Lecture 01
Introduction

CMPU-4008

Advanced Security 2

Module Contents

- Authentication Applications
- Electronic Mail Security
- Internet Protocol Security
- Web security
- Intruders, Crimeware, Firewalls
- Security Policies, Standards, Compliance

Module Contents

- Security Metrics and Auditing
- Penetration Testing
- Social Engineering
- Defences to security attacks
- The impact of Technological developments on Security
- Disaster Recovery, Business Continuity

Assessment Methods

- Written examination – 50%

- Continuous assessment – 50%

Continuous assessment – 50%

- Quiz 1 - 10%.
  - Theory Test in week 6.
- Quiz 2 - 10%.
  - Theory Test in week 12 (All lecture material).
- Assignment 1 - 15% (Week5) (Demo in week 5 & week 6).
  - Research on the skills, certifications and training for security expert.
  - Google hacking, Vulnerabilities and Exploits
- Assignment 2 - 15% (Week11) (Demo in week 11 & week 12).
  - Security Tools

Submission guidelines

- Submission guidelines
  - Use Brightspace, no email submission
  - naming files (Full-Name_Student-Number_Assignment-Name)

- Optional Report guidelines
  - Cover page, introduction, body, discussion, conclusion and references

- Marks will be deducted for late submission

Penetration Testing Tools

- **Resources**
- http://www.darknet.org.uk/
- http://holisticinfosec.org/
- https://brightsec.com/blog/penetration-testing-tools/

Tools used for security training

- Seed - http://www.cis.syr.edu/~wedu/seed/
- Sweet - http://csis.pace.edu/~lchen/sweet/
- Security Shepherd - https://www.owasp.org/index.php/OWASP_Security_Shepherd
- There are a lot of Security Gaming software

Essential Reading

- Computer Security: Principles and Practice, 3rd edition, William Stallings and Lawrie Brown (2015), Pearson.

Supplemental Reading

- Cryptography and Network Security : Principles and Practices, 6th Ed, Williams Stallings (2014) Prentice Hall.

- Network Security Essentials: Applications and Standards, 4th Ed, William Stallings (2011), Prentice Hall

References

- Seymour Bosworth and M.E. Kabay, 2009, Computer Security Handbook, John Wiley & Sons. Inc.
- Andrew Lockhart, 2004, Network Security Hacks 100 Industrial-Strength Tips & Tools, O'Reilly
- Markus Jakobsson, Zulfikar Ramzan, 2008, Crimeware: Understanding New Attacks and Defences,Symantec Press.
- Ed Skoudis and Tom Liston, 2006, Counter Hack Reloaded: A step-by-step Guide to Computer Attacks and Effective Defences, Prentice hall
- Bruce Schneier, 2012, Liars and Outliers: Enabling the Trust that Society Needs to Thrive, John Wiley & Sons ISBN: 978-1118143308

Software license

- This software is provided “as is” and any expressed or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the contributor be liable for any direct, indirect, accidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, or tort (including negligence or otherwise) arising in any way out of use of this software, even if advised of the possibility of such damage.

- In plain English what does the above information mean.

Software license

- We don’t claim this software is good for anything– if you think it is, great, but it’s up to you to decide.

- If this software doesn’t work: tough. If you lose a million dollars because this software messes up, it’s you that’s out of million, not us.

- If you don’t like this disclaimer: tough. We reserve the right to do the absolute minimum provided by law, up to and including nothing.

Software characteristics

- We interact with software on daily basis.
- How and when we touch software and how and when it touches us is less our choice everyday.
- The quality of software matters greatly.
- Software is insecure.
- Insecure software is everywhere interconnected and woven tightly into the fabric of civilisation.

Why Software is insecure

- Software is not necessarily designed and constructed with security in mind.

- Internet Explorer is one of many examples of insecure software.

- Lack of security training:
  - Many software developers do not understand the risks that they are exposing their users to by creating poorly written code.

Costs of Insecure Software

- Maintenance :
  - Network administrator has to spend a reasonable amount of his time installing security patches on the company's machines.
- Lack of productivity:
  - When a piece of software is compromised at work, everyone suffers.
- Reduce Bandwidth

Ongoing Platform Battlegrounds

- Web Search
  - Google vs. Bing/Yahoo, foreign engines
- Smart Phone
  - OS Apple vs. RIM, Nokia/Symbian, Android, Microsoft, Palm, Linux, ARM, Intel Atom)
- Digital Media
  - Apple (iPod, iPad & iTunes) vs. Microsoft (Media Player, Zune) vs. Real?
- Social Networking
  - Facebook, Twitter, LinkedIn, etc.

Ongoing Platform Battlegrounds

- Video Games
  - Sony, Nintendo, Microsoft
- Enterprise software
  - SAP vs. Oracle/Sun, Microsoft, IBM
- Micropayments
  - Sony Felica vs. PayPal, credit cards, Apple Pay,
  - Google Wallet, Softcard, CurrentC etc.
- Displays
  - Oled, 4k, Plasma vs. LCD (Sharp, Sony, Samsung, others)

The future of Security threats

- Cyberwar declared – Stuxnet a politically motivated attack (weaponized malware) :

  Duqu, Flame, and Shamoon

- Advanced Persistent Threat (APT) – advanced malware attack

- VoIP attacks – brute force and directory traversal class attacks against VoIP servers

The future of Security threats

- Car hacking – cars are more connected with built-in Bluetooth, 3G internet, GPS, Onstar, and dashboard computers
- The Facebook challenge - users trust of web (Web 2.0, API etc)
- Manufactured-delivered malware – products arriving with infections out of the box

The future of Security threats

- Fighting internet crime does not come cheap.

  For example, Inga Beale, the CEO of Lloyd’s said that Lloyd’s estimates that cyber attacks cost businesses as much as $400 billion a year, including the damage itself and subsequent disruption to the normal course of business.

Cybercrime Knows No Borders

- Prosecuting cybercrime is no easy task.

One of the biggest problems lies with the scope of legislation within a particular country. “There is a tremendous range in the laws – with many countries not having laws covering such simple concepts as unauthorized access to a computer system or installation of malicious software”.

Cloud apps a click away

- Dropbox – http://www.dropbox.com/
- Google Docs- https://docs.google.com/
- Microsoft OneDrive https://onedrive.live.com
- Evernote - http://www.evernote.com/
- GoToMyPC - http://www.gotomypc.co.uk/
- And many more …

Cloud Security Mechanism

- Take responsibility for your own security
- Ring fence your data
- Think about encryption
- Strong passwords for cloud services

Common Sense Security

- Security is not a specialist subject – it’s everyone’s responsibility

- The attackers only have to get lucky once and the defenders have to get it right 100% of the time

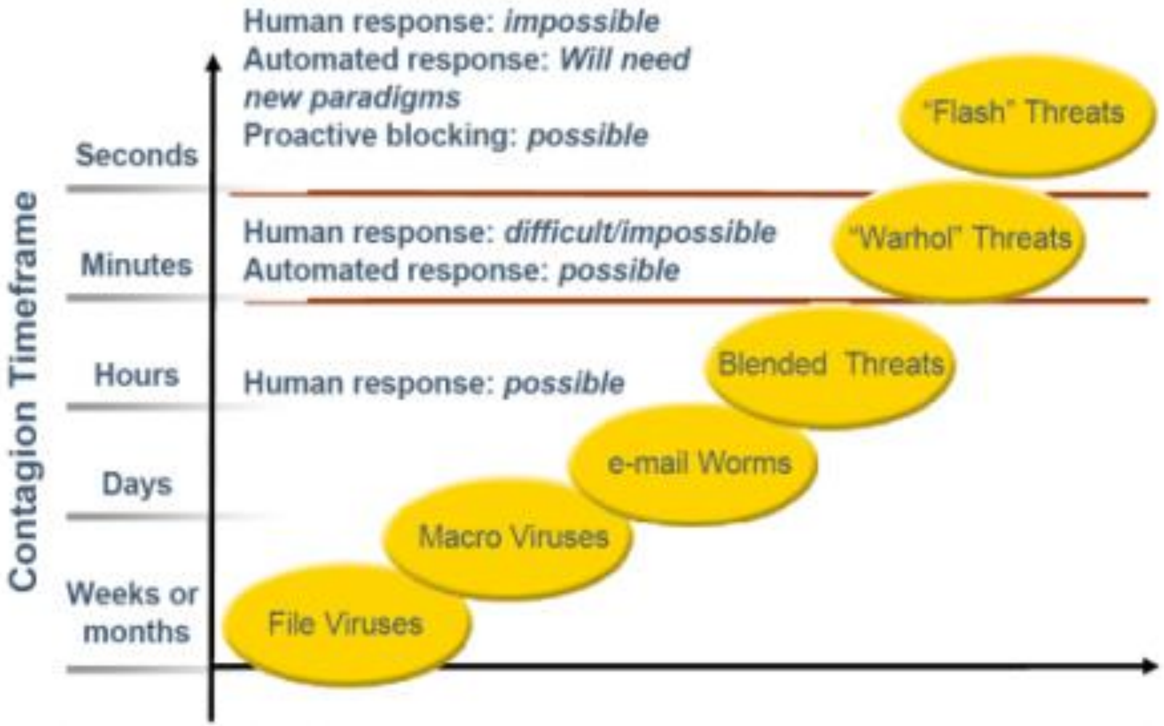
Some Resources on Cloud Security

1. Top Threats to Cloud Computing V1.0, Cloud Security Alliance, March, 2010.
2. Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance,2011.
3. Guidelines on Security and Privacy in Public Cloud Computing, Wayne Jansen and Timothy Grance, NIST, January 2011.
4. Cloud Computing Security: A Survey, Issa M. Khalil , Abdallah Khreishah,Muhammad Azeem, Computers 2014.
5. Overview of Attacks on Cloud Computing, Ajey Singh, Maneesh Shrivastava, IJEIT,2012
6. The Management of Security in Cloud Computing, Ramgovind S, Eloff MM, Smith E, IEEE, 2010

Intruders

- An Intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system.
- Building technical knowledge and skills
- Gaining leverage through automation
- Exploiting network interconnections and moving easily through the infrastructure
- Becoming more skilled at masking their behaviour

Response Time



Human response: *impossible*
Automated response: *Will need new paradigms*
Proactive blocking: *possible*

Human response: *difficult/impossible*
Automated response: *possible*

Human response: *possible*

Vulnerability Trends

- Flaws can be found without source code
  - common: system call trace
  - new: subroutine call trace
  - protocols can be examined for vulnerabilities
  - program instabilities (buffer overflow, etc.)

- Good news — the public & vendors becoming
  - more security conscious
  - Patches now being released via Internet

I am a Developer

- 10 lines of code = 10 issues.

  500 lines of code = "looks fine."

- Code reviews.
  Recent source lines of code (SLOC) reviews and estimates suggest that a very conservative guess would place the number of bugs in most modern software at the rate of about one per 1000 lines of extremely well-written source code with great attention to security detail.
  1000 SLOC = 1 bug (error)

- Source: http://www.techrepublic.com/blog/it-security/thedanger-of-complexity-more-code-more-bugs

Windows: Source Lines of Code (Sloc)

Year	Operating System	Sloc (Million)
1993	Windows 3.1	6
1994	Windows NT 3.5	10
1996	Windows NT 4.0	16
2000	Windows 2000	29
2001	Windows XP	40
2005	Windows Vista Beta 2	50

Linux: Source Lines of Code (Sloc)

Operating System	Sloc (Million)
Red Hat Linux 6.2	17
Red Hat Linux 7.1	30
Debian 2.2	55-59
Debian 3.0	104
Debian 3.1	215
Debian 4.0	283
OpenSolaris	9.

Graphics Programs: Source Lines of Code (Sloc)

Operating System	Sloc (Million)
Mac OS X	86
Linux Kernel 2.6.0	5.2
Graphics Programs	
OpenOffice.org	10
Blender 2.42	1
GIMP v2.3.8	0.65
Paint.NET 3.0	0.13

Air Domain Strategic Context

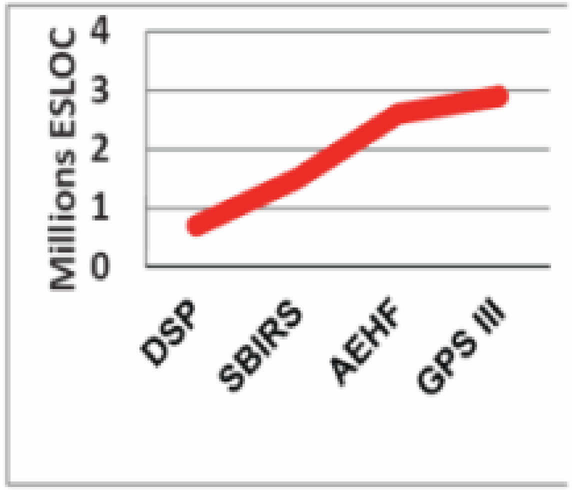


Figure 1b:

Space Systems Software Growth

Source: CMU/SEI

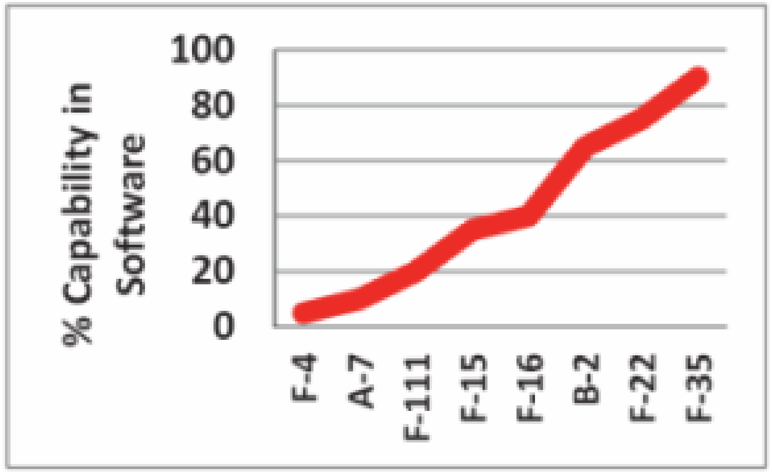


Figure 1a:

Air Platform Software Growth

Source: CMU/SEI and Lockheed Martin

Modernisation Centred Software

- Approximately ninety percent of the functionality in the Joint Strike Fighter (F-35) is dependent upon software (approximately 10 million lines of embedded code on the platform)

- 15 million on the ground-based Autonomic Logistics Information System (ALIS)).

- This contrasts with only five percent in a 1960-era F-4 fighter

Security Threats

- Spyware and Ad ware
- Viruses
- Phishing and Pharming
- Worms, Bots
- SQL injection
- Sophisticated targeted attacks
- Politically motivated attacks (Weaponized malware) - Stuxnet

Security Certification

- Certified Information System Security Professional (CISSP)

  https://www.isc2.org/Certifications/CISSP

- Cisco Certified Security Professional (CCSP)

  https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/security.html#~security-certifications

- Certified Ethical Hacking (CEH)

  https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

It’s going to get worse - 1

- Explosive growth of the Internet continues
  - continues to double in size every 10-12 months
  - where will all the capable system administrators come from?

- Market growth will drive vendors
  - time to market, features, performance, cost are primary
  - “invisible” quality features such as security are secondary

It’s going to get worse - 1

- The death of the firewall
  - traditional approaches depend on complete administrative control and strong perimeter controls
  - today’s business practices and wide area networks violate these basic principles
    - no central point of network control
    - more interconnections with customers, suppliers, partners
    - more network applications

It’s going to get worse - 1

- Beware of snake-oil
  - the market for security products and services is growing faster than the supply of *quality* product and service providers
  - sometimes the suppliers don’t understand Consumer needs

Before it gets better - 1

- Strong market for security professionals will eventually drive graduate and certificate programs.
- Increased understanding by technology users will build demand for quality security products; vendors will pay attention to the market.
- Insurance industry will provide incentives for improved business security practices.

Before it gets better - 1

- Technology will continue to improve and we will figure out how to use it
  - Encryption
  - strong authentication
  - survivable systems
- Increased collaboration across government and industry.

Sensible Security

- All security involves trade-offs
- Security trade-offs depend on power and agenda
- Security is a process and not a product
- Security is a game a never ending one

How Security Works

- You need to know systems and how they fail.
- Know the attackers
- Attackers never change their tunes, just their instruments
- Technology creates security imbalances
- Security is a weakest-link problem
- Security evolves around people
- Detection is useless without response
- Identification, authentication and authorization
- All countermeasures have some value, but no countermeasure is perfect

Computer Security

- The process of preventing and detecting unauthorized use of your computer.
- Attain the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

Key Security Concepts

- Confidentiality
- Integrity
- Availability

Level of Impact

- can define 3 levels of impact from a security breach
- Low
- Moderate
- High

Examples of Security Requirements

- Confidentiality – Student grades, Student enrolment, Staff Directory
- Integrity – patient information, Website Forum, Online poll.
- Availability – Bank authentication service, University Website, telephone directory

Computer Security Challenges

- Not simple
- Must consider potential attacks
- Involve algorithms and secret info
- Must decide where to deploy mechanisms
- Battle of wits between attacker / admin
- Requires regular monitoring

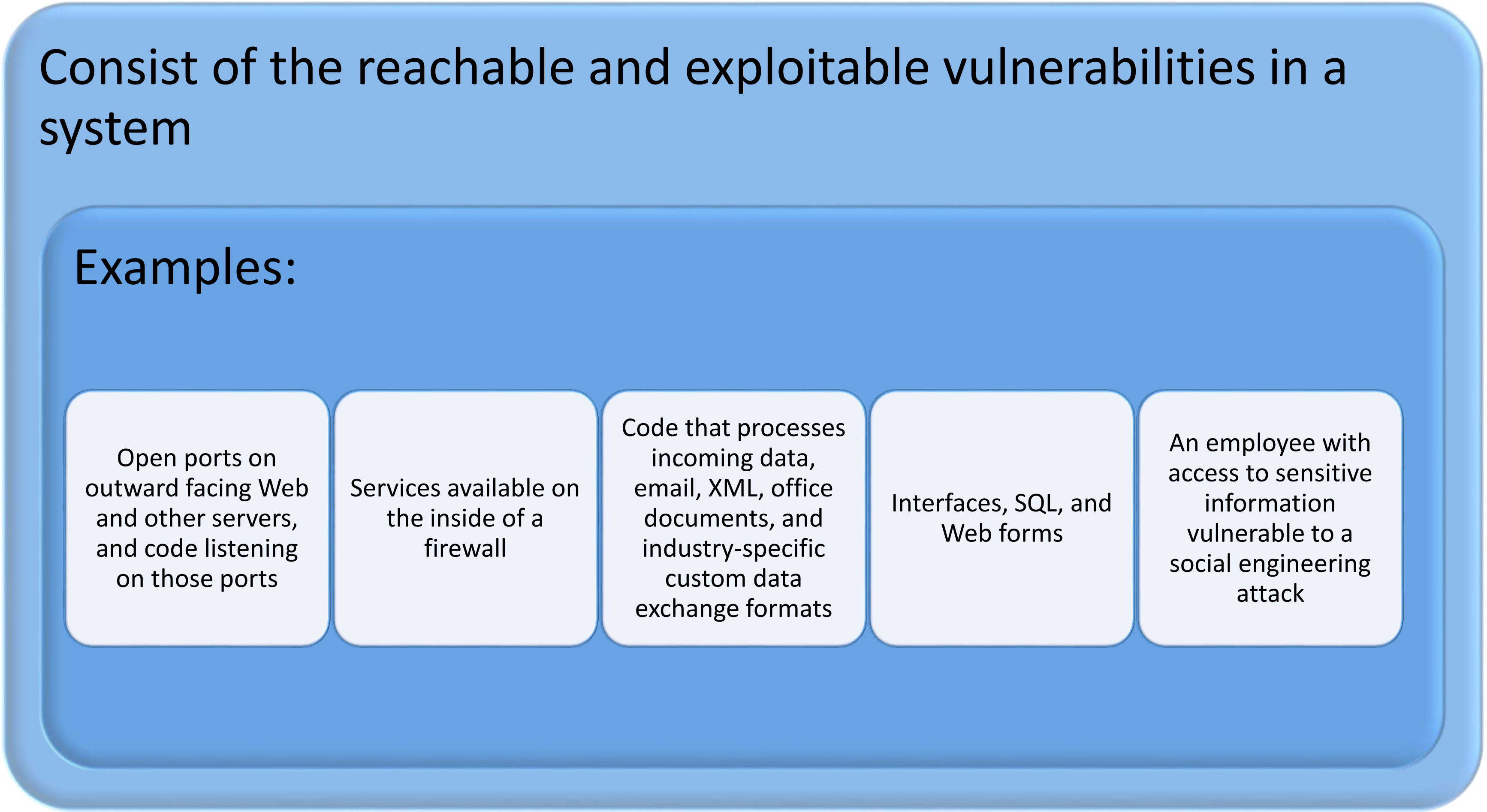
Security Areas

- Consumerization :
  - consumer devices will become trendier, cheaper, and more integrated
- Decentralization
  - increase use of cloud computing
- Deconcetration
  - special purpose hardware like iPhone
- Decustomerization:
  - get more IT function without any business relationship: free Google, Bing, Social, Networking sites etc

Vulnerabilities of the Internet

- The addressing system that finds out where to go on the internet for a specific address DNS
- The routing among ISPs, a systems known as the Border Gateway Protocol
- Almost everything that makes it work is open, unencrypted
- Its ability to propagate intentionally malicious traffic designed to attack computers
- It is one big network with a decentralised design

Attack Surfaces



Consist of the reachable and exploitable vulnerabilities in a system

Examples:

- Open ports on outward facing Web and other servers, and code listening on those ports
- Services available on the inside of a firewall
- Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats
- Interfaces, SQL, and Web forms
- An employee with access to sensitive information vulnerable to a social engineering attack

Attack Surface Categories

Network Attack Surface

Vulnerabilities over an enterprise network, wide-area network, or the Internet

Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks

Software Attack Surface

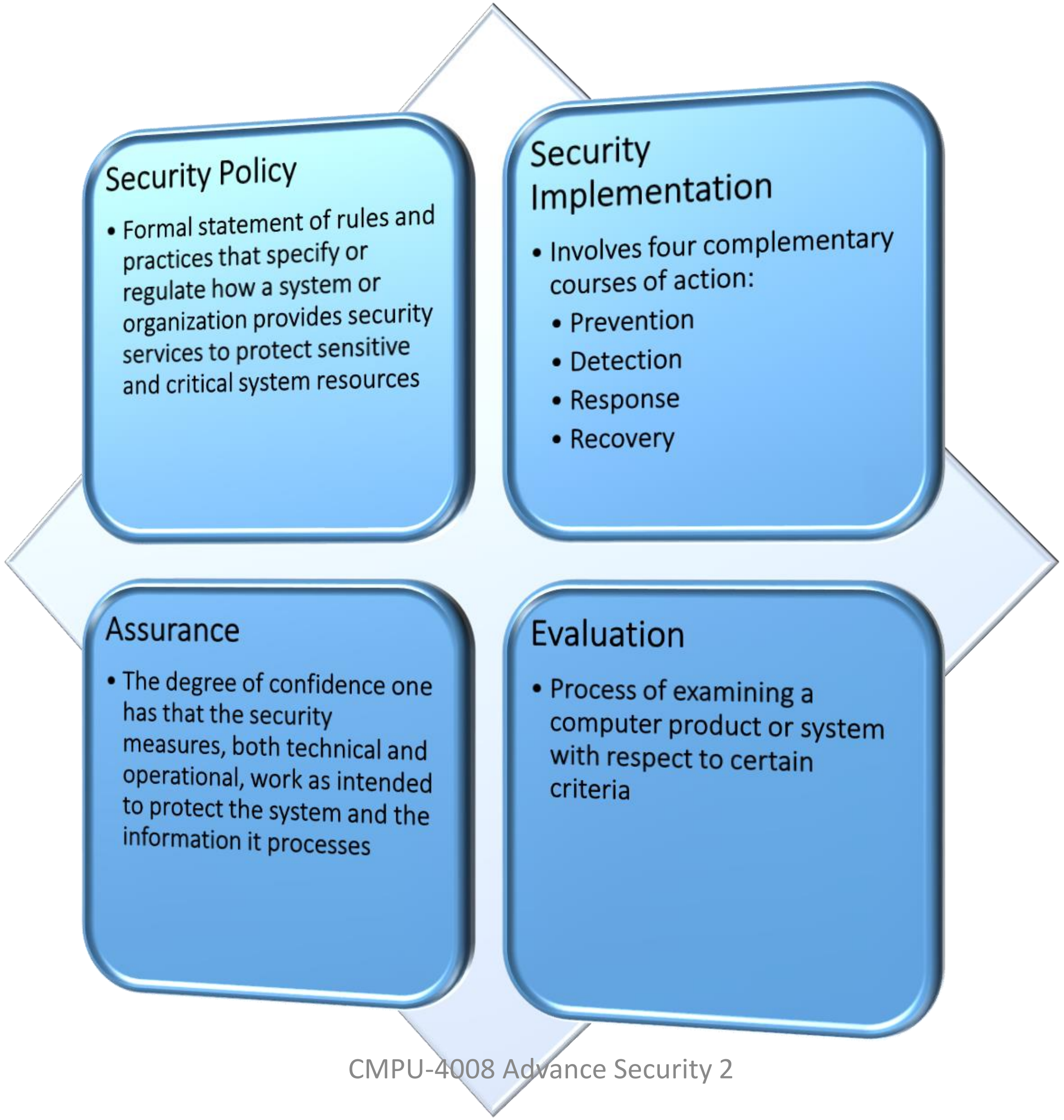
Vulnerabilities in application, utility, or operating system code

Particular focus is Web server software

Human Attack Surface

Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

Computer Security Strategy



Security Policy

- Formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources

Security Implementation

- Involves four complementary courses of action:
  - Prevention
  - Detection
  - Response
  - Recovery

Assurance

- The degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes

Evaluation

- Process of examining a computer product or system with respect to certain criteria