University of Southampton

SESA6085 – Advanced Aerospace Engineering Management

Lecture 20

2023-2024

Dr David Toal

Module Recap

- Probability theory
- Capturing uncertainty e.g. PDFs
- The impact of uncertainty e.g. MC, RBD, FTA
- Design in the presence of uncertainty
- Project uncertainty management
- Scheduling & supply
- Business continuity management

- Cyber security

Moving up the business

University of Southampton

The Role of Information Systems

- We discussed at length the processes involved in business continuity management
  - One of the keys steps in the identification and assessment of risks to the business
- In our discussions on supply chain management we came across the concept of a virtual organization
  - An organization with little or no physical infrastructure
  - One which relies heavily on communication etc.
- When discussing collaborative design we saw the importance of effective communication
  - The passing and communication of data between designers

University of Southampton

The Role of Information Systems

- In our earlier lectures we saw the importance of computational models
  - Modelling risk
  - Modelling physics
  - Modelling geometry etc.
- IT plays an enormous role in any modern business
- The successful operation of IT systems is critical for an organisation to operate
- Understanding the risks and how to mitigate against these is therefore quite important

University of Southampton

Cyber Security Management

University of Southampton

Lecture Overview

- This lecture does not attempt to cover the technical details of cyber security
  - For that we need several entire modules!
- Instead, we will use this lecture to make you aware of
  1. What assets we need to protect
  2. How those assets are threatened
  3. How can we counter those threats
- In other words, at a high level how can you mitigate computer security issues

University of Southampton

Computer Security Definitions

- Computer security has three primary objectives/requirements
  1. Confidentiality – data confidentiality and privacy
  2. Integrity – data and system integrity
  3. Availability – systems work promptly and service is not denied to users
- In addition to this we may also include
  - Authenticity – people are who they say they are and are trusted
  - Accountability – traceability of actions

University of Southampton

Challenges of Computer Security

- Requirements for security are relatively simple but the mechanisms required can be complex
- When developing security algorithms/processes potential attacks must be considered
- Procedures used to guard against attack can often be counter-intuitive – elaborate processes may be required to guard against all sources of attack
- Deciding where to use a security mechanism is not trivial
- More than one algorithm is often required and users often need “secret” information e.g. encryption keys. Questions arise around their creation, distribution and protection etc.

University of Southampton

Challenges of Computer Security

- Security is a battle of wits, one that benefits the attacker e.g. the attacker needs to find one hole, the defender must close all such holes
- There is a tendency to view an investment in security as having little benefit until a failure occurs
- Regular, sometimes constant, monitoring is required which can be difficult
- Security is often an afterthought to be incorporated once a system's design is complete rather than integrated from the ground up
- Users can view security as an impediment to efficient use or operation

University of Southampton

Types of Asset

- The field of computer security covers four main assets or system resources

1. Hardware – computers, data storage systems etc.
2. Software – OS, system utilities and applications
3. Data – files and databases including security data e.g. passwords, encryption keys etc.
4. Communication facilities & networks – comms links, routers, bridges etc.

University of Southampton

Vulnerabilities & Threats

- In general, the system can become…

1. Corrupted – it does the wrong thing or gives the wrong answers, this includes the improper modification of data
2. Leaky – someone has access to data that they should not
3. Unavailable – using the system is slow or impractical

- Threats are capable of exploiting vulnerabilities whereas attacks are threats carried out
  - Active attack – an attempt to alter system resources or operation
  - Passive attack – an attempt to learn or use information – there is no impact on system resources
- Attacks can come from inside or outside the security perimeter

Vulnerabilities & Threats

- The following is a useful illustration of threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted USB drive is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

University of Southampton

Countermeasures

- Countermeasures cover any means taken to deal with a security attack
- They generally fall into three categories:

1. Prevention – mechanisms designed to prevent an attack in the first place
2. Detection – mechanisms to detect that an attack is occurring
3. Recovery – mechanisms to recover from the effects of an attack

- It is possible that a countermeasure, if improperly designed, can itself introduce a vulnerability

University of Southampton

Threats & Attacks

- The consequences of attacks can be summarised into four categories

1. Unauthorised disclosure – access to data not authorised for
2. Deception – an authorised entity receives false data
3. Disruption – preventing the correct operation of system or services
4. Usurpation – control of the system by an unauthorised entity

- There are several potential threats/attacks that can result in each of these consequences
  - Let's consider these now

University of Southampton

Unauthorised Disclosure

- Exposure – sensitive data is directly released to an unauthorised entity e.g. an insider releasing credit card info
- Interception – data is accessed as it travels between authorised sources and destinations e.g. access to data packets on a LAN or email traffic
- Inference – indirect access of sensitive data by reasoning or through by-products of communication – does not necessarily mean they have access to the data within the communication e.g. repeated queries to a database
- Intrusion – access to sensitive data by circumventing security

Deception

- Masquerade – access to a system by posing as an authorised entity e.g. learning someone's user ID and password or Trojan horses
- Falsification – false data received by an authorised entity e.g. altering grades
- Repudiation – One entity deceives another by falsely denying responsibility for an act e.g. sending/receiving data

Disruption

- Incapacitation – prevent or interrupt the system by disabling a system component e.g. viruses, worms, Trojan horses
- Corruption – undesirably alters system operation by adversely modifying system functions or data e.g. inserting a backdoor into the system for future access
- Obstruction – interrupts delivery of system services by hindering system operation e.g. disabling comms links or overloading comms traffic

Usurpation

- Misappropriation – assume unauthorised logical or physical control of a system resource e.g. machines used in a denial of service attack
- Misuse – causing a system component to perform a function or service detrimental to system security e.g. disabling of security functions

Security Functional Requirements

- Note that managerial measures play an important role in defining security functional requirements

1. Access control – limiting access to authorised users
2. Awareness & training – risk awareness and technical training
3. Audit & accountability – maintain records to monitor and investigate unauthorised or inappropriate activity
4. Certification & accreditation – assess security controls and plan for their improvement
5. Configuration management – maintaining baseline configurations and inventories

Security Functional Requirements

6. Contingency planning – establish and maintain plans for emergency response
7. Identification and authentication – identify users as a prerequisite to granting access
8. Incident response – establish an incident handling capability – track, document and report incidents
9. Maintenance – periodic and timely maintenance
10. Media protection – protect paper and digital media including limiting access, sanitising or destroy media
11. Physical & environmental protection – protection for physical infrastructure against environmental hazards

University of Southampton

Security Functional Requirements

12. Planning – develop, document and update security plans
13. Personnel security – ensuring individuals in positions of responsibility are trustworthy – ensuring systems are secure after terminations or transfers – formal sanctions for those not following process
14. Risk assessment – periodically assess risk to operations
15. Systems & services acquisition – ensure third party providers provide adequate security measures
16. System & comms protection – monitor, control and protect communications
17. System & information integrity – identify, report & correct information and system flaws, provide protection from malicious code

University of Southampton

Database Security

University of Southampton

Database Security

- Databases are ubiquitous across modern computing e.g.
  - Financial data
  - Phone records
  - Customer and employee information
  - Product information
  - Medical records etc.
- Databases often contain sensitive personal information which may be a treasure trove to criminals, competitors etc.
- If we think back to IT security issues being reported in the news these are often database breaches impacting potentially millions of people
- Database security is therefore very important

University of Southampton

Database Security

- Database security has so far failed to keep pace with our reliance on databases
  - Security processes have not kept pace with the growth in complexity of database management systems – each new option or capability introduces a potential new flaw to be exploited
  - Structured Query Language (SQL) used to interact with databases is very complex – effective security requires a full understanding of SQL vulnerabilities
  - Organisations typically do not have full-time database security personnel – leading to a skills gap
  - Most systems include a mixture of database platforms – the number of different platforms and their interactions results in additional complexity

University of Southampton

Database Protection

- Protection mechanisms for databases can include
  - Firewalls
  - Authentication mechanisms
  - Access control mechanisms
- Database encryption can also be used, however…
  - Management of keys can be complex e.g. ensuring a key gives a user access to only part of the database
  - Encryption can hamper database searching
- The facility housing the servers running the database also requires protection
  - Redundant power supplies, network connections, environmental controls and physical security

University of Southampton

SQL Injection Attacks

- Modern websites dynamically link information requested to databases in the background – queries handled by SQL
- An SQLi attack is designed to send malicious SQL commands to the database server e.g. to extract, delete or modify data
- Such attacks can occur if user input is incorrectly filtered for SQL statements
- Such attacks are fairly common but can come through various different routes – requiring multiple countermeasures
  - Defensive coding – secure coding practice can help greatly reduce the risk of such an attack
  - In addition there are a number of different detection methods e.g. code analysis

University of Southampton

Inference

- We've already touched briefly on inference. This is the process of performing authorised queries to deduce unauthorised information
- This can be an issue when
  - The number of database entries is more sensitive than the individual entries
  - Combinations of data items can be used to infer sensitive data
- There are generally two approaches to detecting inference
  - During database design e.g. altering database structures by removing dependencies
  - At query time e.g. detecting inference channels automatically upon query and denying access

Inference

Item	Availability	Cost ($)	Department
Shelf support	in-store/online	7.99	hardware
Lid support	online only	5.49	hardware
Decorative chain	in-store/online	104.99	hardware
Cake pan	online only	12.99	housewares
Shower/tub cleaner	in-store/online	11.99	housewares
Rolling pin	in-store/online	10.99	housewares

(a) Inventory table

Availability	Cost ($)
in-store/online	7.99
online only	5.49
in-store/online	104.99

Item	Department
Shelf support	hardware
Lid support	hardware
Decorative chain	hardware

(b) Two views

Item	Availability	Cost ($)	Department
Shelf support	in-store/online	7.99	hardware
Lid support	online only	5.49	hardware
Decorative chain	in-store/online	104.99	hardware

(c) Table derived from combining query answers

Real World Examples

- Yahoo (2017)
  - 3 billion accounts but no passwords or payment info stolen
- Aadhaar (2018)
  - 1.1 billion accounts – biometric data including thumbprints & retinal scans
- First American Financial Corporation (2019)
  - 885 million accounts – bank & social security records

University of Southampton

Malicious Software

University of Southampton

Malicious Software (Malware)

- Malware is one of the most significant threats to computer systems

"a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victim's data, applications or OS or otherwise annoy and disrupt the victim"

University of Southampton

Types of Malware

- Some types of malware include:
  - Adware – generates advertising pop-ups
  - Keyloggers – captures keystrokes
  - Spammer programs – used to send large volumes of email
  - Spyware – collects information and transmits it elsewhere
  - Zombie/bot – program activated to launch attacks
  - Virus – when executed attempts to replicate itself
  - Worm – runs independently and propagates itself onto networked machines
  - Trojan horse – hidden function within seemingly useful software

University of Southampton

Potential Malware Payloads

- System corruption - data destruction, ransomware & physical damage
- Zombie/Bots – computing resources for, denial-of-service attacks, spamming, spreading other malware etc.
- Information theft - credential theft, phishing & identity theft, espionage & data exfiltration
- Stealthing – providing covert access to the system
  - Backdoor – secret entry points into a program
  - Rootkit – maintains covert access but with admin privileges – these can also be at the level of the OS kernel

Malware Countermeasures

- Prevention is the ideal solution to malware
  - Patching/updating systems to remove vulnerabilities
  - Assigning access control to applications
  - Awareness and training for social engineering attacks
- If prevention fails then we rely upon
  - Detection – determining that an infection has occurred
  - Identification – identifying the specific malware
  - Removal – remove all traces of the malware from all systems
- If identification and removal fail then the infected files should be discarded and back-ups used
  - Modern antivirus software helps with all of these steps

WannaCry Attack

- Cyber attack carried out May 2017
- Ransomware cryptoworm
  - Encrypted the users machine and demanded bitcoin payment to unencrypt
- The worm spread from machine to machine exploiting a vulnerability in Windows
- Affected 300,000 computers across 150 countries
- NHS particularly affected
- Nissan UK stopped production

University of Southampton

Firewalls

University of Southampton

Firewalls

- Internet access, for the most part, is of benefit to any organisation
- However, such access also enables the outside world to reach and interact with local network assets
  - This naturally represents a threat
- Equipping each individual machine with high-grade security is not really cost-effective or practical
  - Requires aggressive patching and upgrading etc.
  - An issue given 1000s of machines each with different OS etc.
- The firewall is an alternative – sitting between the local network and the wider internet
  - It erects a single barrier around the entire network

University of Southampton

Firewalls Provide…

- A single choke point to keep out unauthorised users and applications thereby simplifying security management
- A location for monitoring security-related events
- A network management function to log or monitor internet usage
- A means of implementing virtual private networks

University of Southampton

Firewalls Can't…

- Protect against attacks which bypass the firewall e.g. direct communications to other organisations bypassing the firewall
- Protect fully against internal threats e.g. a disgruntled employee or someone unwittingly cooperating with an external attacker
- Protect against an improperly secured wireless LAN accessed from outside the organisation
- Protect against laptops, USB drives etc. infected outside of the network and then used internally

University of Southampton

Software Security

University of Southampton

Software Security

- Poorly written software can itself represent a security vulnerability
  - This is a major source of vulnerabilities
- Awareness of the issues improper coding can introduce and steps taken to remedy this are therefore important
- Such software errors are grouped into three categories
  - Insecure interaction between components e.g. direction to untrusted sites
  - Risky resource management e.g. use of a dangerous function or buffer sizing issues
  - Porous defences e.g. missing authentication or encryption

University of Southampton

Defensive Programming

- The process of designing and implementing software so it continues to function even when under attack
- Software written like this can detect erroneous conditions resulting from some attack and
  - Continue to execute safely
  - Or fail gracefully
- The key rule in this approach is never assuming anything, check all assumptions and handle any possible error states
- Security should be addressed from the start of a program's development otherwise it is difficult to achieve

University of Southampton

Defensive Programming

- Typically, programmers focus on success and normal operation, assumptions are therefore made about the type and nature of inputs etc.
  - These assumptions should be checked by the program
- When changes are required, a programmer focuses on those changes and what needs to be achieved
  - Again, the assumptions made here should be checked
- Defensive programming requires an awareness of the consequences of failure
  - Paranoia is a virtue!

University of Southampton

Writing Safe Programs

- Correct algorithm implementation – care should be taken when designing and implementing a program e.g. all variants of the problem are implemented correctly
- Ensuring that machine language corresponds to the algorithm e.g. a malicious compiler
- Correct interpretation of data values, allocation, sharing & release of memory

University of Southampton

Interacting With The OS & Other Programs

- Any program we write does not run in isolation but within an OS where other processes are running with multiple users
- Environment variables e.g. PATH are inherited by child processes
- Appropriate or least privileges – if a program runs with a higher level of privilege this can give an attacker more freedom
- Assumptions of “perfect” standard libraries
- Safe temporary file use – unique and secure
- Assumed data flow between programs
- Output should conform to a standard


University of
Southampton