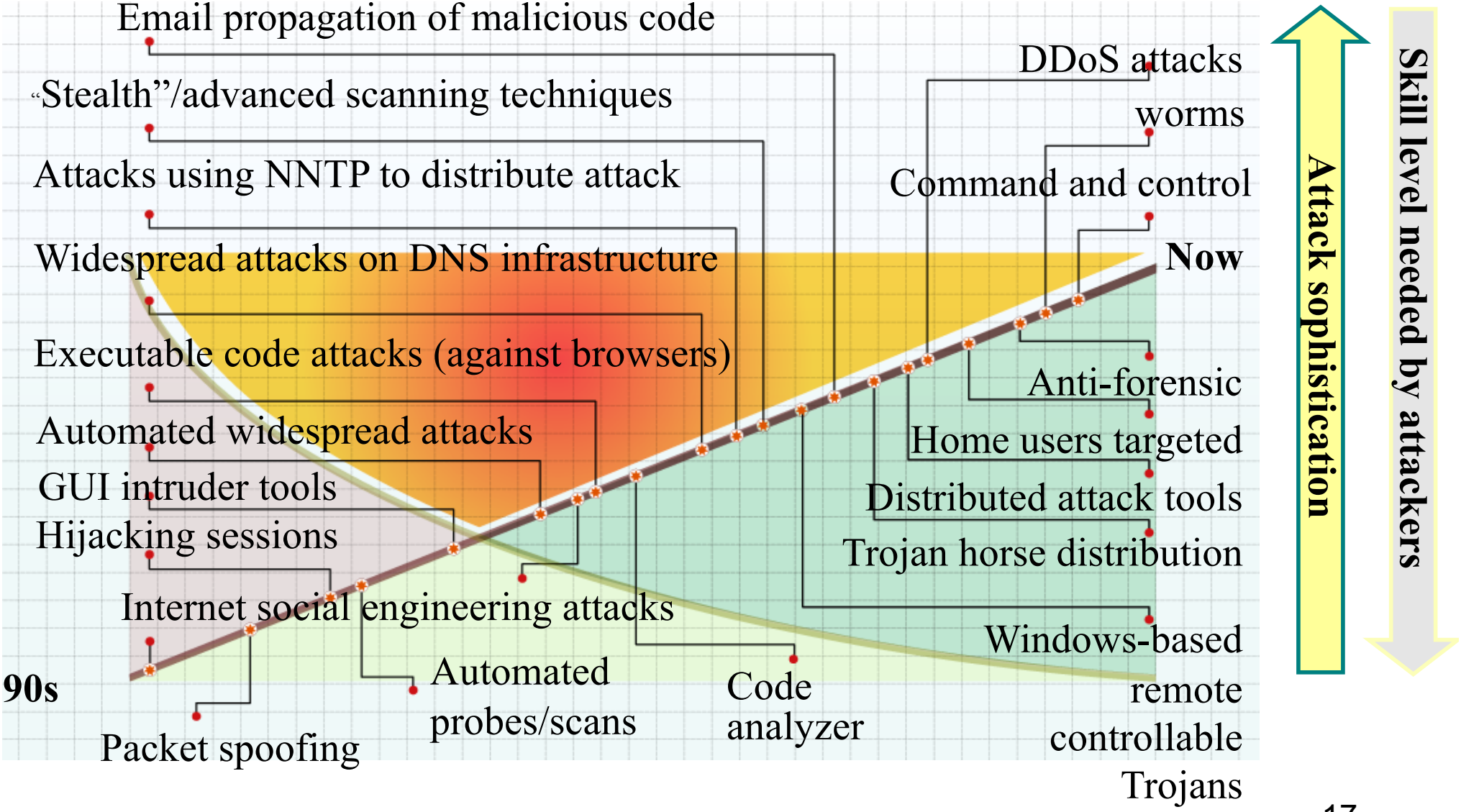
Security: past and now

- Technological advancement and milestones
  - Morris worm – 1988; brought down a large fraction of the Internet
  - E-commerce, ATM/financial transactions – late 80s
  - Mosaic and Netscape – early 90s
  - Mobile Internet - Internet anywhere, anytime and by any devices
  - Cloud Computing - on-demand provisioning of computational and storage resources, elastic resource sharing, service outsourcing.
  - IoT (Internet of Things) – embedded devices, connected world, smart environment, …
  - Crypto currencies, smart contract signing, getting rid of third parties - blockchain technologies

Security: past and now

- Increased technological advancement, digitization and/or system integration or the so called ‘connected world’ increase the risk spectrum
- Mounting attacks is increasingly easier

Security: past and now



Source: SE/CERT CC

Security: past and now

- Heterogeneous devices, e.g. laptops, iPhones and PDAs, with universal connections means that there may not be a one-for-all solution.
- Anonymous nature of many Internet-based services means that legitimate services and software may be exploited by attackers and it can be hard to trace the origin of an attack or the attacker.
- Global networks without national boundaries, so attacks may be mounted anywhere on the Internet and there is a need for international collaborations to address the attacks …

Scope of the Course Unit

- The entire lifecycle of a system (application/service) development is critical: from policy, design, implementation, to management.
- The weakest link principle: any bug in this lifecycle will make the system as weak/vulnerable as where the bug leads to, e.g.
  - **Policy/requirement specification bugs**: inappropriate policy or goals
    - Threat analysis
    - Access control - least privilege
  - **Design bugs**
    - Inappropriate use of cryptographic methods/tools
    - Poor source of randomness
    - Insecurity protocols
    - …

Scope of the Course Unit

- **Implementation bugs**
  - Buffer overflows
  - …
- **Problems with management procedures**
  - Is the implemented system usable? Does it achieve the security goal? Have the risks been mitigated?
  - End-users, employees, administrators …: do they perform their tasks/roles as expected?

- The main focus of this Course Unit is on security issues in the Requirement specification, Design and Implementation stage of the lifecycle…

Course Roadmap

T2 - Security Basics
T3 - Symmetric Cryptography and Applications
T4 - Asymmetric Cryptography and Applications
T5 - Cryptographic Checksums and Applications
T6 - Secret Key Management
T7 - Public Key Infrastructure
T8 - Entity Authentication
T9 - VPNs (Virtual Private Networks)
T10 - Email Security
T11 - Software Security

Exercise Question – E1.1

Respectively assuming yourself as

- the owner/director of an SME (Small and medium-sized enterprise),
- the IT manager in an organization, managing the IT facilities in the organization, and
- the manager of the development team in an IT company, in charge of developing an app for on-line shopping,

carry out some research and identify

i. cybersecurity challenges and
ii. measures to tackle the challenges.