Week 1 – 3 hours on IT Security

Crisis ahead of IT world

cpr.mtninet.com

Snowden incident in 2013

Edward Snowden tells SCMP: 'Let Hong Kong people decide my fate'
Google
SUPPORT EDWARD SNOWDEN HK
PROTECT SNOWDEN
DEFEND FREE SPEECH
NO EXTRADITION
UPHOLD HK LAW

Agenda

What is CyberSecurity

From Computer Systems to Information Security

Security Principles

- CIA Triad
- Security Controls
- Access Control

What is CyberSecurity

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. – *ITU-T X.1205, Overview of cybersecurity*

Cyber security – defined as the protection of systems, networks and data in cyberspace – is a critical issue for all businesses. Cyber security will only become more important as more devices, ‘the internet of things’, become connected to the internet. – *ITGovernance.co.uk*

Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cybersecurity strategies include identity management, risk management and incident management. – *Definition in Techopedia.com*

What’s the difference between Cyberspace and Internet

The Internet is the global communication network, both hardware and software infrastructure that links smaller computer networks throughout the world. Most people use the term as a loose synonym for WWW (World Wide Web), a system of interlinked hypertext documents ("website pages") accessed through the Internet.

Cyberspace, on the other hand, is a vaguely defined term - invented by William Gibson - that refers the non-geographical, virtual, even metaphoric space in which all computer objects "exist". The term can include the entire content on the Internet, as well as the objects created by virtual reality simulations and computer games.

What is Computer System?

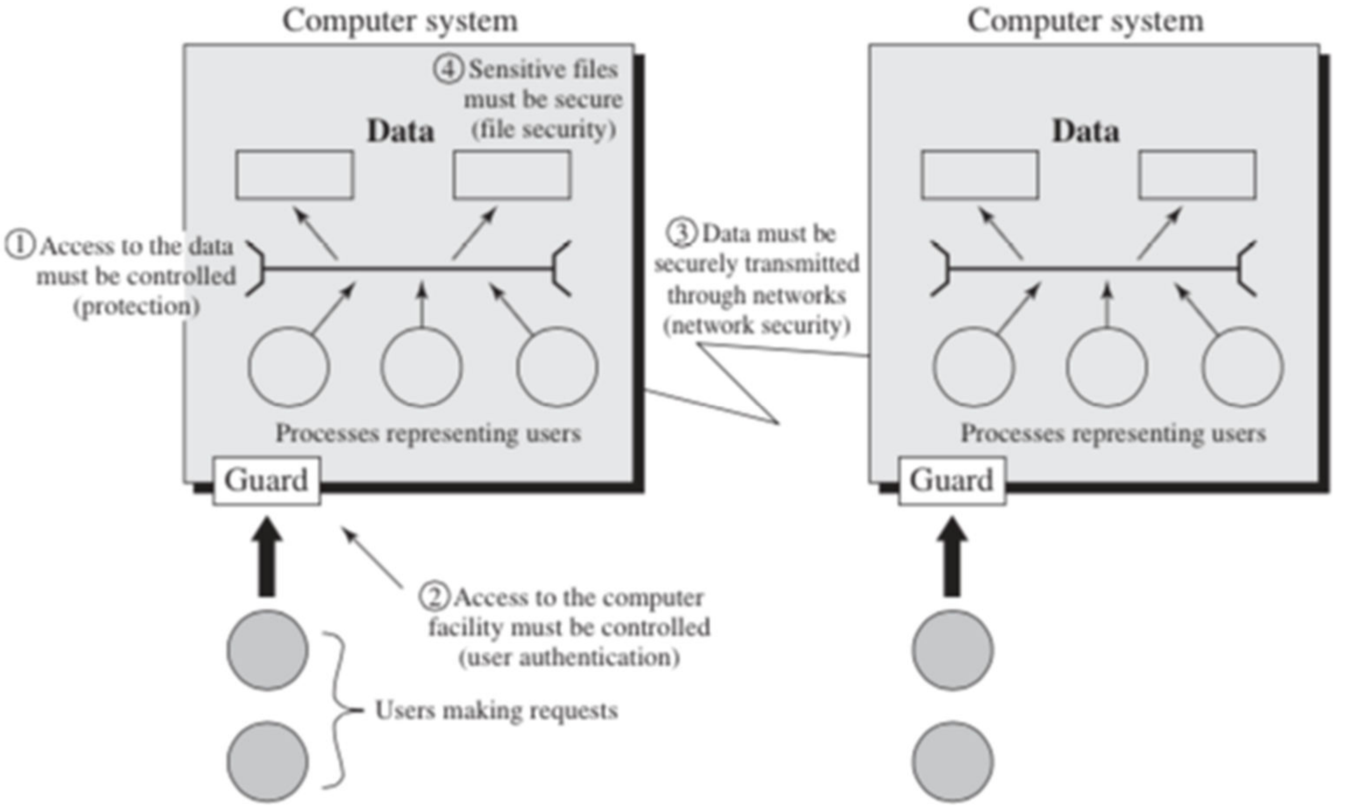

Computer system
④ Sensitive files must be secure (file security)
Data
① Access to the data must be controlled (protection)
Processes representing users
Guard
② Access to the computer facility must be controlled (user authentication)
Users making requests
③ Data must be securely transmitted through networks (network security)
Computer system
Data
Processes representing users
Guard

Figure 1.3 of Computer Security Principles and Practice 2nd Edition, William Stallings

Game Systems

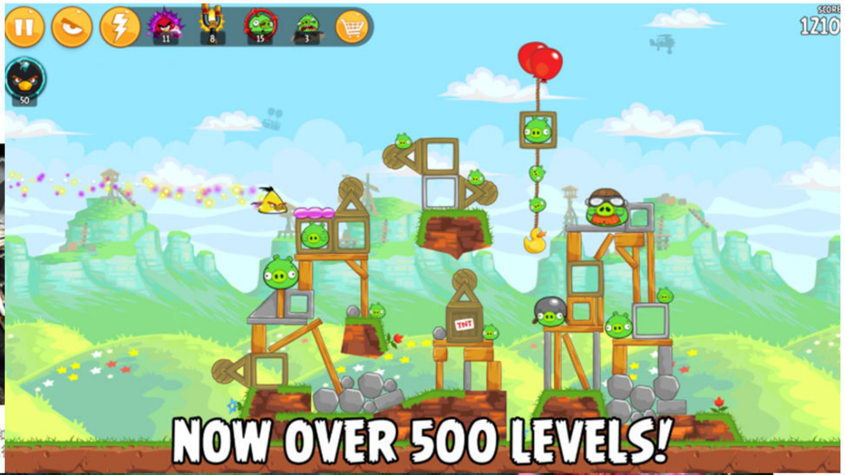
Mobile and Web Application

遊戲故事簡介

兩個風格各走極端的科學家－次方博士和D博士在世界上各領風騷，D博士認為要令世界得到真正和
類，將世界重新定位，同時著力研究『改造人』計劃，將人體重新改造成沒有感覺的殺人機器以進
次方博士識破了他的計劃，利用強化裝備－『鬥神』軍團將D博士消滅…

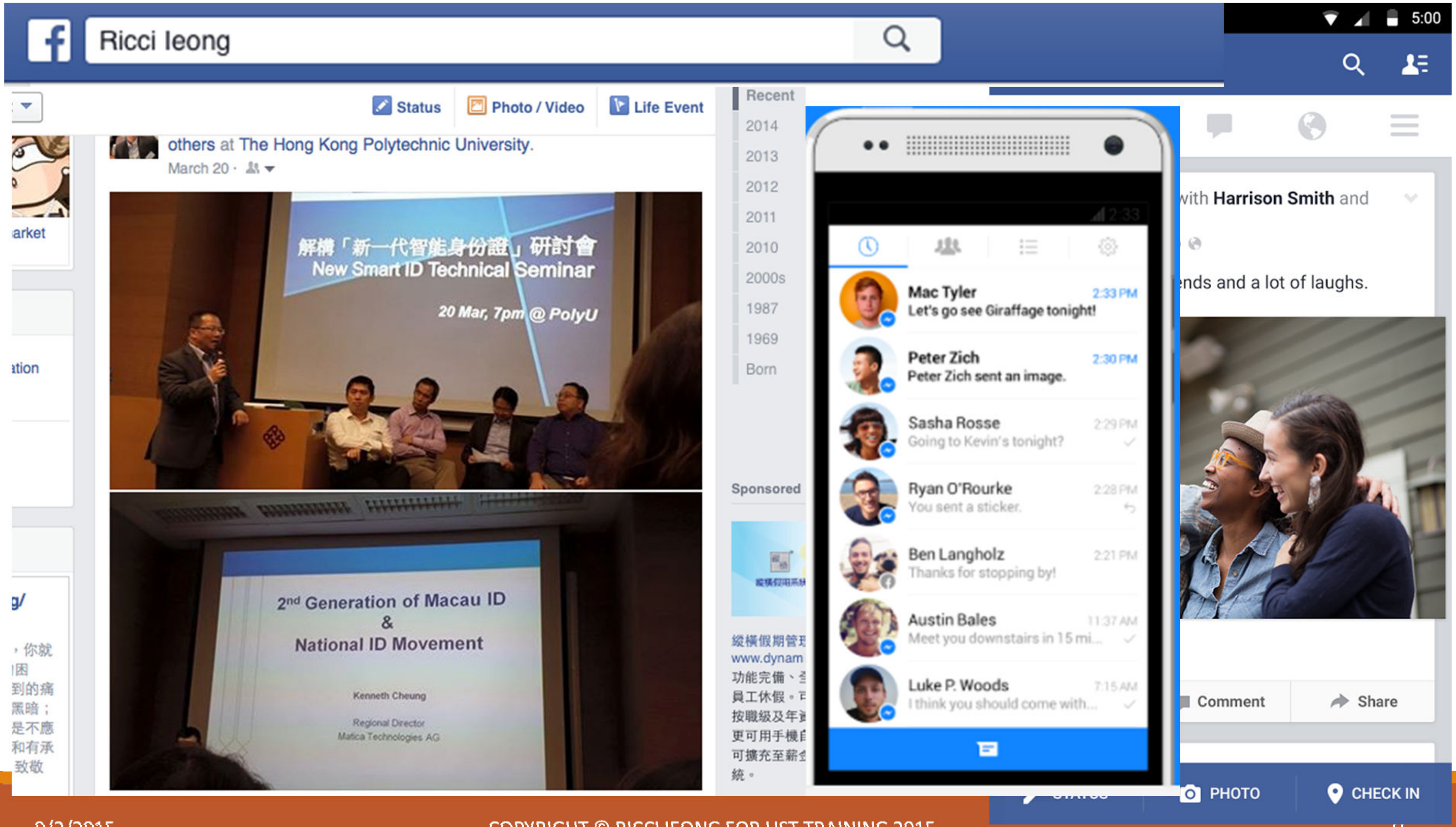
』技術改造自
oyer』裡，企圖

出鬥神大軍直接
製造改組人，



Facebook

Web and Mobile interfaces



others at The Hong Kong Polytechnic University.
March 20 ·

解構「新一代智能身份證」研討會
New Smart ID Technical Seminar
20 Mar, 7pm @ PolyU

2nd Generation of Macau ID
&
National ID Movement
Kenneth Cheung
Regional Director
Matica Technologies AG

Mac Tyler 2:33 PM
Let's go see Giraffage tonight!

Peter Zich 2:30 PM
Peter Zich sent an image.

Sasha Rosse 2:29 PM
Going to Kevin's tonight?

Ryan O'Rourke 2:28 PM
You sent a sticker.

Ben Langholz 2:21 PM
Thanks for stopping by!

Austin Bales 11:37 AM
Meet you downstairs in 15 mi...

Luke P. Woods 7:15 AM
I think you should come with...

with Harrison Smith and

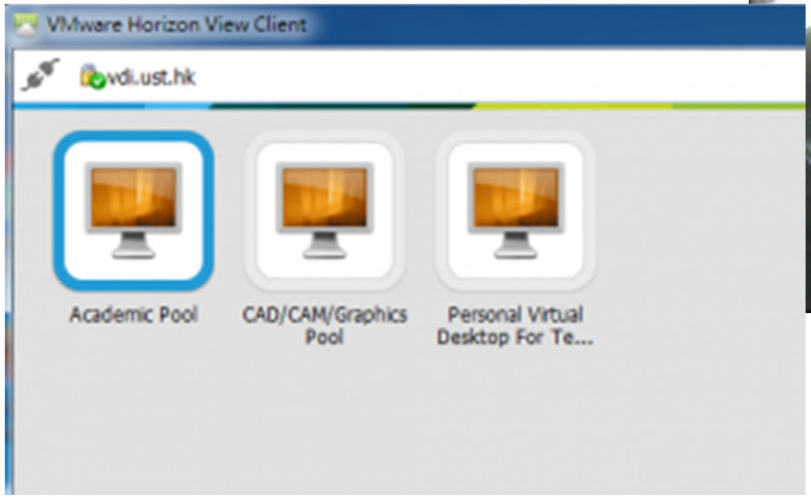
ends and a lot of laughs.

Computer Facilities

Computer Barn in UST

Virtual Barn

Print budget



VMware Horizon View Client

vdi.ust.hk

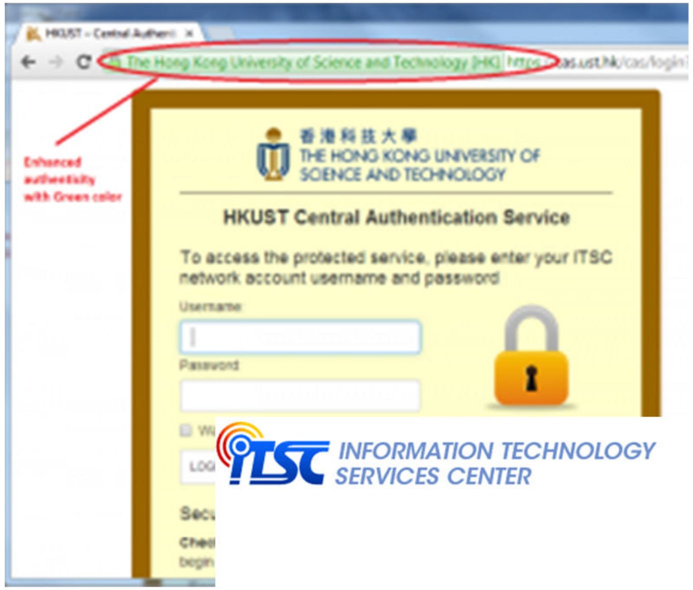
Academic Pool

CAD/CAM/Graphics Pool

Personal Virtual Desktop For Te...

Email system in University

Email on Cloud



HKUST – Central Authent...
The Hong Kong University of Science and Technology [HK] https://cas.ust.hk/cas/login

Enhanced authenticity with Green color

香港科技大學
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

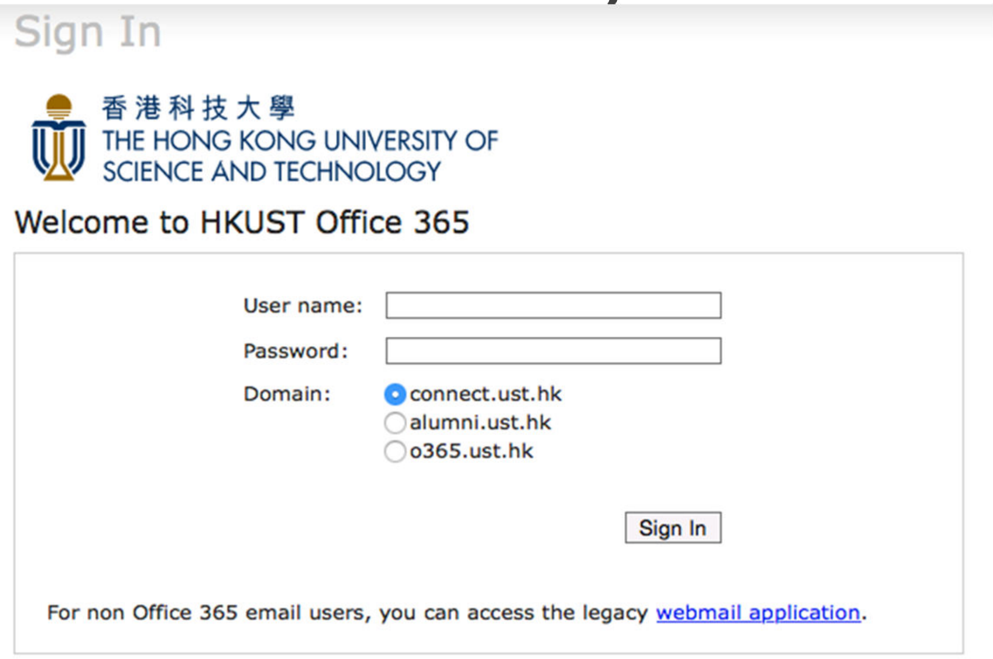
HKUST Central Authentication Service

To access the protected service, please enter your ITSC network account username and password

Username

Password

INFORMATION TECHNOLOGY SERVICES CENTER



Sign In

香港科技大學
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

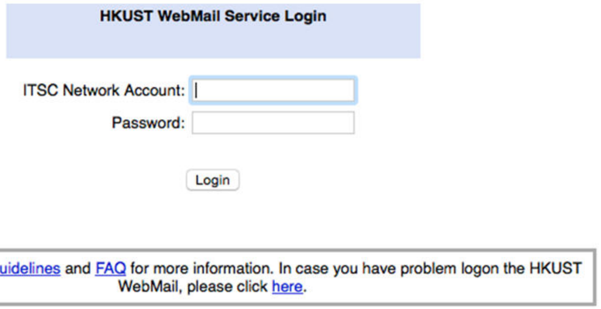
Welcome to HKUST Office 365

User name:

Password:

Domain: ● connect.ust.hk ○ alumni.ust.hk ○ o365.ust.hk

For non Office 365 email users, you can access the legacy webmail application.



HKUST WebMail Service Login

ITSC Network Account:

Password:

You may refer to the Guidelines and FAQ for more information. In case you have problem logon the HKUST WebMail, please click here.

Other IT systems in University

Learning Management system

Course registration

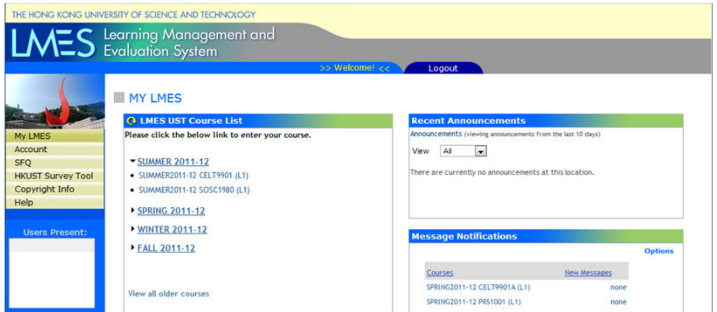
Human resources

Department web system

E-classroom

Library Systems

…



THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

LMES Learning Management and Evaluation System

>> Welcome! << Logout

My LMES
Account
SFQ
HKUST Survey Tool
Copyright Info
Help

Users Present:

MY LMES

LMES UST Course List

Please click the below link to enter your course.

- SUMMER 2011-12
  - SUMMER2011-12 CELT9901 (L1)
  - SUMMER2011-12 SOSC1980 (L1)
- SPRING 2011-12
- WINTER 2011-12
- FALL 2011-12

View all older courses

Recent Announcements

Announcements (viewing announcements from the last 10 days)

View All

There are currently no announcements at this location.

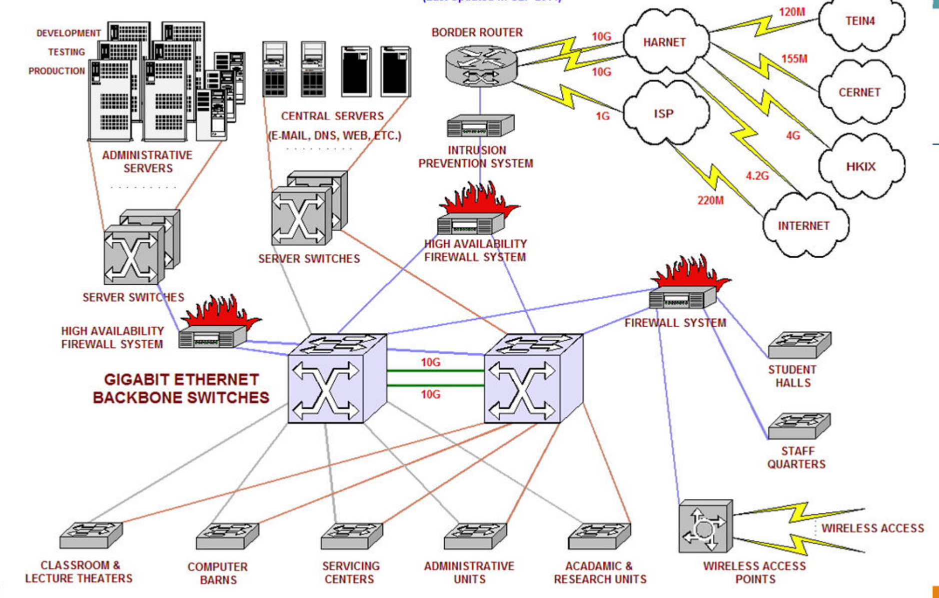
Message Notifications

Options

Courses	New Messages
SPRING2011-12 CELT9901A (L1)	none
SPRING2011-12 PRS1001 (L1)	none

SIMPLIFIED HKUST CAMPUS NETWORK SCHEMATIC

(Last Updated In SEP 2014)



Hacking

“Hacking” is a common term to describe an attack against a network infrastructure, usually but not necessary over the internet.

Types of hacking:

- Web defacement: change the context of a web page.
- Application data attack: obtain secret information, such as customer credit card numbers
- Denial of Service attack: prevent users accessing the server(s).

Hacking events

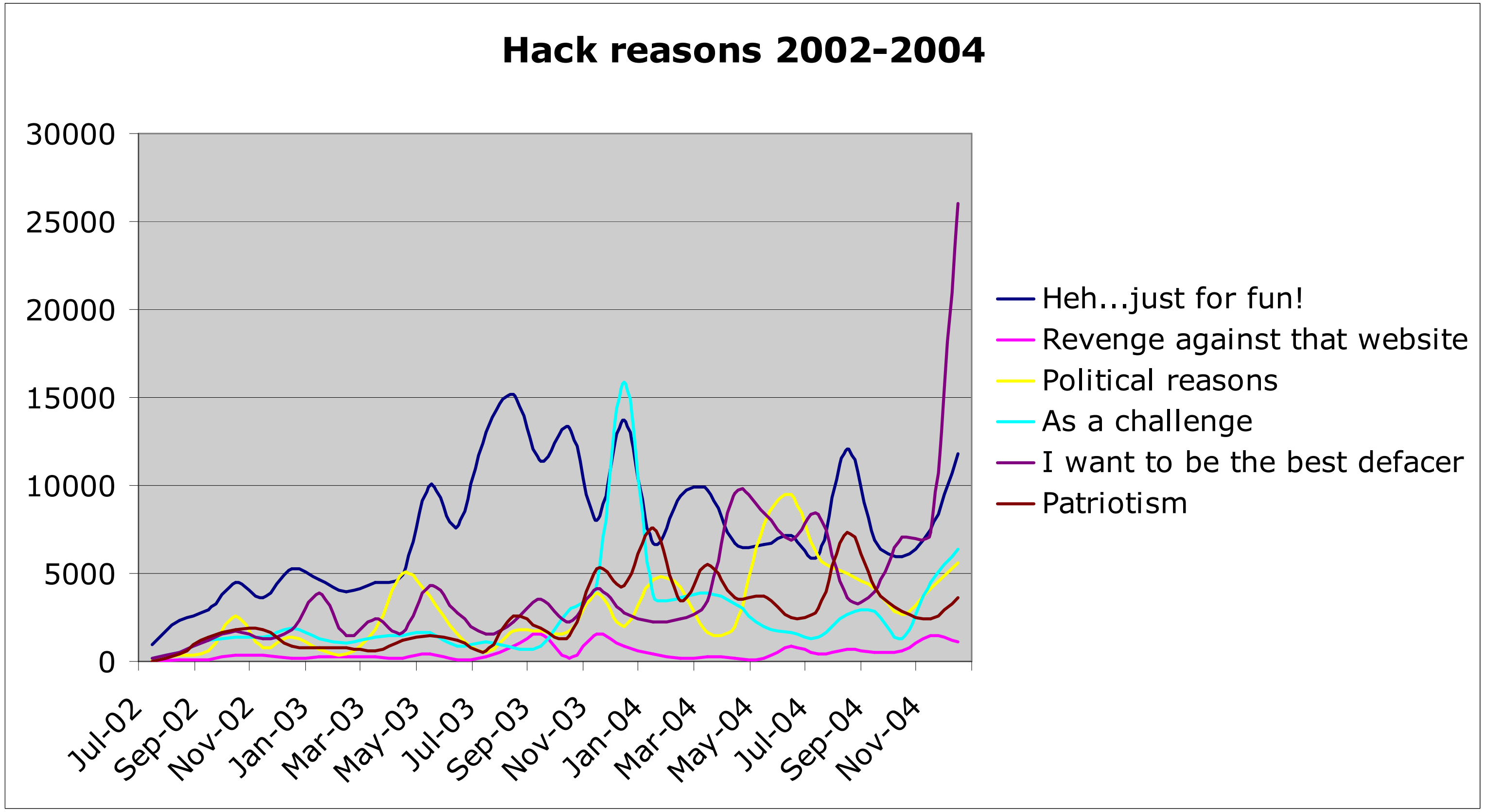
Around over 30 web sites defaced daily!

More on-line banks are hacked:

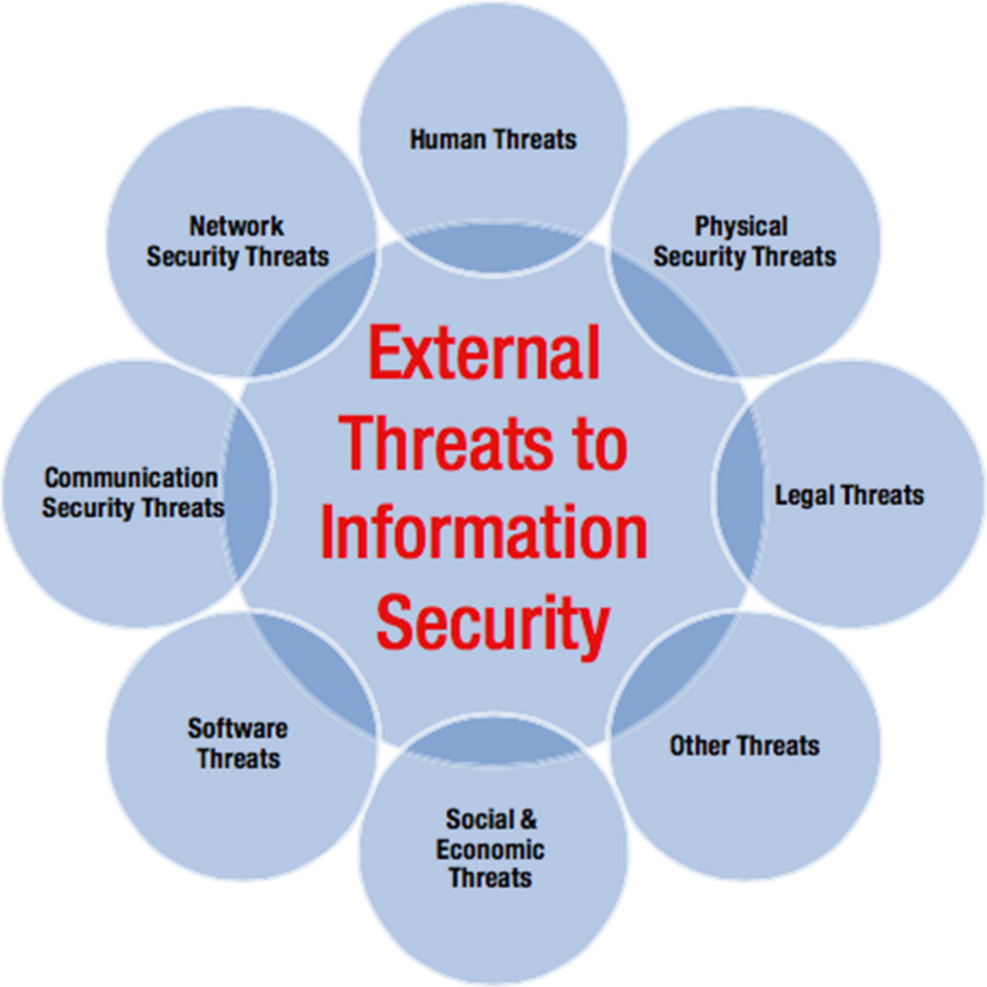
- UK Bank Bardays
- Powergen
- Bank One Online
- HSBC (UK)
- CardSystems Solutions

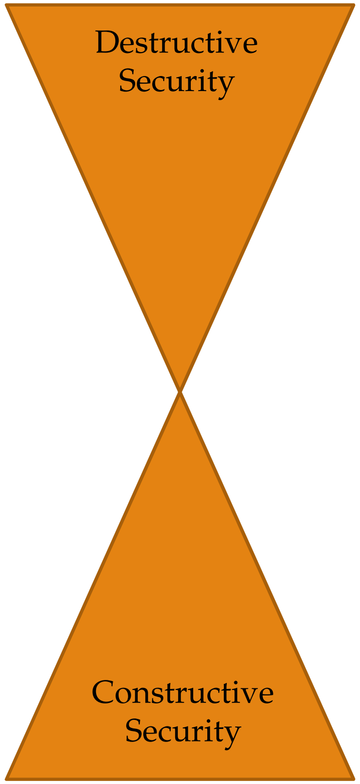
Software giant, Microsoft, has been reported to be hacked 8 times worldwide!

Hack Reasons



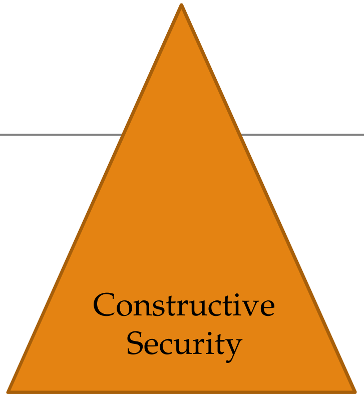
Security Threats and IT Security


Human Threats
Network Security Threats
Physical Security Threats
External Threats to Information Security
Communication Security Threats
Legal Threats
Software Threats
Other Threats
Social & Economic Threats



From InfoSec Handbook (2014)

IT Security Principles



8 Principles of Information Security

Principle 1: Computer Security Supports the Mission of the Organization

Principle 2: Computer Security is an Integral Element of Sound Management

Principle 3: Computer Security Should Be Cost-Effective

Principle 4: Systems Owners Have Security Responsibilities Outside Their Own Organization

Principle 5: Computer Security Responsibilities and Accountability Should Be Made Explicit

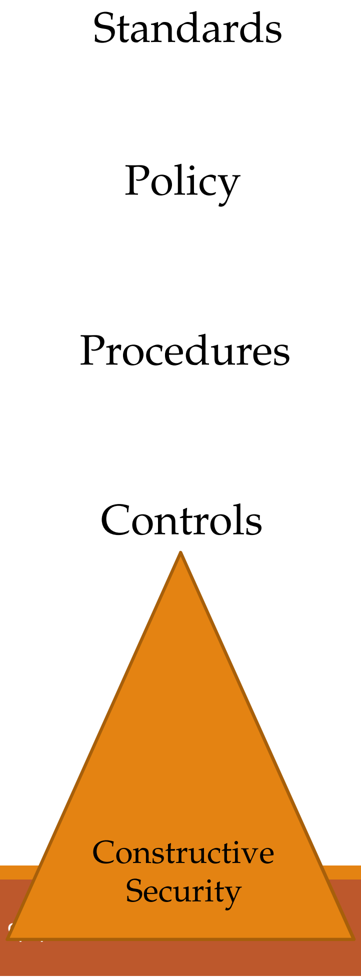
Principle 6: Computer Security Requires a Comprehensive and Integrated Approach

Principle 7: Computer Security Should Be Periodically Reassessed

Principle 8: Computer Security is Constrained by Societal Factors

NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems.

Security from layered approach



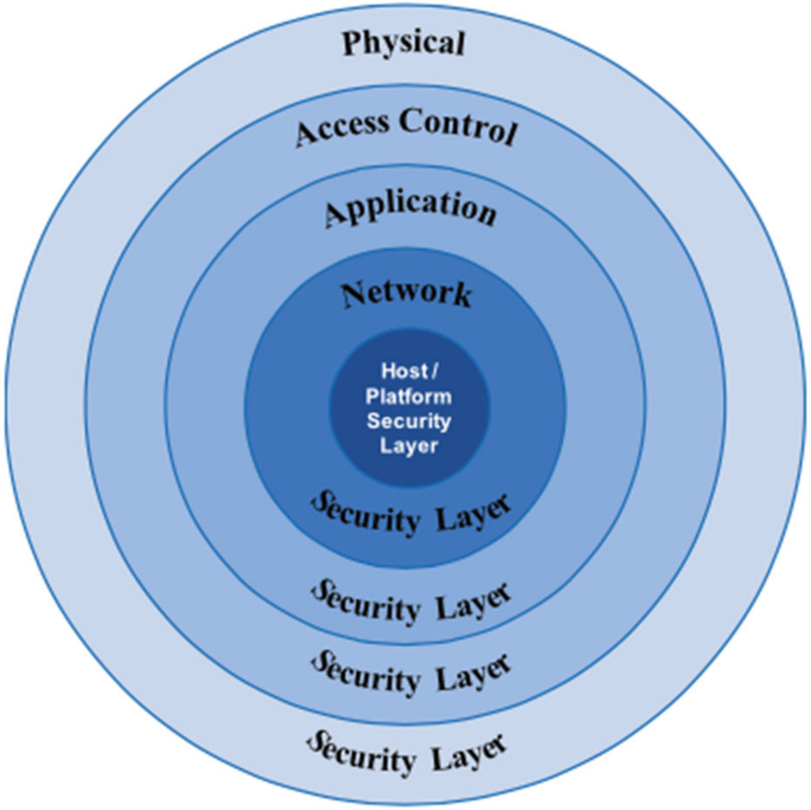
Standards

Policy

Procedures

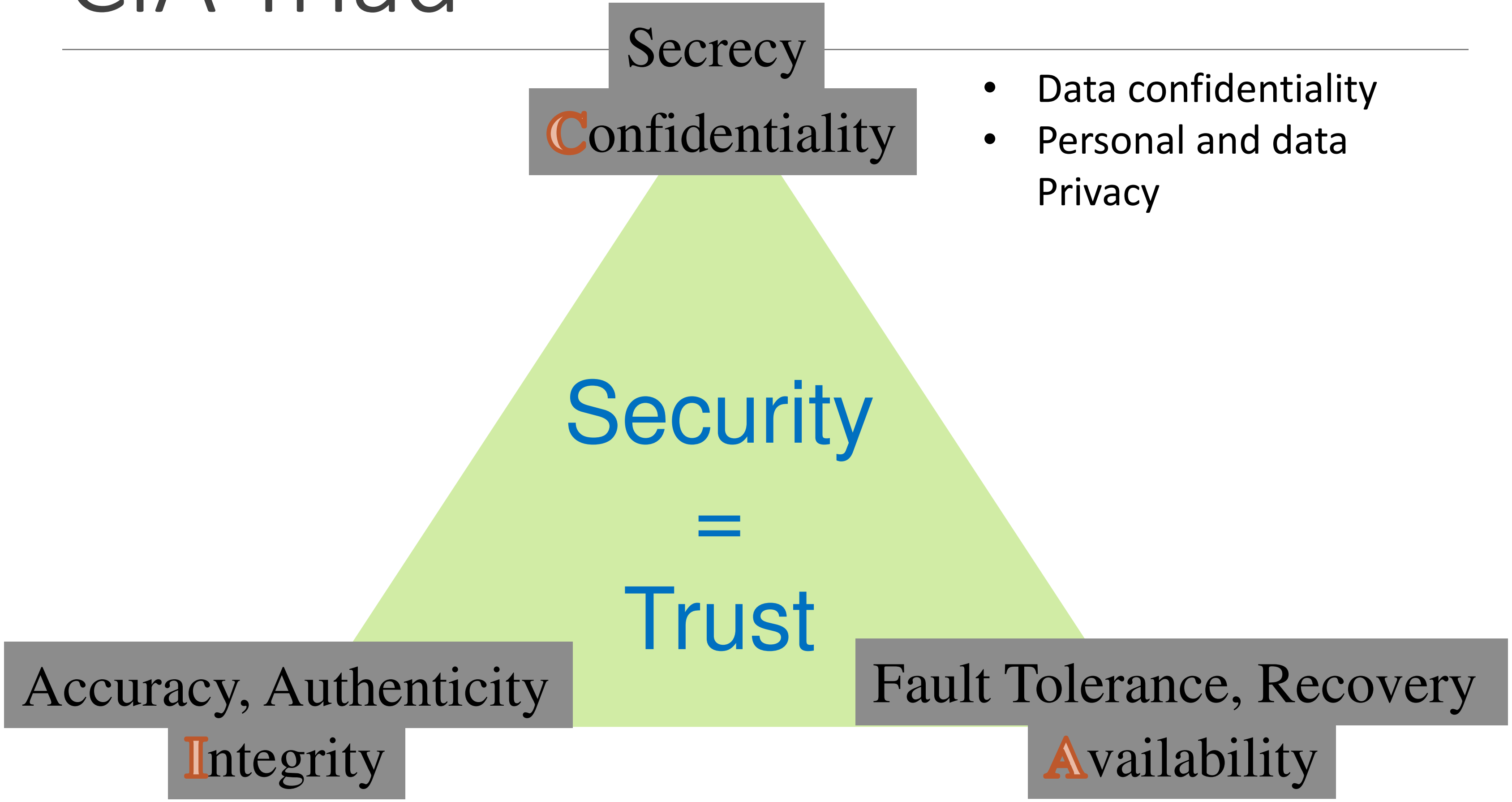
Controls

Constructive Security



From The InfoSec Handbook (2014)

CIA Triad



Secrecy

Confidentiality

Security

=

Trust

Accuracy, Authenticity

Integrity

Fault Tolerance, Recovery

Availability

- Data confidentiality
- Personal and data Privacy

- Data integrity
- System integrity

- System availability

Security Concepts

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems aren't yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

From Computer Security, Principles and Practice (2012)

Security Controls

Controls Types

Preventive

- Prevent errors or omissions from happening
- For example:
  - Employ qualified staff
  - Segregation of duties
  - Physical access control
  - Operational procedure manual

Controls Types

Detective

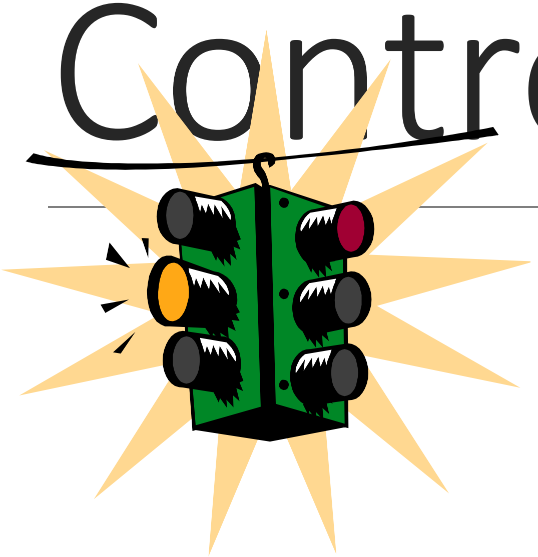
- Detect and report errors or omissions once happened
- For example:
  - Check points in production jobs
  - Tape labels
  - Operations audit

Controls Types

Corrective

- Correct errors
- Mitigate the impact of errors or omissions
- Improve the control mechanism
- For example:
  - System and data backup
  - Re-run jobs
  - Contingency arrangements

What is Access Control?



What is Access Control

In addition to authentication, limit user permission to access other resources according to the assigned privilege

- Art of limiting who can access to which resources
- Entire set of procedures performed using hardware, software and administrators to monitor access, identify users requesting access
- Prevent data from unauthorized viewing, modification or copying
- Prevent system from unauthorized use, modification or denial of service

Access Control Nomenclature

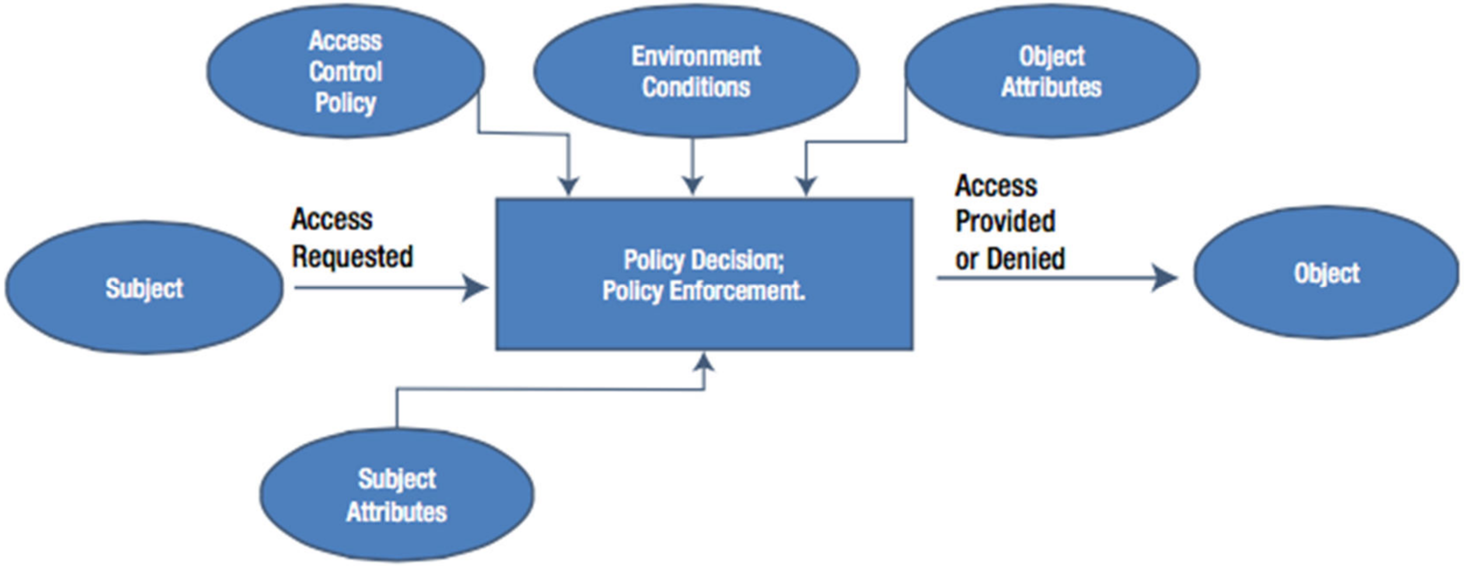
The System Path to identify the person

- Identification
- Authentication
- Authorization
- Accountability

ACSP – Identification & Authentication

Identification and authentication are the keystones of most access control systems.

- Identification is the act of a user professing an identity to a system
- Authentication is verification that the user's claimed identity is valid



From The InfoSec Handbook (2014)

ACSP – Identification & Authentication

Authentication- Identify who you are

- User ID , Password
- Digital Certificate (Cryptographic Keys)
- Passphrase
- Token
- Smart Card
- Memory Card

ACSP – Identification & Authentication

Something you know

- E.g. PIN, password

Something you have

- E.g. Smart token, smart card

Something you inherent

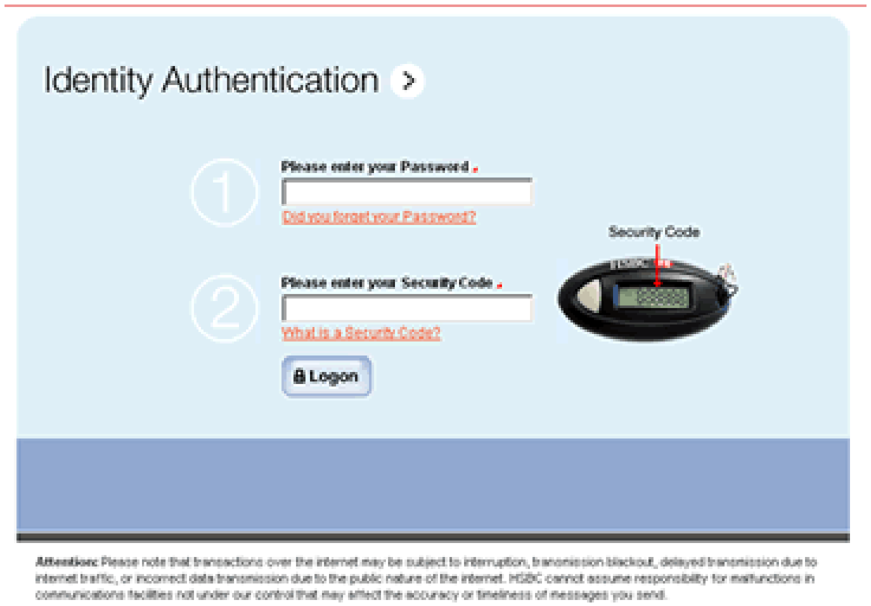
- E.g. fingerprint, voice, retina, handwritten signature

Where you are

- E.g. location of the user logon

ACSP – Authentication -TOKEN

Token is a physical key to identify the person or subject.



Identity Authentication >

1 Please enter your Password .

Did you forget your Password?

2 Please enter your Security Code .

What is a Security Code?

Logon

Attention: Please note that transactions over the internet may be subject to interruption, transmission blackout, delayed transmission due to internet traffic, or incorrect data transmission due to the public nature of the internet. HSBC cannot assume responsibility for malfunctions in communications facilities not under our control that may affect the accuracy or timeliness of messages you send.

ACSP – Authentication – TOKEN (Cont.)

Must possess some tokens

Smart tokens

Smart cards

SecurID

ACSP – Authentication - Smart tokens

Security calculator

Digipass™ 600

Digipass™ 700

ACSP – Authentication - Smart tokens (Cont.)

Credit card-sized devices

Proximity cards, contact card

Using the smart card for authentication

According to the embedded formula in the card

According to the certificate in the card

ACSP – Authentication - Smart tokens (Cont.)

Smart card logon to NT

Smart card access to SunRay-1

PKCS#11 certificate access

CSP certificate usage

ACSP – Authentication - SecurID

One-time password token based generator

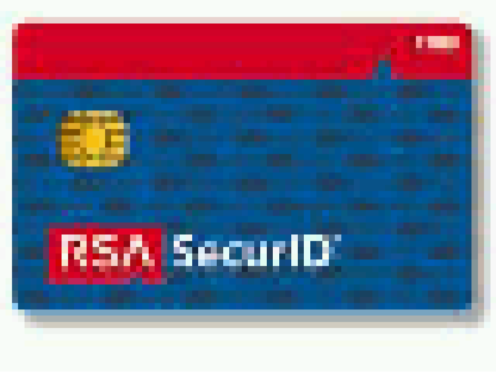
Used for determining the one-time password based on the input value

Using patent technology, the number changes every 30-90 seconds

Using PIN to protect the token

(another example is Vasco token)

ACSP – Authentication – SecurID (Cont.)



ACSP – Authentication - Vasco

gives the system administrators a reliable method of performing, programming, modification or resetting

PIN length, number of PIN trials, number of host com cryptographic algorithm, lengths of challenge and res programmable

can be reactivated locally or remotely using a reverse response scheme

Challenge input can be picked up from the computer can be entered with the keyboard. The maximum ler

Usage of the Data Encryption Standard (DES)

ACSP – Identification & Authentication

Biometric Feature

- Identity of a living person based on physiological or behavioral characteristics
- Identification is a one-to-many search of an individuals characteristics from a database of stored images
- Authentication in biometrics is a one-to-one search to verify a claim to an identity made by a person

ACSP – Identification & Authentication

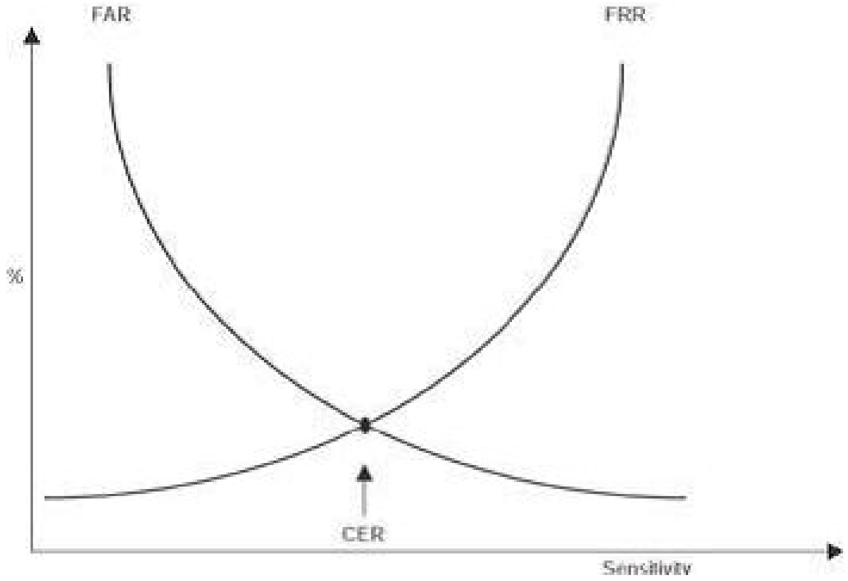
Biometric Feature

- False Rejection Rate (FRR) or Type I Error. The percentage of valid subjects that are falsely rejected
- False Acceptance Rate (FAR) or Type II Error. The percentage of invalid subjects that are falsely accepted
- Crossover Error Rate (CER). The percent in which the False Rejection Rate equals the False Acceptance Rate

ACSP – Identification & Authentication

Biometric Feature

- FRR (Type I Error)
- FAR (Type II Error)
- CER (Crossover Errors)



ACSP – Identification & Authentication

Biometric Feature

- FingerPrints
- Palm Scan
- Hand Geometry
- Retina Scan
- Iris Scan
- Signature Dynamics
- Keyboard Dynamics
- Voice Print
- Facial Scan
- Hand Technology

Biometrics

Measurements of personal characteristics

Comparing and matching of the stored personal information with the input info

Advantages

- Unique
- Difficult to duplicate or forge
- Always possess these data

Voiceprint

Mathematical representations of a person’s speech patterns

Respond to a user’s audible request to speak

May be consists of complete phrases or single, unrelated words

Four steps

- Pre-processing
- Sampling
- Testing
- System response

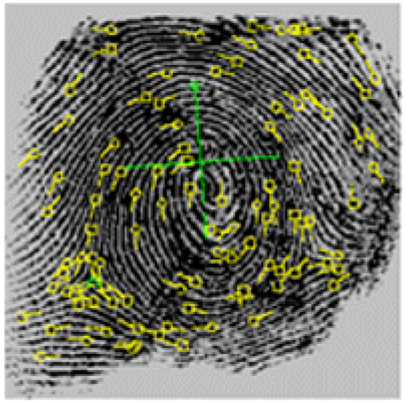
Fingerprint

Granting or denying access based on user's fingerprint

The most widely accepted biometrics verification

Authentication procedures based on 5 processes

- Obtain information
- Fingerprint cleaning
- Feature extraction
- Fingerprint comparison
- System response



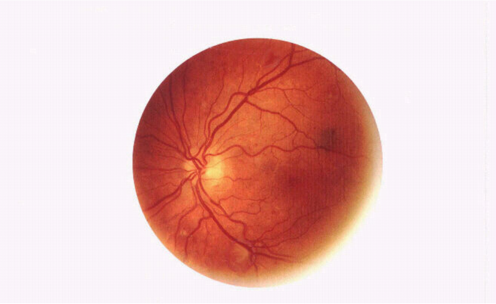
Retina

Based on the blood vessel pattern at the back of the user's eye

Exceptionally accurate and currently impossible to forge or duplicate

Scanned by injecting an infrared beam to the back of the eye

Low user acceptance



Iris

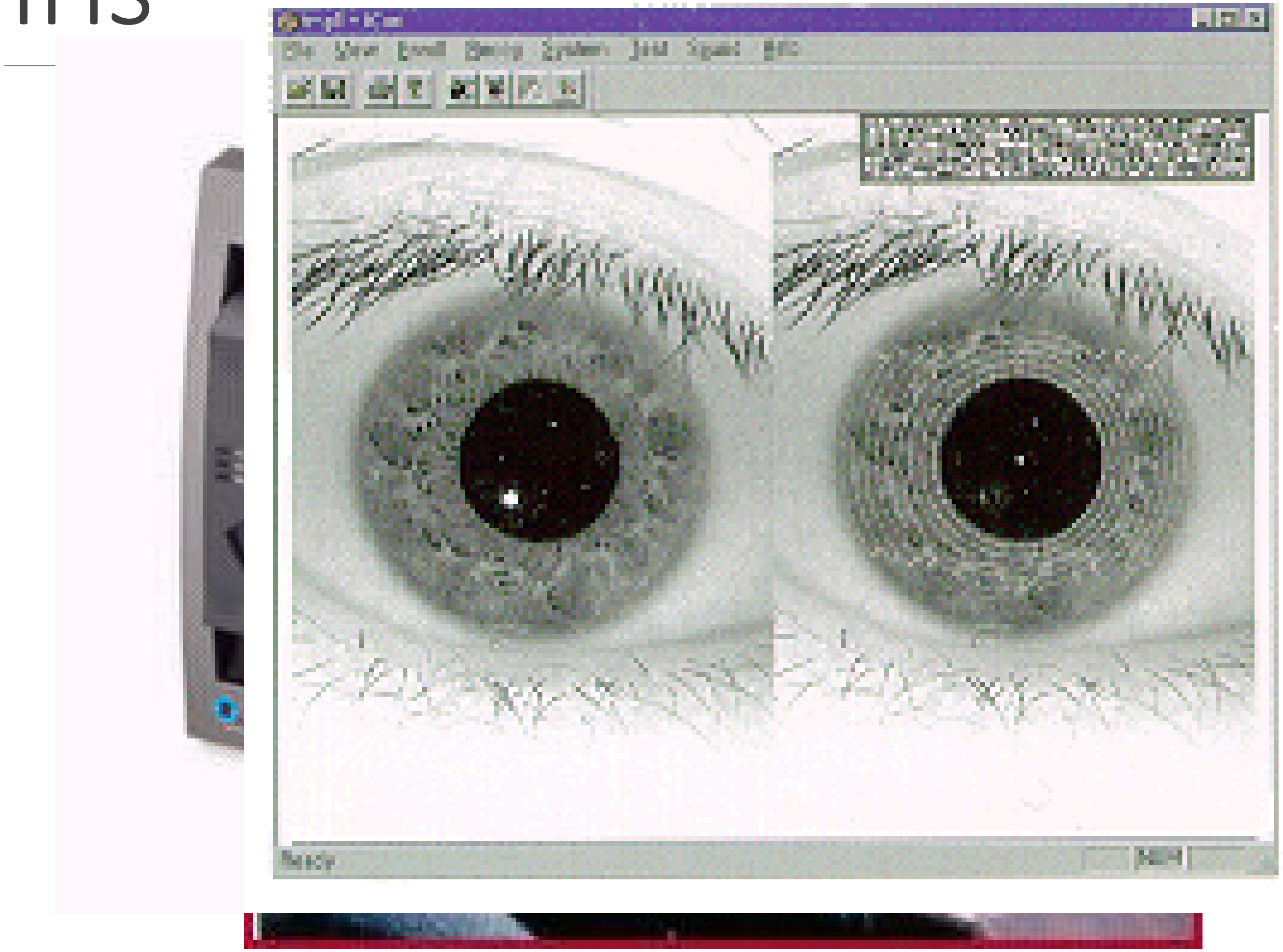
Determining user identity by the pattern on the iris

No light beam is required to be injected to the eye

Normal camera could be used

Exceptionally high accuracy (even higher than fingerprint)

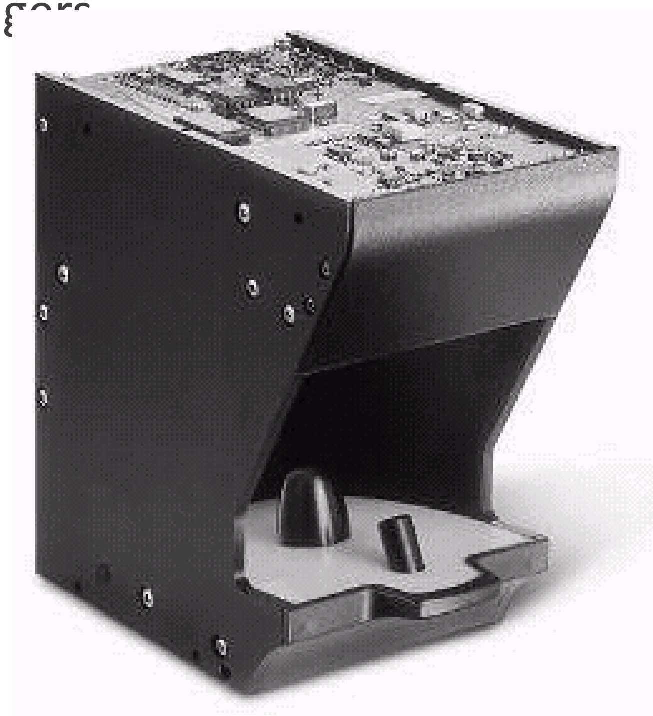
Iris



Hand Geometry

Depends on hyper-accurate measurements of person’s fingers and finger-webbing

Capture the geometry of the palm and fingers



Handwritten Signature

Behavioral biometrics measurement not physiological biometrics

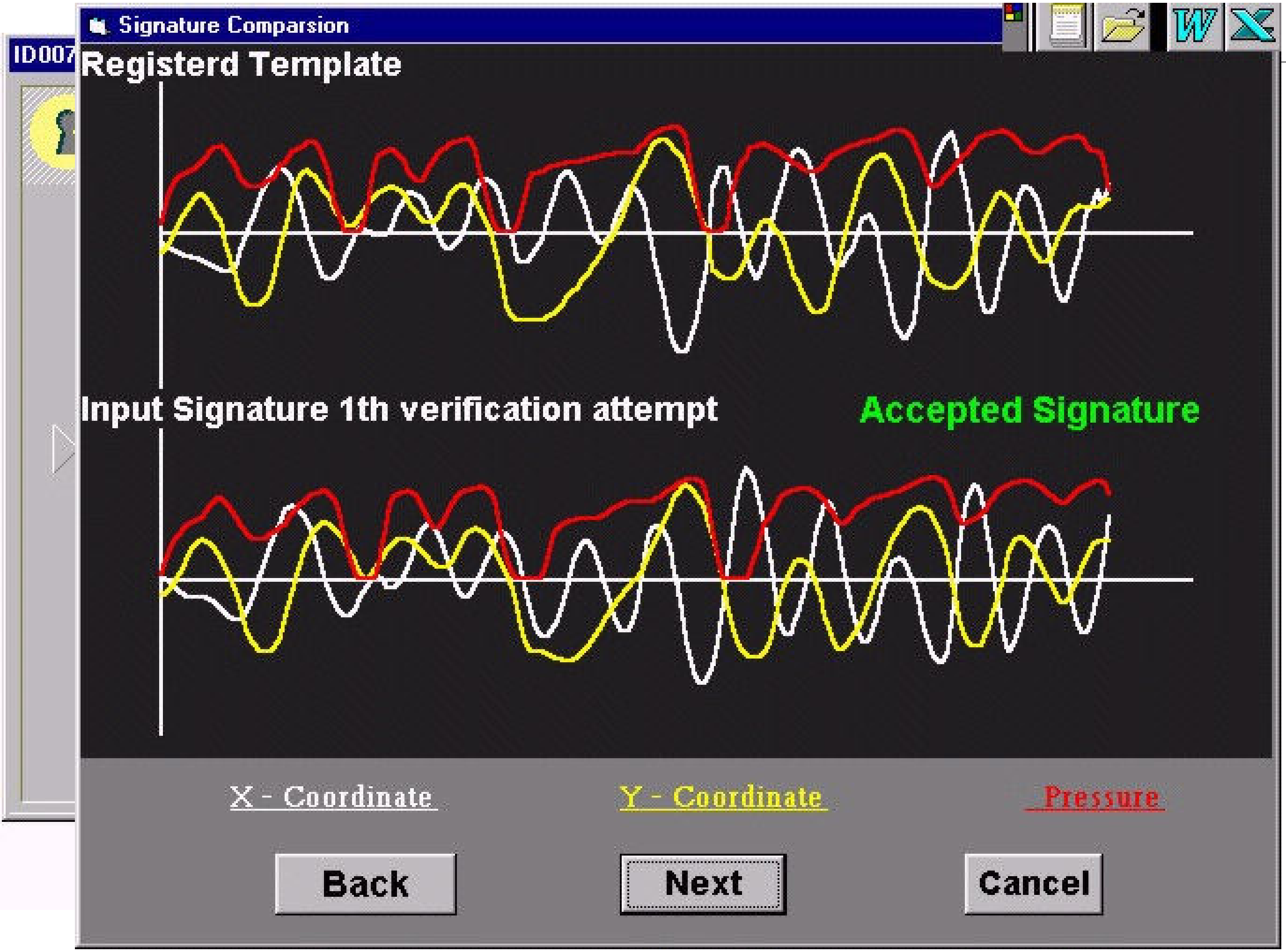
Depends on user's habits

Widely accepted in traditional world

Authentication process in 4 steps

- Obtaining information
- Measuring characteristics
- Comparing signature
- System response

Handwriting Signature



Biometrics Keys Measurement

Not as precise as static key or cryptographic key

Even the same person may not be able to generate the same key

Depends on FAR (false acceptance ratio) and FRR (false rejection ratio)

Reduce FAR may increase FRR

ACSP – Identification & Authentication (Cont.)

One-factor Identification

- Password
  - One-Time password (Max. Security)
  - Static password (same for each login)
  - Dynamic password (regular change password)
- Passphrase
  - A sequence of characters that is usually longer than the allotted number for password

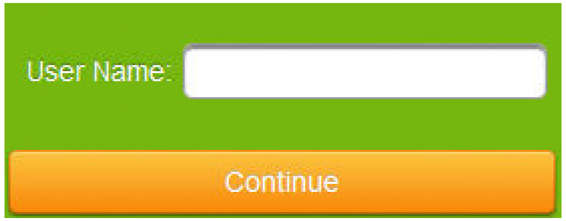
ACSP – Identification & Authentication (Cont.)

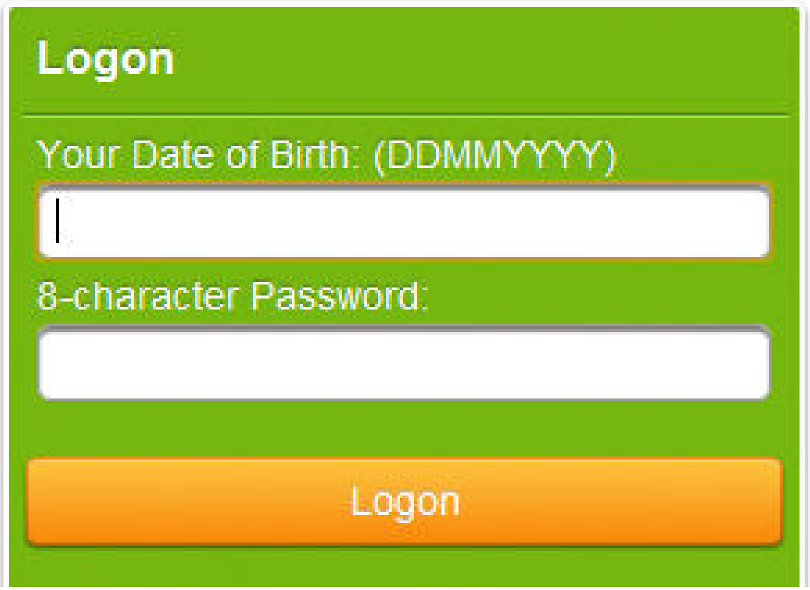
Two-factor Identification

- Token Based (ebanking token, secured token)
- Machines Based (phone sms identification code)
- Biometric Feature
- Card based (HKID card, SSL Cert.)

Two Factor Authentication?

Is this considered two factor authentication?



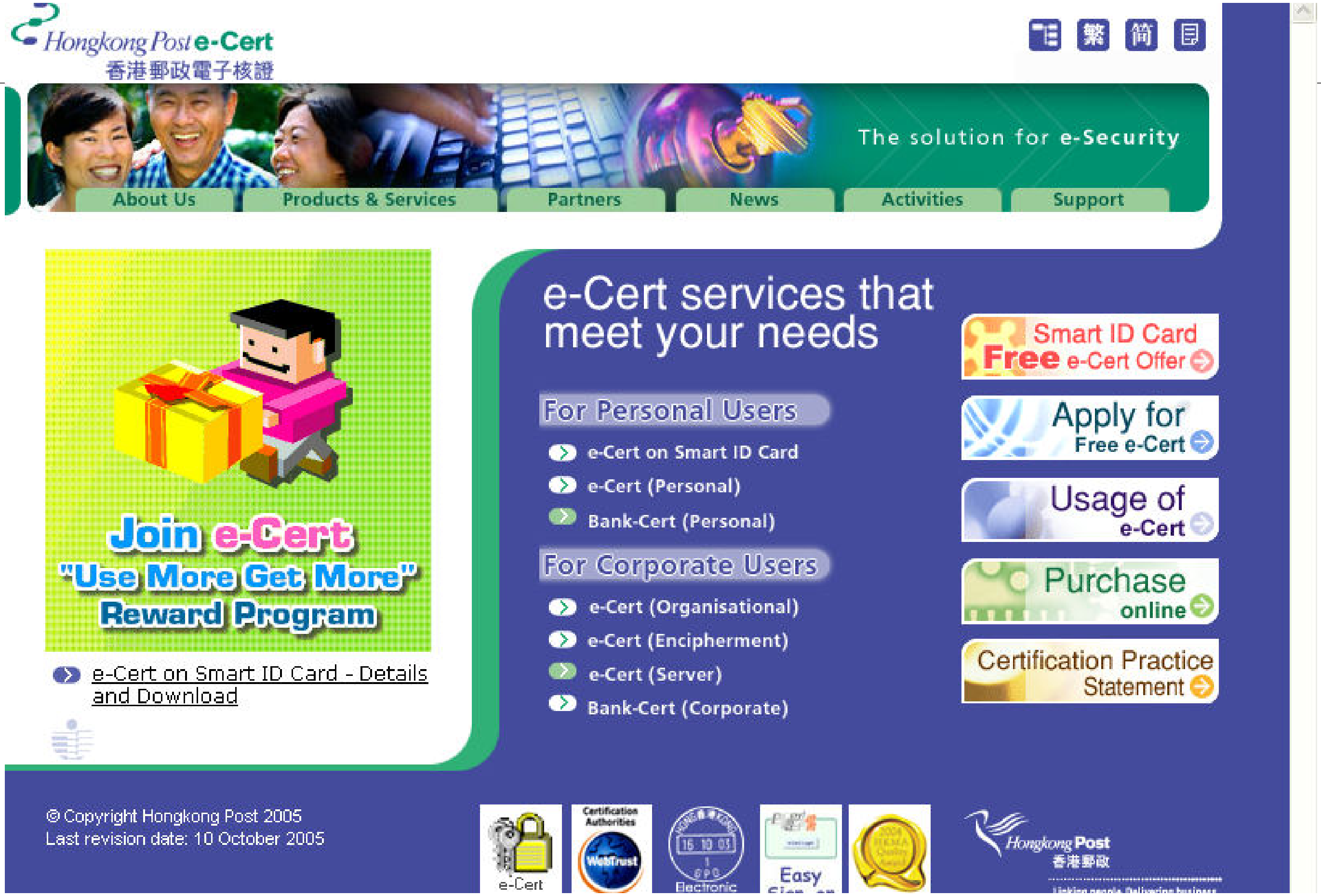


ACSP – Identification - PhoneSMS

What is a One-time Password (OTP)?

- One-time Password (OTP) is a security feature which sends a 6-digit OTP transmitted to your mobile phone number via a SMS
- Example: Standard Chartered ebanking service
  - Add Transfer Payee
  - Add Bill Payee - Jetco Member Bank Credit Cards
  - Online Payment (for payment to "BOCI Securities Limited", "ETrade Securities Hong Kong" and "Savills Property Management Limited")
  - Update Personal Information

ACSP – Authentication - eCert



Hongkong Post e-Cert
香港郵政電子核證

The solution for e-Security

About Us | Products & Services | Partners | News | Activities | Support

Join e-Cert
"Use More Get More"
Reward Program

e-Cert on Smart ID Card - Details and Download

e-Cert services that meet your needs

For Personal Users

- e-Cert on Smart ID Card
- e-Cert (Personal)
- Bank-Cert (Personal)

For Corporate Users

- e-Cert (Organisational)
- e-Cert (Encipherment)
- e-Cert (Server)
- Bank-Cert (Corporate)

Smart ID Card Free e-Cert Offer

Apply for Free e-Cert

Usage of e-Cert

Purchase online

Certification Practice Statement

© Copyright Hongkong Post 2005
Last revision date: 10 October 2005

ACSP – Authentication Method

Single Sign on (SSO)

- cumbersome situation of logging on multiple times to access different resources.
- Pros
  - User and Administration Convenience
  - Efficient tracking of user activities
- Cons
  - Require strong authentication
  - Level of integration into existing system

ACSP – Authentication Method (Cont.)

Kerberos

- Using symmetric key cryptography
- The centralized servers implement the Kerberos-trusted Key Distribution Center (KDC), Kerberos Ticket Granting Service (TGS), and Kerberos Authentication Service (AS)
- Windows 2000 provide Kerberos Service in the Active Directory Service

ACSP – Authentication Method

Kerberos

- The KDC knows the secret keys of all clients and servers on the network.
- The KDC initially exchanges information with the client and server by using these secret keys
- Kerberos authenticates a client to a requested service on a server through TGS, and by issuing temporary symmetric session keys for communications between the client and KDC, the server and the KDC, and the client and server
- Communication then takes place between the client and th
- server using those temporary session keys

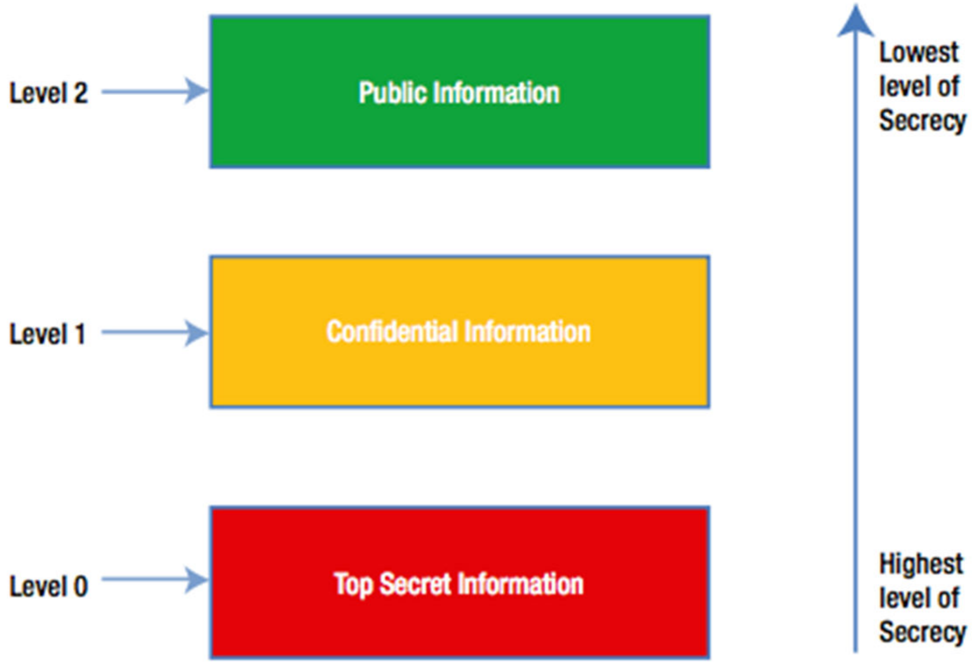
From Authentication to Authorization

Authorization – Access Control Technique

Authorization can occur only after the subject's identity has been verified through authentication

Systems provide authorization through the use of access controls

Access controls manage the type and extent of access subjects have to objects



Authorization – Access Control Technique (Cont.)

Mandatory Access Control (MAC) Model

Discretionary Access Control (DAC) Model

Role-Based Access Control (RBAC) Model

Authorization – Mandatory Access Control Model (MAC)

Use of Labels to identify the level of the SUBJECT and OBJECT

Subjects are labeled by their level of clearance (secret, top secret, confidential and so on). Objects are labeled by their level of classification or sensitivity (secret, top secret, confidential and so on)

This type of model is used in environments where information classification and confidentiality is of utmost importance – like a military institution

Authorization – Discretionary Access Control Model (DAC)

Owner or creator of an object to control and define subject access to that object

Using access control lists (ACLs) on objects

Each ACL defines the types of access granted or restricted to individual or grouped subjects

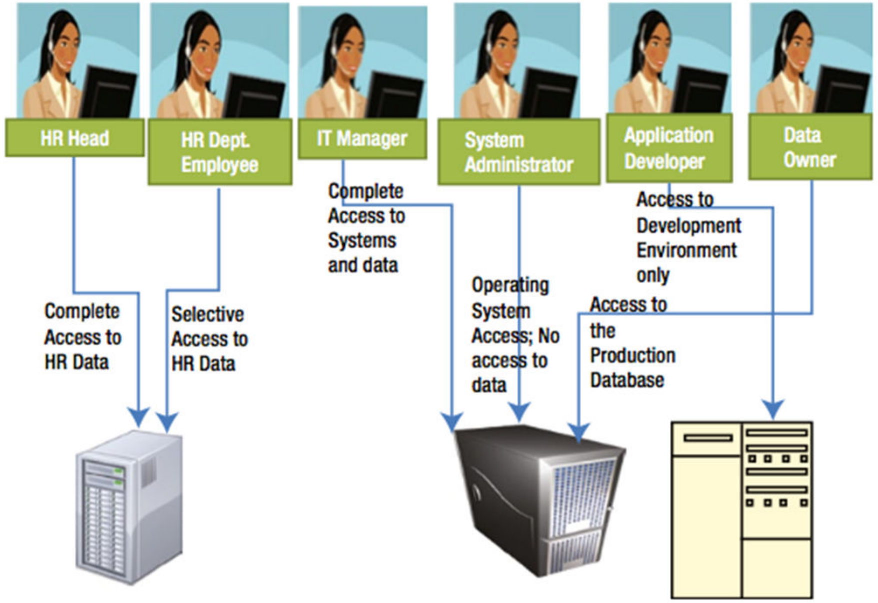
Does not offer a centrally controlled management system because owners can alter the ACLs on their objects

Authorization – Role-Based Access Control Model (RBAC)

Centrally administrated set of controls to determine how subjects and objects interact

Allows access to resources based on the role the user holds within the company

Administrators put users into roles and then assign access rights to those roles

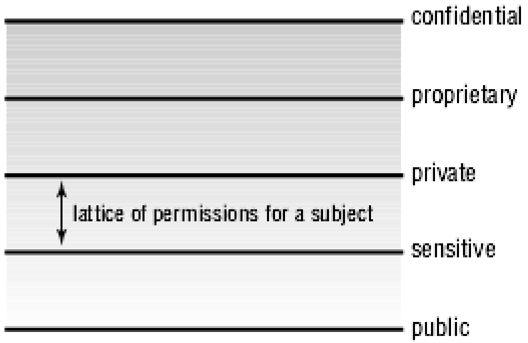


HR Head
HR Dept. Employee
IT Manager
System Administrator
Application Developer
Data Owner
Complete Access to HR Data
Selective Access to HR Data
Complete Access to Systems and data
Operating System Access; No access to data
Access to Development Environment only
Access to the Production Database

Authorization – Lattice-Based Access Control (LBAC)

Variation of RBAC

It provides an upper bound and lower bound of access capabilities for every subject and object relationship.



Authorization – Rule Based Access Control

Specific rules that indicate what can and cannot happen to an objects

Example, routers and firewalls rules to determine which types of packets and requests are allowed into a network and which ones are rejected

Authorization – Restricted Interface

User interfaces restrict users' access abilities by not allowing them to request certain functions, information, or have access to specific system resources

Major types of restricted interfaces: menus and shells, database views, and physically constrained interfaces.

Authorization – Access Control Matrix

Subjects and objects indicating what actions individual subjects can take upon individual objects

Users	File1	File2
Amy	Read/Execute	No access
Peter	Read/Write	Read/Execute

Authorization – Capability Tables

The access rights a certain subject possesses pertaining to specific object

User Amy:

Plotter – print

Printer – print

Abc.xls – full control

Aac.doc – read only

Payrool.xls – no access

Authorization – Access Control List

List of subjects that are authorized to access a specific object

Printer A

Amy – Print

Peter – Print

Administrator – Full Control

David – No access

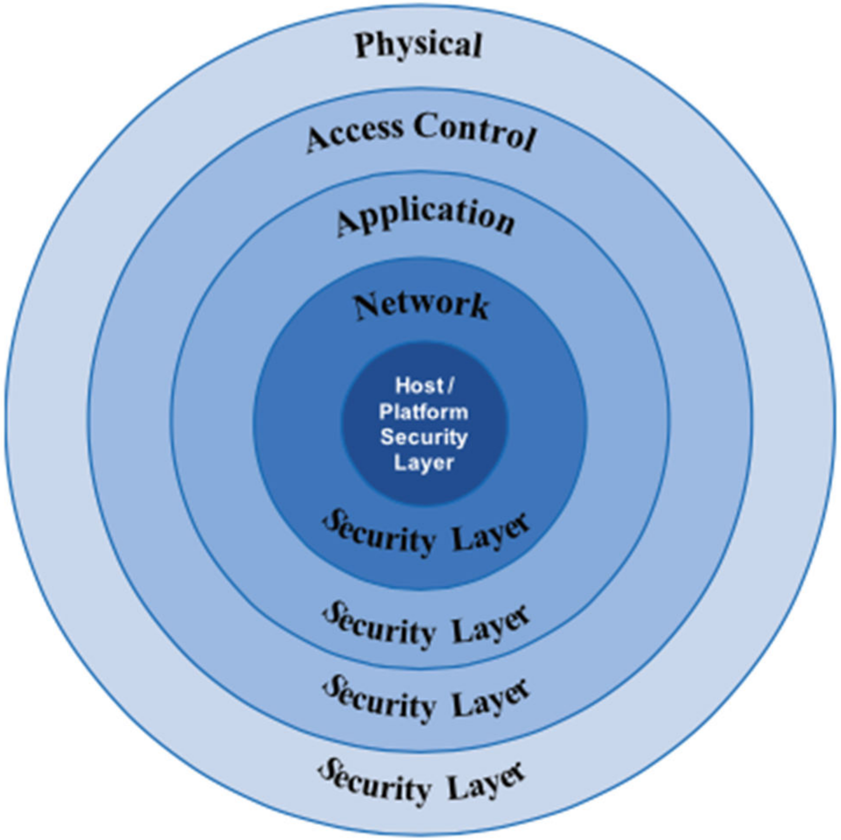
Overall Security Controls

Host Security Layer

- Authentication
- Authorization
- Encryption
- Monitoring
- Accountability

Network Security Layer

- Firewall
- Intrusion Detection/ Prevention
- Encryption



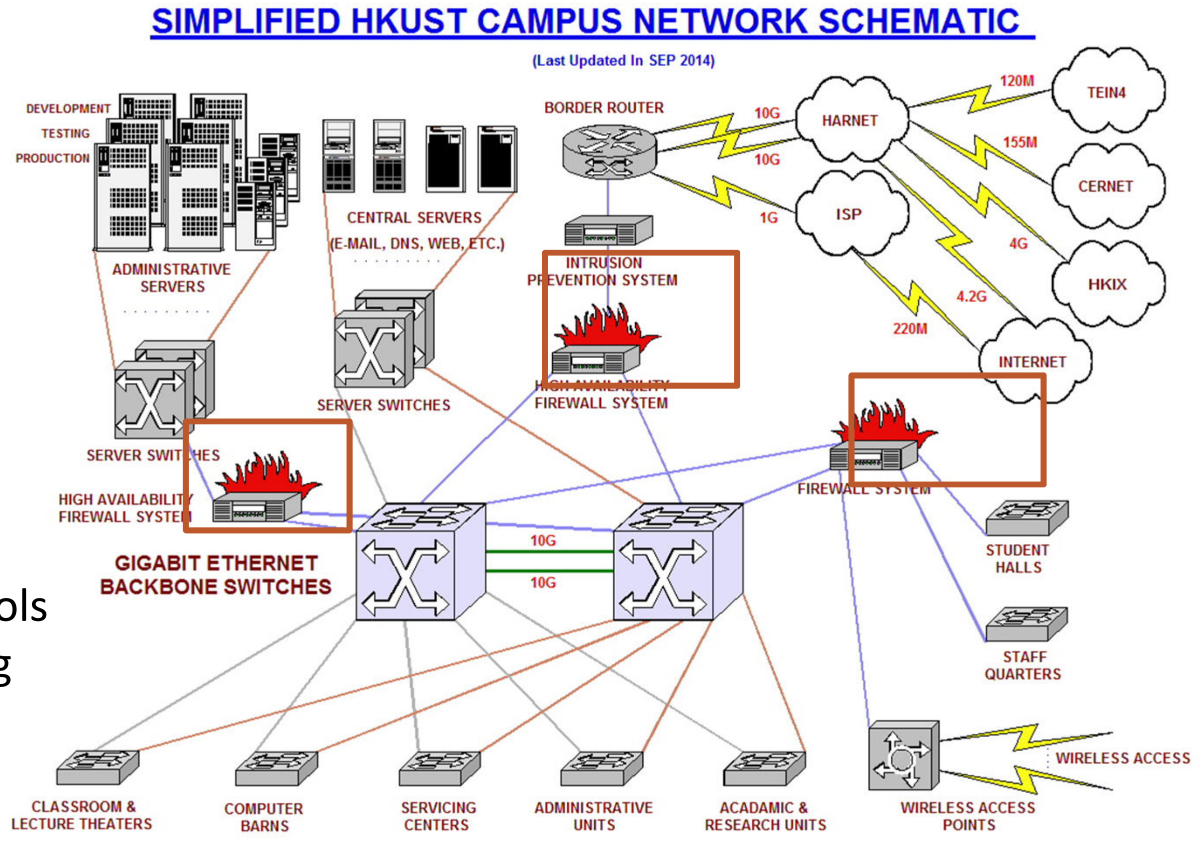
Extend from Host to Network

Access Control (Preventive controls)

- Firewall
- Routers
- VPN/SSL

Detective controls

- Audit logging
- IDS/IPS


SIMPLIFIED HKUST CAMPUS NETWORK SCHEMATIC
(Last Updated In SEP 2014)
DEVELOPMENT
TESTING
PRODUCTION
ADMINISTRATIVE SERVERS
CENTRAL SERVERS (E-MAIL, DNS, WEB, ETC.)
BORDER ROUTER
10G
10G
1G
HARNET
ISP
120M
155M
4G
4.2G
220M
TEIN4
CERNET
HKIX
INTERNET
INTRUSION PREVENTION SYSTEM
HIGH AVAILABILITY FIREWALL SYSTEM
SERVER SWITCHES
SERVER SWITCHES
HIGH AVAILABILITY FIREWALL SYSTEM
FIREWALL SYSTEM
GIGABIT ETHERNET BACKBONE SWITCHES
10G
10G
STUDENT HALLS
STAFF QUARTERS
WIRELESS ACCESS
CLASSROOM & LECTURE THEATERS
COMPUTER BARNS
SERVICING CENTERS
ADMINISTRATIVE UNITS
ACADAMIC & RESEARCH UNITS
WIRELESS ACCESS POINTS

Constructive Security

Access Control Practices & Monitoring

Accountability

Auditing

IDS/IPS

ACPM - Accountability

Capable to link an activity to the initiating party

Essential for legal liability tracking

Remember the quote

- “can deal with security attacks as long as I know who did it ,and where to find it”

Capture

- System – Level Events
- Application – Level Events
- User – Level Events

ACPM - Intrusion Detection

Prevention , Detection , Response

Complement preventive security measures

Same as firewall , you cannot install and go away !

ACPM - Intrusion Detection (Cont.)

Attacks

- Brute force or Dictionary
- Spoofing
- Denial of Service (DOS)
  - TCP SYN, Ping of Death, Teardrop , SMURF
  - Spamming
- Man-in-the-middle
- Sniffer
- Malicious code e.g. Worm , virus, trojan horse

ACPM - Intrusion Detection (Cont.)

IDS Process Model

- Information Source
- Analysis
- Response

IDS Architecture

- Host-Target Co-location
- Host-Target Separation

IDS/IPS types

- Network based IDS/IPS
- Host-based IDS/IPS
- Application based IDS/IPS

ACPM - Intrusion Detection - Analysis

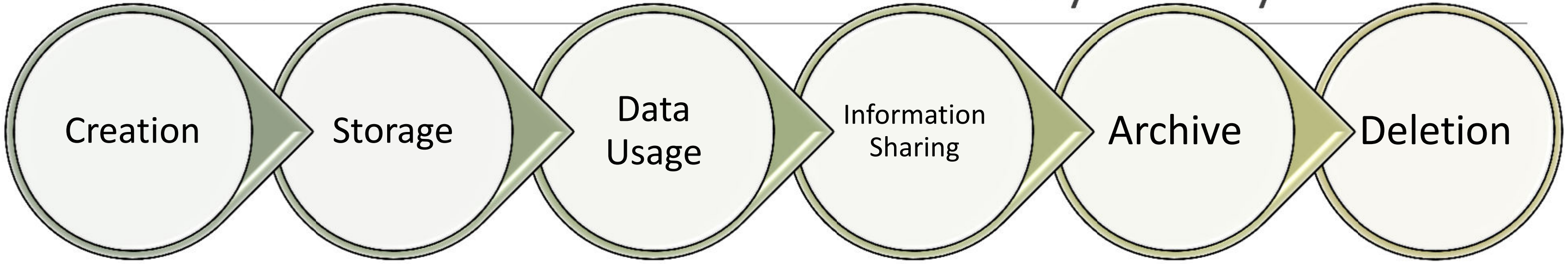
Misuse Detection

- Look for predefined threat (signature)
- Most common in commercial IDS

Anomaly Detection

- Look for abnormal patterns
  - Threshold analysis
  - Statistical measures
  - Others : Rule-based , neural network etc
- Future trend of IDS?

Another direction – Data Security Lifecycle



1. Data creation
2. Storage
   - Enforce access control
   - Sensitive data should be encrypted
3. Data usage
4. Information Sharing
5. Archive
6. Deletion

Security Architecture (Example) - SABSA

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The business	Business risk model	Business process model	Business organization and relationships	Business geography	Business time dependencies
Conceptual	Business attributes profile	Control objectives	Security strategies and architectural layering	Security entity model and trust framework	Security domain model	Security-related lifetime and deadlines
Logical	Business information model	Security policies	Security services	Entity schema and privilege profiles	Security domain definitions and associations	Security processing cycle
Physical	Business data model	Security rules, practices and procedures	Security mechanisms	Users, applications and user interface	Platform and network infrastructure	Control structure execution
Component	Detailed data structures	Security standards	Security products and tools	Identities, functions, actions and ACLs	Processes, nodes, addresses and protocols	Security step timing and sequencing
Operational	Assurance of operational continuity	Operational risk management	Security service management and support	Application and user management and support	Security of sites and platforms	Security operations schedule

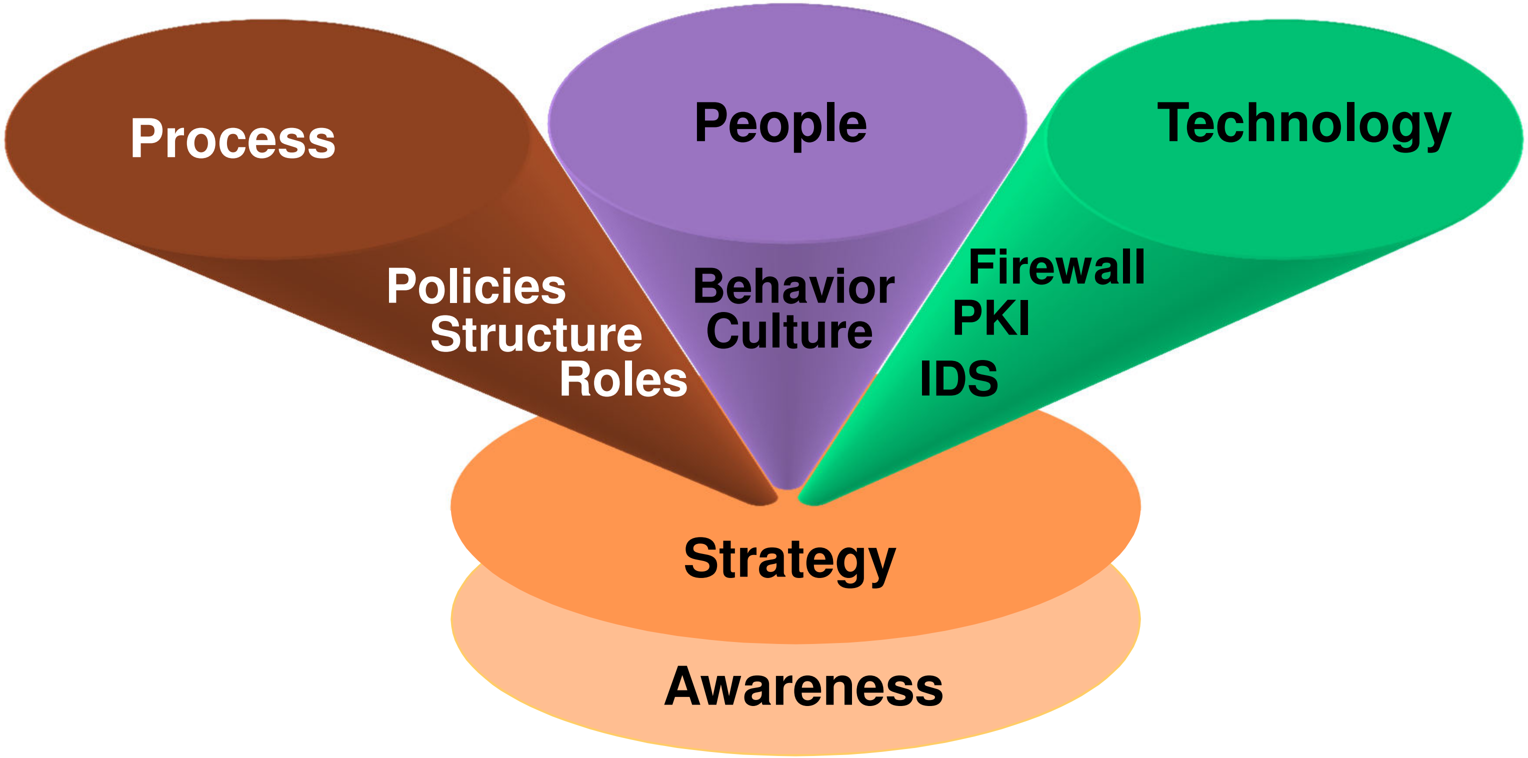
http://en.wikipedia.org/wiki/Sherwood_Applied_Business_Security_Architecture

Security Architecture (Example) – X.800

X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

Five categories of services	14 specific services
Authentication	1. Peer Entity Authentication 2. Data-Origin Authentication
Access Control	1. Access Control
Data Confidentiality	1. Connection Confidentiality 2. Connectionless Confidentiality 3. Selective-Field Confidentiality 4. Traffic-Flow Confidentiality
Data Integrity	1. Connection Integrity with Recovery 2. Connection Integrity without Recovery 3. Selective-Field Connection Integrity 4. Connectionless Integrity 5. Selective-Field Connectionless Integrity
Non-Repudiation	1. Non-Repudiation, Origin 2. Non-Repudiation, Destination

Pillars of Security



Process

Policies
Structure
Roles

People

Behavior
Culture

Technology

Firewall
PKI
IDS

Strategy

Awareness

What is IT Security (10 domains in CISSP)

CISSP Domains	Key topics in domain
Access Control	• Identification, authentication, and authorization technologies • Discretionary versus mandatory access control models • Rule-based and role-based access control
Application Development Security	• Software development models • Database models • Relational database components
Business Continuity and Disaster Recovery Planning	• Planning • Roles and responsibilities • Liability and due care issues • Business impact analysis
Cryptography	• Block and stream ciphers • Explanation and uses of symmetric algorithms • Explanation and uses of asymmetric algorithms
Information Security Governance and Risk Management	• Types of security controls • Security policies, standards, procedures, and guidelines • Risk management and analysis

Table 0.1 of Computer Security Principles and Practice 2nd Edition, William Stallings

What is IT Security (10 domains in CISSP)

CISSP Domains	Key topics in domain
Legal, Regulations, Investigations and Compliance	• Privacy laws and concerns • Computer crime investigation • Types of evidence
Operations Security	• Operations department responsibilities • Personnel and roles • Media library and resource protection
Physical (Environmental) Security	• Facility location and construction issues • Physical vulnerabilities and threats • Perimeter protection
Security Architecture and Design	• Critical components • Access control models • Certification and accreditation
Telecommunications and Network Security	• TCP/IP protocol suite • LAN, MAN, and WAN technologies • Firewall types and architectures

Table 0.1 of Computer Security Principles and Practice 2nd Edition, William Stallings

Destructive Security

What’s the attack methods?

UNDERSTAND HOW NETWORK BASED ATTACK CAN BE INITIATED

Types of Security Attacks

Exploitation
- Buffer Overflow

Cross-site scripting

SQL Injection

Canonicalization

Authentication and authorization attack
- Brute force attacks
- Dictionary attacks
- Cookie replay attacks
- Credentials theft
- Authorization

Sensitive information disclosure
- Disclosure of confidential data
- Sensitive Data

Input manipulation
- Parameter Manipulation
- Query String manipulation
- Form field manipulation
- HTTP Header manipulation
- Data tampering

Configuration issue
- Over-privileged process and accounts
- Configuration management
- Unauthorized access to administration interfaces
- Unauthorized access to configuration stores
- Retrieval of plain text configuration secrets

Lack of individual Accountability

Session Hijacking

Luring Attacks

Network Attack
- Session Replay
- Session Hijacking
- Man in the middle attacks
- Network Eavesdropping

Encryption Attack
- Weak key management
- Weak Encryption

Method of Attacks

Brute Force

- Identifying secret data by testing all possibilities is referred to as an exhaustive attack
  - E.g. identify a valid password by testing all possible passwords until a match is found.
- Prevention:
  - Increasing the length of a password

Method of Attacks (Cont.)

Spoofing

- Spoofing is an attack in which one person or process pretends to be a person or process
  - E.g. user A can mimic behavior to make process B believe user A is user C. In the absence of any other controls, B may be duped into giving to user A the data and privileges that were intended for user C.

Method of Attacks (Cont.)

Denial of Service (DOS)

- Attack on the operating system or software using buffer overflows
- The result is that the target is unable to reply to service requests
  - E.g. TCP SYN Attack
  - E.g. Ping of Death
  - E.g. Land.c. Attack

Method of Attacks (Cont.)

Dictionary

- Dictionaries may be used in a cracking program to determine passwords
- A short dictionary attack involves trying a list of hundreds or thousands of words that are frequently chosen as passwords against several systems

Method of Attacks (Cont.)

Man-in-middle

- Based on asymmetric encryption
- Somebody evil could generate a key pair, give the public key away and tell everybody, that it belongs to somebody else. Now, everyone believing it will use this key for encryption, resulting in the evil man being able to read the messages
- Prevention
  - Making sure public keys are really belong to the one being designated as owner

Method of Attacks (Cont.)

Spamming

- Repeatedly sending an identical email message to a particular address characterize email “bombing”

Sniffer

- A sniffer is a program and/or device that monitor data traveling over a network

Method of Attacks (Cont.)

Cracker

- Crackers are individuals who try to break into a computer system
- Sole aim is to break into secure systems, hackers are more interested in gaining knowledge about computer systems and possibly using this knowledge for playful pranks

Method of Attacks (Cont.)

Buffer overflow

- Through the vulnerabilities in the overwritten issues of memory buffer.

Protocol vulnerability

- Attack to systems based on the vulnerability exists in the protocol used

Software Flaw

- Attack through software error or porous defense of the system

External Security Threats

Physical Threats

- Natural disasters like cyclones, hurricanes, floods, earthquakes, etc.
- Fire
- Terrorist threats like bombs, hostage situation
- Hardware destruction
- Physical intrusion
- Sabotage
- Theft of the assets and Intellectual Property sensitive assets/information

Network Threats

- Sniffing or Eavesdropping
- TCP/IP issues like snooping, authentication attacks, connection hijacking
- Spoofing
- Man in the middle attack
- Denial of service attacks
- SQL injection
- Exploitation of default passwords on network equipment being unchanged
- Exploitation of weak encryption

Software Issues

- Defects leading to errors Defects being exploited
- Malware like Viruses, Worms, Trojans, Back doors
- Bots or Botnets Invalidated inputs
- Authentication attacks
- Exploitation of misconfigurations
- Session Management related issues
- Inappropriate error handling or exception handling by the applications
- Buffer overflow issues
- Cryptography wrongly handled by applications
- Parameter manipulations
- Operating system related issues – security flaws in the operating system

Human Threats

- Social engineering
- Attack by hackers/man in the middle
- Blackmail, extortion
- Espionage

Compliance Threats

From InfoSec Handbook (2014)

Internal Security Threats

Human Threats

- Frauds, misuse of assets or information
- Errors or mistakes by the employees Espionage, Shoulder surfing
- Social Engineering by the employees
- Exploitation of lack of knowledge or ignorance of fellow employees
- Use of weak administrator passwords or passwords of others and gaining unauthorized access
- Theft
- Policies not executed or followed
- Improper segregation of duties leading to fraud or misuse
- Malware infection threats due to infected media usage or unauthorized software downloads

Internal Application Issues

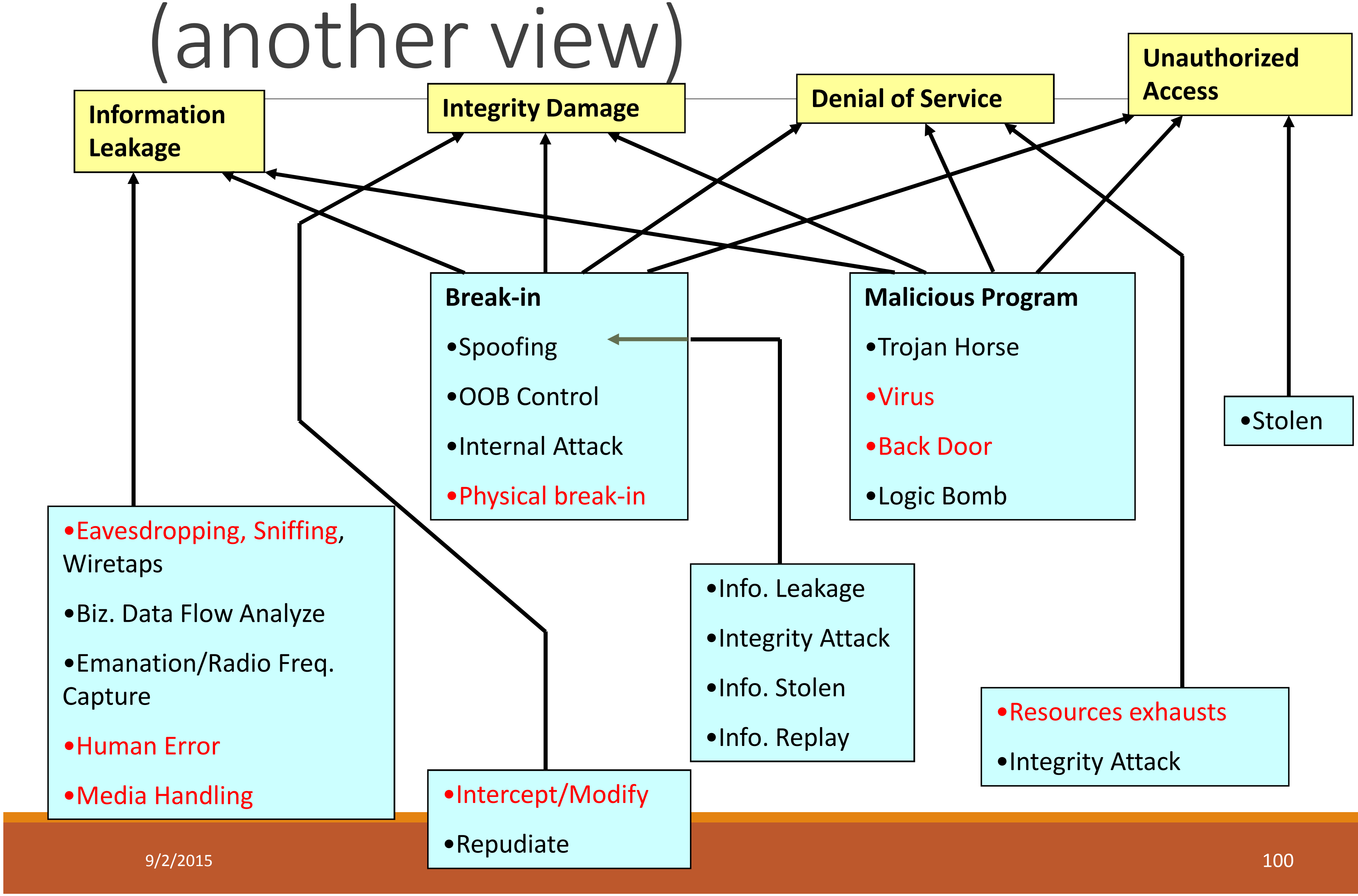
- Invalidated inputs Misconfigured application leading to errors or wrong processing
- Inappropriate error or exception handling leading to issues
- Parameter manipulations
- Manipulation of Buffer Overflows
- Unauthorized access

Other Issues

- Unrestricted access to USB leading to pilferage of information
- System or data corruption may be due to power surges, temperature control failure or for other reasons
- Hardware failure due to malfunctioning
- Infrastructure like UPS failure due to improper maintenance

From InfoSec Handbook (2014)

Type of Security Threats (another view)



Information Leakage

Integrity Damage

Denial of Service

Unauthorized Access

Break-in

- Spoofing
- OOB Control
- Internal Attack
- Physical break-in

Malicious Program

- Trojan Horse
- Virus
- Back Door
- Logic Bomb

- Stolen

- Eavesdropping, Sniffing, Wiretaps
- Biz. Data Flow Analyze
- Emanation/Radio Freq. Capture
- Human Error
- Media Handling

- Intercept/Modify
- Repudiate

- Info. Leakage
- Integrity Attack
- Info. Stolen
- Info. Replay

- Resources exhausts
- Integrity Attack

Risk Assessment Theory

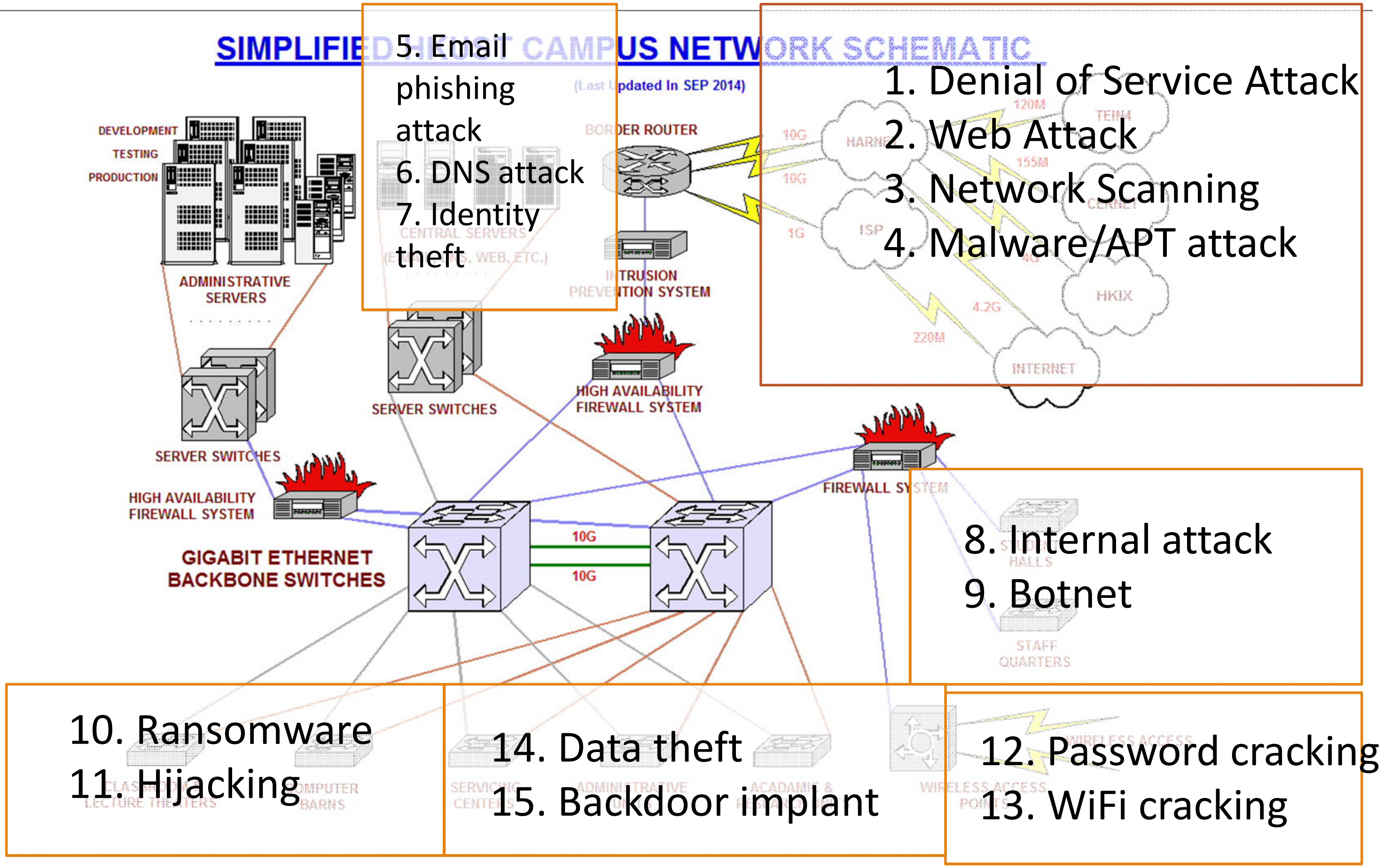
Overall Risk = A x V x T

Asset Value (A) = Confidentiality + Availability + Integrity

Vulnerability Evaluation (V) – does not have any limit in rating

Threats Evaluation (T) – depends on the human and environmental factor

How hacker attack the IT systems?



1. Denial of Service Attack
2. Web Attack
3. Network Scanning
4. Malware/APT attack

5. Email phishing attack
6. DNS attack
7. Identity theft

8. Internal attack
9. Botnet

10. Ransomware
11. Hijacking

12. Password cracking
13. WiFi cracking

14. Data theft
15. Backdoor implant

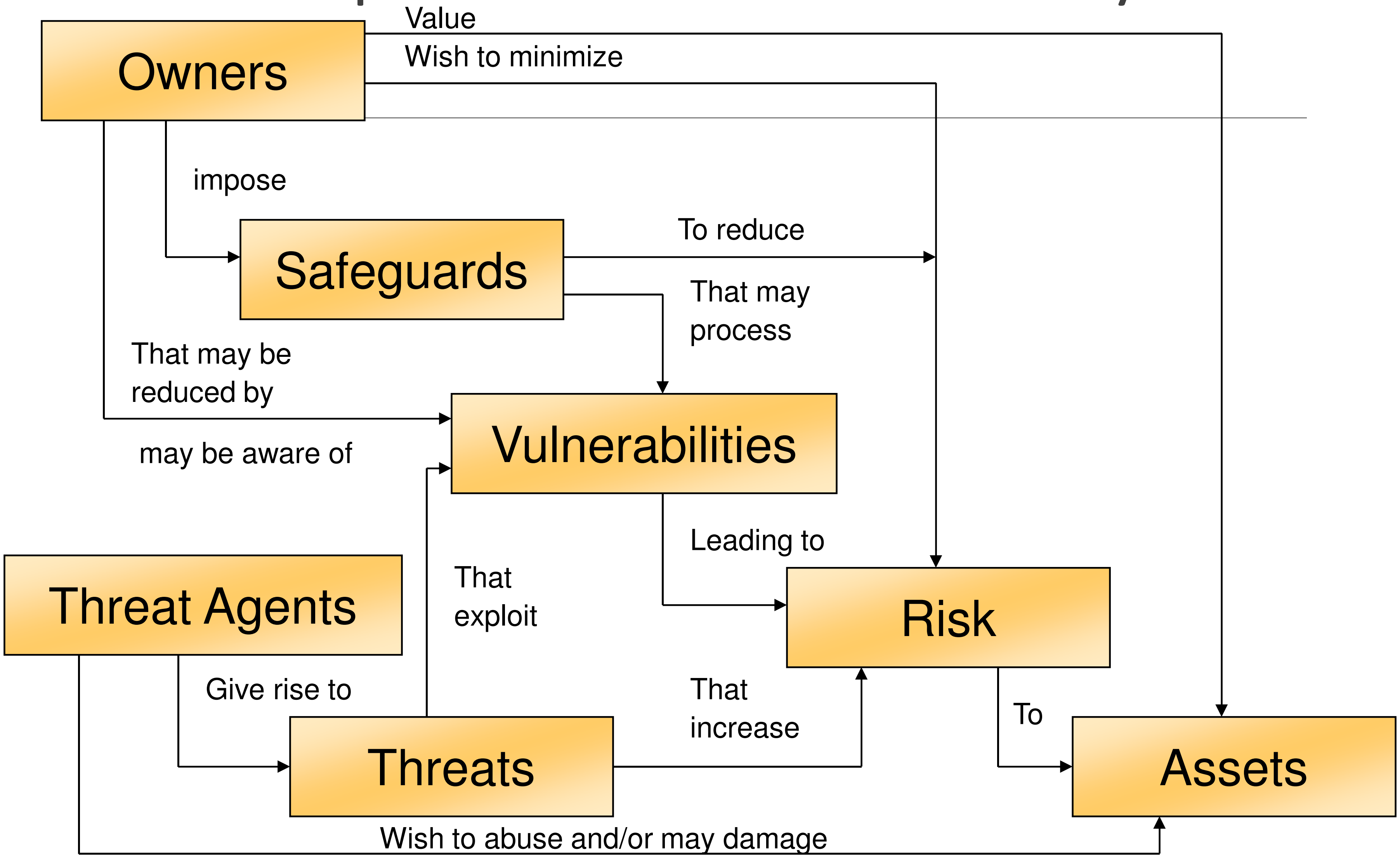
Upcoming Classes

Lecture	Attacks	Defenses
L2: Network Basics	DNS attack	Network architecture and WiFi Security
L3: Network Hacking	Vulnerability scanning, port scanning, Session Replay, Session Hijacking, Man in the middle attacks, Network Eavesdropping, Denial of Services attack, botnet, virus, APT	
L4: Network infrastructure secure design	Exploitation	Firewall, IDS, anti-DDoS
L5: Encryption and Usage	Crack WiFi, Heartbleed, POODLE	Encryption basics, PKI, SSL, TLS
L6: Web Application Programming		
L7: Mobile Application Programming		

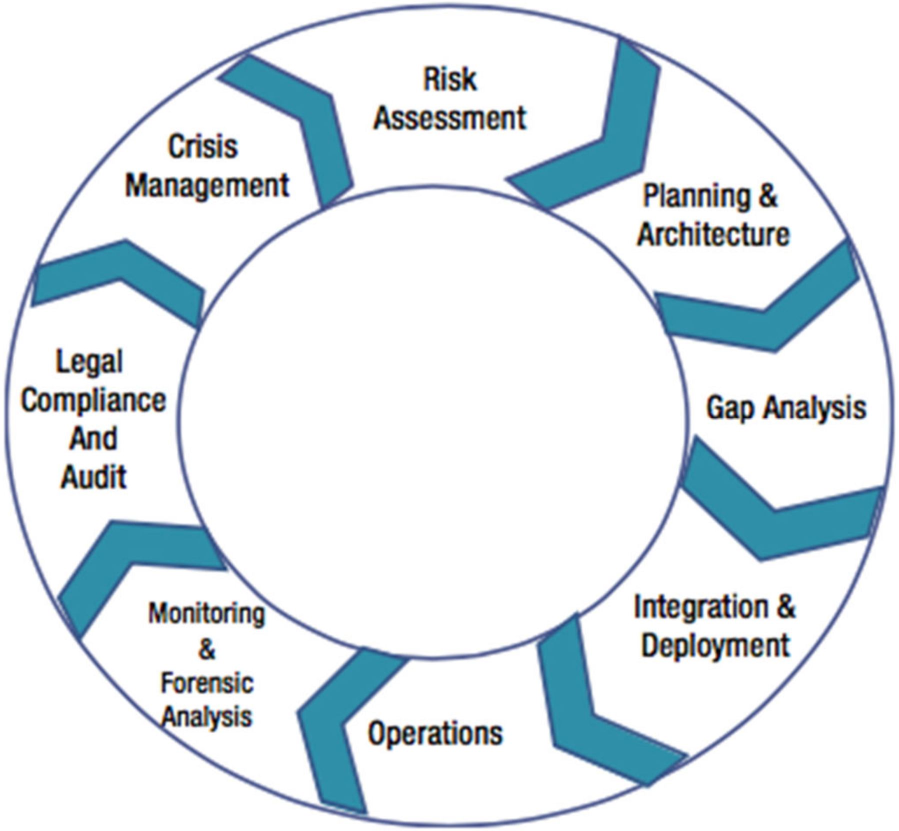
Upcoming Classes (Cont.)

Lecture	Attacks	Defenses
L8: Web Application Hacking	Web hacking, injection attack, cross-site scripting, CSRF	
L9: Web and Mobile Application Hacking	Other OWASP top 10 attacks, mobile related attacks	
L10: Application Security	Buffer overflow	Secure programming life cycle, application layer firewall, secure code review, security assessment
L12: Incident Response		Log analysis, Incident Handling, compliance & risk
L13: Advanced Topics in Security – Cloud Security		Cloud security

Concept Flow of Risk Analysis



Implementation Cycle of information security



From InfoSec Handbook (2014)

Reference Books

Related content	Book	Chapter
W1: Security Threats	Enterprise Cybersecurity (2014)	Chapter 1: Defining the Cybersecurity challenge
W1: Security Threats	Enterprise Cybersecurity (2014)	Chapter 2: Meeting the Cybersecurity challenge
W1: Insider Threat	Computer Security Handbook (2014)	Chapter 13: The Insider Threat
W1 – Security Threats Risk Assessment	Guide to Computer Network Security (2015)	Chapter 3: Security Motives and Threats to Computer Networks
W1: X.800	Cryptography and Network Security (2011)	Chapter 1.4 Security Services (6th edition)
W1: Security Architecture	Enterprise Cybersecurity (2014)	Chapter 3: Enterprise Cybersecurity Architecture
W1 – Forms of Protection Security Standards	Guide to Computer Network Security (2015)	Chapter 2: Computer Network Security Fundamentals
W1: Key Concepts	The InfoSec Handbook (2014)	Chapter 3: Key Concepts and Principles
W1: Security Controls	Computer Security Principles and Practice (2012)	Chapter 15: IT Security Controls, Plans and Procedures
W1: Authentication	Cryptography and Network Security (2011)	Chapter 15: User Authentication Protocols
W1: Authentication	The InfoSec Handbook (2014)	Chapter 4: Access Controls
W1: Authentication	Computer Security Principles and Practice (2012)	Chapter 3: User Authentication
W1: Authentication	Computer Security Principles and Practice (2012)	Chapter 4: Access Control