SECURITY FUNDAMENTALS

RODEL URANI

MAJOR OUTLINES

- Cryptography
- Security technologies
- Cyberstrategy
- Practice(s) in the real world
- Security-related marketing activities

Quickies

- Major activities
  - Social
  - Economic
  - Peace, order and enforcement
  - Governance and leadership
- At present (some local) leaders make decisions without emphasis to the importance and facility of the following:
  - Information technology, and linking it with
  - Environmental domains, where they will be operated

Subject overview

- Security is synonymous to protection
- Major categories, see the following:
    - Information and technology are separate and aspects entirely different
    - Both facilitate each others purpose in an efficient or destructive manner
    - Information
        - Created
        - Stored
        - Retrieved
        - Transferred/moved
        - Changed/manipulated/programmed
        - Copied
    - Technology (with AIM principle)
        - Acquired i.e. systems development if internally built, procure if coming from 3rd party, hiring of human capital or capable practitioners
        - Implemented
        - Managed

IT is

- Changing constantly and so considered disruptive to some even for practitioners
- Both physical and intangibles (virtual)
- Application of
  - Computers, all forms and types
  - Internetworking
  - Television
  - Telephone
- Practice that is adapted in many if not all industries (and activities) known to man
  - Banking
  - Agriculture
  - Power and electricity
  - Airlines
  - Military

Security, what is/are required

- Information
  - Un/structured data

- Computers
  - PC/Mac, mainframe, supercomputers, quantum computers
  - Switches (hubs)
  - Routers
  - Mobile
  - Industrial systems

Technologies

- Cryptography - protects information

- FW (firewall)/ID|PS (intrusion detection and prevention system)/SEIM (security event information management), AV (antivirus) - protects computing systems, its endpoint from
  - Outdated systems
  - Operational misuse
  - Corruptions of systems
  - Incidents inflicted primarily by humans both practitioners and end-users
  - Attacks within and outside of the company and local/private network premises

Nuance, significant security mechanisms

- Beneath their primary purpose
  - Boot, Unified Extensible Firmware Interface (UEFI)
  - Storage, cryptography dependent on CPU/RAM performance and built-in on devices
  - Applications and productivity suites, Systems and Security Development Lifecycle (SSDL), Web Application Security Consortium (WASC), Open Web Application Security Project (OWASP)
  - Operating systems, trusted computing efforts
  - Smartphones, same efforts as those of general purpose computers except for some specific mobile applications
  - Special hardware module, cryptographic acceleration, keys management, strong authentication

Inherent environmental domains

- Cyberconnected i.e. imagine IT here converging, making physical borders not so inutile, see the following
- Land, mission critical utilities grid
- Air,
- Sea,
- Space,

- C L A S S E D*

CLASSED

- Constitutes economic and social underpinnings

- The utility of technology is only second to the above

- Technology exist not primarily for those who created them but its business facility
  - Market-driven, unfortunate but it’s a reality

Didactics, education and enforcement

- Awareness and conference for the entire organization and stakeholders
- Research and technical training for developers and integrators
- Guidance from manufacturers and government for senior management and owners
- Multistakeholderism for policy and lawmakers creating a not so harsh and adaptable regulations conformance and/or compliance

Security

- Make it a norm, part of general practice/endeavors and not as an afterthought

- Making excellence a habit – BSI

- Replace "excellence" with effort e.g. "security", "quality" et al

- Think of your own habit, it has become unthinking, easy to deal on it

- Begin doing things a habit, just a matter of time and realize it's not that hard

Specific security initiatives effectiveness, more scale-based

- Acquisition phase
  - Development
  - Implementation

- Linguistic context
  - Computer
  - Information
  - Cyber, see CLASSED

Computer security

Applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the whole Internet. The field covers all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction, and is of growing importance due to the increasing reliance of computer systems in most societies. It includes physical security to prevent theft of equipment and information security to protect the data on that equipment. It is sometimes referred to as "cyber security" or "IT security".

Information security (IS)

The practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc...)

2 major aspects

- IT security
- Information assurance

IT security

Sometimes referred to as computer security, applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.

Information assurance

The act of ensuring that data is not lost when critical issues arise. These issues include but are not limited to: natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise.

Key concepts

- Security classic trio (triad), deuce-ace
    - Confidentiality
    - Integrity
    - Availability
- Non-repudiation
- Authentication, take Authentication, Authorization and Accounting (AAA)

Confidentiality

- The state of being secret.
- Discretion in keeping secret information.

Integrity

- Maintaining and assuring the accuracy and consistency of data over its entire life-cycle.
- Data cannot be modified in an unauthorized or undetected manner.
- Computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

Availability

- Information must be available when it is needed.

Nonrepudiation

- Implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

Authenticity

- It is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be.
- Further check Authentication, Authorization and Accounting.

IS relation to risk management

- Risk
  - Exposure to a chance of loss or damage.
  - Taking a risk in the hope of a favorable outcome.
- Vulnerability
  - A weakness that could be used to endanger or cause harm to an informational asset.
- Threat
  - Is anything (man-made or act of nature) that has the potential to cause harm.

Risk management process consists of

- Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, other), supplies.
- Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization.
- Conduct a vulnerability assessment, and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.
- Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.
- Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.
- Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost effective protection without discernible loss of productivity.

Research suggests most vulnerable

- Human
    - End-user
    - Operator
    - Designer

ISO/IEC 27002 recommends examination during risk assessment

- Security policy,
- Organization of information security,
- Asset management,
- Human resources security,
- Physical and environmental security (refer to CLASSED),
- Communications and operations management,
- Access control,
- Information systems acquisition, development and maintenance,
- Information security incident management,
- Business continuity management, and
- Regulatory compliance.

Security controls

- Administrative

- Logical

- CLASSED, originally physical/environmental

Administrative controls

Also called procedural controls, consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day-to-day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed – the Payment Card Industry Data Security Standard (PCI DSS) required by Visa and MasterCard is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies.

Logical controls

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host-based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls. An important logical control that is frequently overlooked is the **principle of least privilege**. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read email and surf the web.

Physical controls

Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and workplace into functional areas are also physical controls. An important physical control that is frequently overlooked is the **separation of duties**. Separation of duties ensures that an individual can not complete a critical task by himself.

CLASSED concept with

- Smart City
- Aircraft Computing System
- Computer aided manufacturing
- Industrial electromechanical i.e. nuclear plant

Smart City

- Uses digital technologies to enhance performance and wellbeing, to reduce costs and resource consumption, and to engage more effectively and actively with its citizens. Key 'smart' sectors include transport, energy, health care, water and waste. A smart city should be able to respond faster to city and global challenges than one with a simple 'transactional' relationship with its citizens.
- Brings together technology, government and society to enable the following characteristics: smart cities, a smart economy, smart mobility, a smart environment, smart people, smart living, smart governance. [IEEE]

Aircraft Computing Systems

- For remote controlled aircraft, a modern computer radio transmitter and receiver can be equipped with synthesizer technology, using a phase-locked loop (PLL), with the advantage of giving the pilot the opportunity to select any of the available channels with no need of changing a crystal. This is very popular in flying clubs where a lot of pilots have to share a limited number of channels.
- The movements of flight controls are converted to electronic signals transmitted by wires (hence the fly-by-wire term), and flight control computers determine how to move the actuators at each control surface to provide the expected response.
- Provide built-in flight envelope protection, allowing pilots to extract maximum aircraft performance and efficiency without risk of overstressing the aircraft.
- Features three main flight computers that receive control inputs and direct control movement, backed up by three secondary computers.

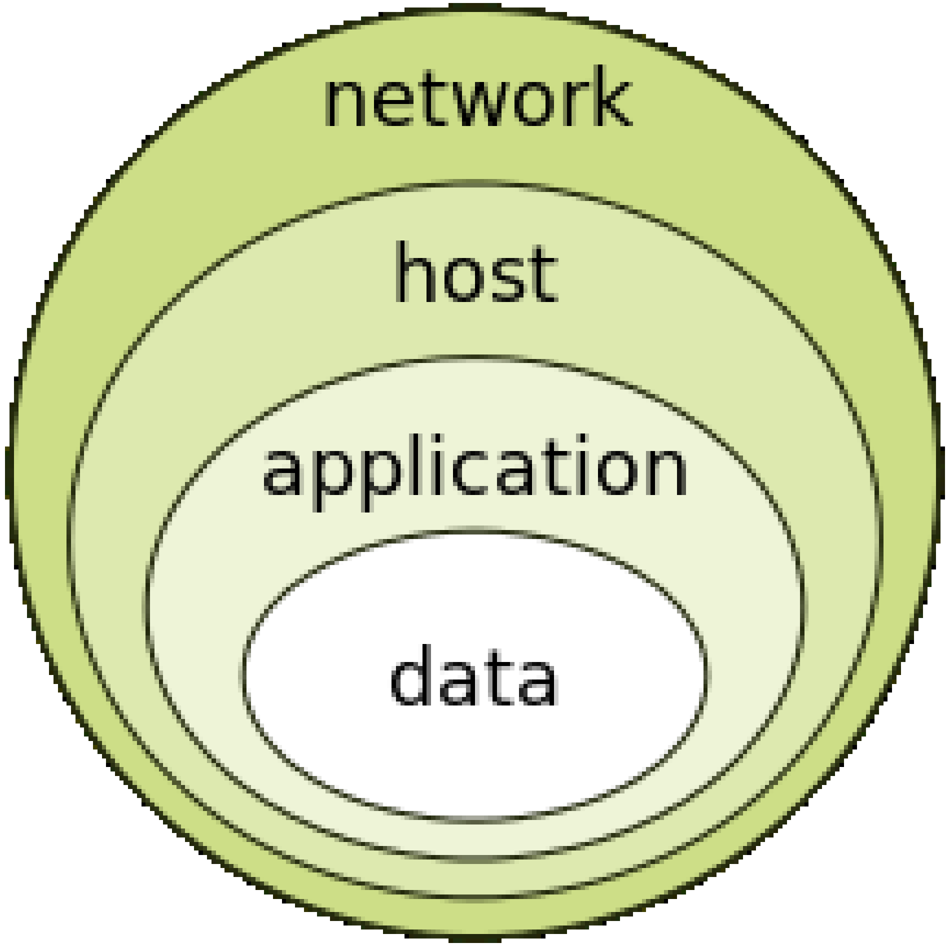
Computer aided manufacturing

- The use of computer software to control machine tools and related machinery in the manufacturing of workpieces. This is not the only definition for CAM, but it is the most common; CAM may also refer to the use of a computer to assist in all operations of a manufacturing plant, including planning, management, transportation and storage.
- Its primary purpose is to create a faster production process and components and tooling with more precise dimensions and material consistency, which in some cases, uses only the required amount of raw material (thus minimizing waste), while simultaneously reducing energy consumption.

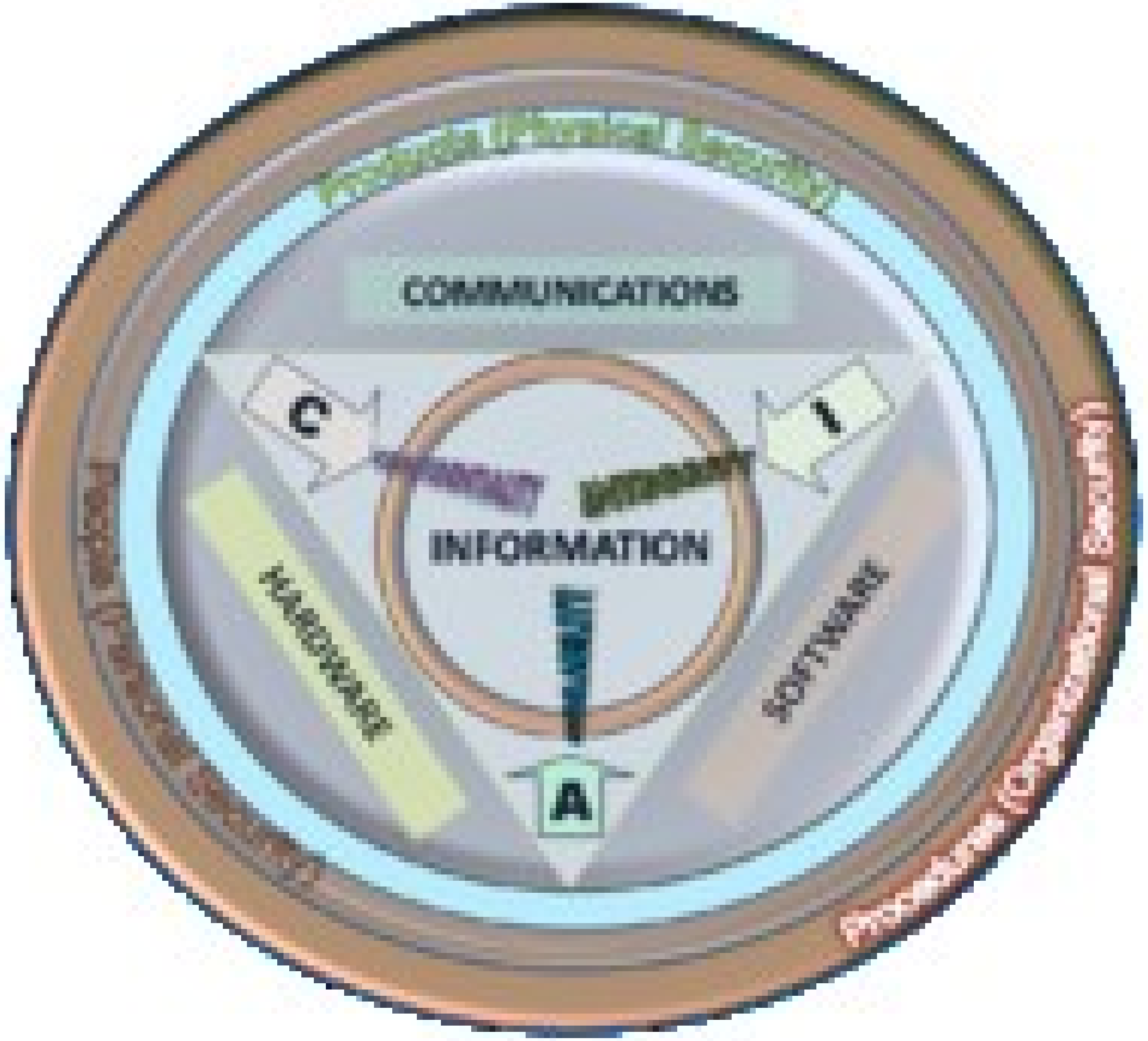
Industrial electromechanical

- Facilitated by digital computer or commonly called programmable logic controller (PLC) to control machinery on factory assembly lines, amusement rides, or light fixtures.
- Industries include power generation, utility distribution, manufacturing et al.

Defense in depth, onion model



IS attri



COMMUNICATIONS
C
I
INFORMATION
HARDWARE
SOFTWARE
A
Procedures (Organizational Security)

Security classification for information

- In the business sector, labels such as: **Public, Sensitive, Private, Confidential**.
- In the government sector, labels such as: **Unclassified**, **Sensitive But Unclassified**, **Restricted**, **Confidential**, **Secret**, **Top Secret** and their non-English equivalents.
- In cross-sectoral formations, the Traffic Light Protocol, which consists of: **White, Green, Amber**, and **Red**.

3 different types of information for authentication

- Something you know: things such as a PIN, a password, or your mother's maiden name.
- Something you have: a driver's license or a magnetic swipe card.
- Something you are: biometrics, including palm prints, fingerprints, voice prints and retina (eye) scans.

Security process objectives

- They have been used in the fields of Finance, Securities, and Law for many years.
    - Due care
    - Due diligence

Due care

- Are steps that are taken to show that a company has taken responsibility for the activities that take place within the corporation and has taken the necessary steps to help protect the company, its resources, and employees.

Due diligence

- The "continual activities that make sure the protection mechanisms are continually maintained and operational."

International practices and laws

- ISO/IEC 27001 family
- UK Data Protection Act 1998
- The Computer Misuse Act 1990 (US, including the ff)
- The Family Educational Rights and Privacy Act
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Gramm–Leach–Bliley Act of 1999 (GLBA)
- Sarbanes–Oxley Act of 2002 (SOX)
- Cybercrime Prevention Act 2012 (PH, including the ff)
- Data Privacy Act 2011
- Payment Card Industry Data Security Standard (PCI DSS) (International, applicable to financial institutions that processes/facilitates credit/debit cards