Computer Security and Networks

Eike Ritter Pascal Berrang Rishiraj Bhattacharyya
Usman Ilyas Panagiotis Andriotis

University of Birmingham

Outline of This Lecture

- Module Arrangements: When, Where, Who.
- Module Outline
- Module Outcome

Module Arrangements at Edgbaston

- Who: Eike, Pascal, and Rishi.

Module Arrangements at Edgbaston

- Who: Eike, Pascal, and Rishi.
- Where: Pre-recorded lectures.
- Where: On Campus lectures.
  - Tuesday 4PM-6PM University Centre Avon Room (T02).
  - One hour on revisiting lectures, one hour pop quiz.

Module Arrangements at Edgbaston

- Who: Eike, Pascal, and Rishi.
- Where: Pre-recorded lectures.
- Where: On Campus lectures.
  - Tuesday 4PM-6PM University Centre Avon Room (T02).
  - One hour on revisiting lectures, one hour pop quiz.
- Hour-long Practicals CPSC UG04: Four sessions in total; each student will be allocated to one

Module Arrangements at Edgbaston

- Who: Eike, Pascal, and Rishi.
- Where: Pre-recorded lectures.
- Where: On Campus lectures.
  - Tuesday 4PM-6PM University Centre Avon Room (T02).
  - One hour on revisiting lectures, one hour pop quiz.
- Hour-long Practicals CPSC UG04: Four sessions in total; each student will be allocated to one
- Microsoft Teams channel.

Module Evaluations

- 20% continuous assessment, 80% exams.
- Token based exercises on VMs.
  - When you complete an exercise on the VM you will usually find a token (or flag).
  - You submit the token to a website, to show you have solved the exervise.
  - Tokens are unique to your VM. You must not share VMs or Tokens.
- Make sure your computer has sufficient space; should be possible to run it from external disks.

DO NOT TRY OUT ANYTHING ON COMPUTERS YOU DO NOT OWN

- It is illegal to access computers without the owner's permission.
- Most access are logged, and it is easy to get caught.
- Trying things "just for fun" could be punishable offense.

Learning Outcome

- Understand basic concepts of cryptography and SQL
- Understand basic concepts of cloud services, in particular storage
- Demonstrate an understanding of the threats to data stored on a computer, locally or in the cloud
- Demonstrate an understanding of the threats to data sent on the network
- Identify risks and use techniques to eliminate or mitigate them.

Module Outline

- Cryptography
- Access Control
- Introduction to Networking
- Security Protocols
- Web Systems and Attacks
- Other Common Attacks and Defenses

What is Computer Security

- Correctness and Efficient algorithms against an attacker.

What is Computer Security

- Correctness and Efficient algorithms against an attacker.
- What do we safeguard?

What is Computer Security

- Correctness and Efficient algorithms against an attacker.
- What do we safeguard?
- Decide on your assets: Information and Infrastructure.

What is Computer Security

- Correctness and Efficient algorithms against an attacker.
- What do we safeguard?
- Decide on your assets: Information and Infrastructure.
  - Sensitive Data.

What is Computer Security

- Correctness and Efficient algorithms against an attacker.
- What do we safeguard?
- Decide on your assets: Information and Infrastructure.
  - Sensitive Data.
  - Control Systems.
  - Hardware devices.

What is Computer Security

- Correctness and Efficient algorithms against an attacker.
- What do we safeguard?
- Decide on your assets: Information and Infrastructure.
  - Sensitive Data.
  - Control Systems.
  - Hardware devices.
- How do you safeguard: security goal, estimate impact of attacks, and design mitigations
- Analyse systems, spot vulnerabilities, build protection.

Information Security:Aims

- **Confidentiality**: Attacker should not retrieve any information.
- **Integrity and Authenticity**: Received data is authentic and the sender is genuine.
- **Availability**: Data should accessible on demand.

Information Security:Potential Attackers

Anyone and Everyone

Information Security:Potential Attackers

- **Hackers**: Potentially learning by running known attacks, exploiting vulnerabilities.
- **Criminals**: Take control of computers via bugs in softwares. Phishing attacks, Denial of Service (DoS attacks)
- **Governments**: Extreme computing powers, control on resources (wiretaps),...
- **Business Houses like ISPs**: Spying to sell your data.

Some Known Attacks

- **Ransomware**:
  - Malwares: Trojan disguised as legitimate files.
  - *Wannacry 2017* moved automatically via unpatched vulnerabilities in Microsoft Windows (Eternal Blue of NSA).
  - The malware encrypted the data on the computer and asked for payments in bitcoins.
  - Widespread impact, NHS and NISSAN among affected.
- **Phishing**:
  - emails pretending to be from known people.
  - emails asks for username and password and asks for software installation, includes word macros.
  - install malware to spread within networks, downloads further malware.

Course Outcome: Informal

First steps on how to stay safe in the digital world.