Advanced Network Security
Lecture 1 - Introduction

Dr Rob Hegarty

Attack Map

- https://threatmap.checkpoint.com/ThreatPortal/livemap.html

Introductions

- Dr Rob Hegarty
- Senior Lecturer in Computer Security & Digital Forensics
  - Consulting / Training / Research for GMP
  - Training for Military Intelligence
- Research Interest; Digital forensics, Computer Network Security, Cloud Computing, Social Network Analysis, Signature Detection
- Previous experience
  - Guest lecturer University of Salford
  - Postdoctoral Researcher Liverpool John Moores University
  - Police Trainer (Merseyside, Abu Dhabi, Kuwait)
  - Software Developer (Merseyside Police, Cheshire Police / EU Funded project)
  - PhD Digital Investigations (Cloud Forensics)
  - System Administrator
  - Secondary School Teacher
  - MSc Computer Network Security
  - BSc Software Engineering

Introductions

- Who are you?
- What is your background? (Employment, studies, etc)
- Why did you choose this MSc?
- What do you hope to do on completion of your MSc?
- Give one memorable fact about yourself? (e.g. a hobby, interest, or anecdote)

Aims & Objectives

- Upon completion of this lecture you will be able to:

- Comprehend the unit structure and assessment strategy
- Describe the need for security
- Describe the goals of network security
- Recognise the size of the problem security poses
- Identify who is responsible for security

Overview

- Unit overview
- Unit contents
- Part 1 topics
- Introduction to network security

Unit Overview

- Advanced Network Security
- Lecturers
  - Dr Rob Hegarty – Part 1
  - Dr Thomas Martin– Part 2
- Assessment
  - 50% Coursework (**Presentation 4th April, Report 12th April**)
  - 50% Exam
- Coursework
  - Practical & Report – Deployment of virtual network and demonstration of ethical hacking techniques (Group Based)
- Exam
  - Two sections each containing 3 questions
  - Answer two questions from each section

Suggested Reading

- Pfleeger and Pfleeger, Security in Computing
- Violent Python – T.J O'Connor
- http://www.diveintopython.net/
- The Art of Deception – Kevin Mitnick
- No Place to Hide: Edward Snowdon, the NSA and the Surveillance State – Glenn Greenwald

Unit Contents

- Topics
  - Introduction to network security
  - Network protocol header related security
  - IP Security, IDS and Firewalls
  - Web security & ethical hacking
  - Wireless security
  - Cloud security & recent developments
- Practical / Research Focus

Part 1 Topics

- Introduction to security
- Web security
- Ethical hacking
- Wireless security
- Cloud security
- Recent developments

Lecture & Lab Format (Weeks 1 – 6)

- 2 Hour lecture, with a tea/coffee break after the first hour followed by an in class task (seminar activity)
- 4 Hour lab session, with a tea/coffee/dinner break after the first two hours. This break provides the opportunity to discuss potential project ideas, employability, research, and emerging security issues with the lecturer.

What the course does

- Provides practical and academic experience of assessing the security of a system
- Gives an appreciation of the issues involved in the area
- Suggests tools and techniques that may be used
- Provides an understating of the analytical process
- Presents some emerging research areas in the field
- Focuses on the technical aspects, rather than the legal aspects

What the course doesn’t do

- Qualify you as a penetration tester
- Provide a single methodology that can be followed
- Teach you to analyse information, however it does provides a number of techniques that you may use
- Provide you with all the experience required to conduct a penetration test

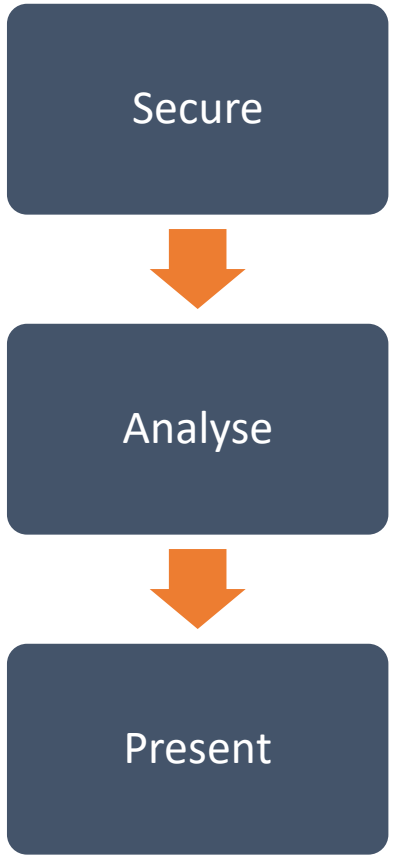
Computer Security vs. Digital Forensics

- Computer security aims to preserve the system state
- Digital forensics aims to identify how a system was compromised and attribute responsibility
- Two areas can be viewed as complementary, however the processes are distinct
- Conflict can arise between security practices and digital forensics (e.g. Encryption)

Digital Forensics Goals

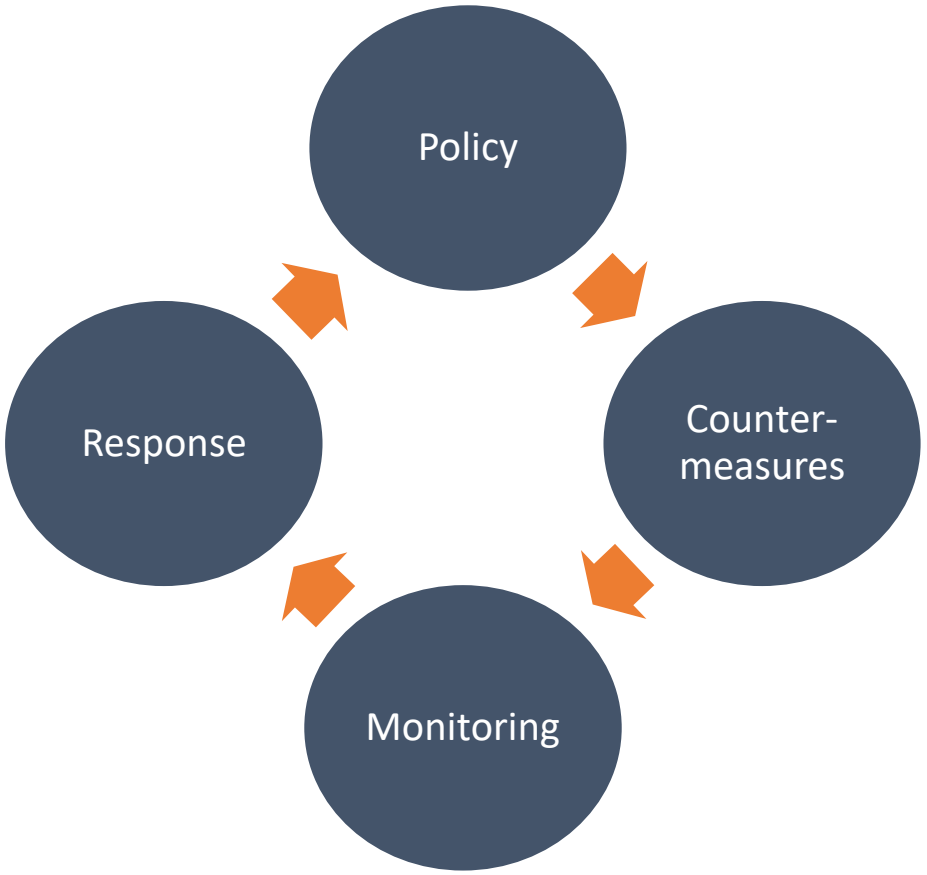
- Identify responsible entity & assign accountability for:
  - Breach of policy
  - Criminal act
- Preserve evidence integrity
- Linear process
  - Secure
  - Analyse
  - Present
- Emphasis on reproducibility

- Intelligence gathering



Computer Security Goals

- Preserve the state of the system
  - Confidentiality
  - Integrity
  - Availability
- Cyclic process
  - Policy
  - Countermeasures
  - Monitoring
  - Response



What is Security?

- Oxford English Dictionary
  - “The state or condition of being or feeling secure”
  - “Freedom from care, anxiety or apprehension; absence of worry or anxiety; confidence in one's safety or well-being.”

What is Security? [2]

- Security is multifaceted
  - Physical –Protection of physical items from unauthorised access or misuse
  - Personal – Protection of the users (employees & users) authorised to access the organisation
  - Operational – Protecting the details of an operation of activity
  - Communication – Protection of communications media (content)
  - Network – Protection of network components (infrastructure)
  - Information – Protection of information

Why do we Need Security?

- Consider vehicle security
  - Central locking
  - Remote locking
  - Alarm
  - Immobilisers
  - Trackers
  - Laser cut keys
- Goals
  - Vehicle theft prevention (Availability)
  - Content protection (Confidentiality, Integrity, Availability)
  - Occupant protection/Car jacking prevention (Integrity)
  - Vandalism deterrent (Integrity)
  - Vehicle recovery (Availability)
- Nothing can provide 100% security, however opportunists can be deterred by countermeasures.

Security for Organisations

- Information is the key to any successful organisation, it provides:
  - A means of efficiently and effectively running an organisation
  - A competitive edge
  - The ability to become/remain profitable
  - A mechanism to deliver products and services to customers
- Organisations, Governments & individuals all have data/information that requires protection
- Due to the importance of information it must be:
  - Available when required
  - Accurate & complete
  - Safe from unauthorised access

Information Characteristics

- The value of information is derived from the following characteristics
  - Availability – Information is available as and when required by authorised users.
  - Accuracy – Information is free from errors or mistakes, has not been intentionally or unintentionally modified to introduce inaccuracies
  - Authenticity – Information genuine, the provenance of the information can be validated
  - Confidentiality – Information is only disclosed to those authorised to view it
  - Integrity – The accuracy and completeness of the information is preserved
  - Utility – Information has inherent value for a specific purpose
  - Possession – Control or ownership of information

In Class Task

- Document your experience of computer security to date.
- Describe what motivated you to undertake this course.
- Research the various aspects of computer security online, describe which area of security is of particular interest to you e.g. Ethical Hacking, Cryptography, Information Assurance, etc
- Review the news story at the link below, and consider:
  - What are the main points?
  - What are the implication?
  - How would you explain the issue to a layperson?
  - https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-every-modern-processor-has-unfixable-security-flaws/

Security Concerns

- Network monitoring (Sniffing traffic to steal credentials/sensitive information)
- Exploitation of vulnerabilities
- Unauthorised access (leading to disclosure, modification, destruction of resources)
- Masquerading by users or systems
- Malicious code
- Message forgery
- Flooding attacks to prevent access to resources
- Use of compromised system to attack other systems

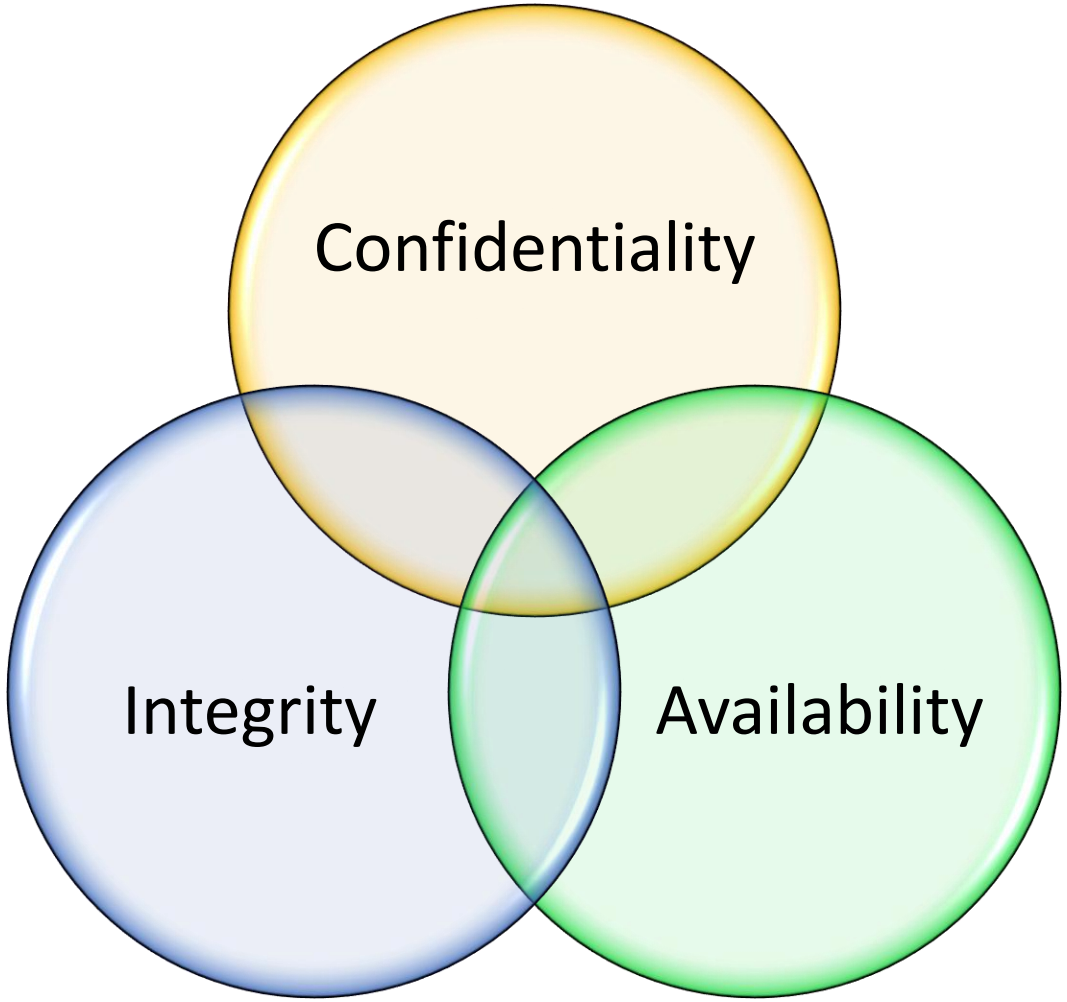
Need for Security - Timeline

- 100 B.C (Approx.) Julius Caesar (Roman Emperor)
  - Used Caesar cipher to encrypt communications (displacement cipher)
- 1920's Enigma machine
  - Used from 1920 and most notably by the Germans in WW2
- 1960's APRANET
  - Advanced Research Projects Agency Network, Early Packet Switched Network, First TCP/IP Network
- 1970's APRANET grows in popularity
  - Potential for misuse increased
  - Fundamental security problems identified
    - End points not secure from unauthorised access
    - Password structure vulnerable
    - No user identification of authentication

Need for Security

- 1980's UNIX OS Security (Bell Labs Grampp & Morris, 1984) (http://tinyurl.com/pegnfy8) (**Computer Security as we Know it**)
- 1990's WWW and Internet, millions of users online
- 2000's Mobile Internet and wireless
- 2005+ Cloud Computing, Internet of Things

CIA - Security Goals



CIA - Descriptions

- Confidentiality
  - Restricting Access
    - To those authorised to access a resource
    - Preventing access by unauthorised users
- Integrity
  - Preserving
    - The accuracy and completeness of data
    - Preventing authorised modification
- Availability
  - Ensuring a resource is available when required

Confidentiality

“EPIC” fail—how OPM hackers tapped the mother lode of espionage data

Two separate "penetrations" exposed 14 million people's personal info.

by Sean Gallagher - Jun 22, 2015 3:30am BST

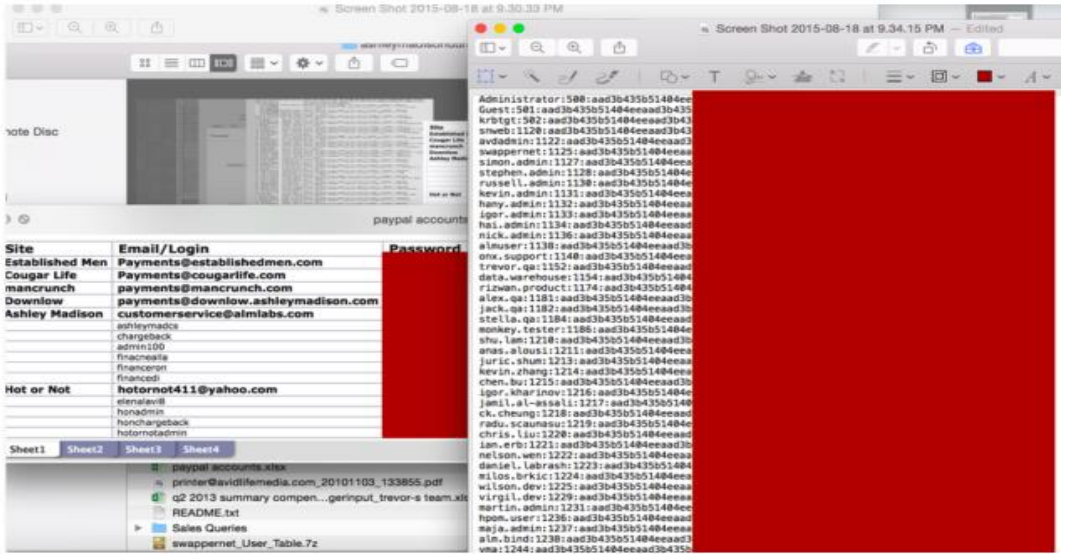
Share Tweet 135

Ashley Madison hack is not only real, it’s worse than we thought

Intimate data for more than 30 million accounts, keys to Windows domain published.

by Dan Goodin (US) - Aug 19, 2015 9:02am BST

Share Tweet 385



Source: www.arstechnica.com

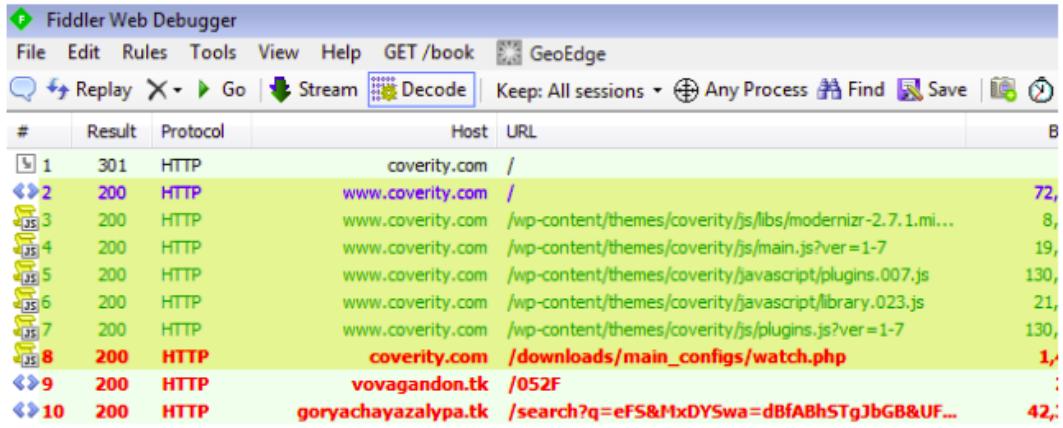
Integrity

Active malware campaign uses thousands of WordPress sites to infect visitors

15-day-old campaign has spiked in past 48 hours, with >5,000 new infections daily.

by Dan Goodin - Sep 18, 2015 5:03am BST

Share Tweet 59



Malware infecting jailbroken iPhones stole 225,000 Apple account logins

Some targeted phones also held for ransom, researchers say.

by Dan Goodin (US) - Aug 31, 2015 7:40pm BST

Share Tweet 174

Source: www.arstechnica.com

Availability

Grinches steal Christmas for Xbox Live, PlayStation Network users

Hacker group knocks gaming networks offline with DDoS attack.

by Eric Bangeman - Dec 26, 2014 1:05am GMT

Share Tweet 178

UK's National Crime Agency hit by Lizard Squad DDoS

NCA slammed by DDoS for 2 hours in fit of pique—or possibly as ad for new service.

by Sean Gallagher (US) - Sep 1, 2015 3:51pm BST

Share Tweet 45

Source: www.arstechnica.com

Concepts & Terminology

- Threats, Vulnerabilities, Risks
  - Threats: Possible attack vectors
  - Vulnerabilities: Weaknesses that could be exploited
  - Risks: Possibility of a security breach, and severity of resultant damage
- Trade-offs
  - Security = Constraints on functionality/operational properties
  - Which in turn impacts system usability/ease of use
- Non-Repudiation (of origin)
  - Proving a message was sent by the person claiming to send the message
  - Digital signature used

Security is a Significant Problem

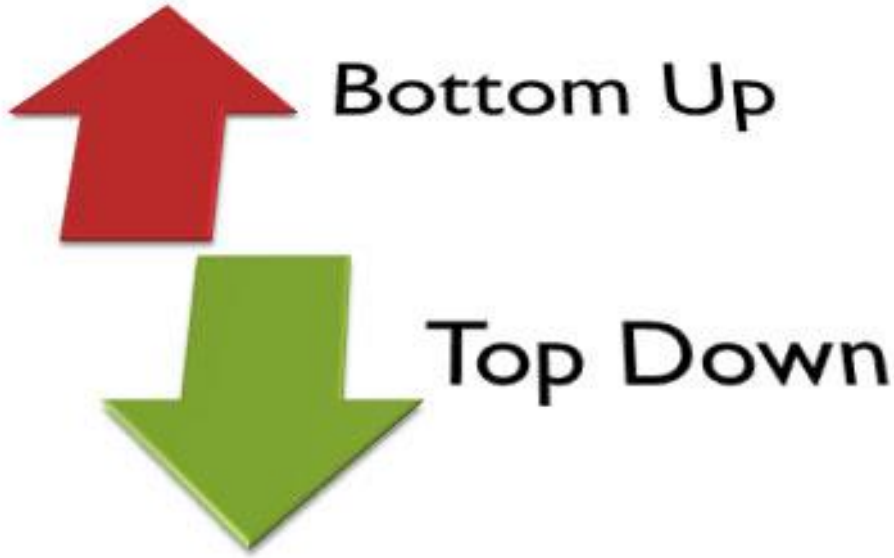
- Even large well resourced organisations fail at security
  - http://tinyurl.com/lgyx9lc
- The number and scale of data breaches reported is growing annually

Types of Attacker

- Diverse set of goals and approaches
- Amateur/Layperson
  - Most frequent offenders
  - Determine there is a weakness in a system they observer or are part of
- Hacker (Cracker not coder)
  - Students / Computing enthusiasts
  - Attempting to gain access without permission
  - Enjoy the challenge
- Career Criminal
  - A computing professional, using their skill set to engage in criminal activity
- State Sponsored
  - Well resourced
  - Aiming to improve situational awareness
  - Used for offense/defence

Security Responsibility

- EVERYONE should be responsible for security
- Security responsibility ideally falls into three main groups
  - Senior management
  - Project teams
  - Users
- BYOD makes this well established approach even more relevant



Security Approaches – Bottom-Up

- Driven by people at the coal face (e.g. system administrators*)
- Goals – Maintain system, Secure system
- Advantages – Understanding of the technical challenges, implications, and potential solutions.
- Disadvantages – Participant support, influence over management, inability to directly set and enact policy, ad-hoc reactive approach

- * Full disclosure, this was my role in the past

Security Approaches – Top-Down

- Driven by upper management
- Goals – Usability, Ability to determine accountability, Cost reduction, System security
- Advantages – Ability to directly prescribe policy, procedures and processes, formal development strategy.
- Disadvantages – Little understanding of technical issues, conflicting goals

Security Functions

- Four main functions of security in the organisation
  - Protect the organisations ability to function
  - Enables safe operation of applications and services hosted by the organisation
  - Protects data collected and used by the organisation
  - Safeguards technology and media assets the organisation uses

Security Countermeasures

- Various controls can be used to provide security
- A multi-pronged approach is best
- Countermeasures will be discussed throughout the course
- Countermeasures
  - Encryption
  - Software controls
  - Hardware controls
  - Policies and procedures
  - Physical controls

Summary

- Security is long standing problem
- Weak security is detrimental to the organisation or individual
- There are a number of countermeasures that can be used to provide security
- There is no such thing as a 100% secure system

Next Lecture

- Introduction to ethical hacking
- Ethical hacking procurement