Introduction to Information Security

Ashish Nanda

Ashish.Nanda@uts.edu.au

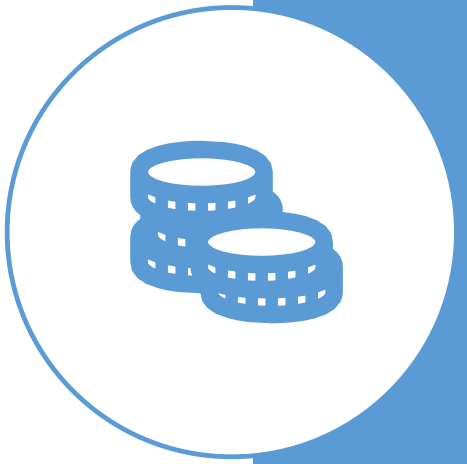
Lets Start Simple

- The **digital world** behaves very differently to the physical world
- Everything digital is made of **bits**
- Bits have **no uniqueness**
- It's **easy to copy** bits perfectly
- Therefore, if you have bits, I can copy it.
- Information, privileges, identity, photos, videos, software, digital money, secrets, etc… Are all made of bits
- Much of **information security** revolves around making it hard to copy bits.
- **This is like trying to make water not wet.**

It’s all a resources game

You spend X so that your opponent has to spend Y to do something you don’t want them to do.

Y is rarely greater than X... and there are may opponents.



The currency used in the game game:

- Time
- Money $$$
- Computational Power (== time X $$$)

Implications

GIVEN ENOUGH RESOURCES, SOMEONE WILL GET IN.

GIVEN ENOUGH ATTACKERS, SOMEONE WILL GET IN.

GIVEN ENOUGH TIME, SOMEONE WILL GET IN.

THE ONLY PERFECT SYSTEM IS ONE THAT IS THEORETICAL.

A SYSTEM CAN AND WILL EVENTUALLY FAIL.

THE TRICK IS TO RAISE THE BAR TO AN ADEQUATE LEVEL OF (IN)SECURITY FOR THE RESOURCE YOU'RE TRYING TO PROTECT

How do systems fail?

Systems often fail because designers:

- Protect the **wrong things**
- Protect the **right things** in the **wrong way**
- Make **poor assumptions** about their systems
- Do not understand the **threat model properly**
- Fail to account for **paradigm shifts** (e.g. the Internet)
- Fail to understand the **scope** of their system

It’s a lot easier to break a system than to make it secure

What can be classified as a system?

A product or component

Plus infrastructure

Plus applications

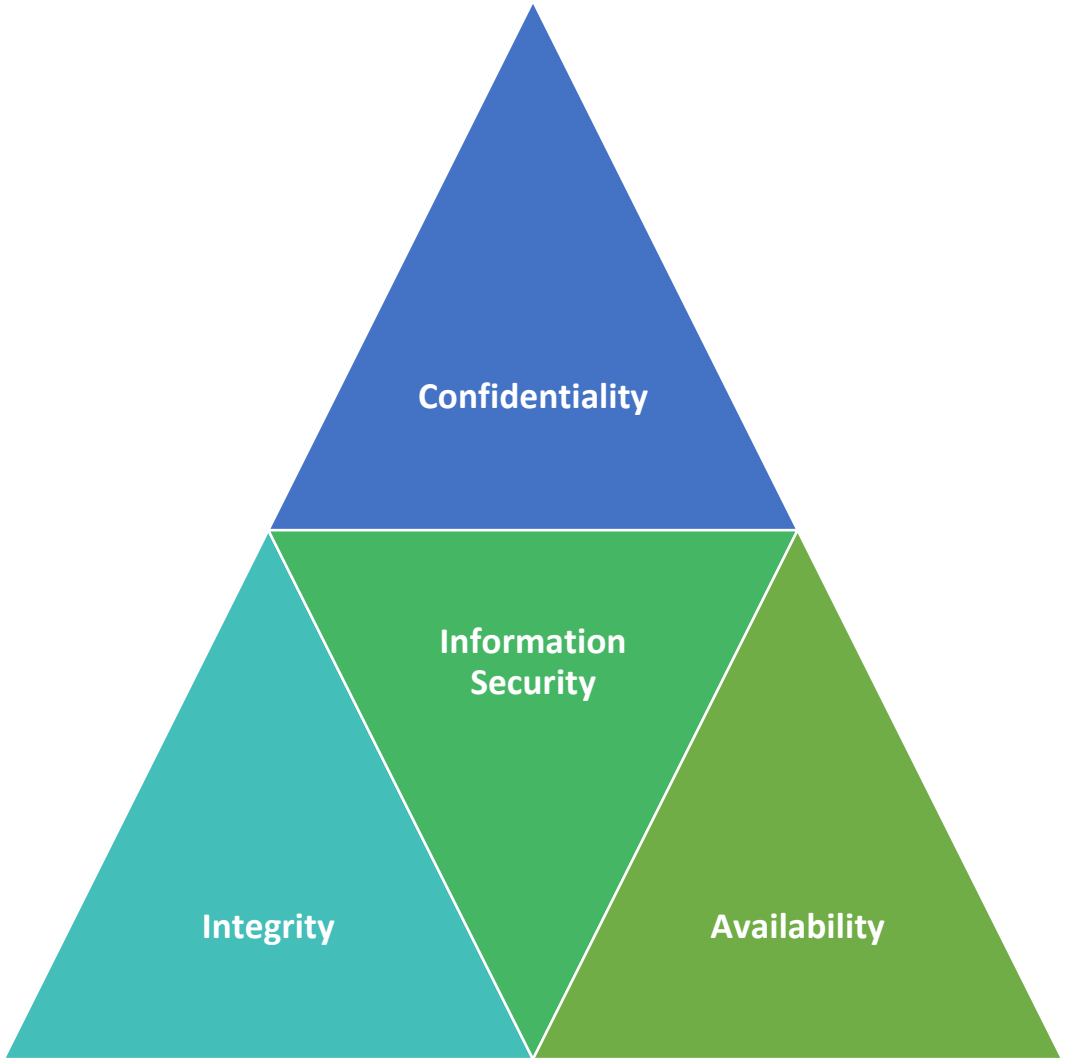
Plus IT staff

Plus users and management

Plus customers and external users

Plus partners, vendors

Plus the law, the media, competitors, politicians, regulators…


Confidentiality
Information Security
Integrity
Availability

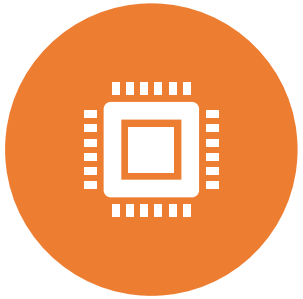
C I A Triad

C I A Triad (Aspects of Security)

- **Confidentiality** – only authorized people, resources, processes have access
- **Integrity** – protect data from intentional or accidental changes
- **Availability** – Data or system is available by authorized users when needed

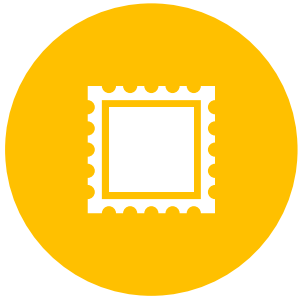
- **Authenticity –** proof of a message's origin Integrity plus freshness (i.e. message is not a replay)
- **Non-Repudiation –** message enciphered with private key came from someone who knew it
- **Covertness –** massage existence secrecy (related to anonymity)

Some key figures in security

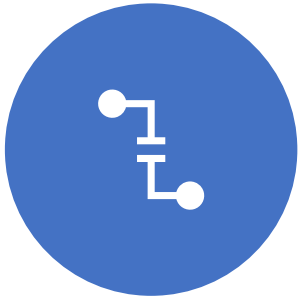


Cryptography: process of creation, development, application and testing of encryption methods

Encryption: converting original message into a form unreadable by unauthorized individuals



Cryptanalysis: process of breaking encrypted message to obtain original message

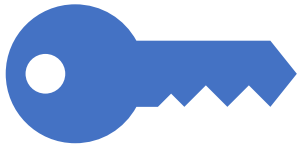


Cryptology: is cryptanalysis combined with cryptography

Types of Cryptography

Classical Cryptography	DES (Data Encryption Standard) AES (Advanced Encryption Standard)
Public Key Cryptography	Diffie-Hellman RSA
Cryptographic Checksums	HMAC

Classical Cryptography



Sender & Receiver share common key

Key may be the same, or trivial enough to be derived from one another

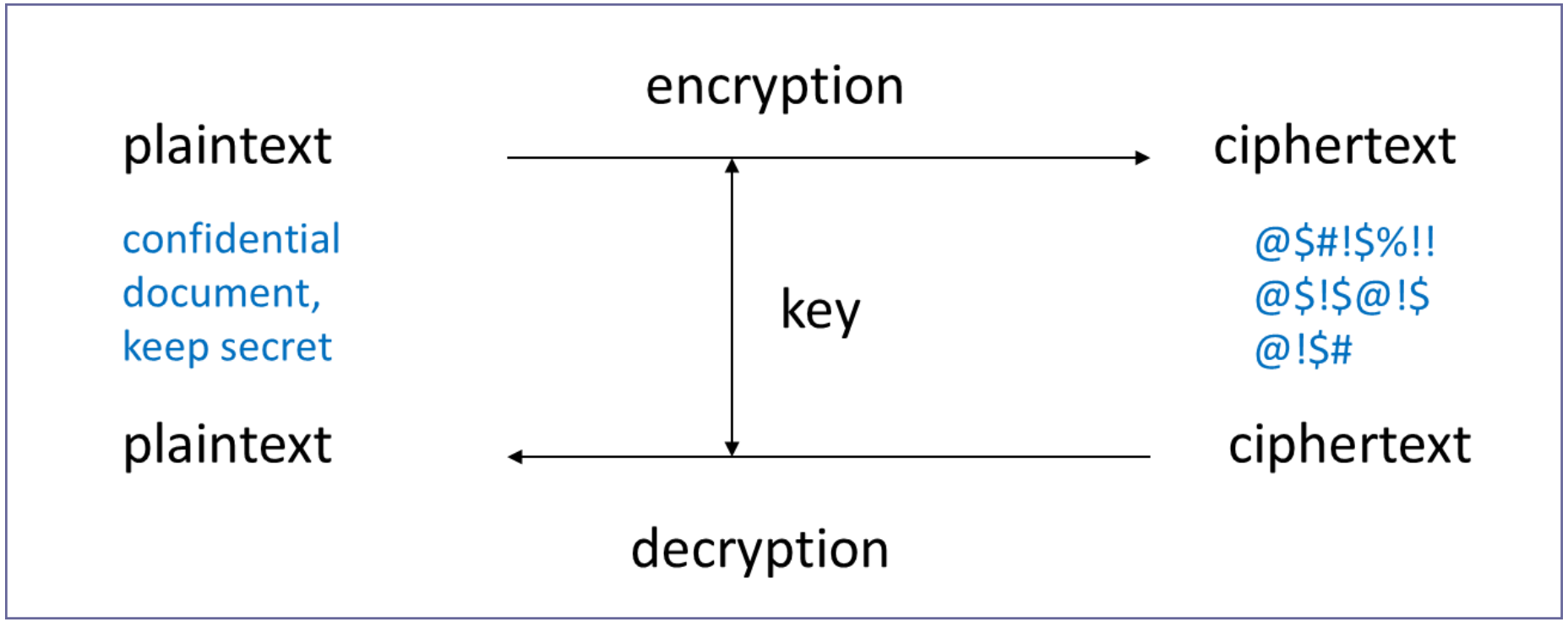
Also called *symmetric cryptography*

Two basic types

Transposition ciphers

Substitution ciphers

A combinations of both is called *product ciphers*



Symmetric cryptography

Uses a single key for encryption/decryption.

The plaintext and the ciphertext having the same size.

Public Key Cryptography

Sender & Receiver use two keys

Private key known only to individual

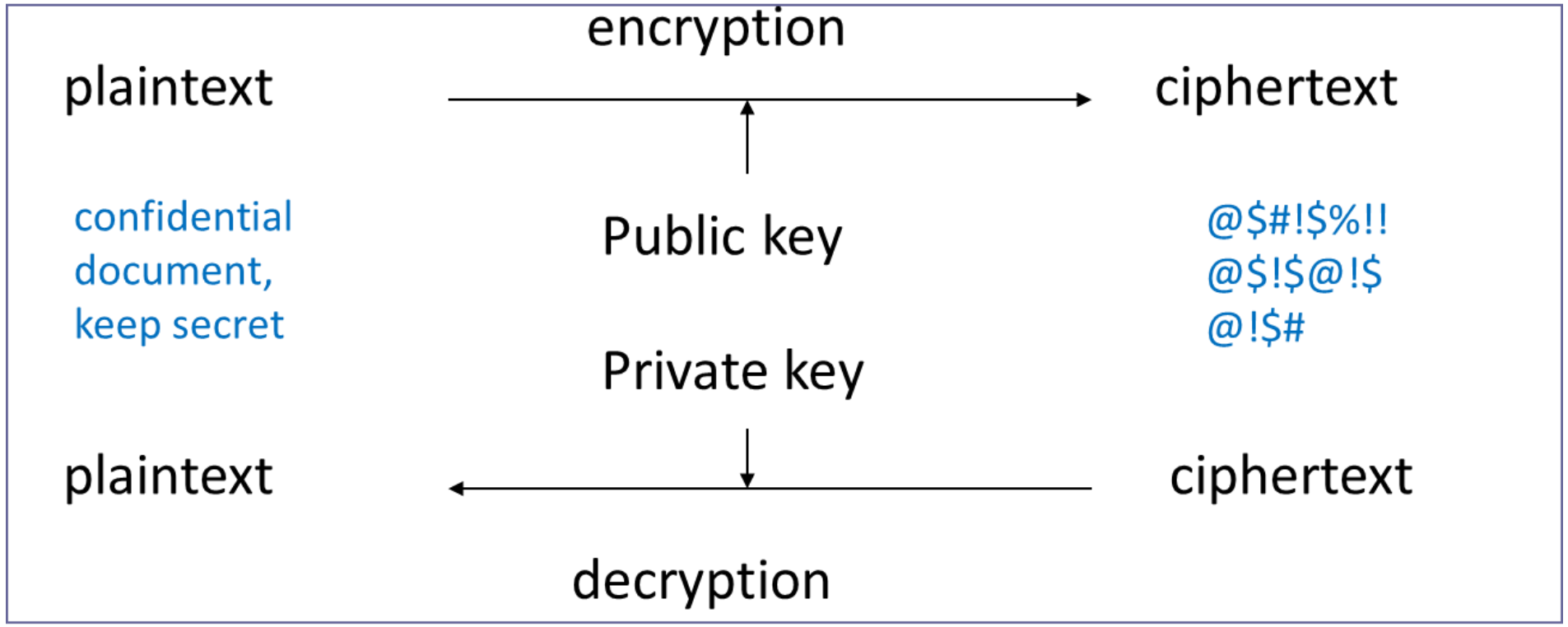
Public key available to anyone

Also called *asymmetric cryptography*

The main Idea

Confidentiality: encrypt using the public key, decrypt using the private key

Integrity/Authentication: encrypt using private key, decrypt using public one



Asymmetric cryptography

Private key: to be kept securely

Public key: to be shared with the world

Public Key Cryptography: Requirements

- It must be **computationally easy to encrypt or decrypt** a message given the appropriate key
- It must be **computationally infeasible to derive** the private key from the public key
- It must be **computationally infeasible to determine** the private key from a chosen plaintext attack

Cryptographic Checksums

Mathematical function to generate a set of *k* bits from a set of *n* bits (where $k \leq n$).

- *k* is smaller then *n* except in unusual circumstances

Example: ASCII parity bit

- ASCII has 7 bits; 8th bit is “parity”
- Even parity: even number of 1 bits
- Odd parity: odd number of 1 bits

Hash Functions

A hash function (**h**) is an efficiently computable mapping of arbitrarily long string (**m**) to short fixed length strings.

Minimum properties:

- Compression: Typically any number of bits to < 512 bits e.g. MD5, SHA256, SHA512
- Ease of computation: Given **h** and **m**, **h(m)** is easy to compute.

Keyed Hash Functions

- Some hash functions take both a key **(k)** and a message **(m)**
- **$MAC_k(m) = h(m, k)$**

They are also called message authentication codes (**MAC**) or hash-based message authentication codes (**HMAC**).

Digital Signatures

Encrypted messages that can be mathematically proven to be authentic

Created in response to rising need to verify information transferred using electronic systems

Asymmetric encryption processes used to create digital signatures

Digital Certificates

Electronic document containing key value and identifying information about entity that controls key.

Digital signature attached to certificate’s container file to certify file is from the entity it claims to be from.

- Encrypting data is required for eCommerce
- Understanding how and when cryptography is used is not optional
- Data needs to be shared securely, and the only viable solution is cryptography
- Correct implementation of cryptography is essential
- Poor implementations result in breaches

Key Points: Cryptography

Attacks on Information Security

- **Passive Attack**
  - Does not involve the modification or fabrication of data.
  - An unauthorized party gains access to an asset.
  - Release of message contents → an attack on confidentiality.
  - Traffic analysis → an attack on covertness.

- **Active Attack**
  - Fabrication → an attack on authenticity.
  - Interruption → an attack on availability.
  - Modification → an attack on integrity.

Basis for Attacks

Mathematical attacks

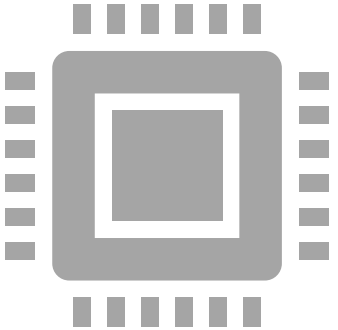
- Based on analysis of underlying mathematics

Statistical attacks

- Make assumptions about the distribution of letters, pairs of letters (digrams), triplets of letters (trigrams), *etc.*
- Examine ciphertext, correlate properties with the assumptions.

Attack Meathods

Brute Force: This method goes through all the available keys, testing each one until the correct key is found.

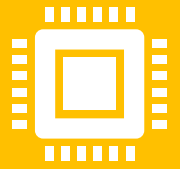


Exploitation: This method takes advantage of a weakness in the encryption algorithm.

Brute Force Attack

Brute Force attack will always find the key… you know … eventually.

Main defence is to make the number of possible keys a large number – at least 2128. This makes the search for the key time-prohibitive.



The effectiveness of brute force attacks can be enhanced by adding more hardware. Purpose designed hardware can be even more effective.

Exploitation Attacks

All of the commonly used protocols have been extensively analysed.

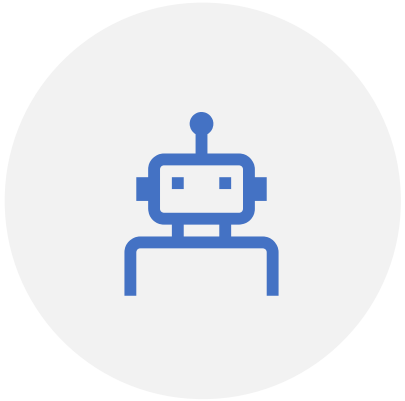
Encryption standards with known weaknesses are dropped fairly quickly.

Networking protocols that exchange encrypted data allow attackers to collect encrypted data and from there possibly mount an attack.

Mandatory Security

- **Bell and La Padula Security Policy**
  - Subjects have clearance levels, Objects have sensitivity levels; clearance and sensitivity levels are also called security levels
  - Unclassified < Confidential < Secret < TopSecret
  - Compartments are also possible
  - Compartments and Security levels form a partially ordered lattice
- **Security Properties**
  - Simple Security Property: Subject has READ access to an object of the subject's security level dominates that of the objects
  - Star (*) Property: Subject has WRITE access to an object if the subject's security level is dominated by that of the objects

Physical Security: Data Center



FACILITY MUST BE DESIGNED TO INCLUDE PHYSICAL SAFEGUARDS

PHYSICAL ACCESS TRUMPS ALL OTHER FORMS OF SECURITY

NO ONE SOLUTION IS PERFECT: EACH FACILITY NEEDS ARE UNIQUE

Physical Security: Process and Plan

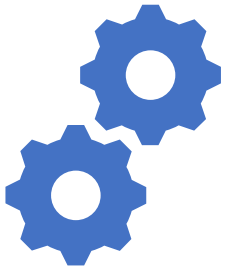
Effectiveness is ensured by making certain that:

- Threats have been identified
- Associated vulnerabilities have been accurately characterized, prioritized, and addressed
- Implementation is based on a plan
- Supervised and enforced by consistent and ongoing management

Application Security

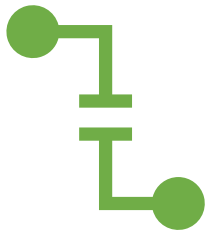
- Average sized organization has hundreds of in-house and externally developed applications.
- Business process are continually moving towards web services
- However, data and critical business services are being exposed:
  - Lack of testing
  - Insecure applications
  - Human error (leaving things where they shouldn’t be)

Application Security



Initial concept to final disposal

Security must be an integral part of application lifecycle



Application security: golden rule

You cannot test security! It must be designed into the application and verified each step of the lifecycle.

Network Security

- Network protocols are not secure.
  - Port scan/direct attack
  - Malicious Web Sites
  - Social Engineering
  - Phishing/Pharming
  - Denial of Service attacks
  - Insider attacks
  - Viruses/Worms
  - Information Leakage
  - Others

Network Security

Switches are vulnerable

MAC address Flooding

Other issues on local network

ARP Poisoning

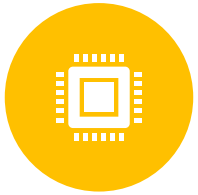
Rogue DHCP Servers

Physical access to wiring closets

Network Hubs

Insecure!

No traffic isolation or traffic control



All data is replicated to all ports

Any station on the hub can examine ALL traffic

Collision problems on busy network

Access Control

A key principle to preserve Confidentiality

Properly implemented Access Controls ensures only authorized access and denies all else.

Several methods are used

- Mandatory Access Control
- Discretionary Access Control
- Role Base Access Control

Security Architecture

- Framework unifies reusable services and process to implement policy standards and risk management decisions.
- Strategic framework that allows the development and operations staff to align efforts
- Parameters
  - Policies
  - Standards
  - Guidelines
  - Baselines
  - Procedures

Operations Security

Processes and controls placed around your operations.

Assures Confidentiality/Integrity

Can help assure availability

Provides mitigation for incidents

Includes HR processes (background checks)!

Audits

Only good way to find out if controls are working as designed

Internal vs. External

Legal requirements

What if things go wrong?

Business Continuity Planning/Disaster Recovery Planning

An extremely important and rapidly growing part of Information Assurance!

A proper security program is deficient if there isn't business continuity and disaster recovery planning

Investigations

- Log analysis
- Network analysis
- Digital Forensics
- Evidence handling
- eDiscovery

Risk Management

- **What is risk?**
  - Risk = Threat * Vulnerability
- **Mitigation can take three forms:**
  - Accept the risk
  - Mitigate the risk
  - Transfer the risk

Legal, Regulations, Compliance and Investigations

- We are in the “Regulation Age”
- There are certain legal requirements and regulations which apply to many businesses
  - HIPPA, SOX, GLBA, FERPA, HEA, PCI DSS, PATRIOT Act, more!
- Compliance with these requirements and regulations are not optional
- Passing Audits necessary. Understanding the requirements and compliance now imperative