UNIVERSITY OF WESTMINSTER

CyberSecurity and Forensic

4COSC003W - Trends in Computer Science

Dr Ayman El Hajjar

December 14, 2022

School of Computer Science and Engineering
University of Westminster

OUTLINE

1. What is Cyber Security
2. Cyber Security challenges
3. Cyber Threats
4. Digital forensics
5. Ethics & Legal aspects
6. Careers

Who am I

- 15 years experience in Cyber security and forensics
- Head of Cyber Security research group
- Course leader MSc Cyber Security and Forensics
- Research focus:
  - Research security of the Internet of Things and smart cities
  - Cryptography algorithms for low power systems
  - Blockchain security.
- Supervise several PhD students
- Director of research for several KTP and governmental projects

Contact

- Email: a.elhajjar@westminster.ac.uk
- Twitter: @azelhajjar

What is Cyber Security

Defining Security

A brief definition

- Security is ensuring that only authorised people can perform authorised actions, without interference from others and without risk of data interception.

- The security of a system, application, or protocol is always relative to
  - A set of desired properties
  - An adversary with specific capabilities

Security Definition

- What is Computer Security?
  - The protection of computing systems and the data that they store or access, including defense against attack, interference, espionage, etc.
- Why is Computer Security Important?
  - Enable people to carry out their jobs, education, and research.
  - Support critical business process.
  - Protecting personal and sensitive information.

WHY CYBER SECURITY IS IMPORTANT?

Why do I need to learn about Computer Security?

- 2020 Cyber Crime statistics
  - In 2020, the UK Office for National Statistics conducted a survey on 1348 businesses. The findings were shocking:
    - Almost half of businesses (46%) and a quarter of charities (26%) reported having cyber security breaches or attacks in the last 12 months.
  - in the previous year there had been 5.1 million cases of fraud and cybercrime in England and Wales alone.
  - The upshot of this is that most people in the UK are now far more likely to be the victims of cybercrime than good old-fashioned burglary.

CYBER SECURITY IN THE WIDER CONTEXT

- Cyber security overlaps with several other aspects of security, and Figure below shows these relationships pictorially:

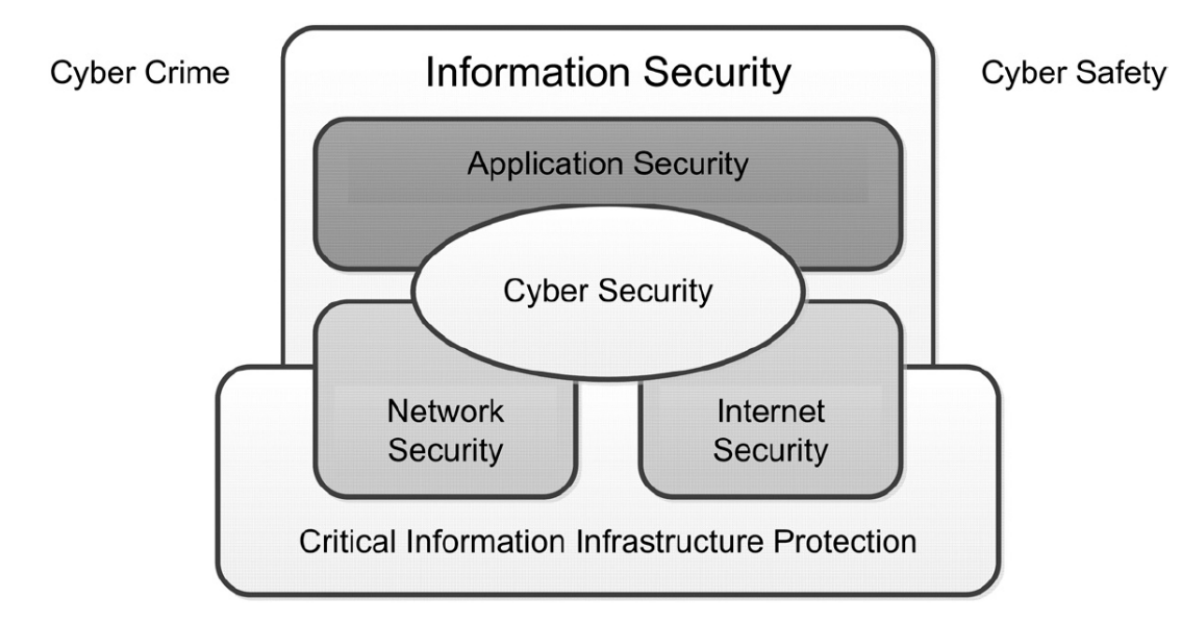


Figure 1: Relationship between security domains [1]

CYBER SECURITY GOALS- PROTECTING ASSETS

- Cyber Security is about protecting assets
- This can be private data, business and commercial data or military secrets.
- Assets examples :
  - Customer Data
  - Private data such as photos and documents
  - IT and network infrastructure
  - Intellectual property
  - Services availability and productivity
  - Reputation

SECURITY GOALS

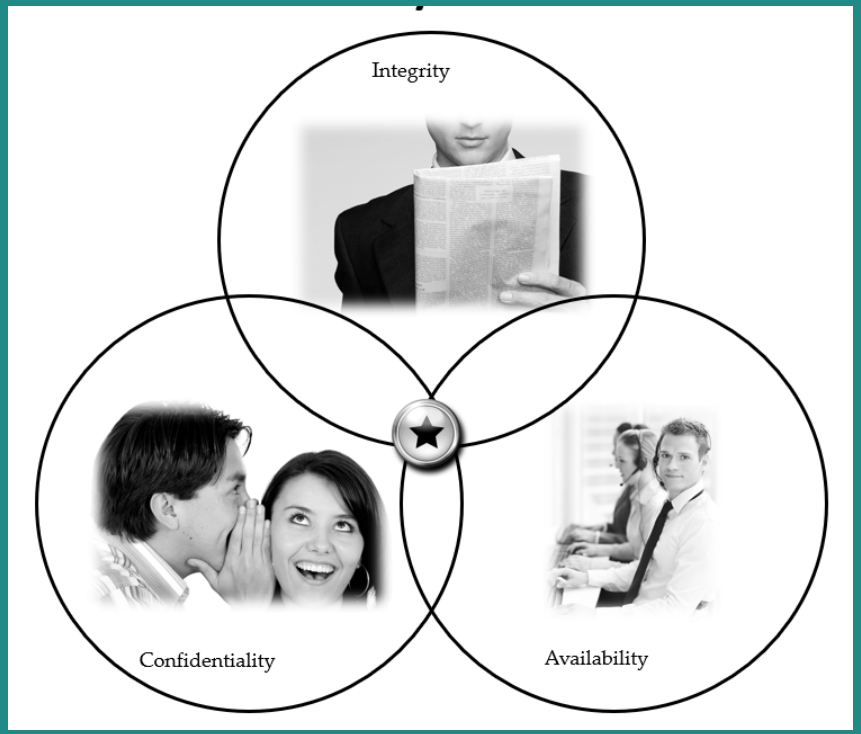
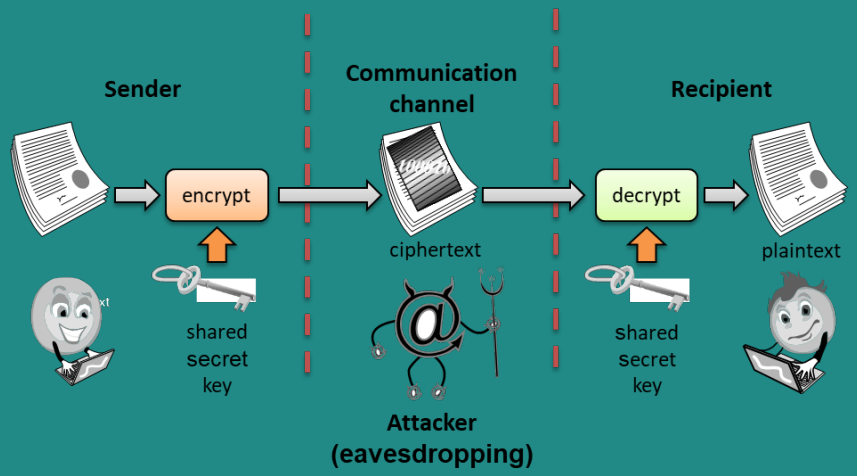


Figure 2: CIA Tenets

- Protect the confidentiality of data
- Preserve the integrity of data
- Promote the availability of data for authorized use

GOAL: CONFIDENTIALITY

- Confidentiality: is the avoidance of the unauthorized disclosure of information.
  - Privacy of personal financial/health records,military records, commercial records, etc.
- Tools for Confidentiality examples
  - **Encryption**: the transformation of information using a secret. Only recipient can understand it
  - **Access control**: rules and policies that limit access to confidential information



GOAL: INTEGRITY

- **Integrity:** the property that information has not be altered in an unauthorized way.
  - Integrity models Maintain valid, uncorrupted, and accurate information
  - Integrity models keep data pure and trustworthy by protecting system data from intentional and accidental changes
  - A loss of integrity is the unauthorized modification or destruction of information.
- Tools for Integrity examples
  - **Backups**: the periodic archiving of data.
  - **Checksums**: the computation of a function that maps the contents of a file to a numerical value.

GOAL: AVAILABILITY

- **Availability**: the property that information is accessible and modifiable in a timely fashion by those authorized to do so.
- Availability models keep data and resources available for authorized use, especially during emergencies or disasters.
- Tools for Availability examples
  - **Physical protections**: infrastructure meant to keep information available even in the event of physical challenges.
  - **Computational redundancies**: computers and storage devices that serve as fallbacks in the case of failures.

Cyber Security challenges

Principles of Information Security

1. There Is No Such Thing as Absolute Security
2. CIA Security Goals should be addressed
3. Security Controls Are Preventative, Detective, and Responsive
4. Users are the weakest link
5. Computer Security Depends on Two Types of Requirements: Functional and Assurance
6. Defence in Depth as Strategy should overlap between all elements of security assets
7. Security Through Obscurity Is Not an Answer
8. Complexity Is the Enemy of Security
9. People, Process, and Technology Are All Needed to Adequately Secure a System or Facility
10. Open Disclosure of Vulnerabilities Is Good for Security!

Anatomy of an Attack

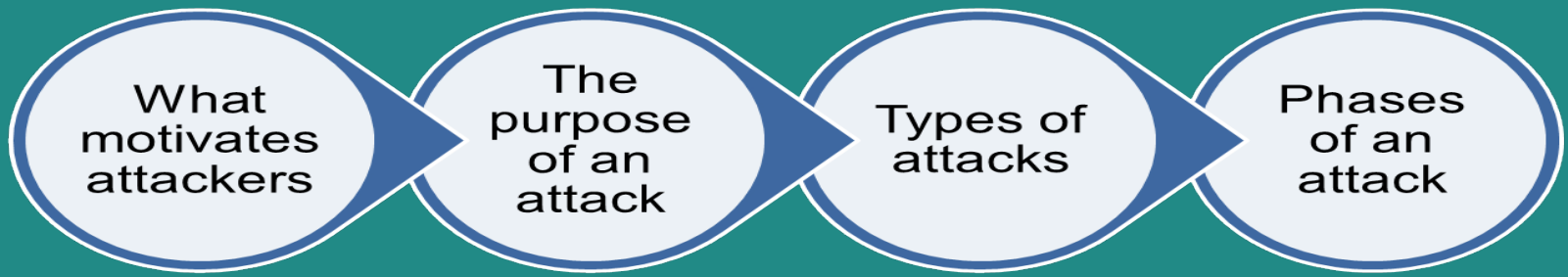


Figure 3: Anatomy of an Attack [3]

WHAT MOTIVATES ATTACKERS?

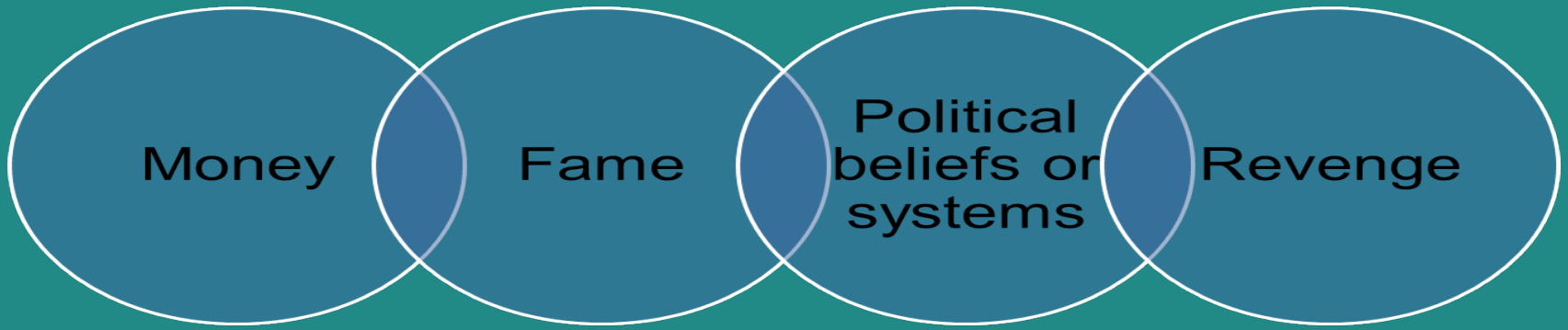


Figure 4: Motivation of attacks [3]

CYBER SECURITY AND COVID - AN EXAMPLE

The great lockdown, a reality check

- Changing environment: Working from home
  - Security environment focus shifted
  - Some conventional security measures became ineffective

Oppotrunists

- Opportunities: Malicious actors taking advantage
  - Phishing SMS and Emails related to COVID
  - Spoofed websites
  - Attacks on Health services

Types of Intruders/Hackers

- **script kiddie**
  - People who steal resources for their own uses
  - Not very sophisticated
  - Usually unskilled
- **Crackers**
  - Access resources without permission
  - Typically for fun, but maybe other reasons
- **Career criminal**
  - Well-planned attacks
  - Usually for financial gain
- **Military**
  - Done to disable opposing forces
  - Gain strategic advantage

Cyber Threats

Cyber Security Breach

- Any event that results in a violation of any of the CIA security tenets
  - Breaches that compromise confidentiality of private data such as releasing information to unauthorized actors
  - Breaches that compromise the Integrity of data such as the manipulation and alteration of data
  - Breaches that compromised the Availability of services such as interruption of services
- Some security breaches disrupt system services on purpose
- Some are accidental and may result from hardware or software failures

CYBER SECURITY BREACHES AND THREATS

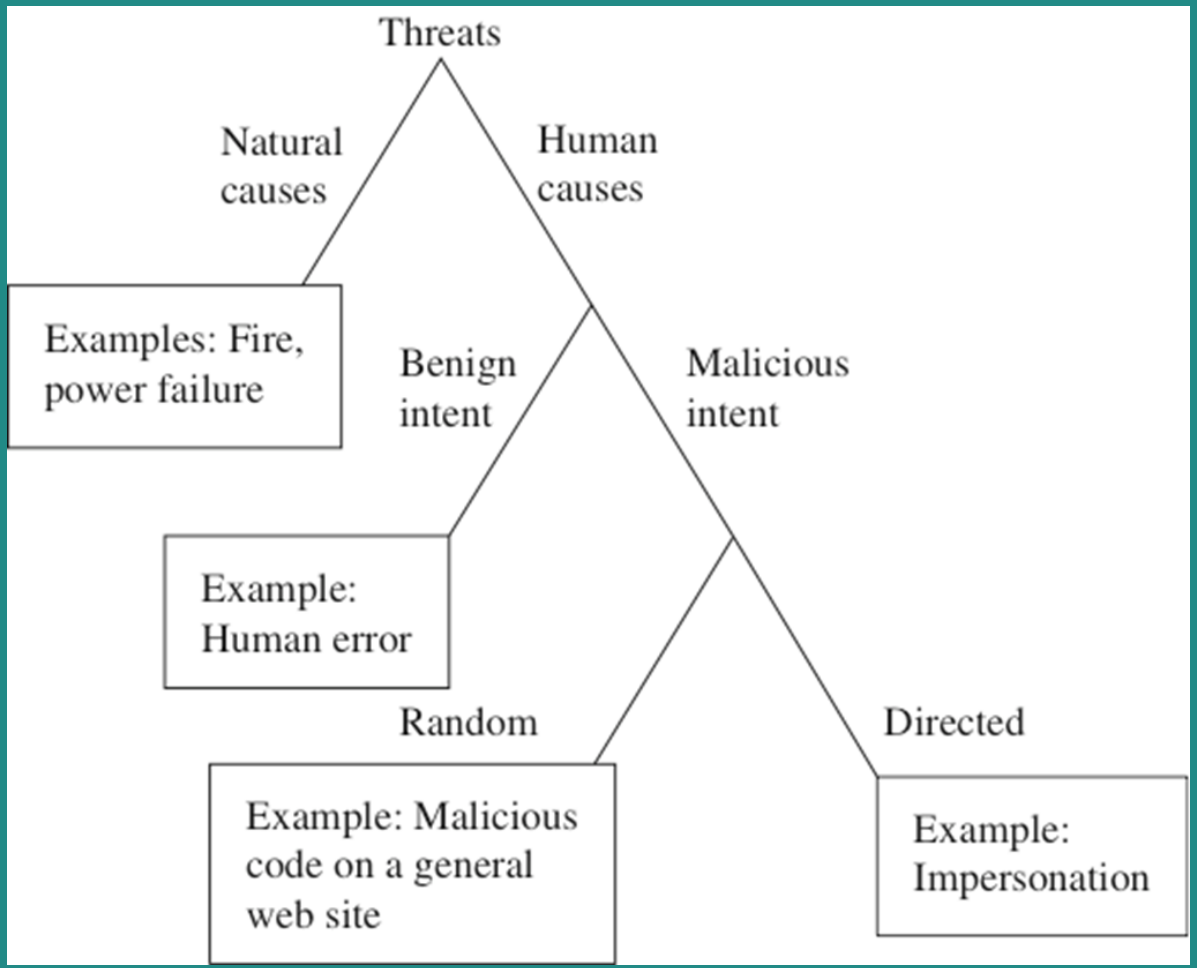


Figure 5: Type of threats [4.]

THE THREAT IS REAL!

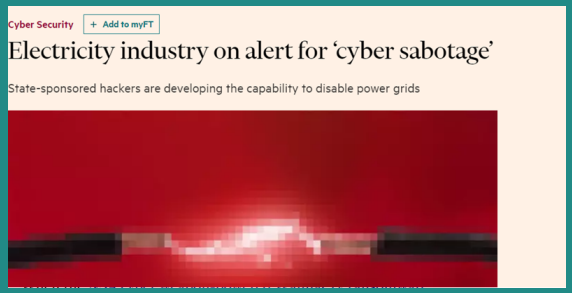


Figure 6: The threats are tangible

THE THREAT IS REAL!

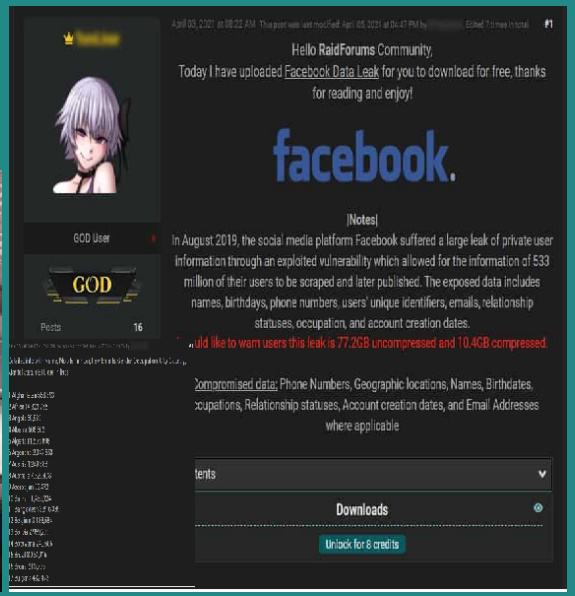


Figure 7: The threats are tangible

CYBER SECURITY ISSUES

- The key cyber security issues that concern us, both as individuals and organisations, regardless of the inherent threats, vulnerabilities or the actual impacts or consequences tend to resolve themselves into one of four areas of cyber security:
  - Cybercrime;
  - cyber harassment or cyber bullying;
  - cyber warfare;
  - cyber surveillance.

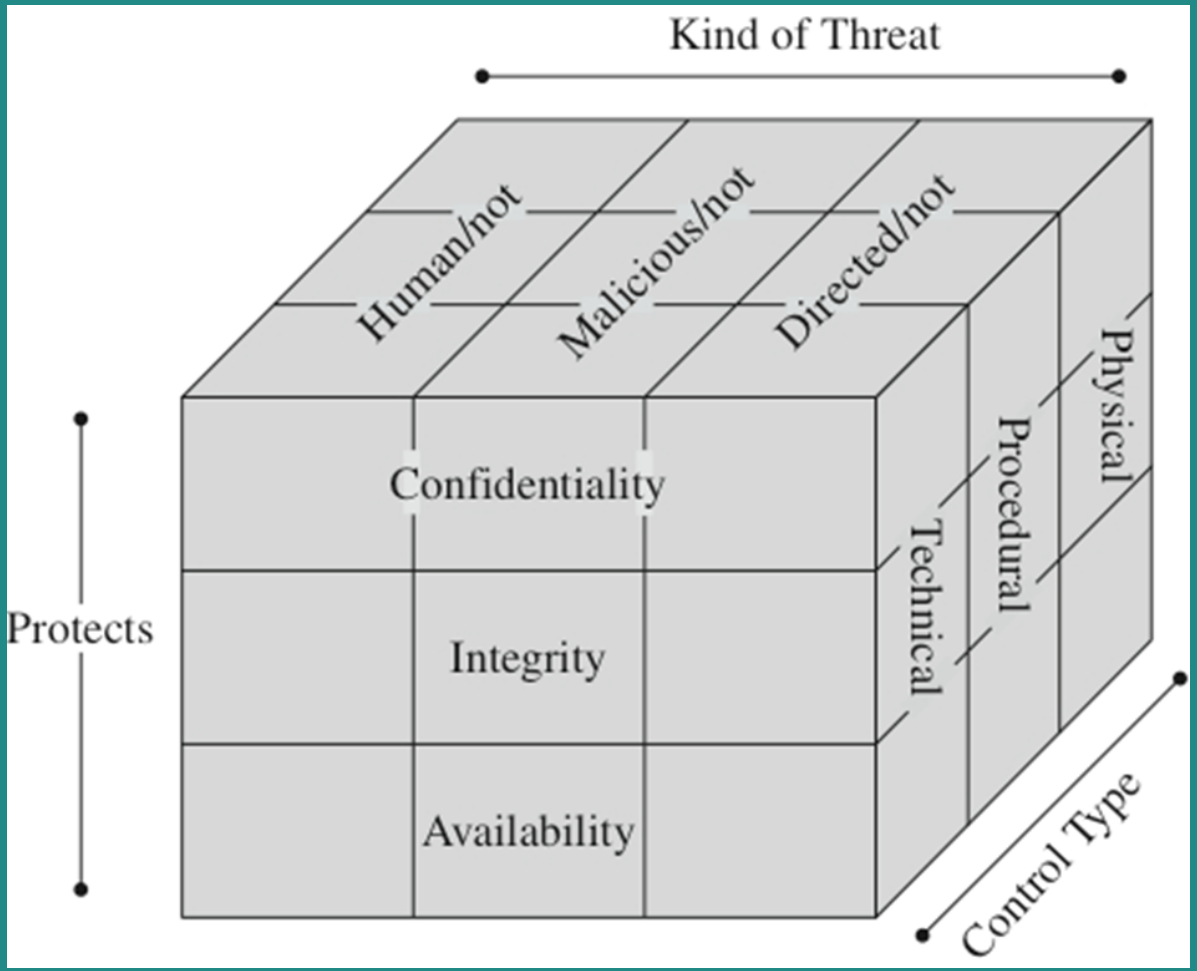
THREATS CLASSIFICATION

- Disclosure
  - Unauthorized access of information
  - Snooping Unauthorized interception of information
- Deception
  - Acceptance of false data
- Disruption
  - Interruption or prevention of correct operation

THREATS CLASSIFICATION EXAMPLES

1. Modification (Alteration)
   - Unauthorized change of information
2. Deception
   - if incorrect information is release as correct
3. Disruption
   - If modified data controls the operation of the system
4. Masquerading (Spoofing)
   - Impersonation of one entity by another
5. Reputation of Origin
   - False denial that an entity sent something
6. Denial of Receipt
   - False denial that an entity received a message
7. Availability
   - Denial of Service

TYPE OF COUNTERMEASURES



GOALS OF COUNTERMEASURES

Prevention

- Prevent attackers from violating security policy

Detection

- Detect attackers violating security policy

Recovery

- Stop attack, assess and repair damage
- Continue to function correctly even if attack succeeds

Digital forensics

Digital Forensics

Digital Forensics Definition

- Scientific process of preserving, identifying, extracting, documenting, and interpreting data on an electronic device
- Computer forensics needs to follow a strict digital forensics framework for it to be used to obtain potential legal evidence

Digital Forensics

Digital Forensics Definition

- Scientific process of preserving, identifying, extracting, documenting, and interpreting data on an electronic device
- Computer forensics needs to follow a strict digital forensics framework for it to be used to obtain potential legal evidence

Digital Forensics and Cyber Security

- Digital forensics looks at:
  - Auditing cyber incidents
  - Investigating a digital device for crime committing.
  - Meeting standards and frameworks

DIGITAL FORENSICS PHASES

- Computer Forensics procedures and Paradigm:
  1. Identification
     - Identify specific objects that store data for the case analysis
  2. Collection
     - Establish a chain of custody and document all steps
  3. Analysis andEvaluation
     - Determine the type of information stored on digital evidence
  4. Reporting
     - Prepare and deliver an official report

IDENTIFICATION

- You are the investigator, which objects do you think will be useful for investigations?
  1. Computer (case and power supply)
  2. Just the hard drive (without computer)
  3. Monitor
  4. Keyboard and mouse
  5. Media (CD, DVD, USB drives, etc.)
  6. Printer
- Digital forensics do not replace traditional forensic analysis
- Any action that modifies the crime scene could invalidate evidence in court

COLLECTION

- To collect computer evidence, care must be taken not to change the evidence
- Imaging media using a write-blocking tool to ensure the suspect device is not be modified
- Establishing and maintaining the **chain of custody**
- Documenting everything that has been done
- Using only tools and methods that have been tested and evaluated to validate their accuracy and reliability

COLLECTION- FORENSIC CONSTRAINTS

- Chain of custody
  - Maintain possession of all objects
  - Must be able to trace evidence back to source
  - “Prove” source integrity
- Priority by volatility
  - Some data is more volatile
  - RAM $\rightarrow$ swap $\rightarrow$ disk $\rightarrow$ External storage (DVD/USB/etc..)
  - Idea: capture more volatile evidence first

Analysis and Evaluation

- Know where evidence can be found
- Understand techniques used to hide or “destroy” digital data
- Toolbox of techniques to discover hidden data and recover “destroyed” data
- Cope with HUGE quantities of digital data. . .
- Ignore the irrelevant, target the relevant
- Thoroughly understand circumstances which may make “evidence” unreliable
- Where is the evidence An example
  - Undeleted files, expect some names to be incorrect
  - Deleted files
  - Windows registry
  - Internet browsing histories
  - Alternate or “hidden” partitions

REPORTING

- Accurately describe the details of an incident
- Be understandable to decision makers
- Be able to withstand legal scrutiny
- Be unambiguous and not open to misinterpretation
- Be easily referenced
- Contain all information required to explain the conclusions
- Offer valid conclusions, opinions, or recommendations when needed
- Create report in a timely manner

REPORTING

Corporation X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Description of evidence:		Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of ___

Figure 8: Computer Forensics Evidence record

Ethics & Legal aspects

ETHICAL HACKERS AND PENETRATION TESTING

Definitions

- **Penetration Testing** A ”simulated attack” with a predetermined goal that has to be obtained within a fixed time
- **Ethical Hacker** Ethical hackers perform penetration tests. They perform the same activities a hacker would but without malicious intent.

- Penetration testing is to test the security of systems and architectures from the point of view of an attacker (hacker, cracker)
- Ethical Hackers work closely with the host organization to understand what the organization is trying to protect, who they are trying to protect these assets from, and how much money and resources the organization is willing to expend to protect the assets.

ETHICS AND LEGALITY

- An ethical hacker does need to understand laws pertaining to hackers and hacking and understand that the most important part of the pretest activities is to obtain written authorization from the person who can approve it.
- No test should be performed without the written permission of the network or service owner.
- Following this simple rule will help you stay focused on the legitimate test objectives and avoid any activities or actions that might be seen as unethical or unlawful.

ETHICS AND LEGALITY

- Ethical hacking should Typically follow a structured approach such as the following to evaluate new regulations that may lead to compliance issues:
  - Step 1. Interpret the law or regulation and the way it applies to the organization.
  - Step 2. Identify the gaps in the compliance and determine where the organization stands regarding the mandate, law, or requirement.
  - Step 3. Devise a plan to close the gaps identified.
  - Step 4. Execute the plan to bring the organization into compliance.

LEGAL NOTES- ILLEGAL HACKING [5.]

- **Hacking for fun and/or notoriety** Conducting hacking activity carried out often by script kiddies against a company or a person without their permission is viewed as an offence under the Computer Misuse Act 1990 “unauthorised access to computer material”.
  - The Computer Misuse Act (1990) is one of the primary pieces of legislation that covers hacking offences, along with other pieces of legislation such as the Data Protection Act 2018.
- **Hacking for political purposes** When a political party resonates with hackers they can often take the law into their own hands.
- **Hacking as part of organised crime** Hacking for profit is an organized crime that has proven extremely lucrative for criminals and the techniques used mean that hackers can often evade law enforcement.

LEGAL NOTES- LEGAL HACKING [5.]

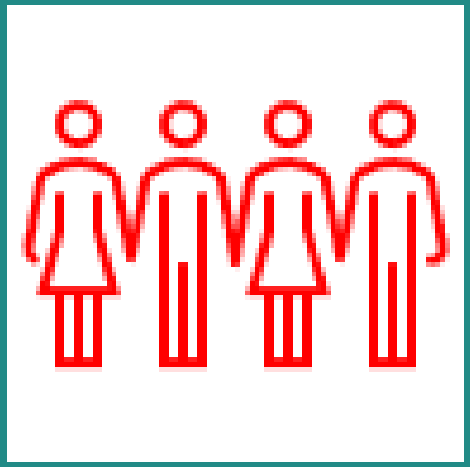
- Legal hacking includes:
  - **Research** This type of hacking consists of passive techniques, which means conducting activity that does not actively impact on a computer, system or service.
  - **Bug Bounty** Many organisations such as Twitter and Facebook offer monetary rewards for vulnerabilities found in their systems.
  - **Professional Penetration Testing** Working as a penetration tester is one of the best legal ways for security professionals to apply their skills and make a career out of hacking.
    - **Web Application Penetration Testing**
    - **Infrastructure Penetration Testing**
    - **Mobile Device and Mobile Application Penetration Testing**

LEGAL NOTES- DIGITAL FORENSICS [6.]

- Modifying evidence on purpose by forensics analysts is a crime by itself
- evidence, to be admissible in court, must be relevant, material and competent, and its probative value must outweigh any prejudicial effect prejudicial effect.
- Digital forensic evidence proposed for admission in court must satisfy two conditions:
  - it must be relevant -arguably a very weak requirement
  - it must be ”derived by the scientific method” and ”supported by appropriate validation.

Careers

CYBER SECURITY CAREERS - TEAMS



Red Team

Blue Team

Purple Team

- Each team carry different set of activities in the field of Cyber Security and/or Digital Forensics.
- All complete each other and large organisations often have all the three teams.

Career in Cyber Security and Forensics

- Security Engineer
- Security Analyst (SOC)
- Security administrator
- Cryptographer/cryptologist
- Source code auditor
- Intrusion detection specialist
- Computer Security incident responder
- Penetration tester / Ethical
- Digital Forensic analyst
- Vulnerability assessor
- Forensics investigator
- Recovery support analyst
- Cyber threats analyst
- Malware analysis
- Foreign disclosure analyst
- Evidence analyst

References and Readings

REFERENCES

- The lecture notes and contents were compiled from:

1. David Sutton, Cyber Security: A practitioner's guide, Published by BCS Learning & Development Limited, 2017
2. https://www.ncsc.gov.uk/information/how-cyber-attacks-work
3. Christopher Hadnagy, Social Engineering: The Art of Human Hacking, John Wiley & Sons, December 2010, Indianapolis, USA.
4. From Analysing Computer Security by Charles P. Pfleeger and Shari Lawrence Pfleeger (ISBN: 0132789469) ©2012 Pearson Education, Inc.
5. Birdwell Consulting, When is hacking illegal and legal February 12, 2019.
6. Daniel Ryan, Gal Shpantzer, Legal Aspects of Digital Forensics , The George Washington University, Washington D.C.