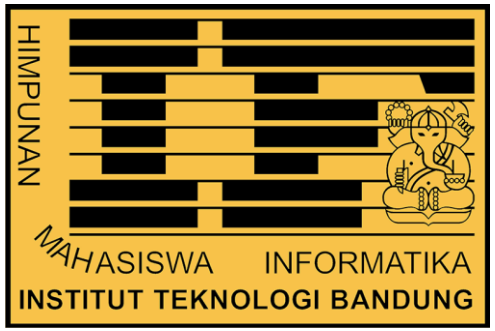
Socio - Informatika dan Profesionalisme

Information Security Introduction

Teguh Eko Budiarto ST., MT., CISA

7 April 2017

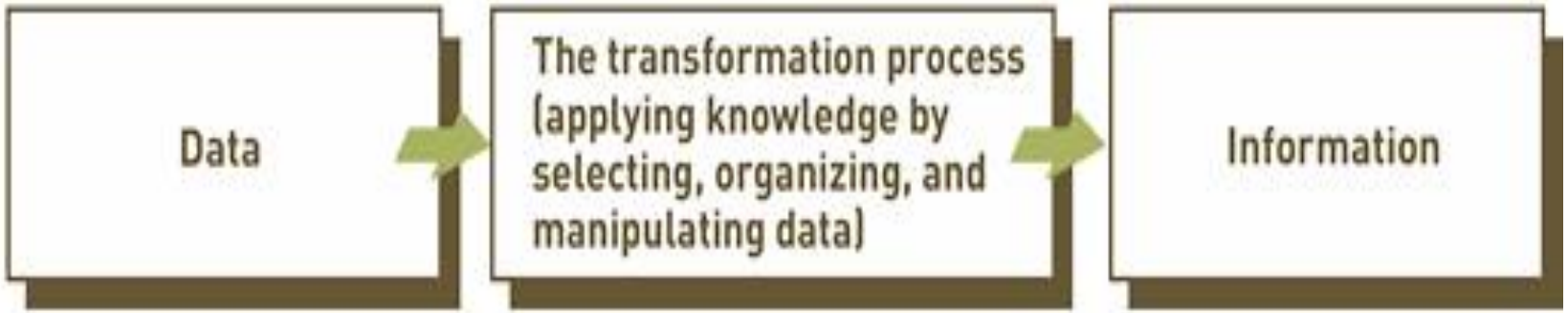
Introduction



98

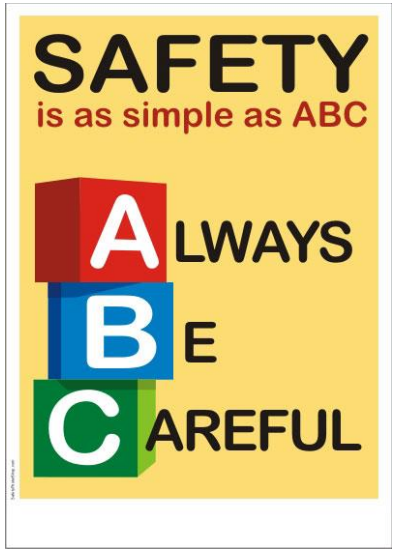
Basics of Information System

- IS accepts data from their environment and manipulate data to produce information that is used to solve a business problem or to help in taking business decisions.



Why Information Security is important for everyone, especially nowadays ?

Security vs. Safety



- **Safety** is the state of being "safe“ or the state of being protected from something that may cause a failure, damage, error, accidents, harm, etc.

Safe from harm

- **Security** is also called social safety or public safety, security is the risk of harm due to intentional criminal acts such as assault, burglary or vandalism.

Secure from Intruder

We live in an internet connected world

Vehicle,asset,person & pet monitoring & controlling

Agriculture automation

Energy consumption

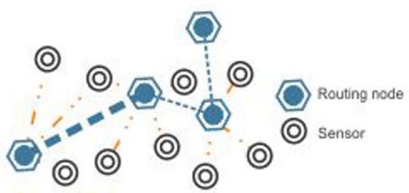
Security & surveillance

Building managment

Embedded Mobile

Internet of things

Everyday things get connected for smarter tomorrow



M2M & wireless sensor network

Everyday things

Smart homes & cities

Telemedicine & helthcare

https://www.bristoltechnology.com/cyber-security-challenges-2016/

No 1 Challenge : IoT and BYOD

Information System Security

- Today most of the IS are connected to internet.
- Thus they are exposed to the outside world directly.
- Threats from the outside world must be addressed.
- Damage from a non-secure IS can result in catastrophic consequences for the organization.
- Thus organizations must investigate and evaluate the factors that could be a threat.

Basic Elements of Information Security

http://www.opentext.com/what-we-do/business-needs/information-governance/ensure-compliance/information-security-and-privacy

In another words …….

……Information security means making sure to provide required information for the correct people at the correct time.

However, lately…

We found many
Information Security Breaches

MALWARE

Brazilian bank hacked, loses control of its online presense

DOUG OLENICK, APR 05, 2017

The Hacker News™
Security in a serious way

Hackers Threaten to Remotely Wipe 300 Million iPhones Unless Apple Pays Ransom

Tuesday, March 21, 2017 Mohit Kumar

If you use iCloud to sync your Apple devices, your private data may be at risk of getting exposed or deleted by April 7th.

by Doug Olenick, Online Editor

Follow @DougOlenick

April 04, 2017

4,000 WordPress sites infected through fake plugin

About 4,000 WordPress websites have been infected with malware that disguises itself as a search engine optimization plugin to attract unwary webmasters.

The plugin contains code belonging to a real SEO plugin.

The fake plugin is called WP-Base-SEO and is based on a legitimate SEO module so it is easily overlooked during security scans and seems to be a viable tool by a web team intent on boosting its traffic, said a research team at SiteLock. What the plugin actually does is create a backdoor to the victimized site. The cyberattacker is likely scanning the internet looking for outdated WordPress plugins, particularly those running a plugin called RevSlider, SiteLock said.

ThreatPost cited SiteLock analyst Weston Henry who noted that a large portion of the WordPress sites had an out of date version of RevSlider installed. An examination of the plugin finds two malicious files located in /wp-content/plugins/wp-base-seo/wp-seo-main.php.

Apple users, beware: First live ransomware targeting Macs found 'in the wild'

Researchers discover what they say is the first real-world ransomware meant to hit Macs. If you've downloaded torrenting software recently, you may be at risk.

B

Security

Sorry, Mac fans. Now you're no better off than regular old PC users.

Security researchers have discovered what they believe to be the first-ever ransomware attack targeted at Apple users that actually vild," meaning it's a

Politik

Diretas, Tiket.com Rugi Rp 4,1 Miliar

Magang Dua | Jumat, 31 Maret 2017 - 10:18:29 WIB | dibaca: 33 pembaca

JAKARTA, SATELITPOST-Kelompok peretas atau *hacker* berusia remaja pimpinan Haikal alias SH (19 tahun) berhasil membobol akun situs jual beli tiket *online* *Tiket.com* di *server* Citilink. Akibatnya, *Tiket.com* mengalami kerugian Rp 4,1 miliar dan Citilink rugi sekitar Rp 2 miliar.

Kepala Biro Penerangan Masyarakat (Karopenmas) Divisi Humas Polri,

Hackers Using Fake Cellphone Towers to Spread Android Banking Trojan

Wednesday, March 22, 2017 Swati Khandelwal

Chinese Hackers have taken Smishing attack to the next level, using rogue cell phone towers to distribute Android banking malware via spoofed SMS messages.

SMiShing — phishing attacks sent via SMS — is a type of attack wherein fraudsters use number spoofing attack to send convincing bogus messages to trick mobile users into downloading a malware app onto their smartphones or lures victims into giving up sensitive information.

Why Information Security should become our concern as Informatics Engineers ?

Many software systems are critical

- Safety-critical: systems whose failure can cause life losses or serious environmental damage
- Mission-critical: systems whose failure can cause the failure of the goals of important missions
- Business-critical: systems whose failure can cause the loss of big or huge amounts of money

GEEKS

More powerfull than Goths, Vandals, and Huns combined

Aksi Hacker

Begini Cara Hacker Haikal Membobol 4.600 Situs Online

Kamis, 30 Maret 2017 22:32 WIB

- http://www.tribunnews.com/nasional/2017/03/30/begini-cara-hacker-haikal-membobol-4600-situs-online

blog.compactbyte.com/2017/04/02/cara-cepat-hacking-ribuan-site-dan-menjadi-kaya-secara-ilegal/

Cara cepat hacking ribuan site dan menjadi kaya secara ilegal

yohanes

02/04/2017

security

Like 807 people like this. Be the first of your friends.

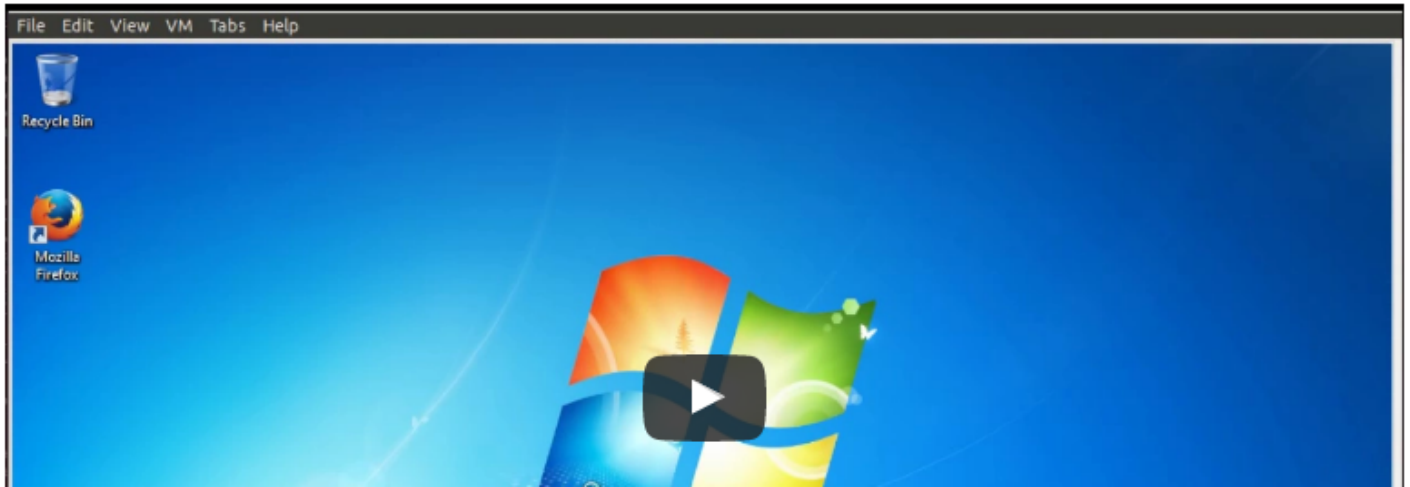
Baru-baru ini membaca berita tentang tertangkapnya 'hacker' muda yang membobol 'ribuan' site. Bagi yang melek dunia security, berita ini biasa saja. Tapi tentunya bagi orang awam ini kedengaran hebat.

- http://blog.compactbyte.com/2017/04/02/cara-cepat-hacking-ribuan-site-dan-menjadi-kaya-secara-ilegal/

Feature or flaw? How to hijack a Windows account in less than a minute

By the researcher's own admission, he's not sure if it's a newly-discovered security flaw — or a feature.

By Zack Whittaker for Zero Day | March 18, 2017 -- 17:23 GMT (01:23 GMT+08:00) | Topic: Security



RELATED STORIES

Enterprise Software

Adversaries Profile

- Adversaries that target corporate system are numerous:
- These can be general classified in the following categories:
  - Hackers
  - Employees (both malicious and unintentional)
  - Terrorists groups
  - Governments
  - Opposing Industries

Why internet is a playground for hackers

- **Ubiquity**
  - 80% web site have serious security – White Hat Security 2009 report
- **Profitability**
  - Automation makes attacks with a minimal rate of return profitable
- **Simplicity**
  - Attack tools are published on the internet so only the first attacker has to be skilled
- **Anonymity**
  - Attacks often go undetected
  - Attackers are difficult to trace → worked overseas

Cost-Benefit Ratio of criminals

(Clark and Davis, 1995)

$$M_b + P_b > O_{cp} + O_{cm}\, P_a\, P_c$$

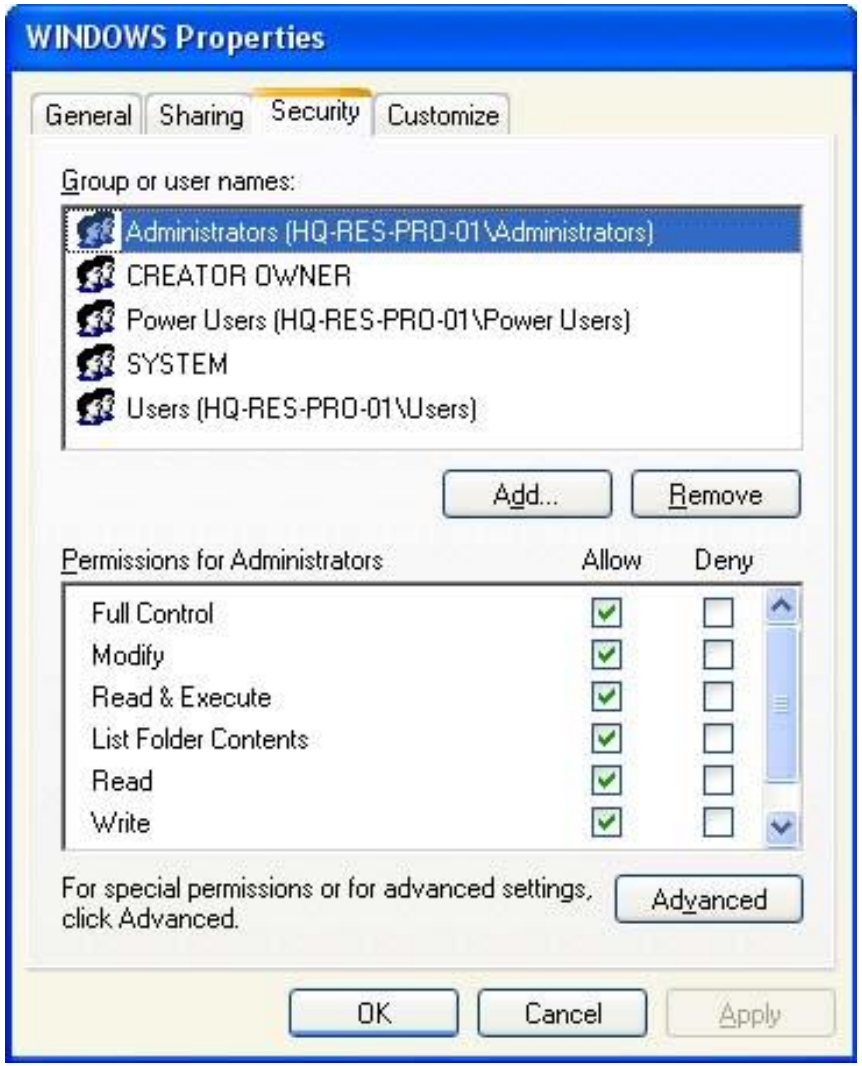
- Mb is the monetary benefit for the attacker.
- Pb is the psychological benefit for the attacker.
- **Ocp is the cost of committing the crime.**
- Ocm is the monetary costs of conviction for the attacker (future lost opportunities and legal costs).
- **Pa is the probability of being apprehended and arrested.**
- Pc is the probability of conviction for the attacker.

Other Elements of Information Security

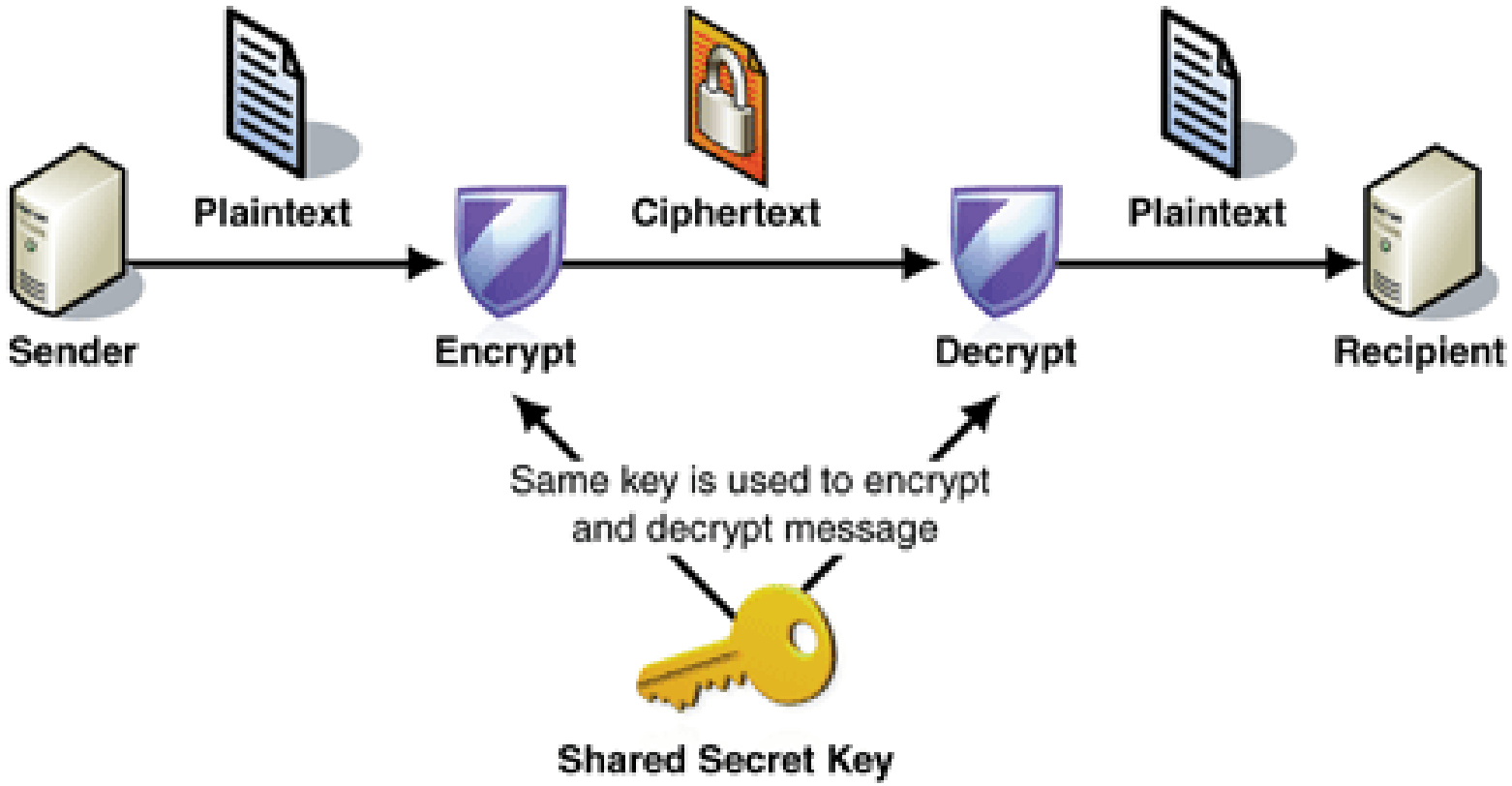
- ***Authentication*** - Process of verifying identity.
- ***Accountability*** – Tracing activities of individual on a system.
- ***Authorization*** - Granting access or other permissions.
- ***Identification*** **(Non Repudiation)** – recognition of an entity by a system.
- ***Privacy*** - Right of individual to control the sharing of information about him.

Authentication

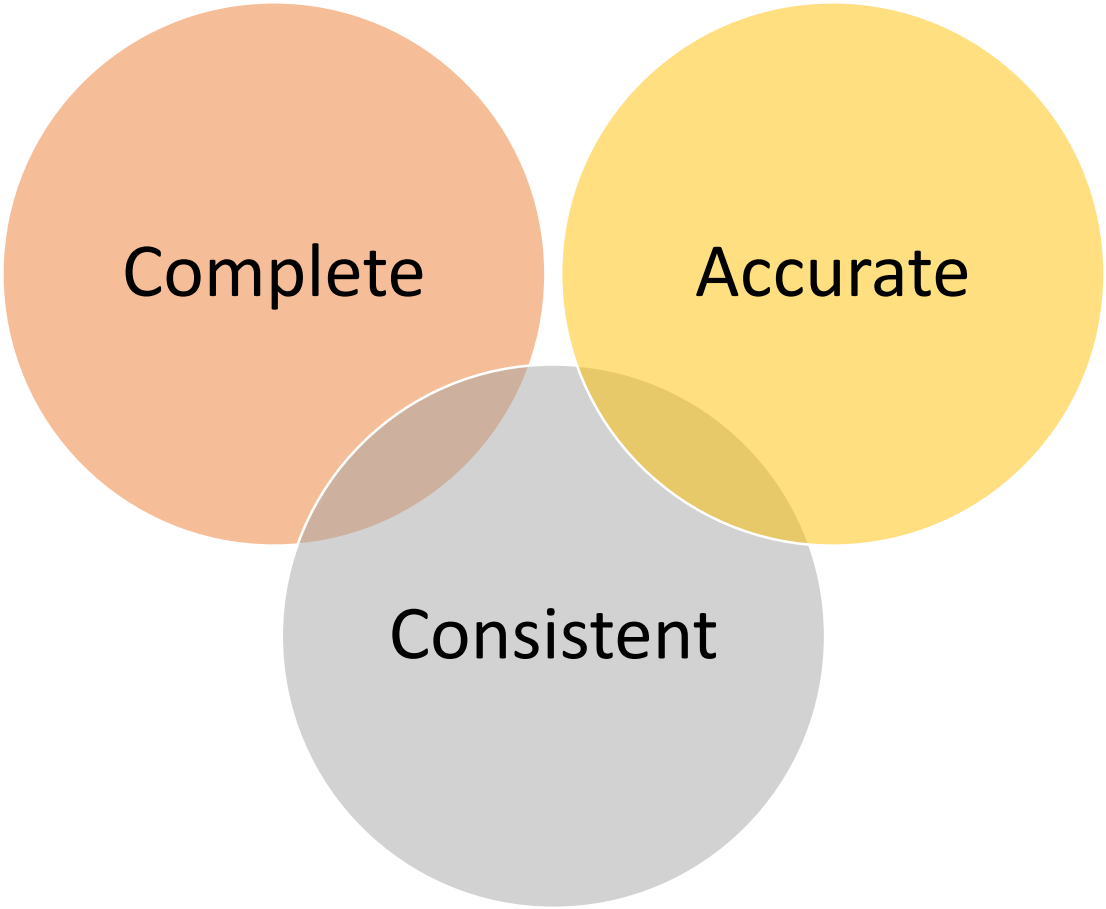
Authorization



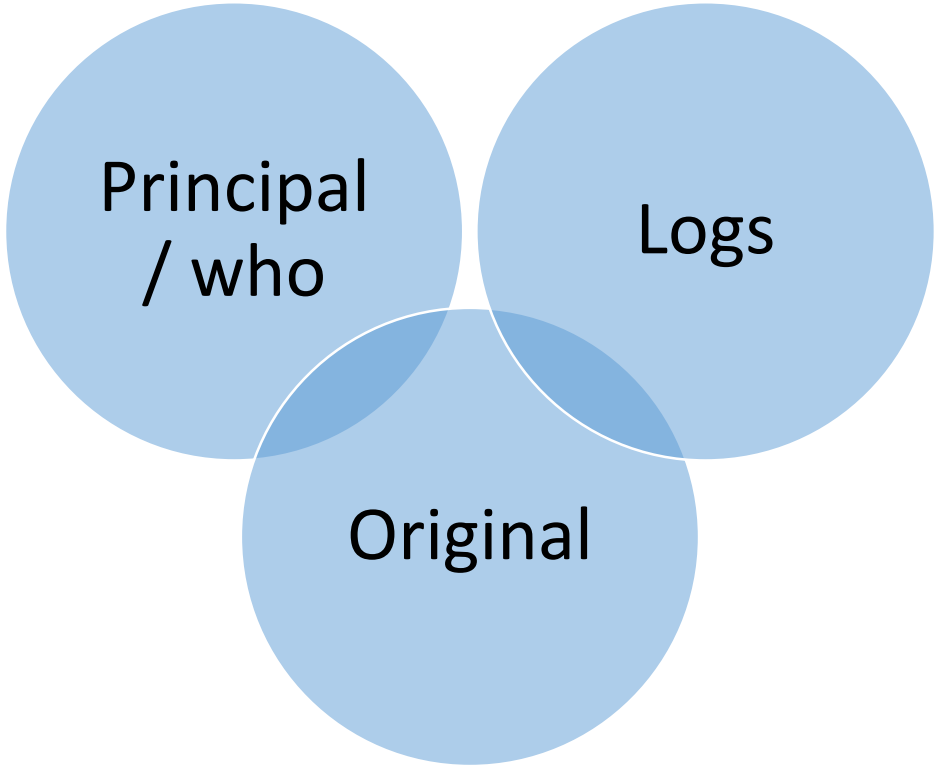
Confidentiality



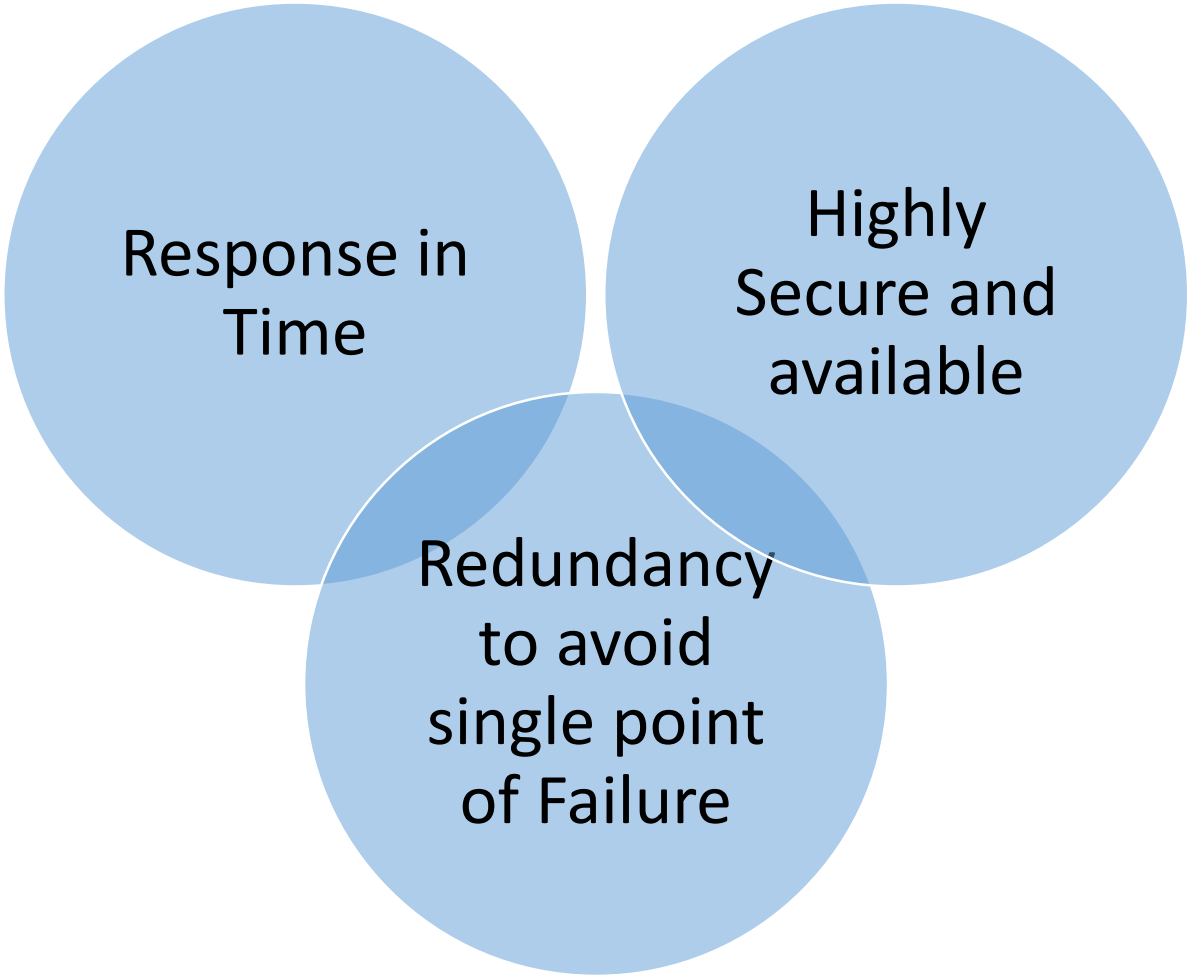
Message/Data Integrity



Accountability



Availability



Non Repudiation

- The goal of *non-repudiation* is to ensure un-deniability of a transaction by any of the parties involved
- Alice interacted with Bob at some point, and she does not want Bob to deny that she interacted with him
- A trusted third party can be used to accomplish this

How to achieve Information Security ?

Information Security is the responsibility of everyone who can affect the security of a system.

Apply Defense in Depth (layered security)

- **Administrative Controls-** Policies, standards, procedures, guidelines, employee screening, change control, Security awareness trainings.
- **Technical Controls-** Access controls, encryption, Firewalls, IDS, IPS,HTTPS
- **Physical Controls-** controlled physical access to resources, monitoring, no USB or CDROM etc.

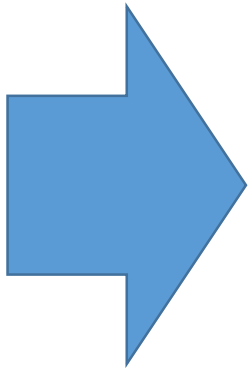
Security: easy to understand, difficult to implement

- Computer Security is difficult to implement due to the following:
  - **The cost** of implementing a security system should not exceed the value of the data to be secured.
  - Industries pay huge amount of money for **industrial espionage**.
  - **Users** feel that security is going to take their freedom away and so often they **sabotage the security measures**.
  - **Computer prices have fallen** dramatically and the number of hackers have been multiplied.
  - Security managers work under **strict money and time schedule**. Criminals do not have any time schedule and they do not need any specialised software.
  - Hackers are often **cooperate with known criminals**.

That is why, total security is almost infeasible.

Basic Knowledge – Website Hacking

- Mapping the application (Information Gathering)
  - Infrastructure
    - Server Identification
    - Port Scanning
  - Application profiling
    - URL Query String and Parameters
    - Authentication Mechanisms
    - Use of TLS/SSL
    - Application software in use
    - Directory Structure
    - Session Management

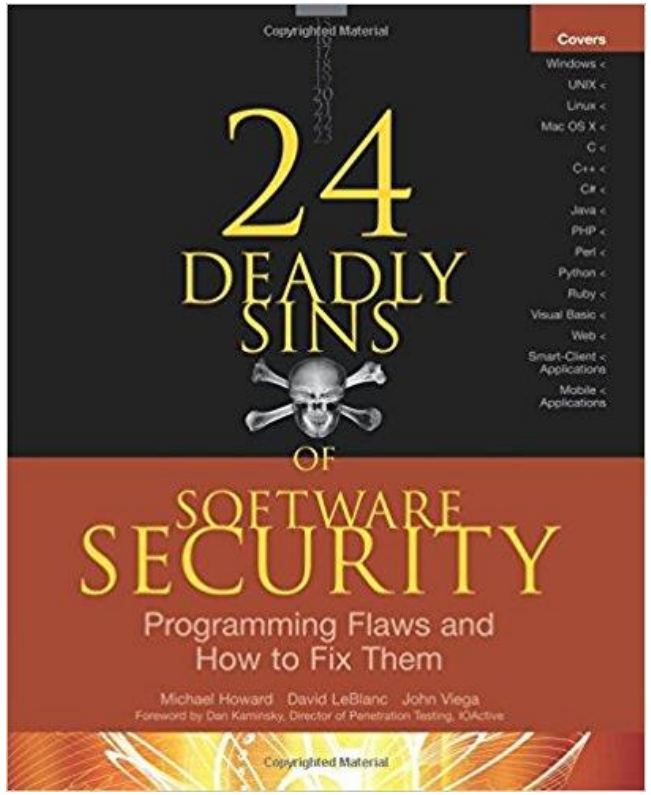


Launch Attack:

- SQL Injection
- XSS
- DDoS
- MITM
- Password Crack
  - Brute Force
  - Dictionary
- Viruses
- Social Engineering
- Etc…

Secure Coding

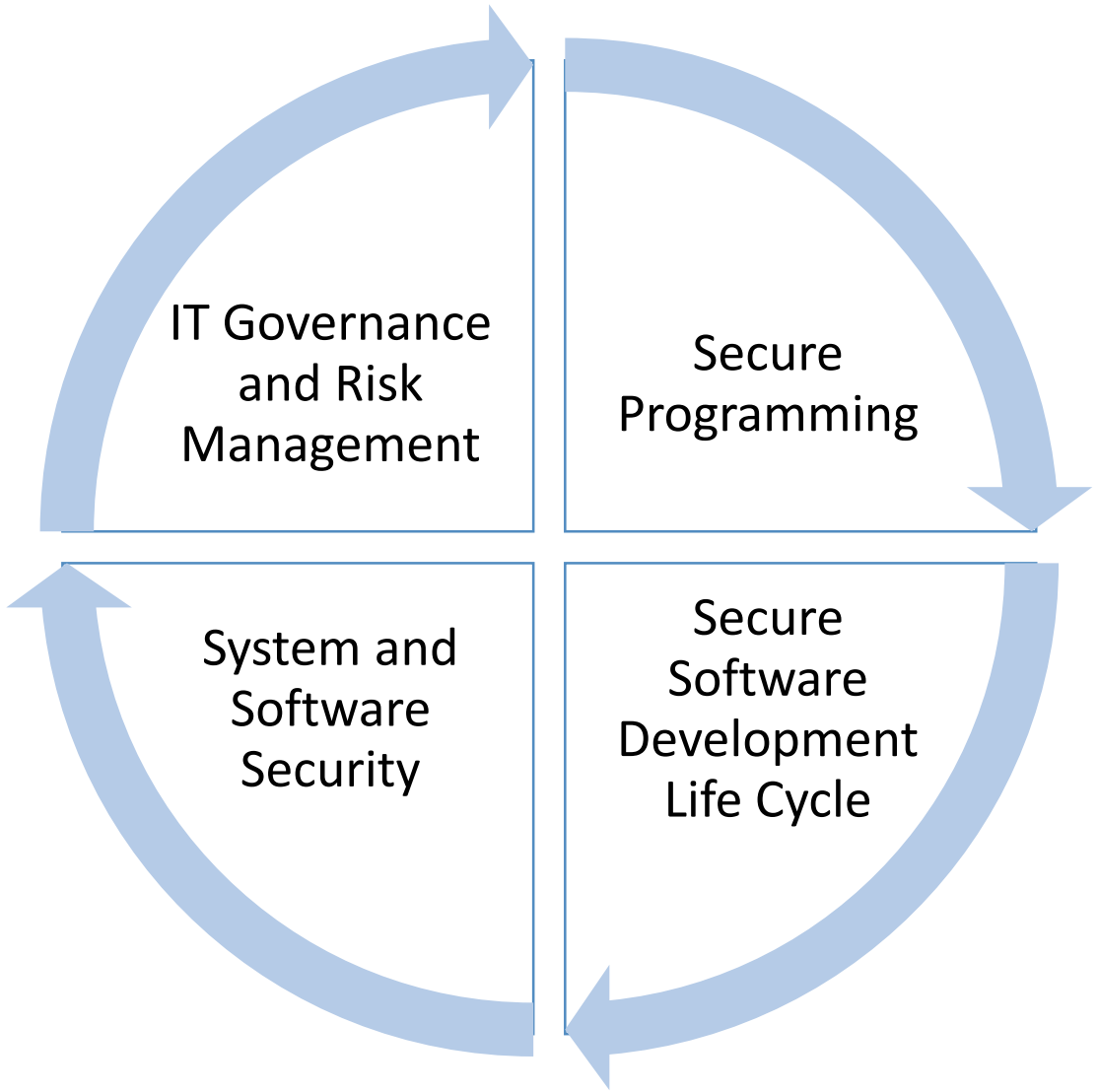
- Use a Framework
- Don’t EVER, EVER, EVER trust user input → sanitize, validate
- Always hash passwords
- Build APIs with authentication
- Check https://www.owasp.org/ for most updated info
- More comprehensive information on 24 Deadly Sins of Software Security Book



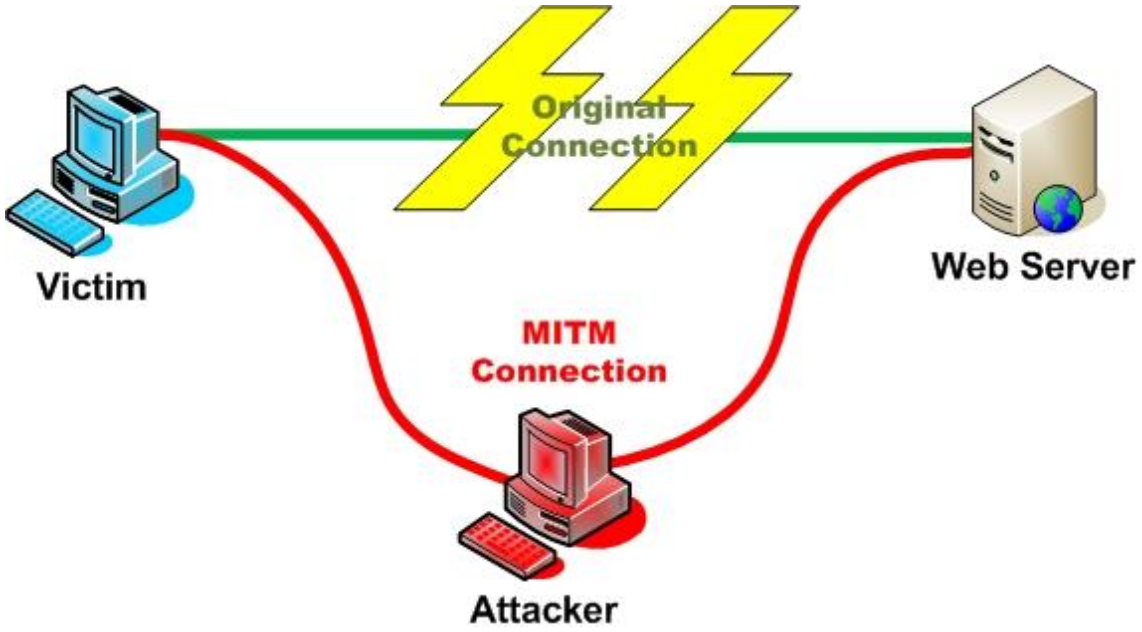
Platform Security

- Always keep the core up to date, and also the plugins
- Use as few plugins as possible
- NEVER pirate themes/plugins as most of are full of malwares
- Use specialist hosting when possible

Kuliah Selanjutnya



Demo MITM – ARP Spoofing



- https://toschprod.files.wordpress.com/2011/11/main_the_middle.jpg

Life is a choice

The Choices is available

All is about setting Right Mindset

Mahasiswa IF ITB harus jadi Pahlawan

Be the HERO

Be Aware

How do we as

Informatics Engineers

Could give **positive impact** to

the benefit of human life and its society

on the aspect of

Information Security


thank you
danke
謝謝
ngiyabonga
teşekkür ederim
gracias
merci
obrigado
bedankt
dziękuję
go raibh maith agat
sukriya
kop khun krap
mochchakkeram
спасибо
terima kasih
grazie
arigatô
dakujem
takk
tapadh leat
dank je
мерси
감사합니다
ありがとう
ευχαριστώ
рахмат
Баярлалаа
хвала
mersi
barka
welalin
tack
spas
kia ora
taafetai lava
vinaka
blagodaram
misaotra
matondo
paldies
grazzi
mahalo
kiitos
dankie
dhanyavad
nanni
nandri
mauruuru
köszönöm
hvala
gracie
bayarlalaa
enkosi
asante
manana
obrigada
tenki
murakoze
djiere dieuf
tau
дякую
mamnun
shokrane
chnorakaloutioun
gratias ago
gracies
sulpay
taiku
akun
dankon
aciú
sobodi
dėkuji
sagolun
mèsi
didi madloba
najis tuke
kam sah hamnida
rahmat
tanemirt
rahmet
diolch
dhanyavadagalu
shukriya
merce
trugarez
xiexie
спасибі