Security of Networks, Services, and Systems

`Class Introduction`

Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC

Goal

- Explore the concepts and practice of network security by understanding:
  - the limitations of protocols, services, systems, and communication infrastructure when facing a motivated attacker
  - some of the existing solutions to mitigate or avoid the impact of these limitations

Learning objectives

1. Know transversal security concepts
2. Identify and exploit known network and system vulnerabilities
3. Identify and design security mechanisms for networks and systems
4. Develop and analyze applications that use cryptography-based communication protocols;
5. Autonomously explore new topics in security by analyzing scientific papers and other reports and by experimenting with the new topics in a lab.

Program

1. Security-related concepts including threat model, vulnerabilities and exploits, security policies, security by design and by obfuscation, risk management, and penetration testing methodology.
2. Known vulnerabilities in networks and systems -- sniffing and spoofing including scapy programming, higher layer attacks (TCP, HTTP, etc).
3. Security mechanisms based in access control and in network and traffic segmentation; filtering, firewalls, intrusion detection, and VPNs.
4. Cryptography-based communication protocols such as TLS, IPSec, 802.11, secure DNS, and secure BGP.
5. Selected topics in security including privacy, denial of service, malware and IoT malware, sandboxing, honeypots, cyber intelligence, and security operations centers.

Also – you get pinch of cryptography

If you haven't looked into this yet

- Symmetric ciphers and modes of operation
- Asymmetric ciphers
- Hashing, data integrity, digital signatures

And lots of attacks to try out

- Mostly from the SEED Security Labs at the Univ. Syracuse / Prof. Du

Approach and evaluation

- Approach
  - Investigate and discuss white papers, standards, academic papers
  - Go through numerous labs that will give you a sense of attacking and defending
  - Come up with threat models for your target networks
- Evaluation
  - Test on network security concepts and cryptography – 50%
  - Project in selected topics in security – 50%

Flipped class room

- We’re trying this approach – instead of going through slides in class
- Study before coming to class – watch content, read papers, etc
- Ask questions, argue, discuss in class
- Content on Moodle
- Check out the syllabus for what to do before class

Security of Networks, Services, and Systems

`Class Introduction`

Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC