4th StudentGuru Patras MeetUp @ CEID

ICT Security Basics

Demystifying the Sec puzzle

Anestis Bechtsoudis

{ http(s)://bechtsoudis.com }

$whoami

- Undergraduate Student @CEID
- NOC Administrator at CEID C.C. Lab
- Penetration Tester (aka ethical hacker)
- Applied Cryptography Researcher
- Security Researcher

Agenda

- Introduction to ICT Security
- How it affects users & administrators
- ICT Security objectives
- Attack Taxonomy
- Live Hacking Demo

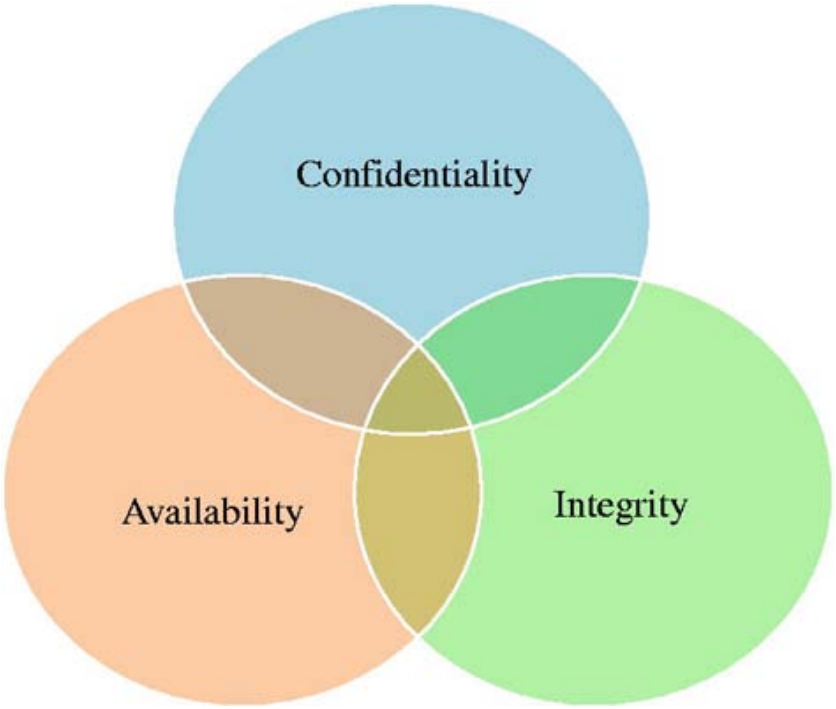
Scope

- Decode ICT security definitions
- Understand why security is important
- Real examples in enterprise networks
- Motivate future {ethical} hackers
- Persuade you to adopt good security practices in your everyday life

What security means?

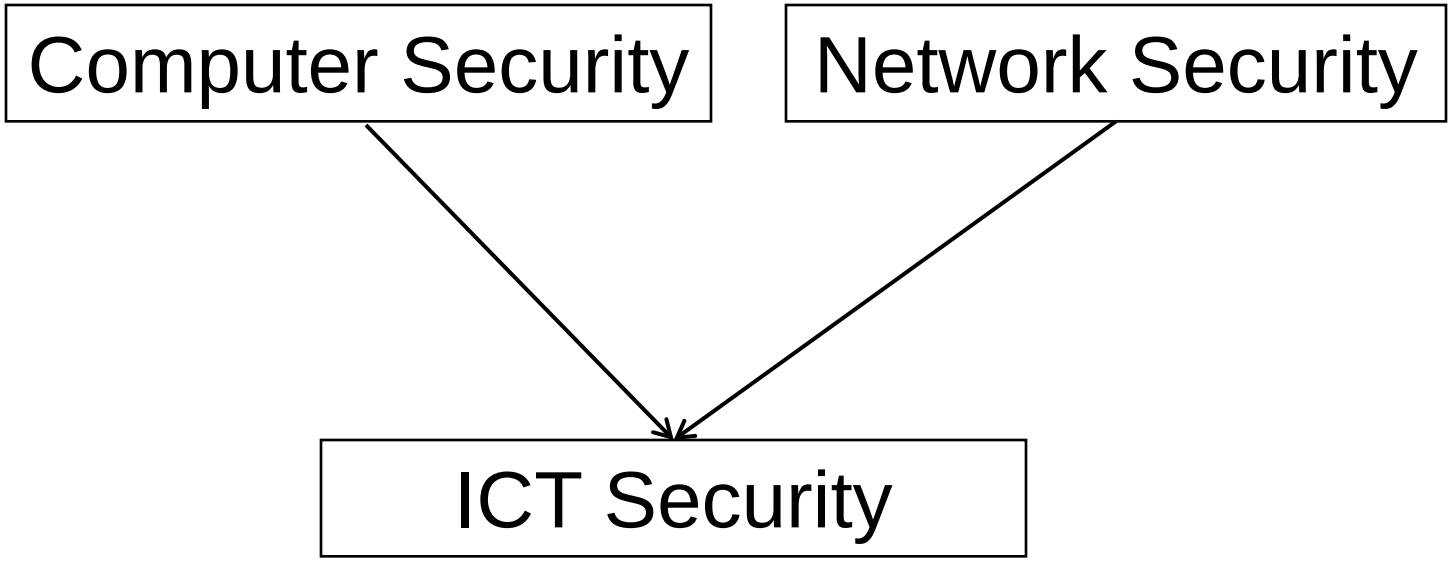
Information Security

- Protect **information** & **informational** systems



ICT Security

- Point of view definitions



Why is ICT Security important?

- Protecting personal information
- Allows companies, organizations & institutes to carry out their mission by:
  - Enabling people to carry out their jobs
  - Protecting personal & sensitive information
  - Supporting critical organization processes
- Social responsibility

Why do we need to learn about it?

Isn't this just an ICT problem?

Regular Security Standards follow the “90/10” rule!

- 10% of security safeguards are technical
- 90% of security safeguards rely on the user to adhere good practices

You need to cover all aspects for effective security!!!

What does this mean for me?

- Everyone who uses a computer or mobile device needs to understand how to keep the device and its data secure
- Information Technology is everyone's responsibility

Hacked systems can be used to

- Generate large volumes of traffic slowing down entire systems/networks
- Access restricted or personal information
- Record keystrokes & steal passwords
- Hide programs that launch attacks on other systems/networks
- Send spam & phishing material
- Distribute illegal material

Objectives – User Approach

- Learn good security practices
- Adopt these practices into everyday routine
- Learn to work efficiently through them
- Report anything unusual to the appropriate contacts
- Track latest security issues

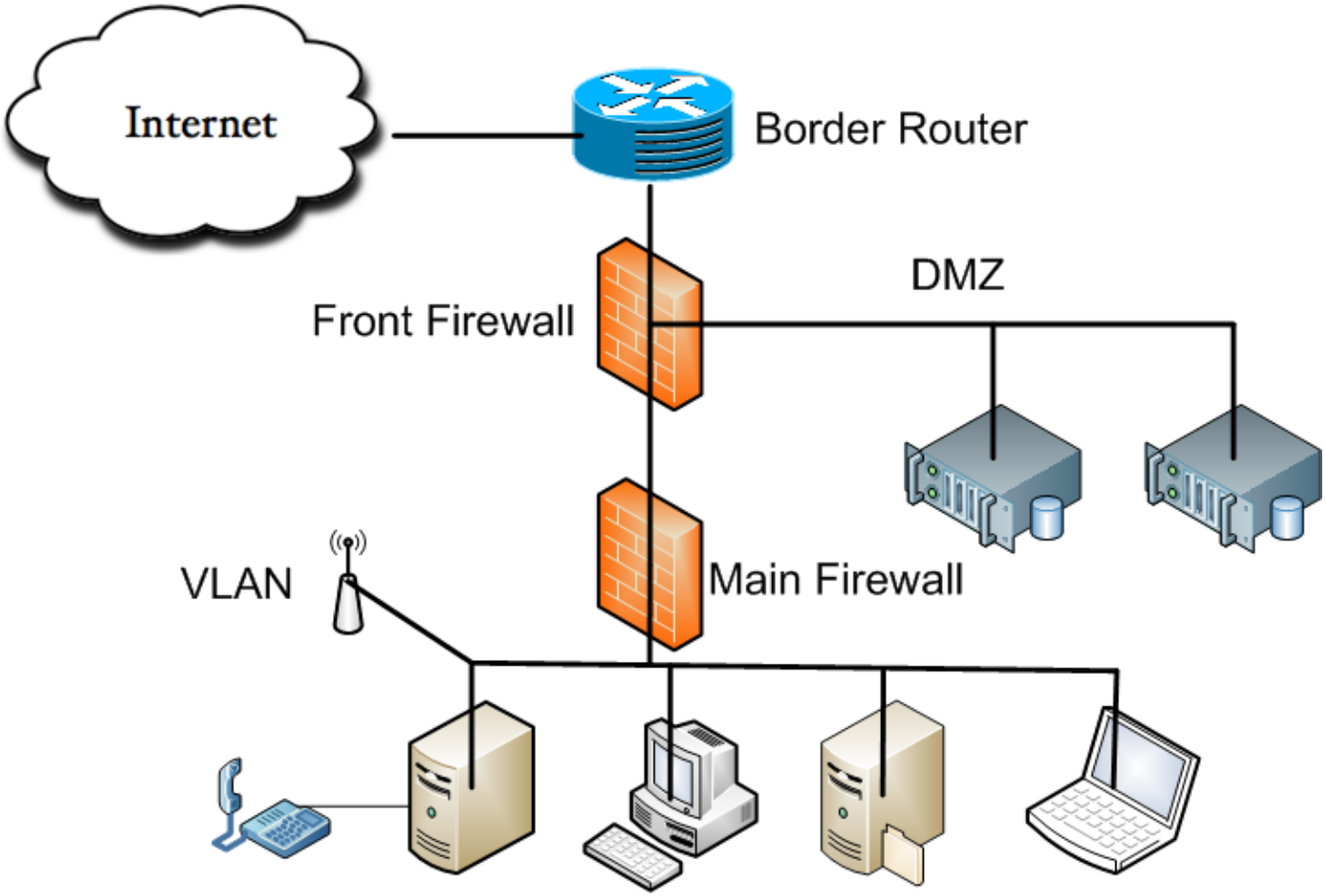
Objectives – Admin Approach

- Provide system/data/network CIA
- Instruct the users
- Be proactive – up-to-date policies are not enough
- Regular security audits
- Report to appropriate CERT if attacking incident occurs

Attacker Goals

- Interruption – attack availability
- Interception – gain authorized access
- Modification – tamper with the resource
- Counterfeiting – social engineering

Simple Network Infrastructure



How many entry points can you locate?

Can you suggest any security improvements?

Live Hacking Demo

Disclaimer: This information is for educational purposes only. Presenter is not responsible for any damage that you may create!

Thank You!

Questions?