CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

Computer Security Principles

Lecture 1: Module Overview and Introduction

Description

This module introduces the student to the fundamental concepts of information security.

It identifies the threats associated with the use of networked computing devices in the modern world and provides a practical guide in the defence against those threats.

Learning Outcomes

On successful completion of this module the learner will be able to:

- Describe different types of security threats.
- Recognise the issues involved in being a security aware computer user.
- Compare and contrast common cryptographic protocols.
- Identify threats and use security software to mitigate risk.
- Analyse the issues involved in the secure usage of the Internet.

Course Sections & Assessment Approach

Areas to be covered:

- Information security concept – CIA triad, defense in depth
- Malware – viruses, spyware, rootkits, adware
- Authentication – passwords, biometrics, two-factor auth
- Using the internet – firewalls, browser security, email
- Using a PC securely – backups, patching, disaster recovery
- Mobile Phone Security – Threats and Solutions

Assessment

- Lab Project 1 Reports (25%) Week 6
- Lab Project 2 Reports (25%) Week 11
- End of Semester Exam (50%) Week 14

Lab Reports

You will be most likely required to complete labs on the following :

- Malware Threats
- OS Hardening
- Browser Security
- Social Media
- Footprinting
- Encryption
- Mobile Security
- Wireless Issues

Assessment - Marks & Standards

Coursework which is submitted after the submission date will attract a penalty as follows:

- Up to 1 calendar week delay 10% of the marks available for the assessment
- Up to 2 calendar weeks delay 20% of the marks available for the assessment
- Over 2 calendar weeks delay 100% of the marks available for the assessment

Assessment - Marks & Standards

If valid extenuating circumstances have been established in accordance with Institute guidelines and to the satisfaction of the MEB, then the MEB may, at its discretion:

- remove or mitigate any late submission penalty;

and/or

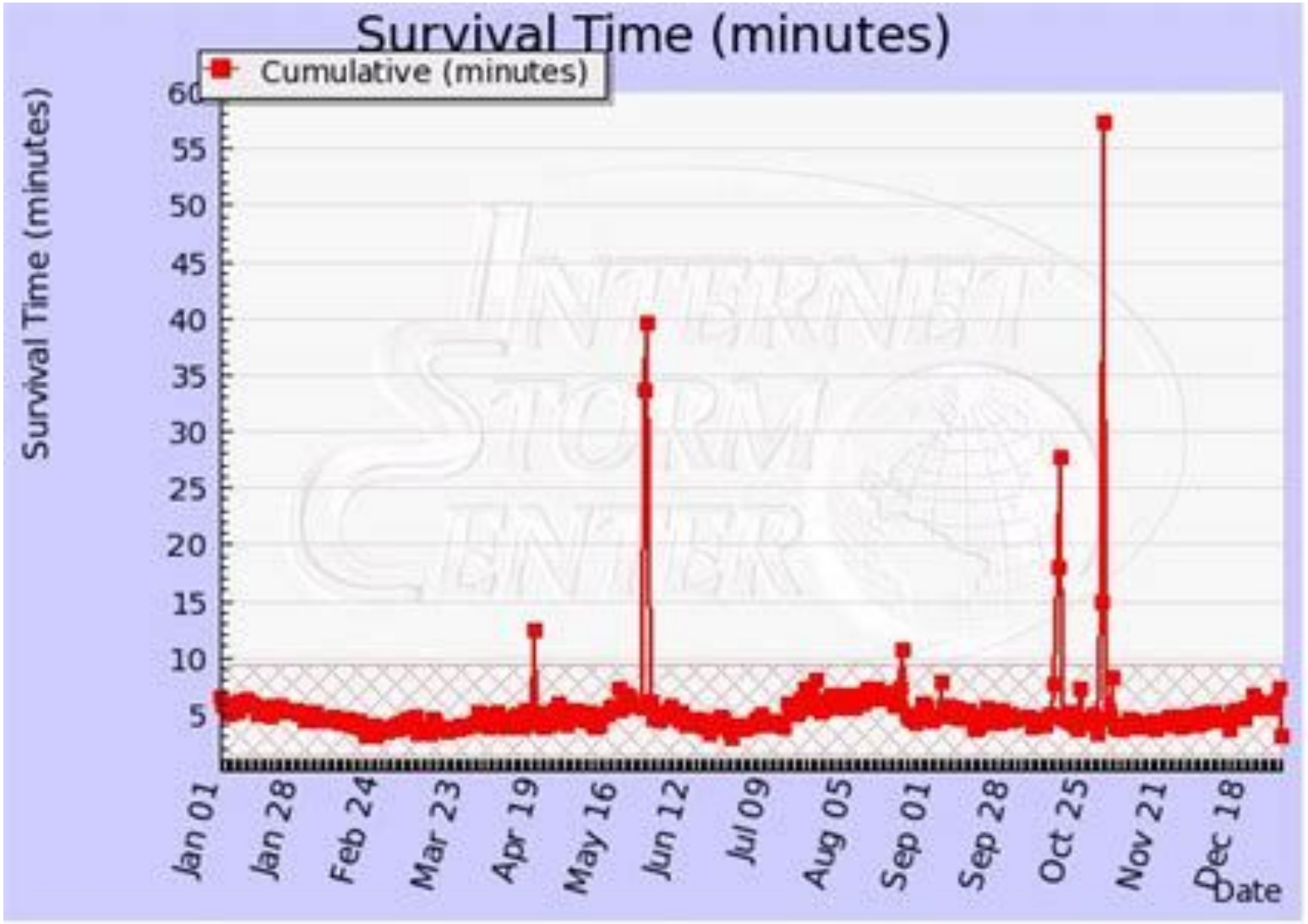
- record a Deferral to enable the candidate to repeat or be reassessed in the module as a first attempt.

Individual Extenuating Circumstances

Your risk online

If you connect an unprotected computer to the internet, how long will it take before it is infected by malicious software?

Your risk online



The Players?

The Hacktivist

- Simply put, hacktivists are politically motivated cyber attackers.
- Over the past five years, activists have realized the power of the Internet, and have started using cyber attacks to get their political message across.
- Anonymous, Syrian Electronic Army.

The Players?

Cyber Criminals

- This group's motive to make money using any means necessary.
- Cyber criminal groups can range from a few lone actors to big cyber crime organizations financed and headed by traditional criminal organizations.
- They are the group of hackers responsible for stealing billions of dollars from consumers and businesses each year.

The Players?

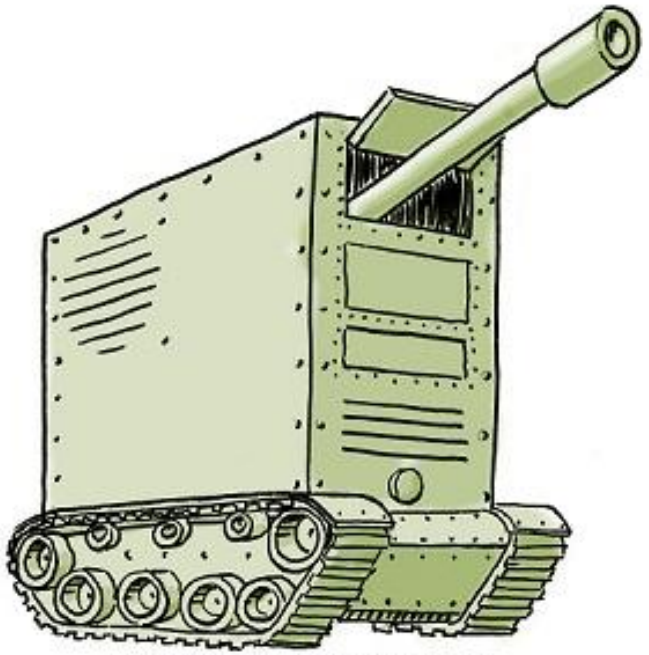
Cyber Criminals (contd)

- These criminal attackers participate in a rich underground economy, where they buy, sell and trade attack toolkits, zero day exploit code, botnet services, and much more.
- They also buy and sell the private information and intellectual property they steal from victims.
- Lately, they're focusing on web exploit kits, such as Blackhole, Phoenix, and Nuclear Pack, which they use to automate and simplify drive-by download attacks.

The Players?

Nation States

- The newest, and most concerning new threat actors are the state-sponsored cyber attackers.
- These are government-funded and guided attackers, ordered to launch operations from cyber espionage to intellectual property theft.
- These attackers have the biggest bankroll, and thus can afford to hire the best talent to create the most advanced, nefarious, and stealthy threats.



Nation-state-sponsored cyber attacks

McAfee Labs Threats Predictions

Mobile malware

- The rate of growth in the appearance of new mobile malware, which almost exclusively targets the Android platform, has been **far greater than the growth rate of new malware targeting PCs**.
- Expect to see **Ransomware** attacks aimed at mobile devices that will encrypt key data on the device and hold it for ransom.
- Expect to see attacks on vulnerabilities in the **near-field communications features**

Virtual currencies

- Virtual currencies have provided cybercriminals with the perfect unregulated and anonymous payment infrastructure they need to collect money from their victims.
- Expect attacks such as CryptoLocker to proliferate for as long as such attacks remain (very) profitable.
- Expect to see new ransomware attacks aimed at enterprises that will purport to encrypt key corporate data assets.

New stealth attacks

- A popular evasion technique that will see broad adoption by cybercriminals is the use of **sandbox-aware attacks** that do not fully deploy unless they believe they are running directly on an unprotected device.
- Expect **return-oriented programming attacks** that cause legitimate applications to behave in malicious ways, self-deleting malware the covers its tracks after subverting a target, and advanced attacks on dedicated industrial control systems that have the potential to damage public and private infrastructure.

McAfee Labs Threats Predictions

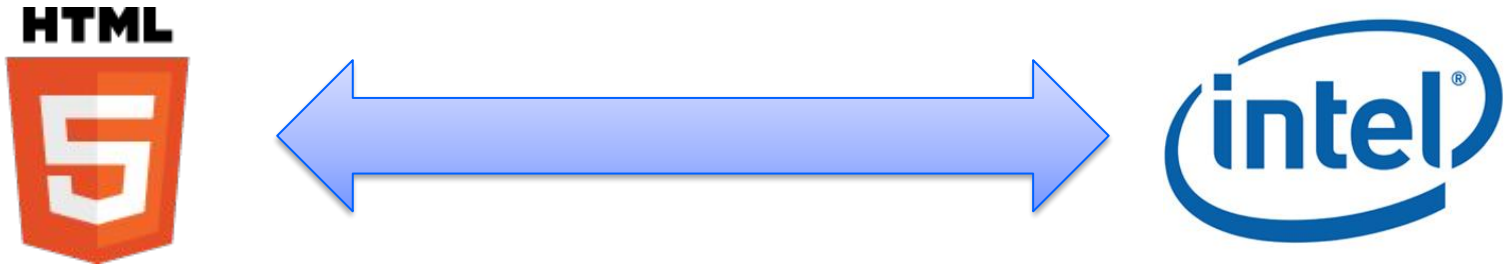
"Social attacks"

- Expect to see attacks that employ the unique features of the social platforms to deliver data about user contacts, location, or business activities that can be used to target advertising or perpetrate virtual or real-world crimes.
- One of the most common platform attacks simply steals users' authentication credentials, which are then used to extract personal data from unsuspecting "friends" and colleagues.

McAfee Labs Threats Predictions

Attacks above and below the operating system.

- New attacks we'll see will, however, not simply attack the operating system, but will also exploit vulnerabilities both above and below the OS.
- Expect to see exploitation of vulnerabilities in **HTML5**, which allows websites to come alive with interaction, personalization, and rich capabilities for programmers. However, HTML5 also exposes a number of new attack surfaces.
- Cybercriminals will increasingly target vulnerabilities below the operating system in the storage stack and even the **BIOS**.



Your threats

Do you have AV software on your mobile?

Do you have bitcoins?

What could I learn about you from your social media pages?

Defense-in-Depth

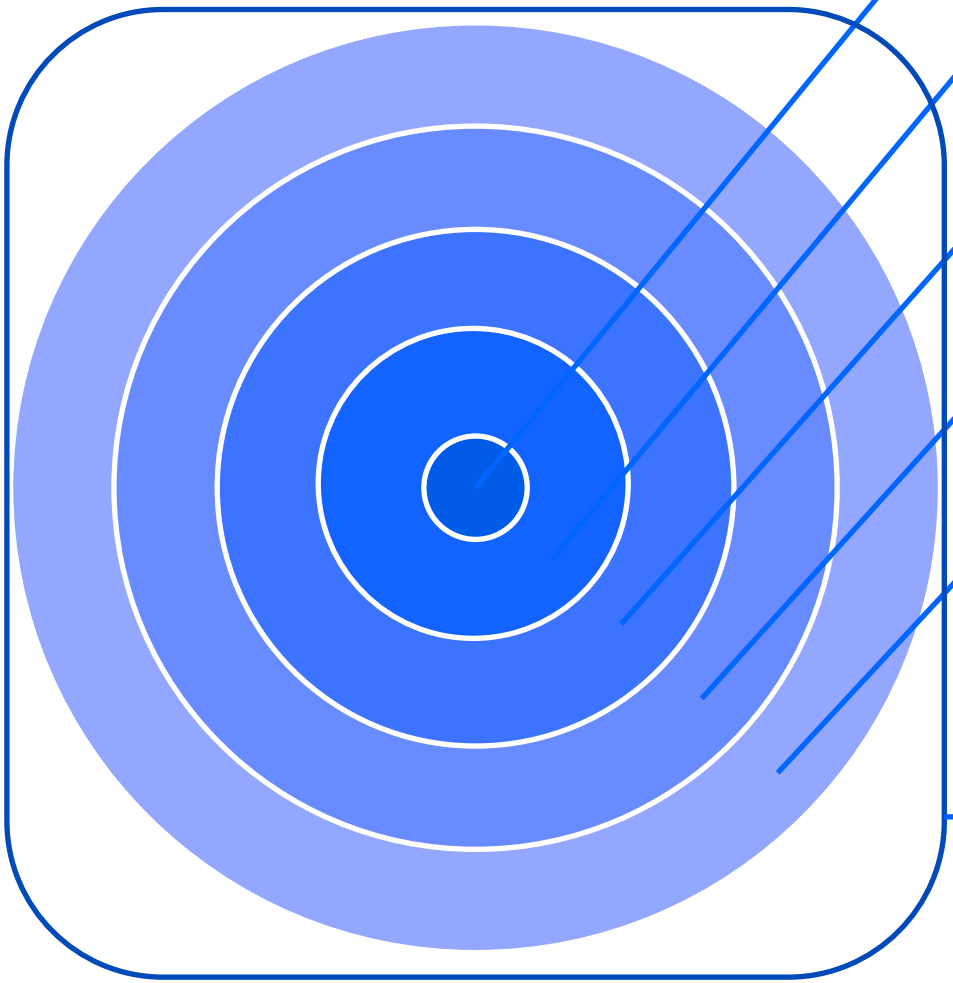
No “silver bullet” when dealing with network security.

No single security solution would make an organization secure.

Multiple levels of protection need to be deployed.

Preventative and detective measures needed.

Defense in Depth



Data

Application

Host

Network

Physical

Policies, Procedures & Awareness

Your Computer is not your own

Do you lock your doors at night to keep out burglars?

Does your car have an alarm system?

And yet, every day, when you turn on your computer, you leave yourself vulnerable to online criminal activity.

Threat Overview

Malicious Web Scripts

Pop ups

Cookies

Spyware

Adware

Home Page Hijackers

Viruses

Worms

Trojan Horses

Backdoor Programs

Keyloggers

Spam

Phishing Attacks

Network Threats

Mobile Threats

Ransomware

Your Computer is not your own

Because of this, you need to arm yourself with the right tools and knowledge to fight back.

During the course of this module, you'll learn how to kill spyware, fight spam, block intruders, protect your wireless and wired home network, stop scammers in their tracks, and more.

Software alone can never do the job!

Malware and anti-malware software are in an escalating arms race

Where you are vulnerable

Booting Up Your Computer

- Turn on your computer. What could be less dangerous?
- Unfortunately, you're in danger as soon as your computer starts to boot.
- If you are infected then the malware may start up automatically when you turn on your computer.

And if it does, it'll start without your knowing it.

Where you are vulnerable

Windows Registry

- The Windows Registry is, in essence, a large database that contains all the information about how Windows is supposed to work on your computer.
- It includes entries that determine how programs run, when they should run, what they should do when they run, and so on.
- Many malware, notably spyware and home page hijackers, run invisibly without your knowledge.
- Because the Registry is made up of so many entries, and is so difficult to understand, it's hard to examine to find out whether malware has invaded your system.

Where you are vulnerable

Connecting to the Internet

- Regardless of how you connect to the internet, this connection causes all your problems.
- After all, malware doesn't start off living on your computer, it gets there because you've gone online at some point.
- Simply connecting to the Internet makes you exceedingly vulnerable to attack.
- When you connect to the Internet, you connect through virtual "ports " that use the TCP/IP protocols that form the underlying basis for all Internet communications.

Where you are vulnerable

- Unfortunately, intruders and malware can use these ports without your knowledge.
- Often, malware authors probe your ports to see whether specific ports are open.
- Other kinds of Trojans use randomized ports and receive instructions via IRC channels—a kind of Internet chat technology.

Where you are vulnerable

Checking Your Email

Spam

Phishing

Where you are vulnerable

Using Instant Messaging

- Malware can spread via instant-messaging programs in a variety of different ways.
  - Instant-messaging worms have become increasingly popular. They work much like email worms, by taking over the buddy list of an instant-messaging program, sending out instant messages to everyone on the list, and asking them to click a link.
- Spyware
- Keyloggers
- Trojans

Where you are vulnerable

Sharing Files

- Lots of people use file-sharing program. And lots of people get infected with spyware.
- There are many reasons why you want to share files with others.
  - Trade music files.
  - Home network sharing

Your risky activites

Do you regularly check for software updates?

Do you use IM or filesharing?

How long had you your computer before you installed AV?

An Inside Look at where you are vulnerable

When you unpack and plug in your Computer, it's free of malware—no home page hijackers, viruses, back-doors, or Trojans.

But the moment you connect to the Internet, visit a web page, or receive email, they start trying to worm their way into your system.

Ram and System Resources

- Spyware and other malware run in the background. They hoard RAM and system resources, and slow down the computer.

File system and Hard Disk

- Malware installs dozens of unneeded files and clog the hard disk.

An Inside Look at where you are vulnerable

CIT

Browser Home Page

- A home page hijacker reroutes the home page to a unsavoury site. Every time you change your home page, it gets hijacked again.

Cookies

- Malware can place tracking cookies on your hard disk, allowing websites to track and log your surfing activities.

Spyware

- Spyware, installed during a "drive-by download," reports on your surfing activities to a web server.

An Inside Look at where you are vulnerable

CIT

Pop-up Swarms

- Spyware infects the system and delivers swarms of pop ups whenever you visit the Web.

Browser Favorites

- Malware adds new Favorites, including links to unsavoury web sites, to the Favorites list.

Windows Registry

- The Windows Registry is filled with dozens of references to spyware, Trojans, and other pests, launching them automatically on startup. The clogged-up Registry slows down your system.

An Inside Look at where you are vulnerable

CIT

Keyloggers

- A keylogger installed on the computer watches every keystroke you make and then sends a log to a remote user, who can monitor everything you do on your Computer.

Viruses

- Viruses infect the system when you click an attachment in an email. At the moment, they're still replicating and have yet to spring into action, but they are gradually slowing down your system. When they do their dirty work, they will delete important system files from your computer.

An Inside Look at where you are vulnerable

Backdoors and Trojans

- Backdoors have been installed on your Computer, and when intruders scan your system for open ports, they are able to connect to those backdoors and take complete control of your computer.

Worm Infestation

- A worm infects a computer network.
- An email worm infects Outlook and mails copies of itself to every person on the Outlook contact list.

An Inside Look at where you are vulnerable

"Bot" Attacks

- Bots have been planted on your Computer. When someone wants to attack a website using a denial of service (DoS) attack, he/she sends a command to the bots on your Computer, and they all begin transmitting messages to a web site, trying to flood it with so much traffic that it can no longer function.

Web Beacon

- Emails sent to you contain web beacons, also called web bugs, which can then be used to tell someone whether you've read the email, report on how long you've spent reading the email, and whether you've clicked on any links in the email.

An Inside Look at where you are vulnerable

Ransomware

- Ransomware works by taking control of your system and holding your information hostage until you pay the ransom to your attackers to get your data back. Ransomware is one of the most blatant and obvious criminal money-making schemes out there.

Home Network Intruder

- A war driver, with a wirelessly equipped laptop and special software, parks outside your home and jumps on your wireless network. He uses all its resources, steals its bandwidth, and reads all the files on your Computers, including personal and financial information.

Optional Further Reading

Visualisations:

- Visualisation of World's Biggest Data Breaches
- Kaspersky Threat Map

Articles:

- Biggest Data Breaches of 21st Century
- Smart Toilets