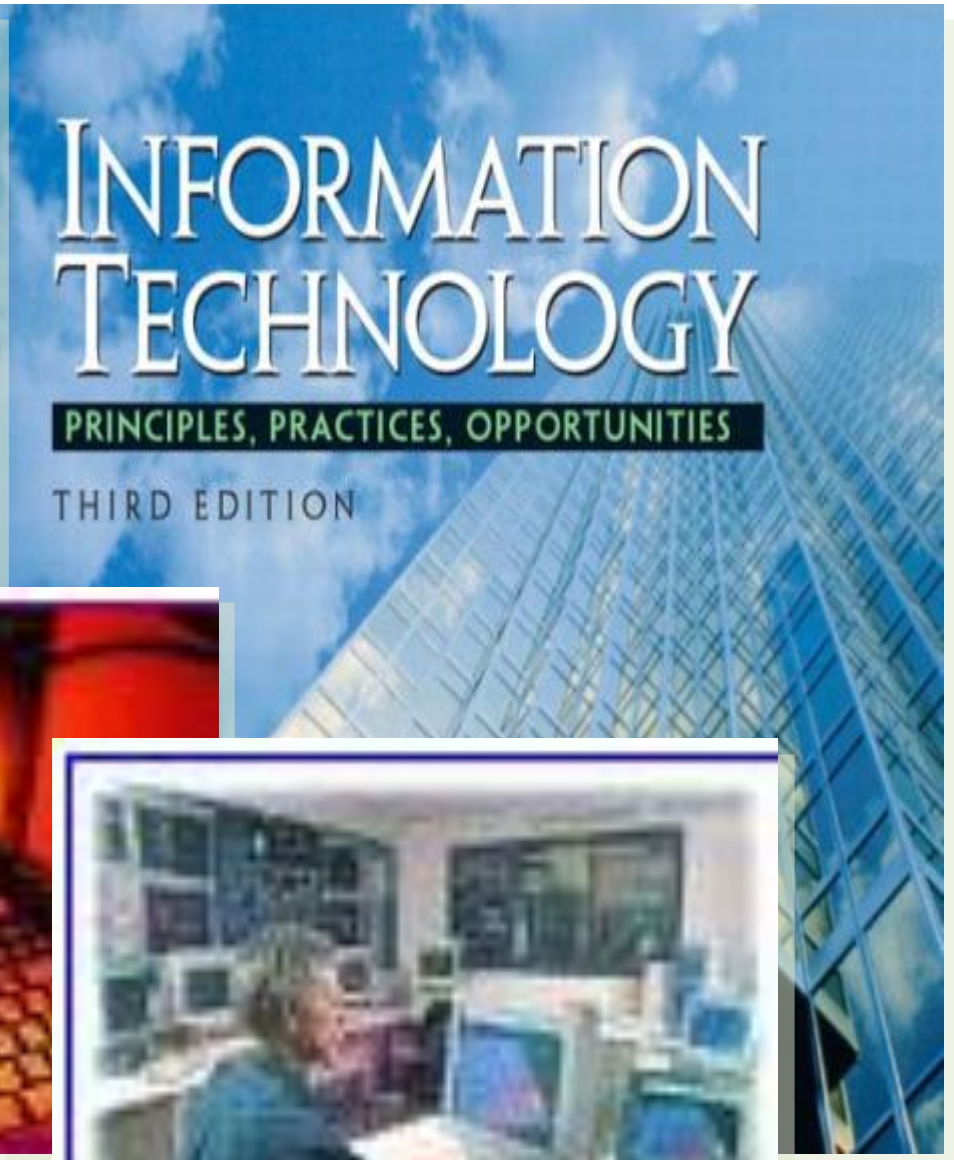
CYBER-SECURITY FUNDAMENTAL

PAST TO FUTURE

Agriculture

Industrial


Information Technology


INFORMATION
TECHNOLOGY
PRINCIPLES, PRACTICES, OPPORTUNITIES
THIRD EDITION

IT


Knowledge
is power
ks2

- **Agriculture Industrial**
  - Technology come from WAR
  - Mass Production exam gun, plane, food
  - Baby Boomer > Cold war
- **IT**
- **ICT (Internet)** > **Today** > Fast Information around the world > **Knowledge is Power**
- **Nano Technology** > Future Trend ??
- RFID / NFC / <NEW>
- Virtualization / Cloud Computing

FROM PASS TO FUTURE

VeriChip - Wikipedia, the free encyclopedia - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites History

Address http://en.wikipedia.org/wiki/VeriChip Go Links SnagIt

Sign in / create account

article | discussion | edit this page | history

Your continued donations keep Wikipedia running!

WIKIPEDIA
The Free Encyclopedia

navigation

- Main Page
- Community Portal
- Featured articles
- Current events
- Recent changes
- Random article
- Help
- Contact Wikipedia
- Donations

VeriChip

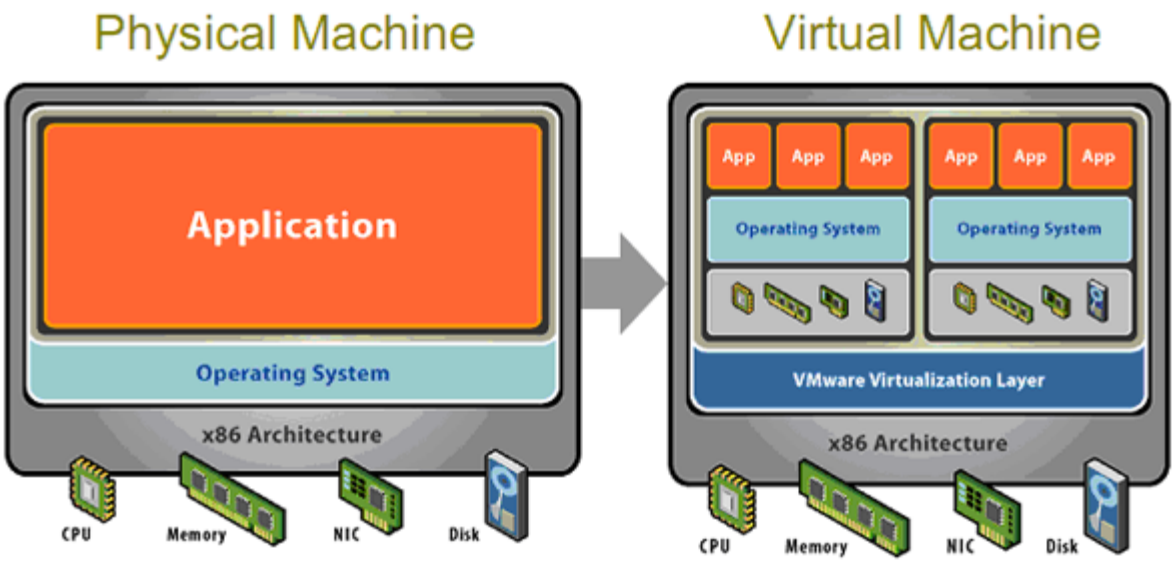
From Wikipedia, the free encyclopedia

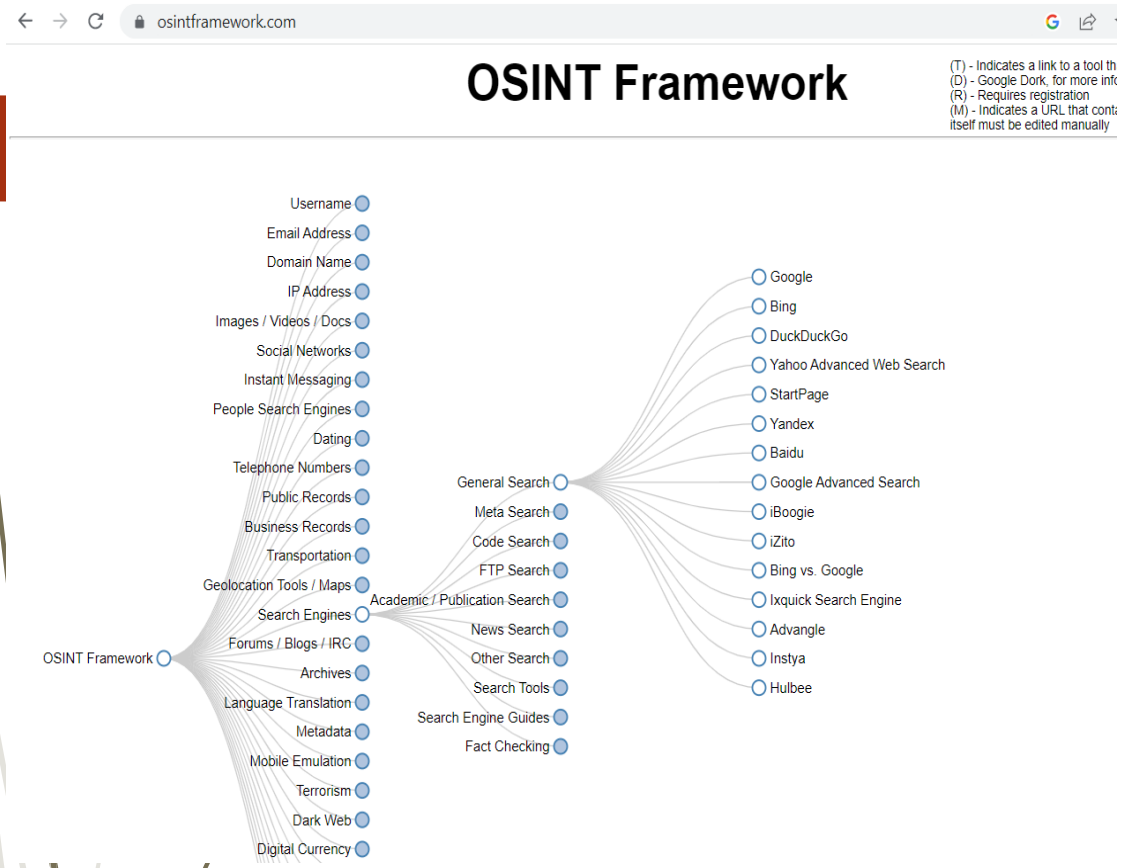
VeriChip is a human-implantable RFID (radio frequency identification) device from VeriChip Corporation, a wholly owned subsidiary of Applied Digital Solutions of Delray Beach, Florida. The chip can also be attached to a watch or other piece of jewelry so it can be removed for privacy reasons.

VeriChip is the first Food and Drug Administration (FDA)-approved human-implantable RFID microchip. VeriChip received United States FDA approval in 2002. About twice the size of a grain of rice, the device is typically implanted above the triceps area of an individual's right arm, though is sometimes implanted in the hand, or attached to jewelry outside the body to be easily removed for privacy. Once scanned at the proper frequency, the VeriChip responds with a unique 16-digit number which can correlate the user to information stored on a database for identity verification, medical records access and other uses. The insertion procedure is performed under local anesthetic and once inserted, is invisible to the naked eye. The process can easily

Promotional photo of the chip

EXAMPLE VERICHIP


Physical Machine
Virtual Machine
Application
Operating System
x86 Architecture
CPU
Memory
NIC
Disk
App
App
App
App
App
App
Operating System
Operating System
VMware Virtualization Layer
x86 Architecture
CPU
Memory
NIC
Disk

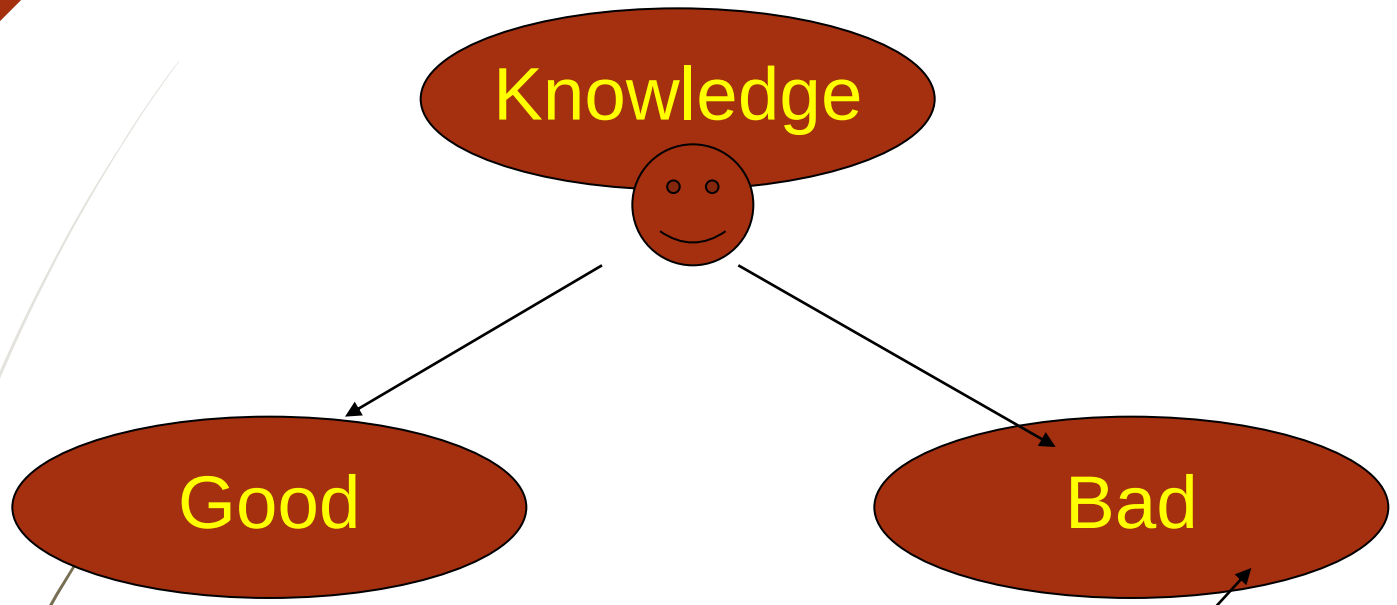


- **Cyber Attack**

  >> Malware code

- **Threat Intelligence**
- **Open Source Intelligence**
- **Cyber Threat Intelligence**

Everything can get from internet



KNOWLEDGE CONCEPT

We need to **protect** & **prevent** people from this site

chrome web store

Home › Extensions › Tamper Chrome (extension)

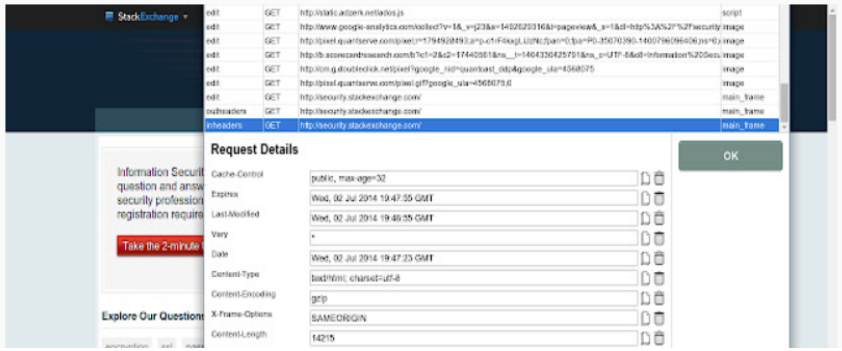
Tamper Chrome (extension)

tamper.dev

Remove from Chrome

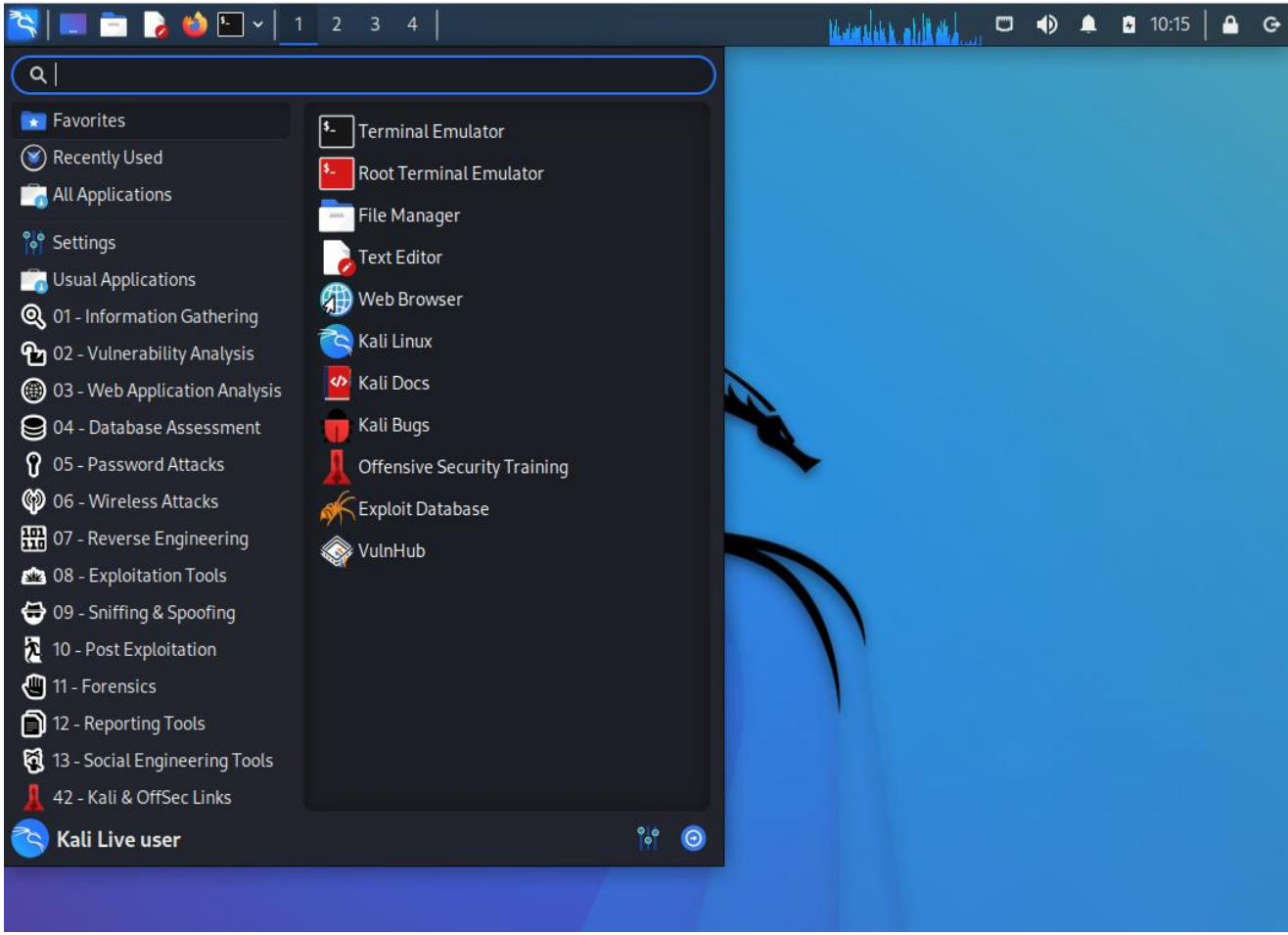
235 | Developer Tools | 50,000+ users

Overview | Privacy practices | Reviews | Support | Related



Tamper DATA

- Live bootable
- Remote Exploit
- Has many tools of Hacking in here



: Linux Live Tools for Hacking <Kali>

CYBER SECURITY

Chapter 1 – what is information security?

- Physical พูดถึงตัวข้อมูลและอุปกรณ์ที่เป็นกระดาษ Hard Copy
- Alexander Graham Bell ประดิษฐ์โทรศัพท์ เกิดปัญหาเรื่องการดักฟัง ทำให้ต้องมีการคิดเรื่อง Communication Security
- Computer เกิดขึ้นทศวรรษที่ 70 > มีคนพัฒนาไวรัสที่เรียกว่า Worm เกิดขึ้นในโลกพร้อมกับ Computer > เลยต้องมีมาตรฐานป้องกันในยุคทศวรรษที่ 80 คือ C2 Security

ประวัติของความปลอดภัย

- ในทศวรรษที่ 90 เริ่มมีการต่อเครือข่าย LAN, WAN และทำให้เราต้องป้องกันระบบเครือข่ายในองค์กร
- ปลายทศวรรษที่ 90 มีการใช้ internet อย่างแพร่หลายและเริ่มถูกรุกรานจาก Hacker ทำให้มีหลายองค์กรที่ถูกต้องขึ้นมาเพื่อทำงานทางด้านการป้องกัน เช่น InfoSec, CompuSec, NetSec

ประวัติของความปลอดภัย (ต่อ)

- A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Law Data = Cipher Data

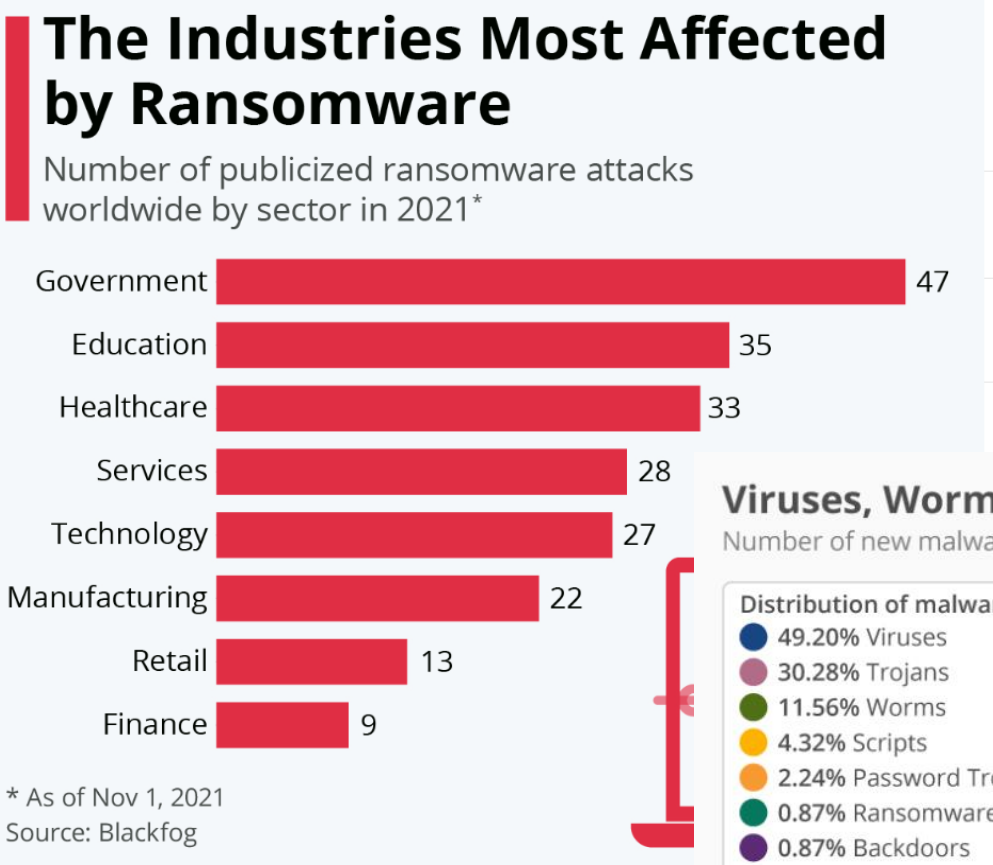
BAD = EDG (ship 3 step)

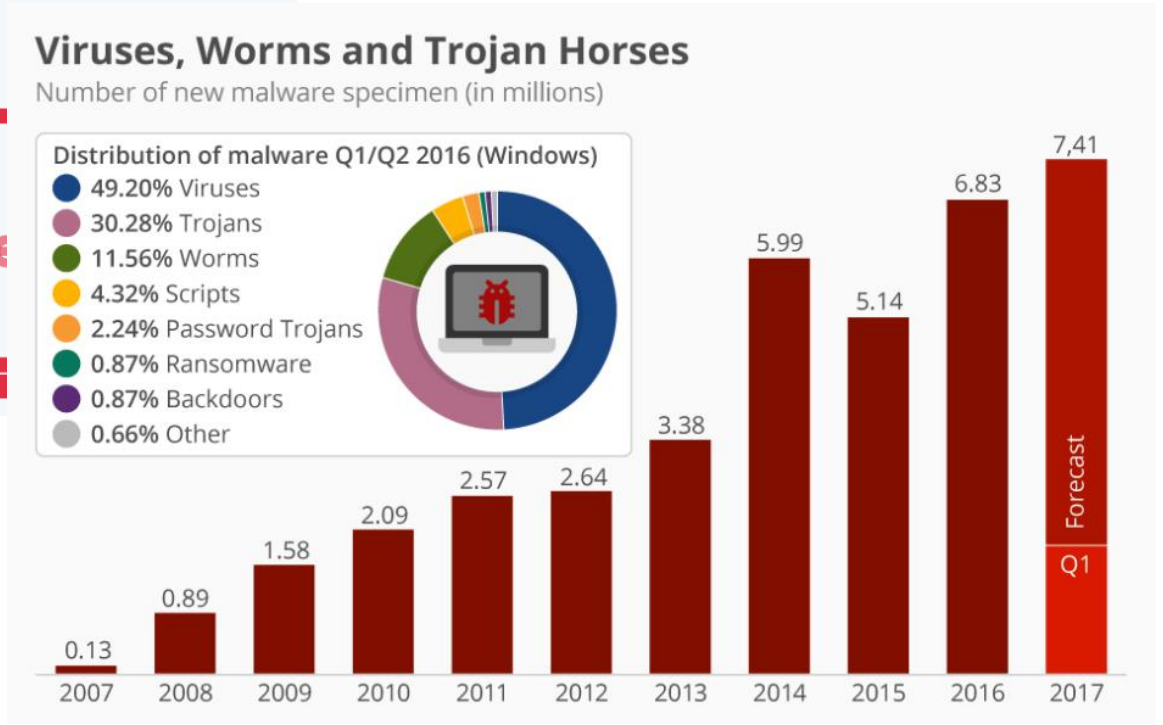
Julius Caesar invented the first cipher

- Create for Encryption Data.

Enigma was used during World War 2

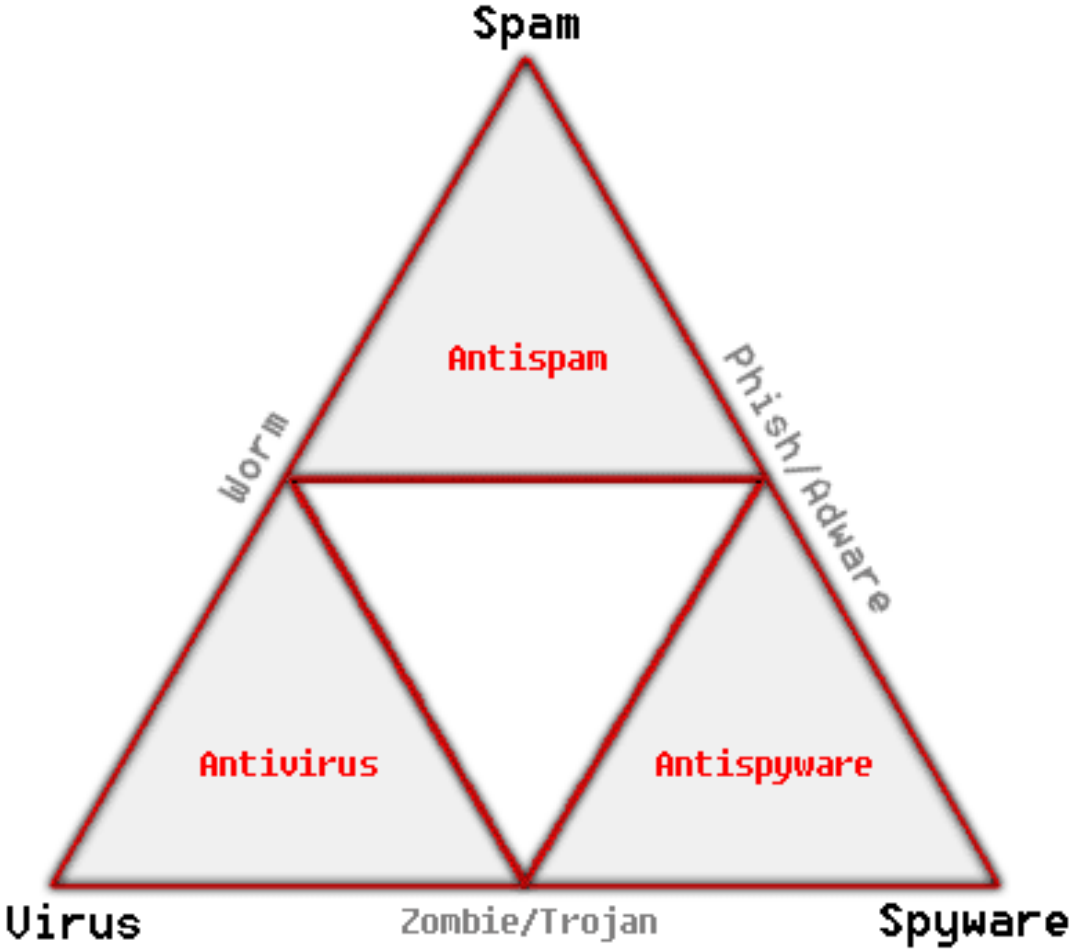
ปัญหาต่างๆที่เกิดขึ้นในปัจจุบันในโลกของ Cyber



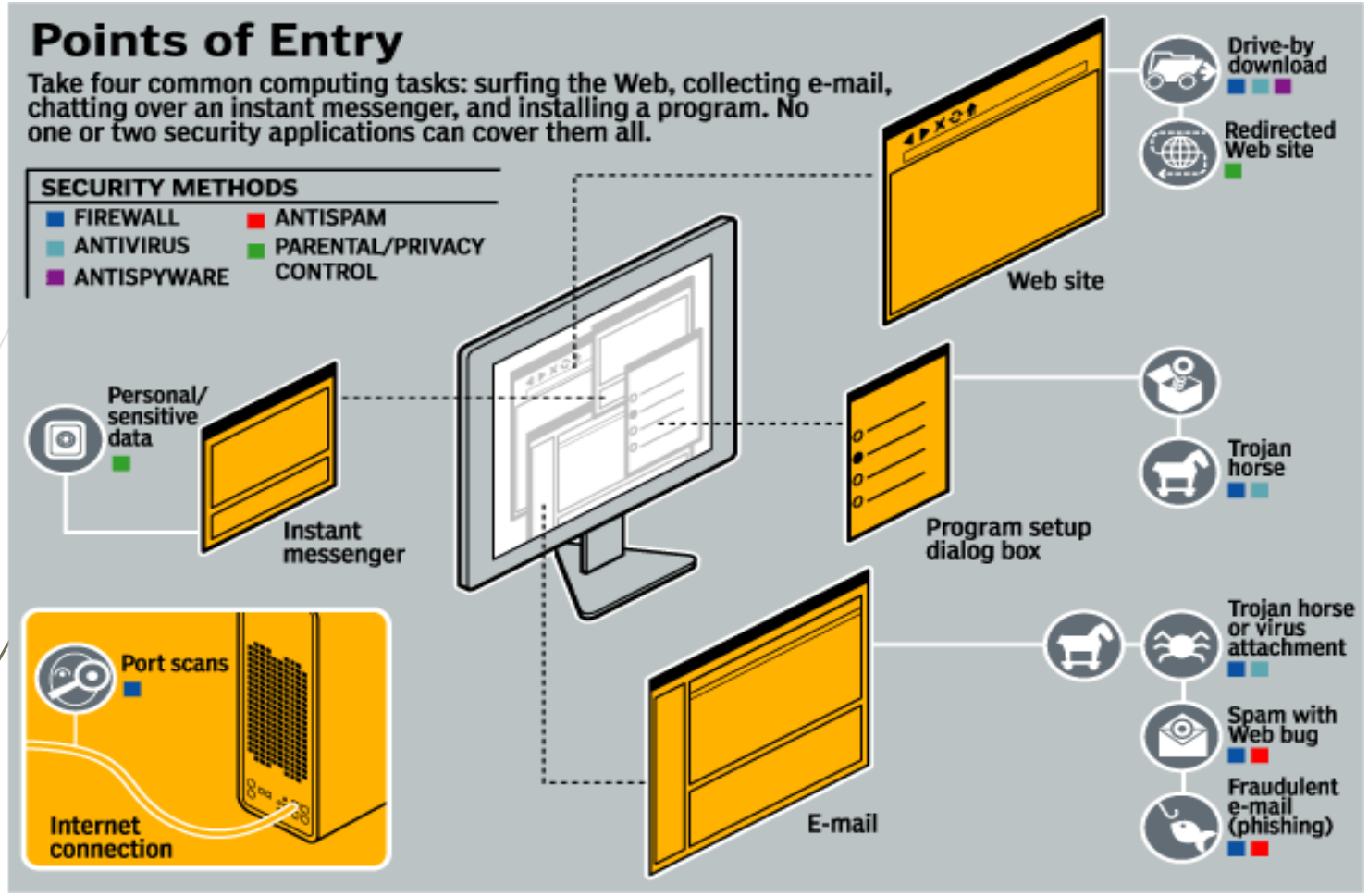


Ransomware & Malware

https://www.statista.com/chart/26148/number-of-publicized-ransomware-attacks-worldwide-by-sector/



Virus, Spam and Spyware relationship



How does Malware attack your computer?
=> Too Many "Point of Entry"

Image of Cyber Crime On Social Media by Unisense Advisory

Social Media Malicious (come with Spyware)

https://medium.com/@unisenseadvisory/cybercrimes-on-social-media-the-ultimate-guide-06b329e1e11f

การควบคุมการเข้าใช้ทรัพยากร

- IP Address

- Mac Address (12 Digit)

- Mac Address + Port (Switch)

วิธีและแนวทางในการแก้ปัญหา

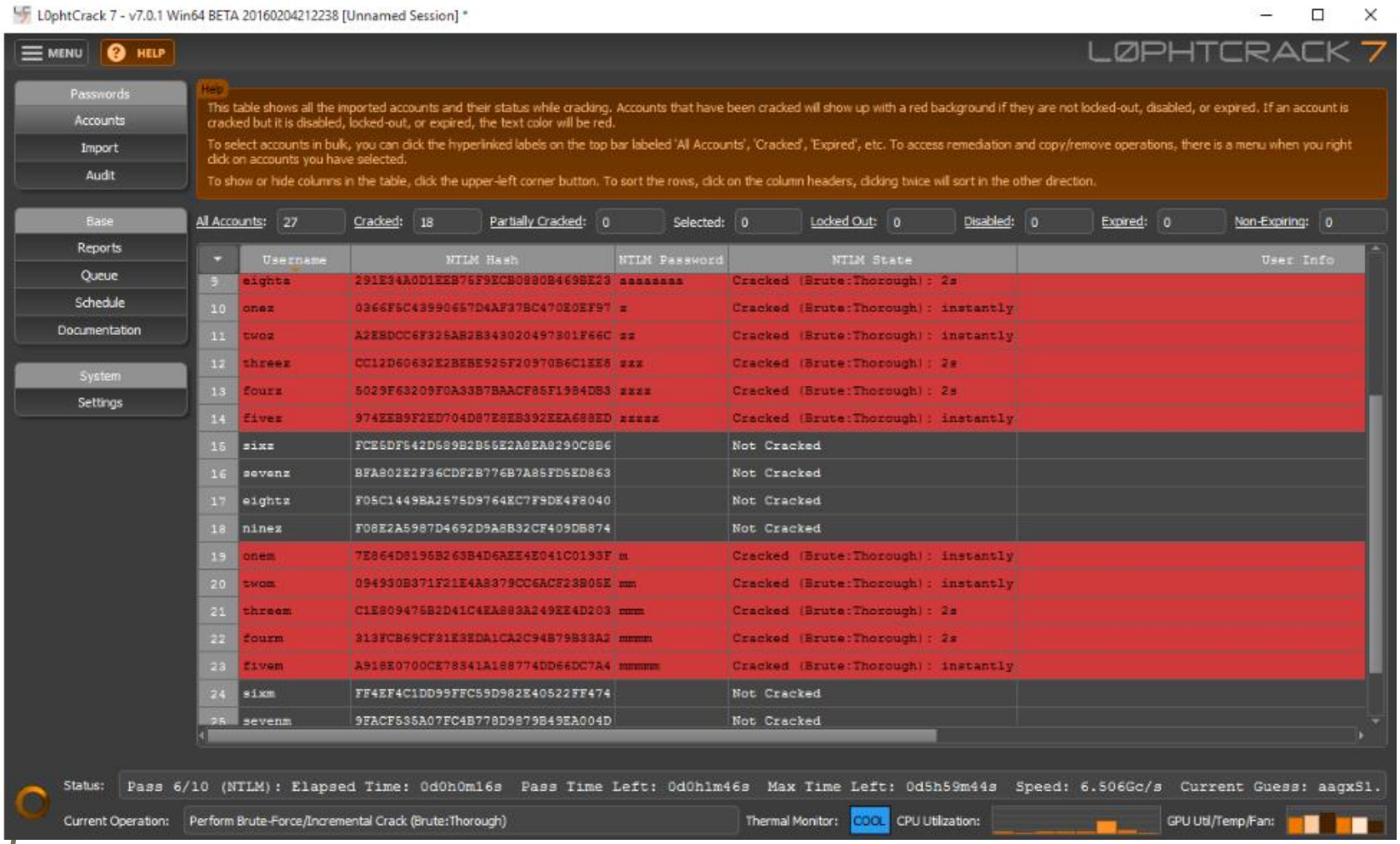
การใช้ระบบตรวจสอบตัวตน (Authentication)

- User and Password
- Smart Card
- Biometric System
- SecureID, Thump, Hard Lock, One Time Password

วิธีและแนวทางในการแก้ปัญหา

1. **Complexity**
2. **Don’t use Dictionary Word**
3. **Length of Password > more than 8 ??**
4. **Change often**

Good Password



Password Auditing

- **Process Authentication need to use more than one factor (MFA = Multi Factor Authentication)**
- **Example**

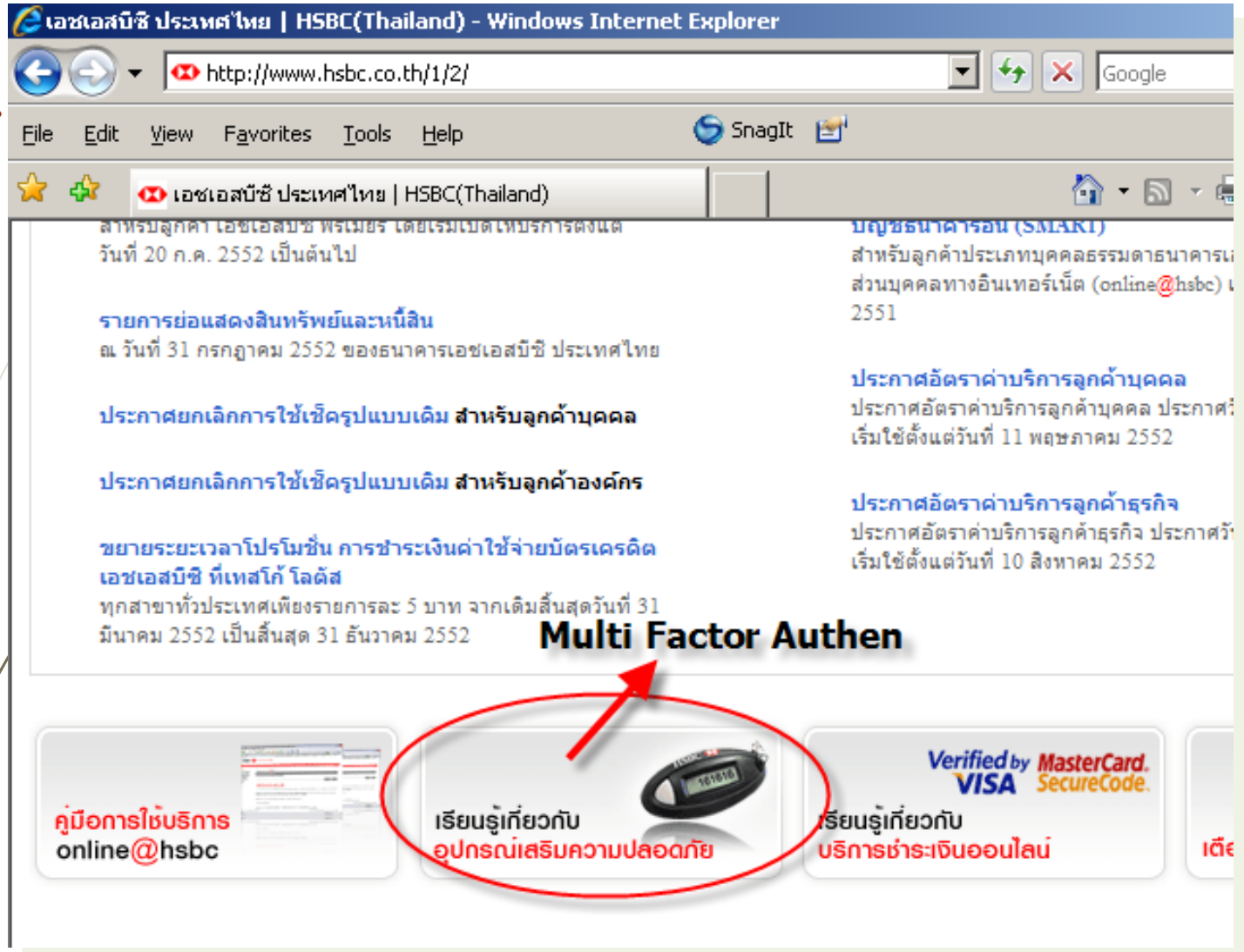
  password + smart card > 2 factors

  smart card + finger print > 2 factors

  password + finger print + smart card > 3 factors

Factor Authentication

Retina Scan (Biometric)



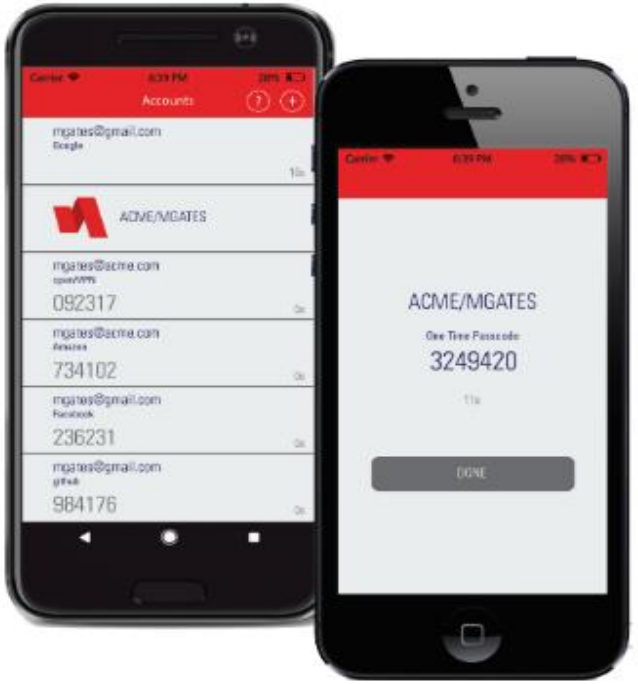
Multi Factor Authentication

Overview Secure ID

1 request

Generate password 2

RSA Server



Firewall มีอยู่ 3 ชนิด

1. Packet Filtering Firewall
2. StateFul Firewall
3. Application Firewall
4. WAF > Web Application Firewall

- Next Generation
- Unified Threat Management
- SIEM & SOAR
- EDR (XDR)

วิธีและแนวทางในการแก้ปัญหา

- **IDS and IPS ไว้ใช้ในการตรวจสอบผู้บุกรุกมีทั้ง Hardware Based และ Software Based**
- **กำหนดนโยบายในองค์กร หรือ Policy**
- **Network-based & Host-based**

วิธีและแนวทางในการแก้ปัญหา

- การตรวจสอบช่องโหว่ในระบบ ซึ่งเป็นหน้าที่ของ **Security Admin Team**

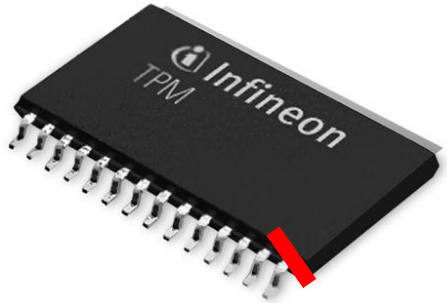
- ตรวจสอบความแข็งแกร่งของรหัสผ่าน
- ตรวจสอบช่องโหว่ของระบบปฏิบัติการ
- ตรวจสอบช่องโหว่ของอุปกรณ์เชื่อมต่อเครือข่าย
- ตรวจสอบต่อความไม่เข้มงวดของพนักงานในเรื่องความปลอดภัย

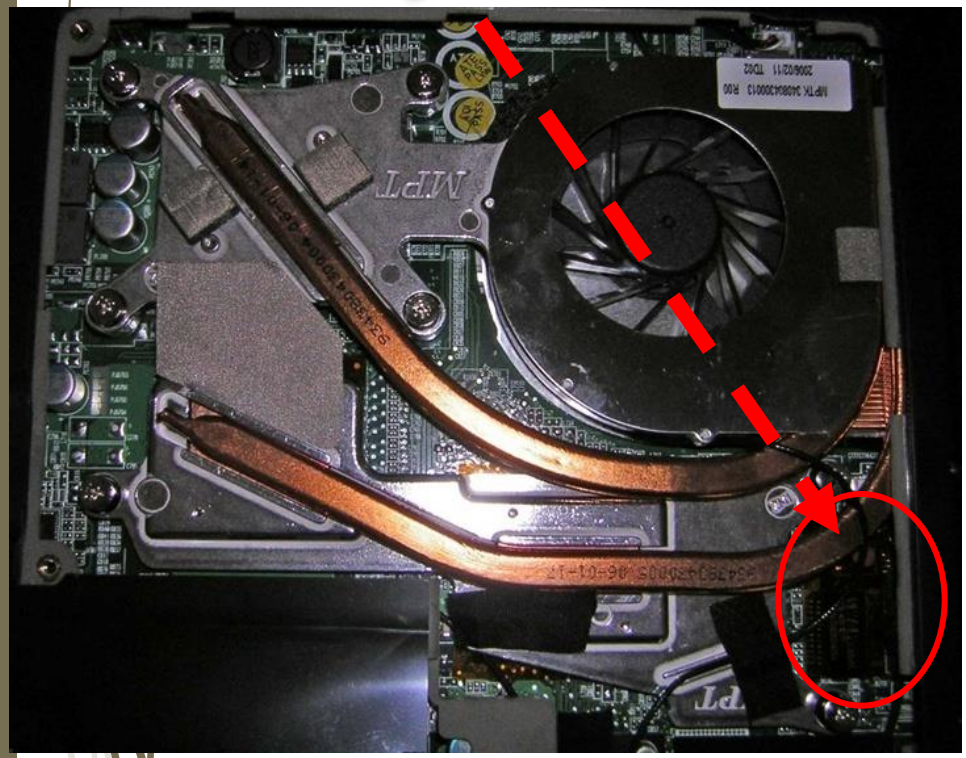
วิธีและแนวทางในการแก้ปัญหา

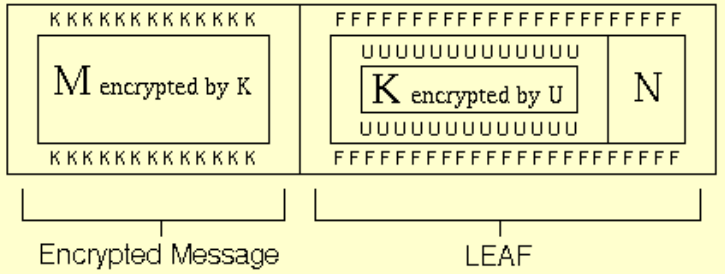
ทำการเข้ารหัส เช่น

- save with password
- Compression เข้ารหัสผ่าน
- Password Vault
- ใช้ฟังค์ชั่นในระบบปฏิบัติการเข้ารหัส เช่น VPN, IPSec เป็นต้น
- TPM Chip Encryption
- Drive Encryption

วิธีและแนวทางในการแก้ปัญหา







F = Family key (common to all Clipper Chips) - 80 bits
N = serial Number of chip - 30 bits
U = secret key for chip - 80 bits
K = Key specific to particular conversation - 80 bits
M = the Message

Law enforcement officers who have a court order permitting them to intercept a phone conversation can decrypt the conversation using the following procedure:

- use F to decrypt outer layer of LEAF revealing N and K encrypted by U
- obtain escrowed key halves for chip with serial number N
- put key halves together (with XOR) to reveal U
- use U to decrypt K
- use K to decrypt M (the message)

TPM Chip

- การควบคุมการเข้าออกห้องคอมพิวเตอร์ รวมถึงมีการควบคุมระบบไฟฟ้า, น้ำท่วม, ไฟไหม้, แผ่นดินไหว เป็นต้น

(SCADA Attack)

วิธีและแนวทางในการแก้ปัญหา

Secured Doors and Vaults

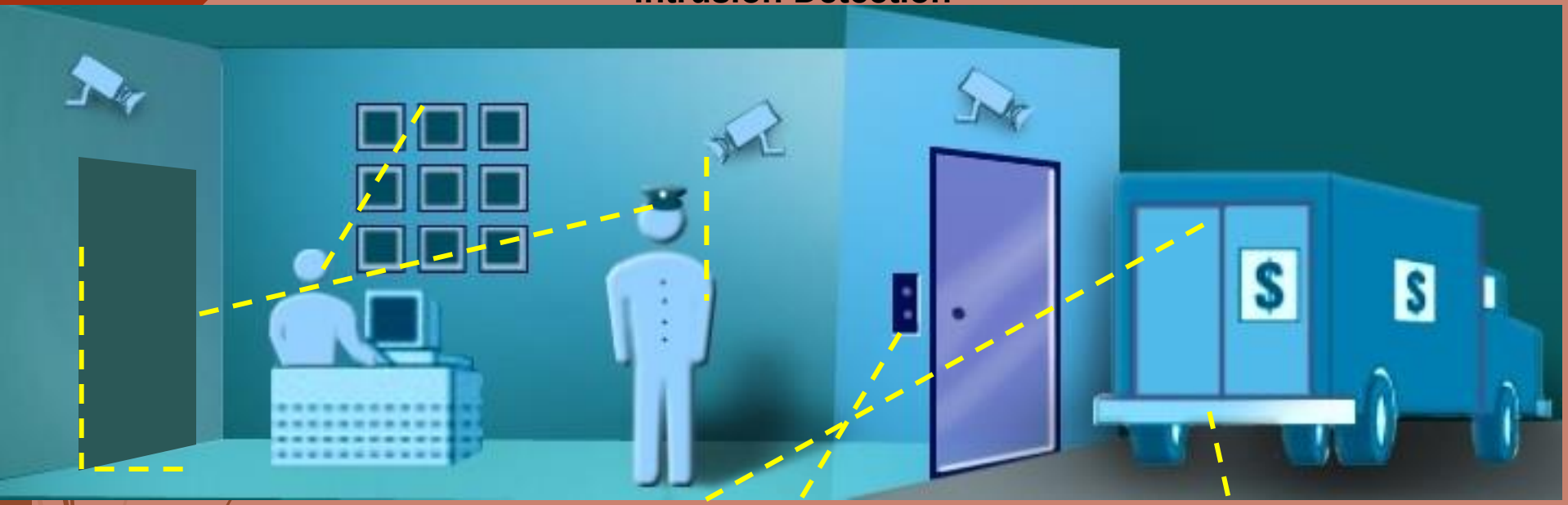
Firewalls and Router ACLs

Surveillance and Alarms

Network and Host-based Intrusion Detection

Patrolling Security Guard

Catalyst Integrated Security



Security Room CCTV

Centralized Security and Policy Management

Card Readers

Identity, AAA, Access Control Servers and Certificate Authorities

Secure Transport

Encryption and Virtual Private Networks (VPN's)

Information Security Is Like Physical Security

Deploy Security as an Integrated System

Chapter 2

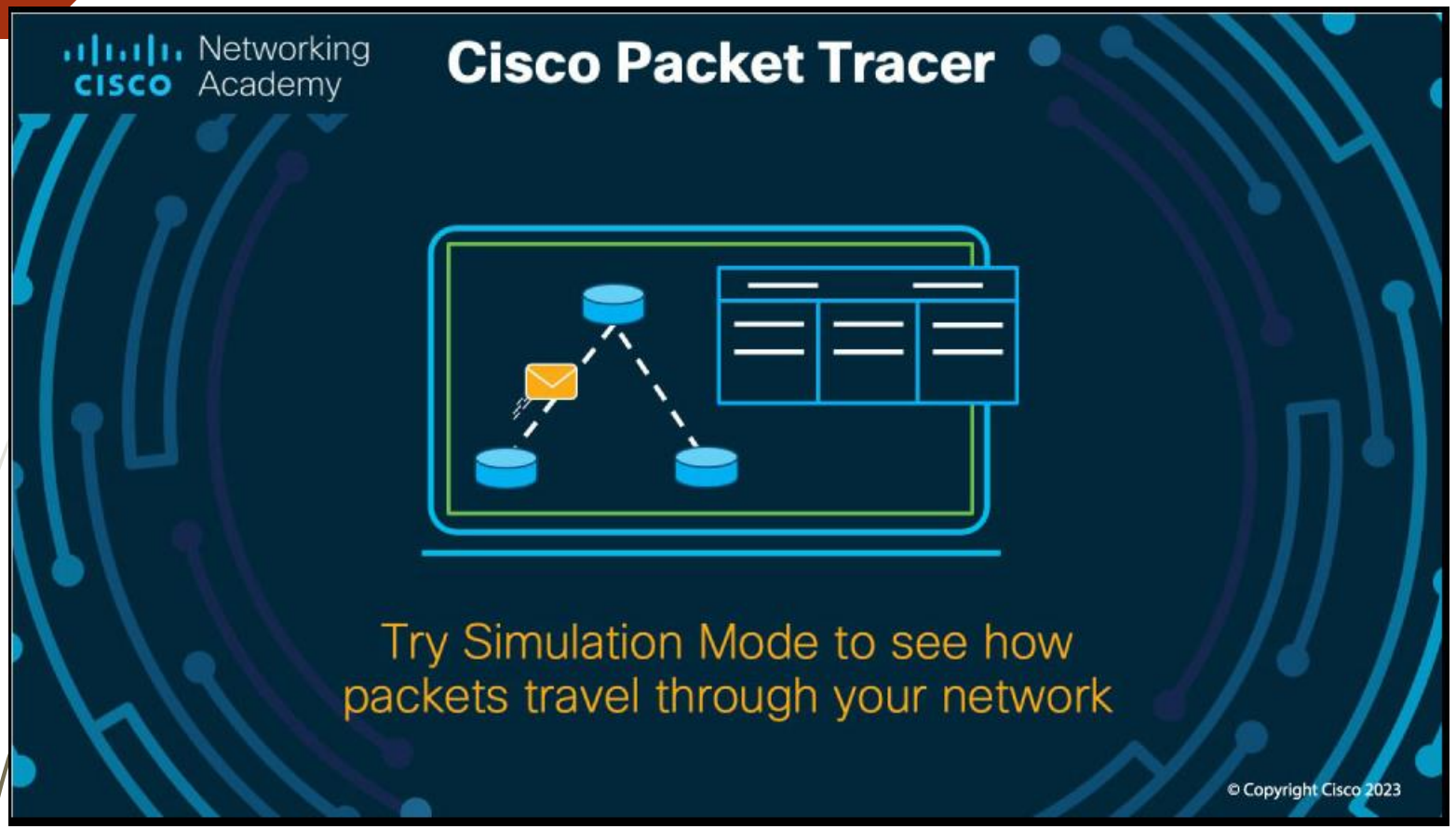
Types of Attacks

Types of Attacks

- They are 4 categories of attack
  1. Access Attack
  2. Modification Attack
  3. Denial of Service Attack
  4. Repudiation Attack

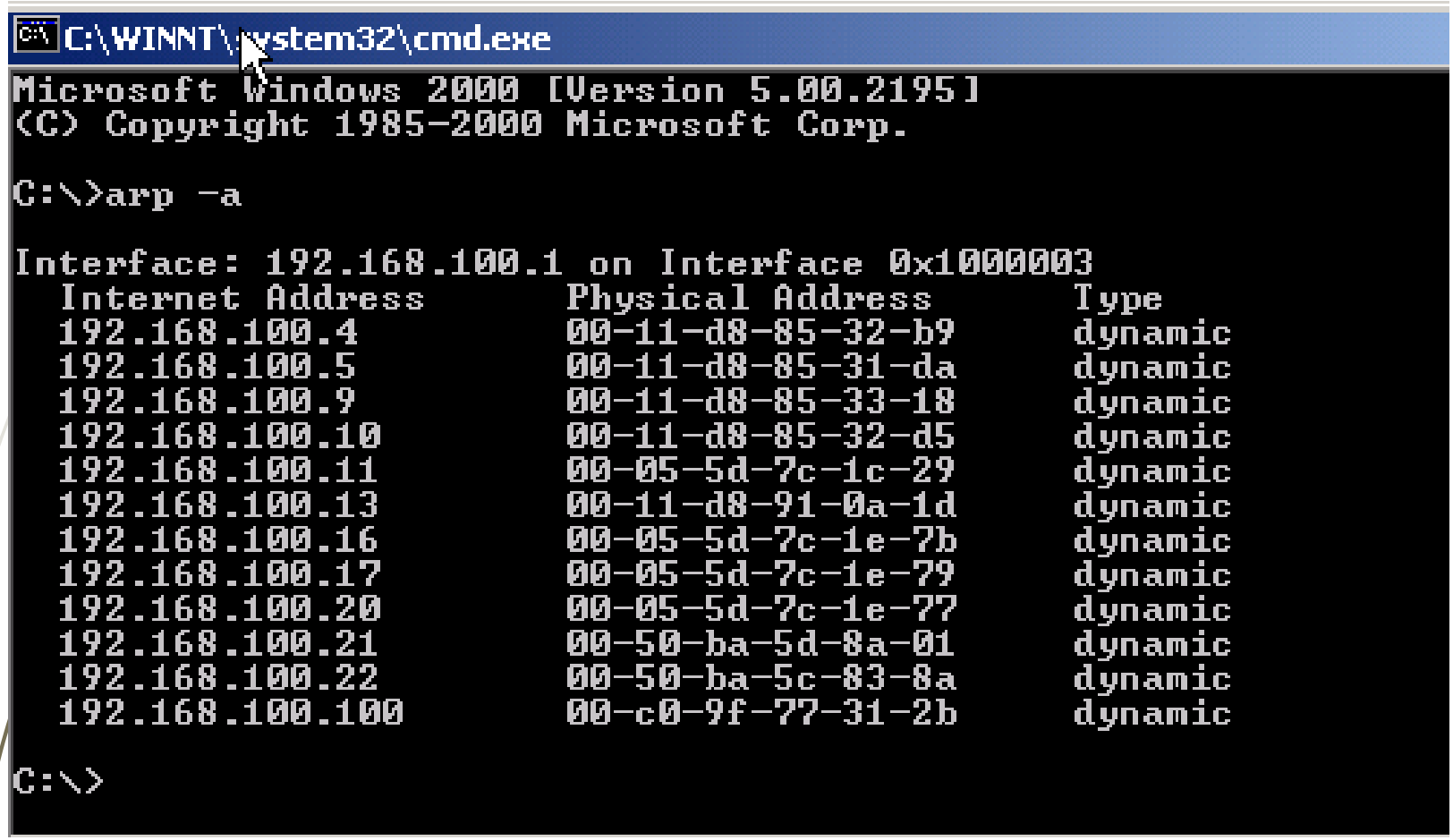
TCP/IP

Basic for Hacking Technique

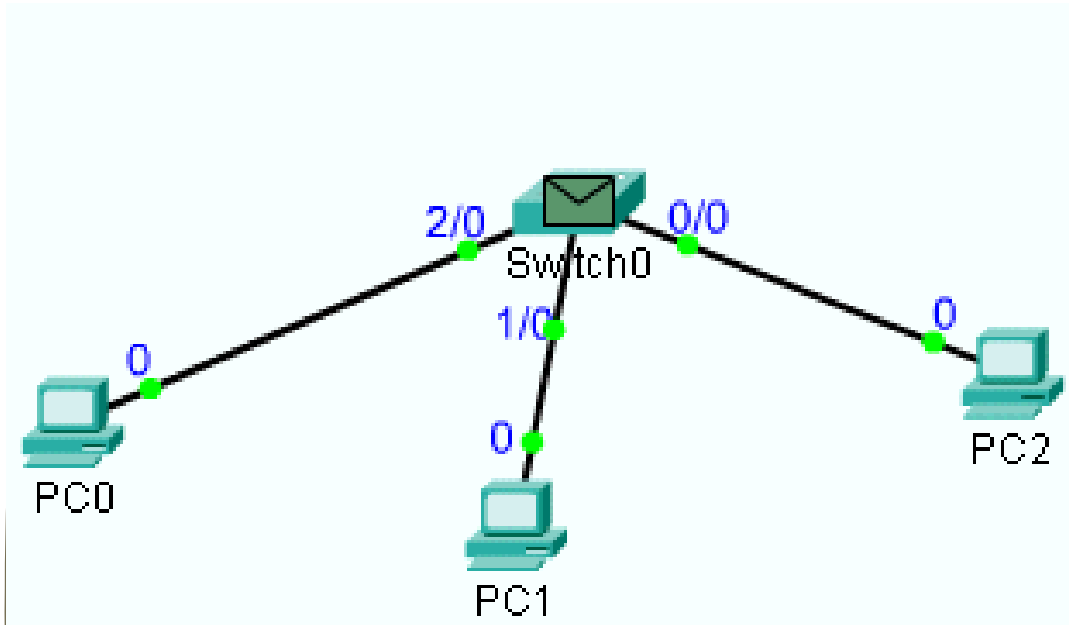


: Packet Tracer

ARP



- arp –a Listname mac adress and ip computer.



Packet Info at Device: Sv

At Device: Switch0
Source: PC0
Destination: PC2
TX time: 0.082 ms

× Layer 7
× Layer 6
× Layer 5
× Layer 4
× Layer 3
+ Layer 2: 0060.2F28.D5DF >> 0000.0CFA.3363
+ Layer 1: Port 2

Switch works on Layer 2 in OSI Model
And they consider only MAC Address…

- ป้องกันโดย ระบุว่า คนนอกที่เข้ามาในบริษัทจำเป็นต้องอยู่ใน **zone** ที่กำหนด เท่านั้น
- กรณีถ้าเป็นคนใน หรือ คนนอก ก็ได้ ก็อาจใช้วิธีการป้องกันโดยการเข้ารหัสใน **network** คุณนั่นเอง เช่น การใช้ **IPSec, VPN** เป็นต้น **>> recommend**
- ติดตั้งพวก **IDS** หรือ **IPS**
- เทคนิคในการเข้ารหัสนั้นไม่สามารถป้องกันการดักฟังข้อมูลได้ **100%**

การป้องกันการดักฟัง (Sniffer)

- **Threat from Username/Password and Identity theft**
- **SET, Pharming**

: Modification Attack

Threat from Username/Password and Identity theft

Denial of Service Attack

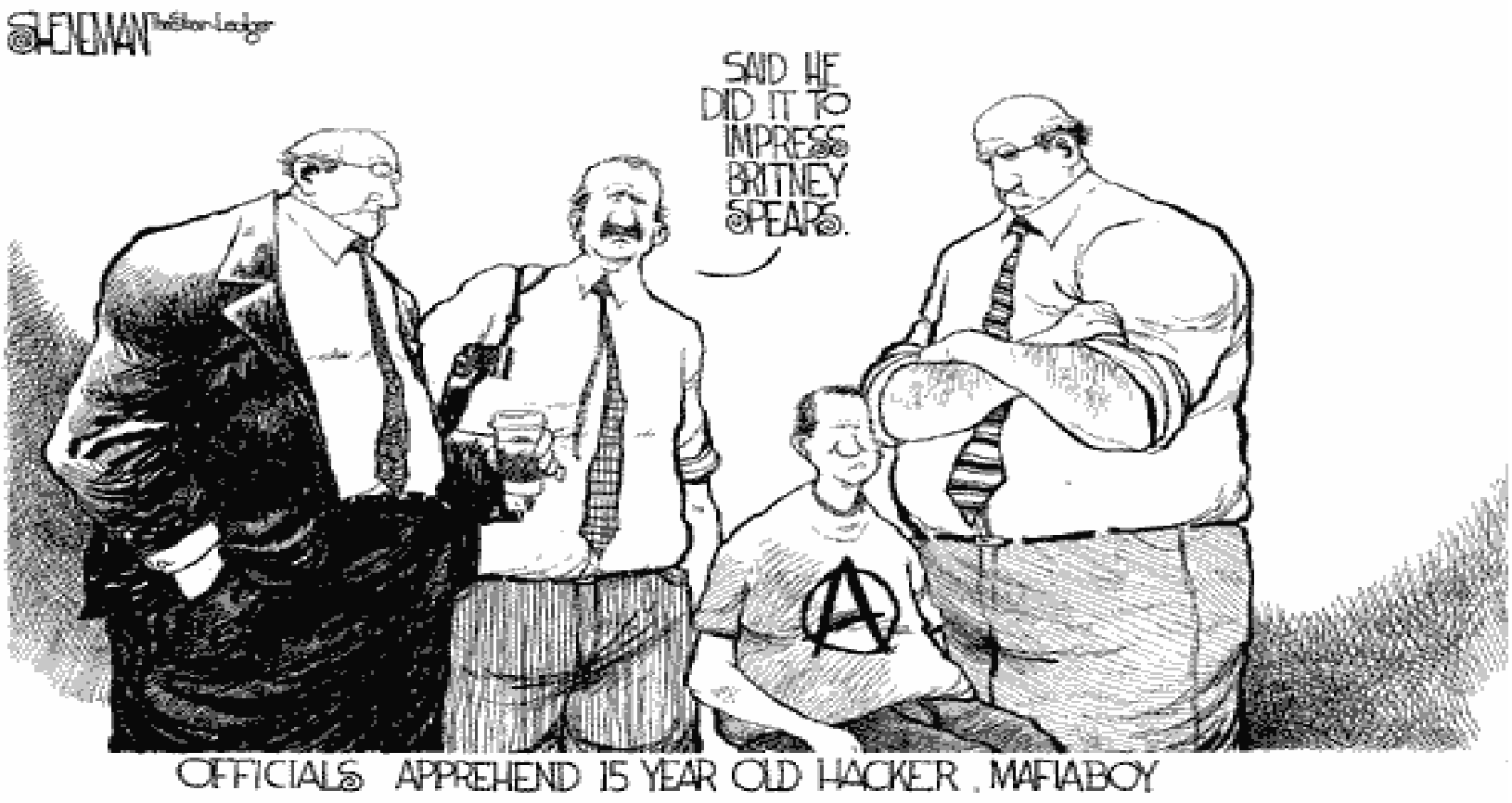
- **Ping of Death**
- **Smurf**
- **SMBDie**
- **Syndos**

DOS Computer

- **Ether Flood >> DOS Switch**
- **Metasploit**
- **DDoS (Distributed Denial of Service)**

King of DDoS : Mafiaboy and his objective

Source: BlackHAT, Las Vegas



Critical Infrastructure Attack

- **Ping package** มหาศาลไปให้เครื่องเหยื่อ โดยใช้คำสั่ง

  ping ip ของเหยื่อ **–l 65000 –t**

กรณีนี้อาจใช้ การบอมบ์แบบ รุมกินโต๊ะ เรียกว่า Distributed DOS ช่วยกันเป็นทีม

Ping of Death

- Denial of Service Switch.
- Distributed Denial of Service
- Exploit
- Tools → macof, hping

EtherFlood

- Phishing
- Pharming
  - Spear Phishing
  - Whaling
- Vishing
- Smishing
- Defacement Web

Etc.

Repudiation Attack

- คล้ายกับ **Phishing** โดยทั่วไป คุณจะทำการเข้าไปที่ **website** ที่หลอกลวงผ่าน **link** แต่กรณีที่เป็น **Pharming** จะทำการหลอกการ **resolve name**

Process ปกติ

www.yahoo.com > 202.44.33.100 > webserver จริง

Process Pharming

www.yahoo.com > IP ของเครื่องที่ตั้งหลอกไว้

Pharming

Chapter 3

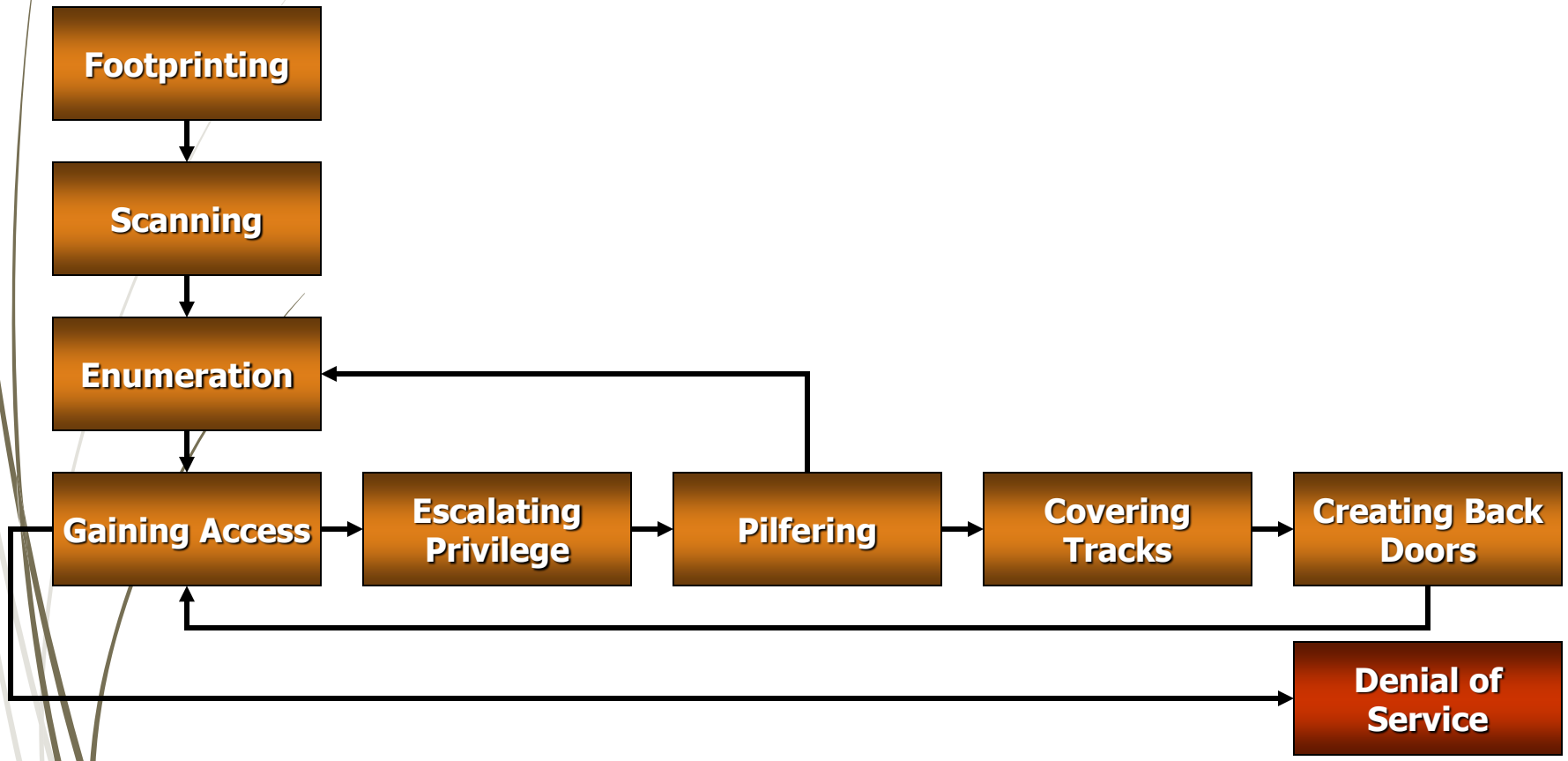
HACKING TECHNIQUE

Defcon: Hacker Meeting

Phase of Hacking

https://www.nwkings.com/what-is-the-first-phase-of-hacking

THE METHODOLOGY



FootPrinting

ค้นหาข้อมูลทั่วไป HTTP, IP address, DNS, Mail Pop3

Scanning

ตรวจสอบช่วง IP address และ Port

Enumeration

เครื่องมือการสำรวจเฉพาะระบบเช่น Web, Microsoft,

Gaining access

ได้ผู้ใช้ทั่วไป หรือเข้าใช้เครือข่ายได้

Denial of Service

รบกวนให้ระบบทำงานไม่ได้

Escalating Priv

ได้ Administrator, root จาก spyware, sniffer

Pilfering

ขโมยข้อมูล หรือรหัสผ่านของบุคคลต่างๆ

Covering track

การทำลาย Log หรือป้องกันการตามรอย

Back doors

สร้างช่องทางในการเข้าใช้ครั้งต่อไป

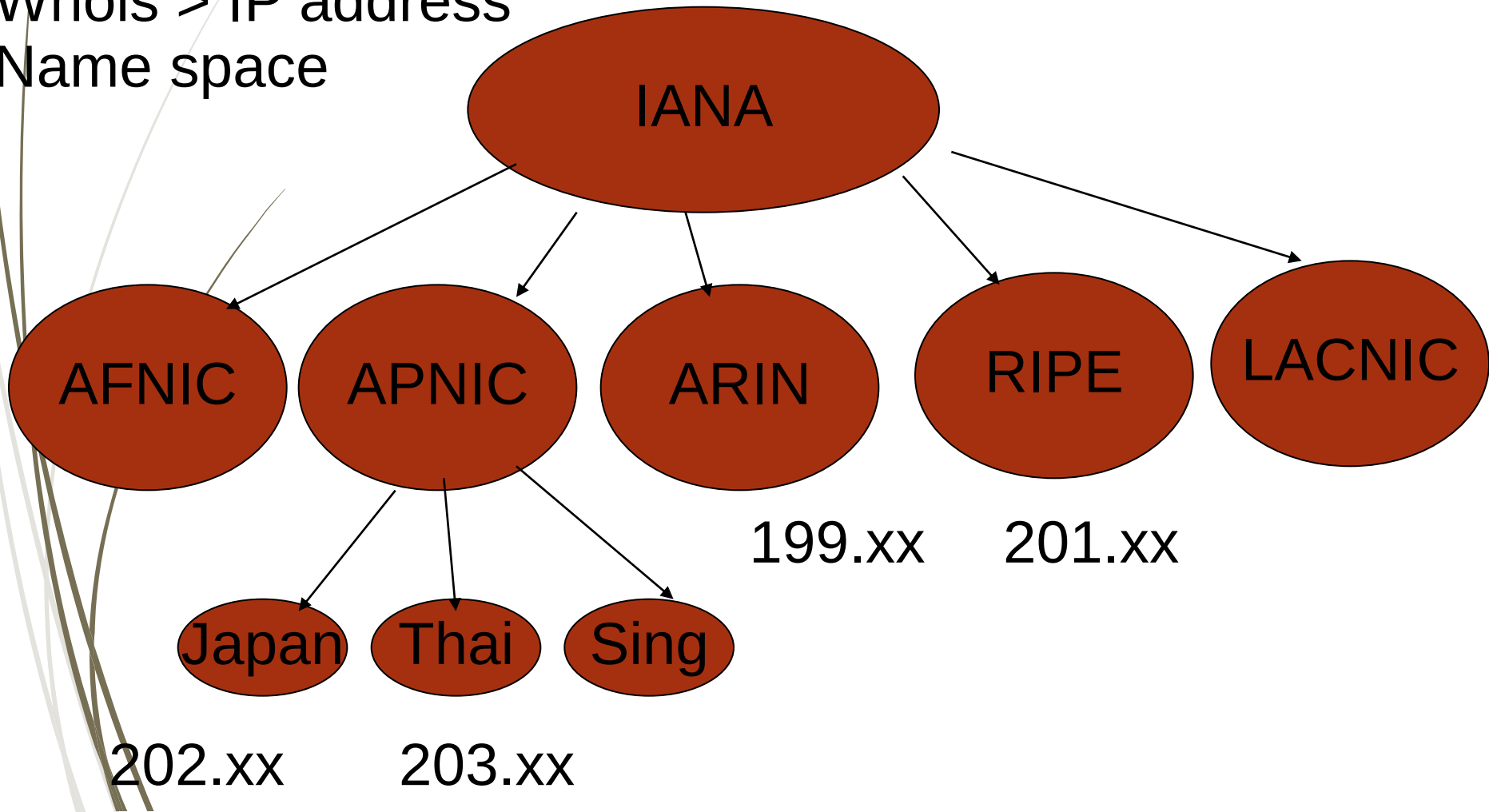
องค์กรดูแลเครือข่าย

www.iana.org

Internet Assign Number Authority

Whois > IP address

Name space

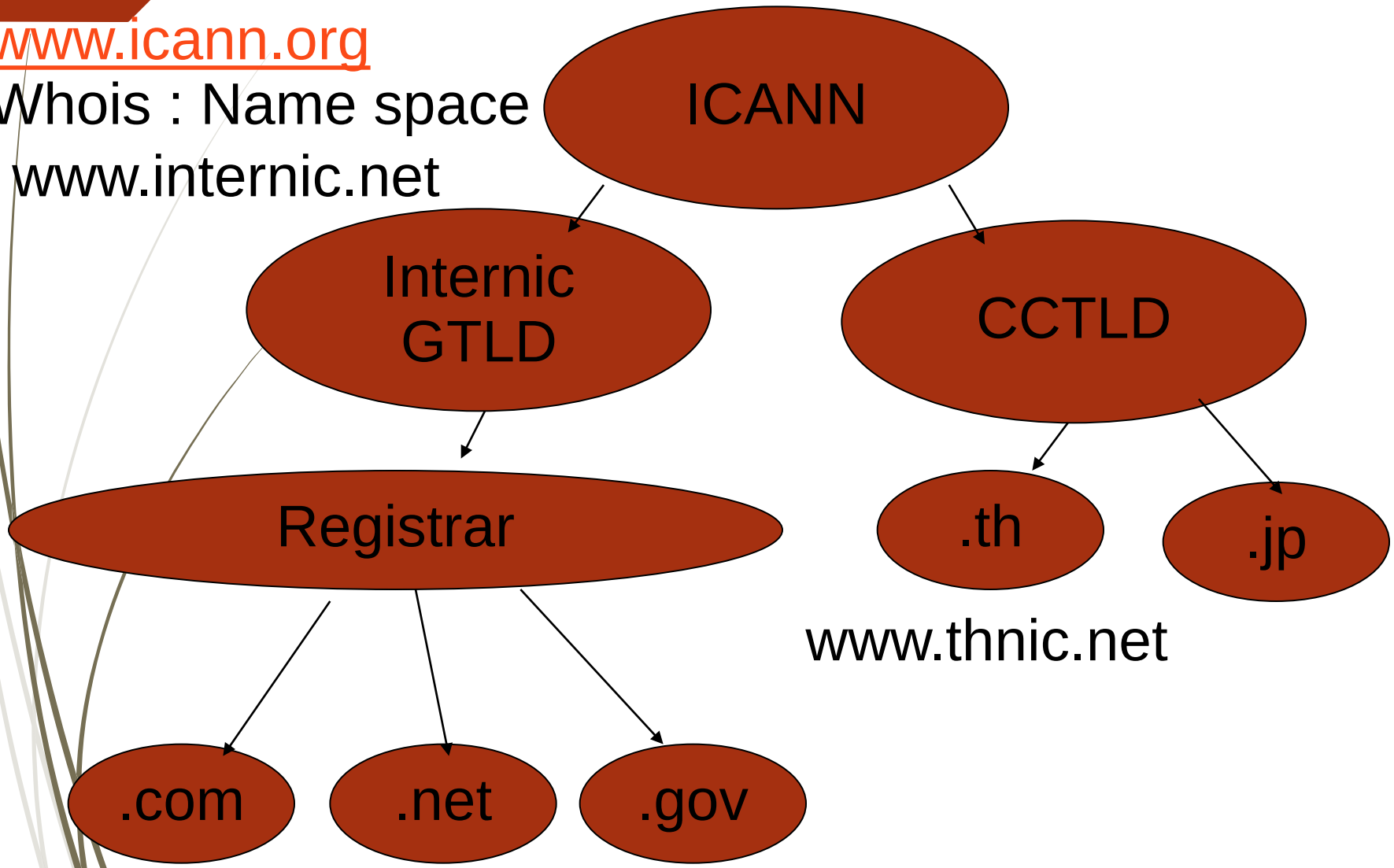


องค์กรดูแลชื่อที่ใช้

www.icann.org

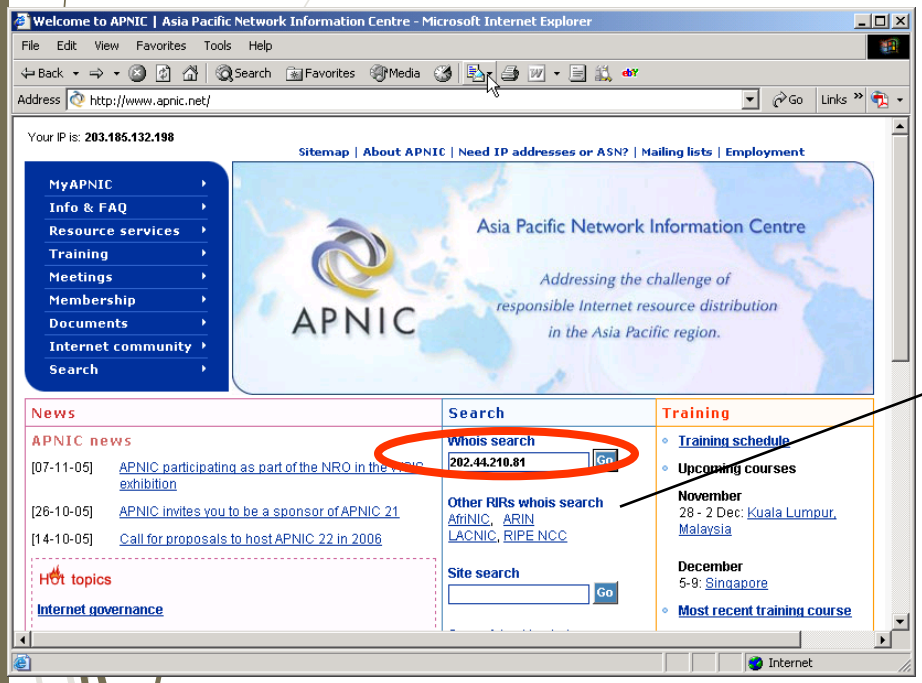
Whois : Name space

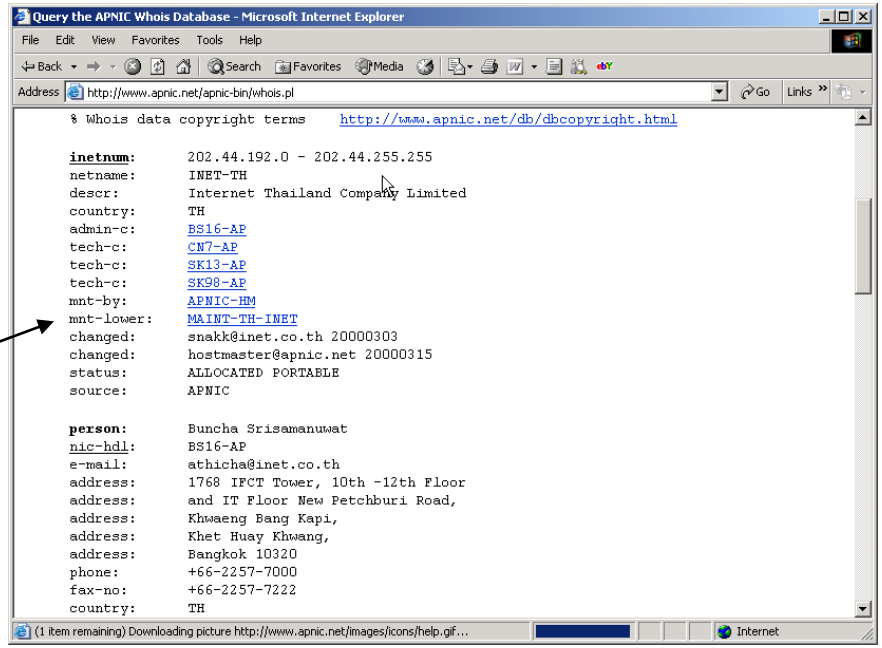
www.internic.net



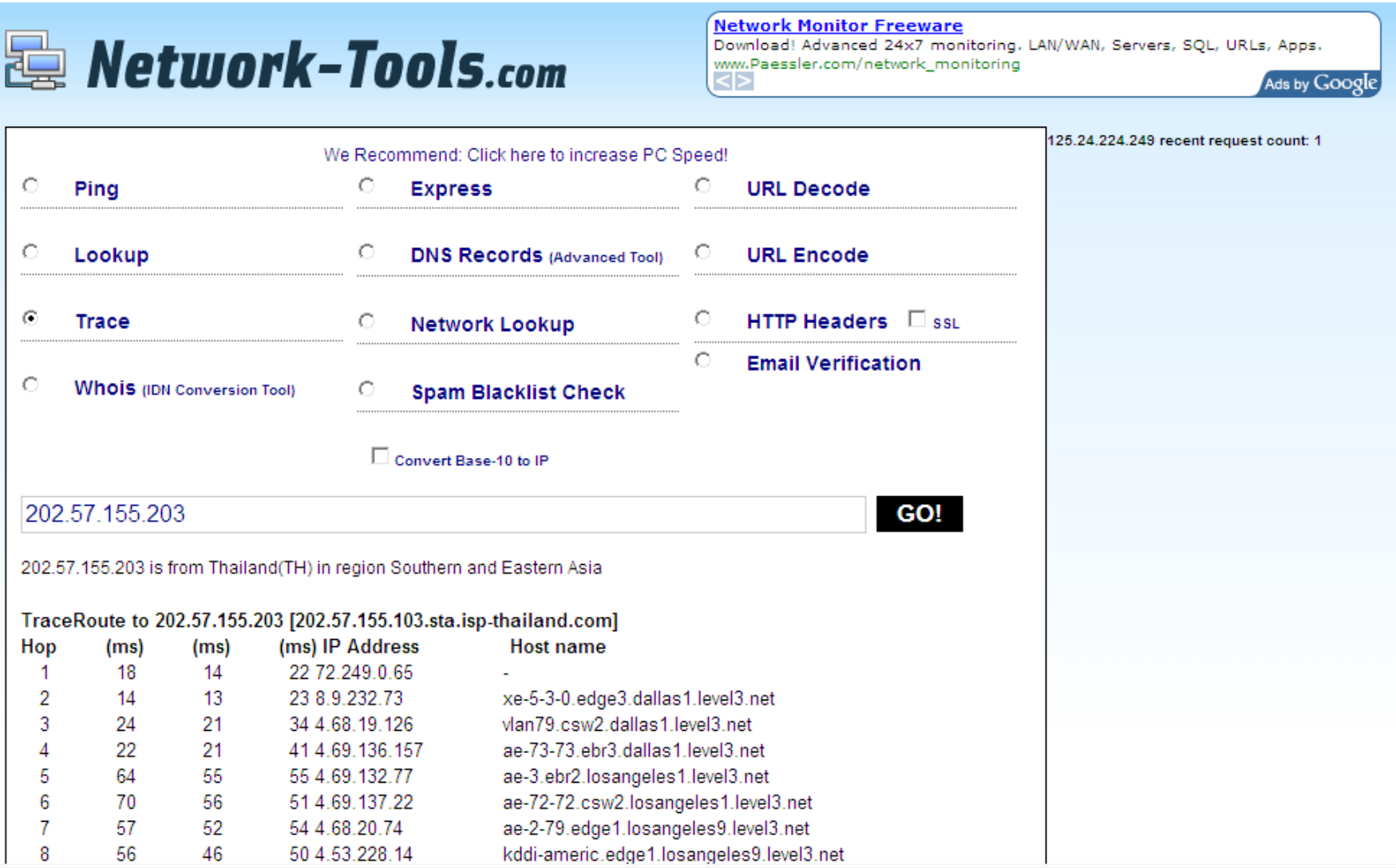
www.thnic.net

www.apnic.net

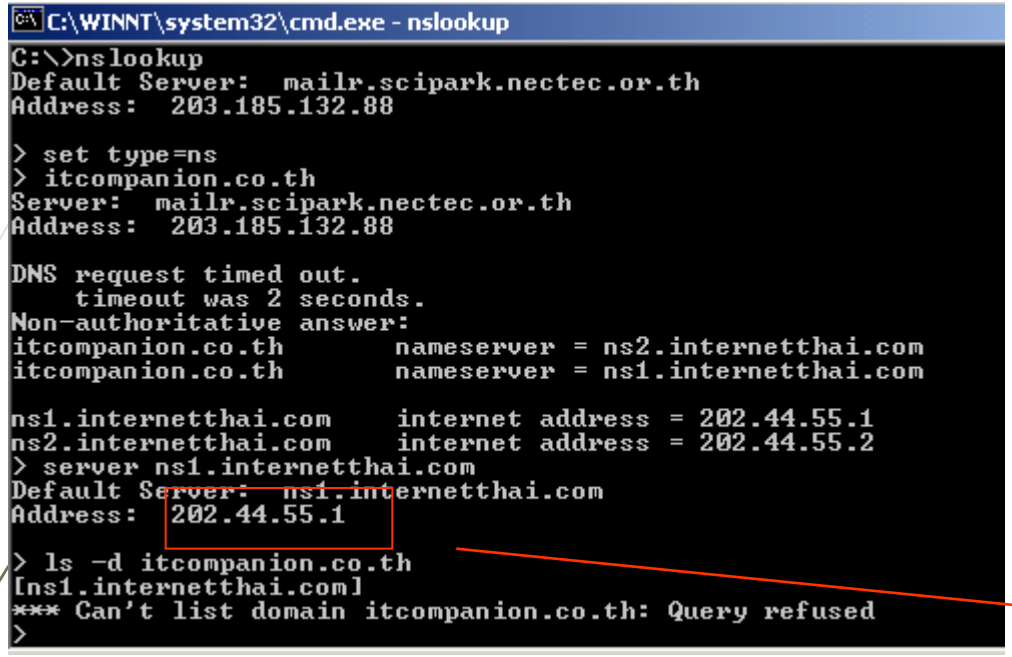




www.network-tools.com



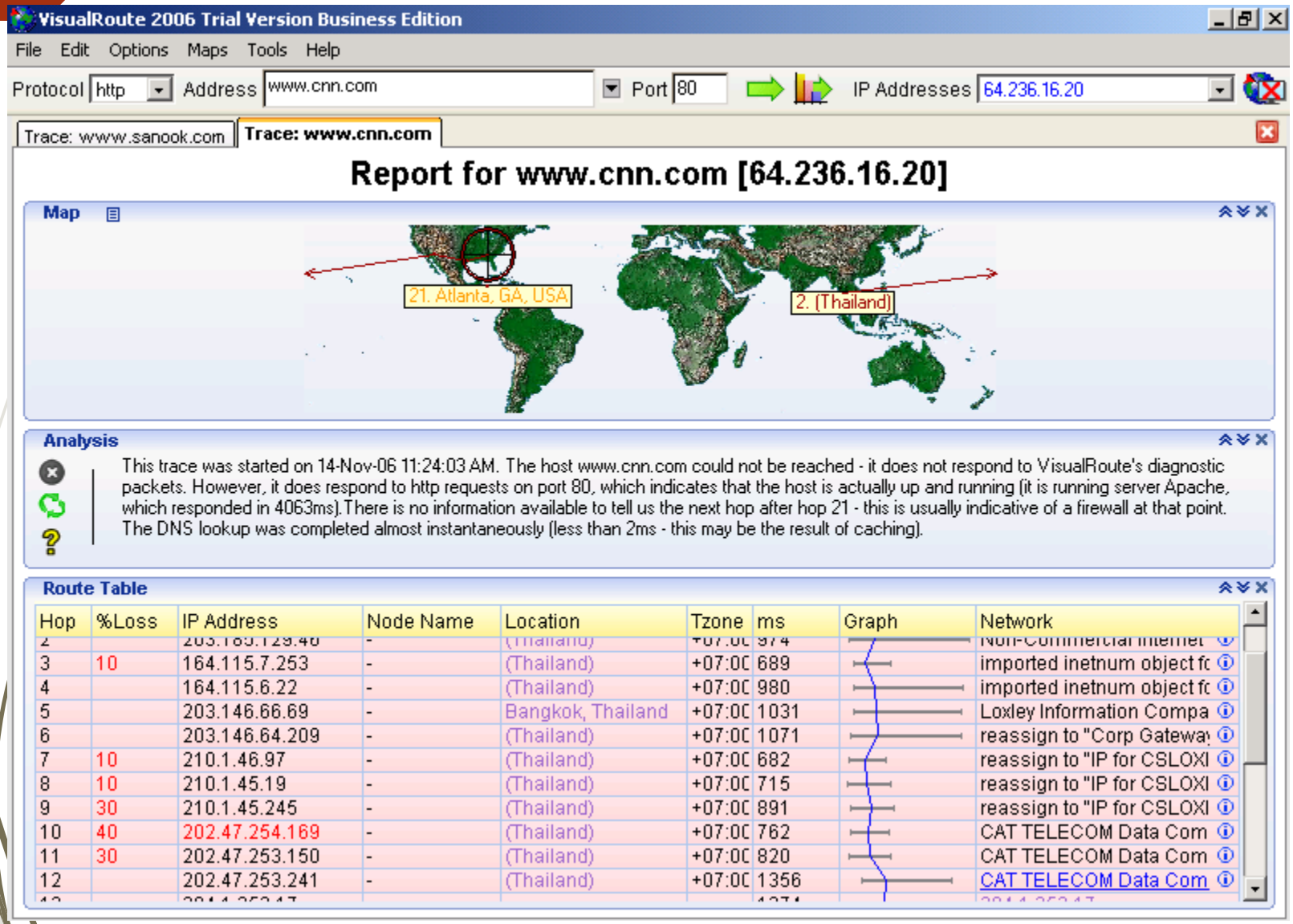
NSLookup



This zone is protect already!!

- Cmd > nslookup > set type=ns > domainname.zonename > server NSservername
- ls –d domainname.zonename

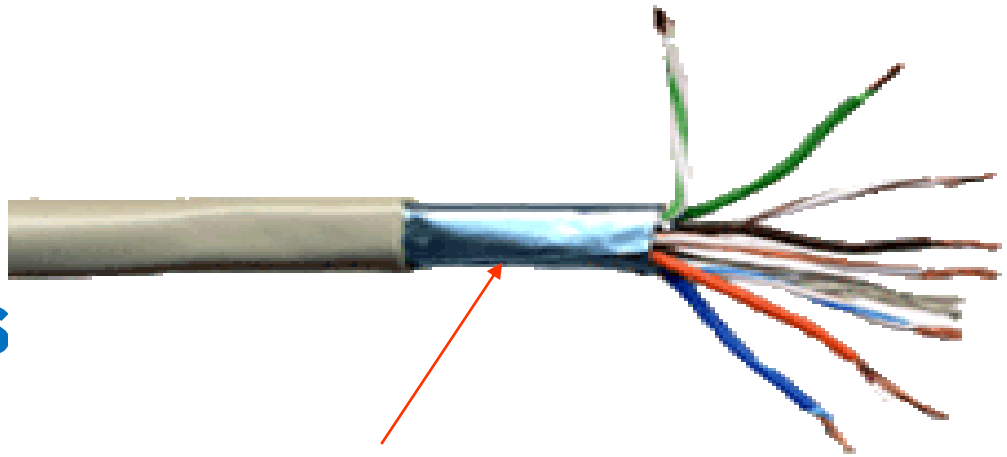
Visual Route



Hacking : Physical Layer

Physical Layer

- Coax
- Fiber
- Wireles



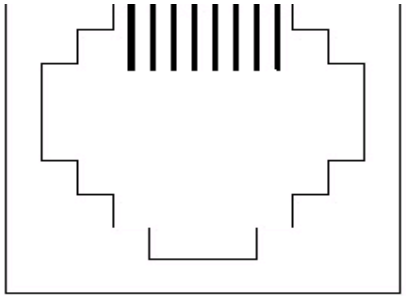
Shield : For reduce noise from EMI and RFI..

Ethertap

standard RJ4

RD+
RD-
TD+
NC
NC
TD-
NC
NC

IC = Not Connected
D = Receive Data
D = Transmit Data



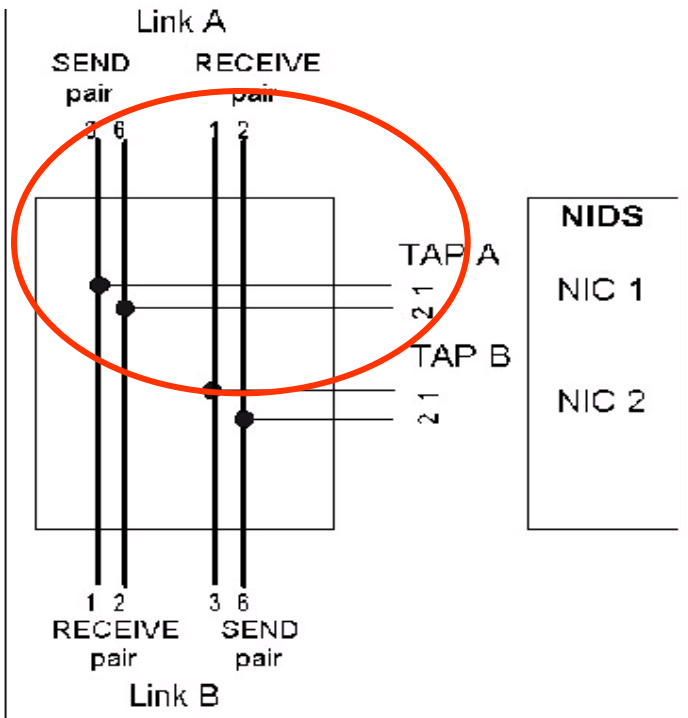
Host witch | Host Switch | Host | Switch

TD+ — 3 TD+ — 3 TD+ — 3 TD+
TD- — 6 TD- — 6 TD- — 6 TD-
RD+ — 1 RD+ — 1RD+ — 1 RD+
RD- — 2 RD- — 2 RD- — 2 RD-

common pin reservations for Ethernet

Ethernet tap

Network IDS with two NICs



tap-only network tap principle

Phone Tapping

Cell Phone Jammer

WORLDWIDE CELL PHONE JAMMER SPECIALISTS

If you have a problem with mobile phone usage in your establishment and want to eliminate it, then look no further! We can supply you with equipment to either detect and monitor cell phone usage, or prevent the use of it all together with our cell phone jammer products.

Our cell phone detectors and cell phone jammers are used worldwide in prisons, schools, restaurants, cafes, libraries, bars, commercial offices, religious & military establishments for general noise disturbance problems or for security and anti-terrorism type issues. We supply governments and military forces.

Our products are available to buy on-line by mail order today. We offer a fast worldwide delivery service and a 12 month no quibble manufacturers warranty on all products. We accept payment by credit/debit cards, PAYPAL, money orders or cheques (Sterling, Euro, $US) and regular bank T/Ts.

We welcome all trade enquiries, please contact us for full pricing and sales information. We can supply any quantity to any country and offer excellent bulk purchase deals. See our customer comments here

Delivery to The Americas 2 days, rest of world 4 days with

Don't want somebody to use mobile phone !!!

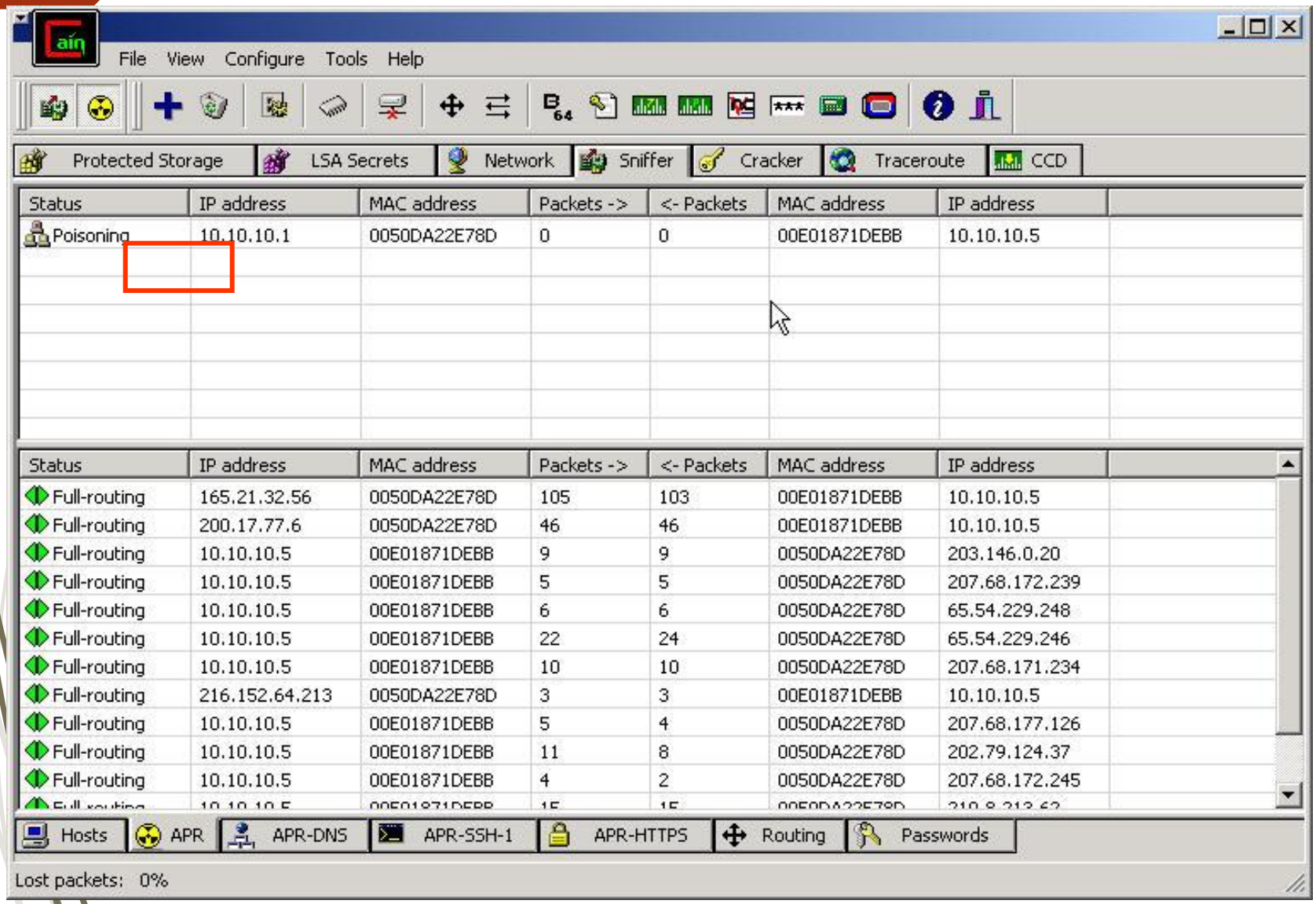
Hacking: Data Link Layer

ARP Poison Result!!!

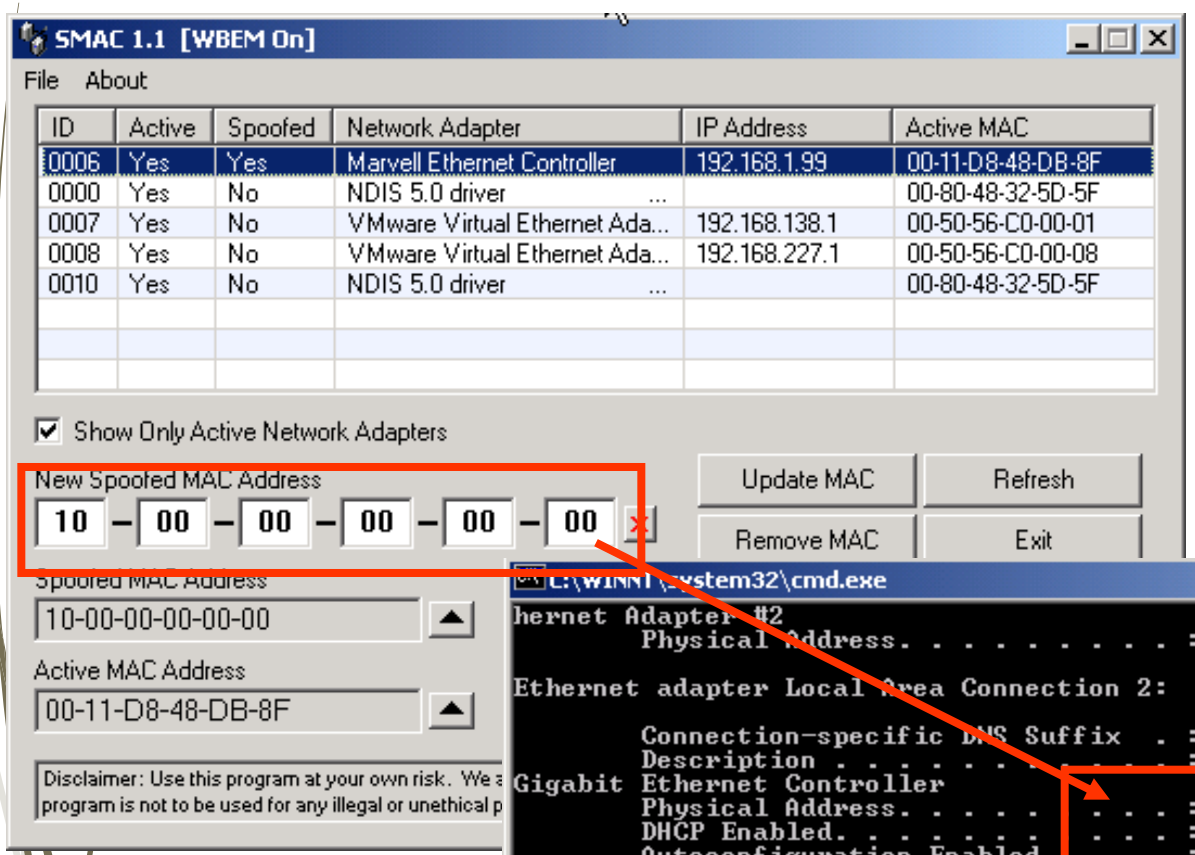
```
  UDP    192.168.175.1:137      *:*
  UDP    192.168.175.1:138      *:*
  UDP    192.168.175.1:500      *:*

C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time<10ms TTL=128
Reply from 10.10.10.2: bytes=32 time<10ms TTL=128

Ping statistics for 10.10.10.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
Control-C
^C
C:\>arp -a

Interface: 10.10.10.5 on Interface 0x1000004
  Internet Address      Physical Address      Type
  10.10.10.1            00-10-60-74-13-97     dynamic
  10.10.10.2            00-10-60-74-13-97     dynamic

C:\>
```

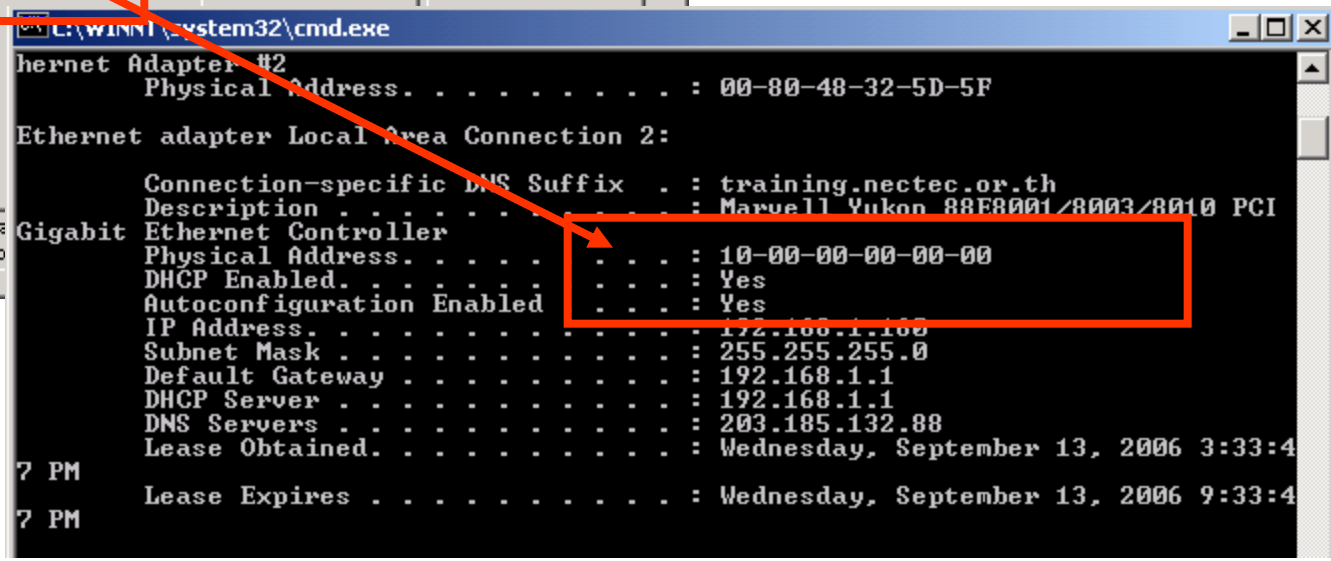
ARP Poison!!!

Sniffer is Man-in-the-Middle



: SMAC (MAC spoofing)

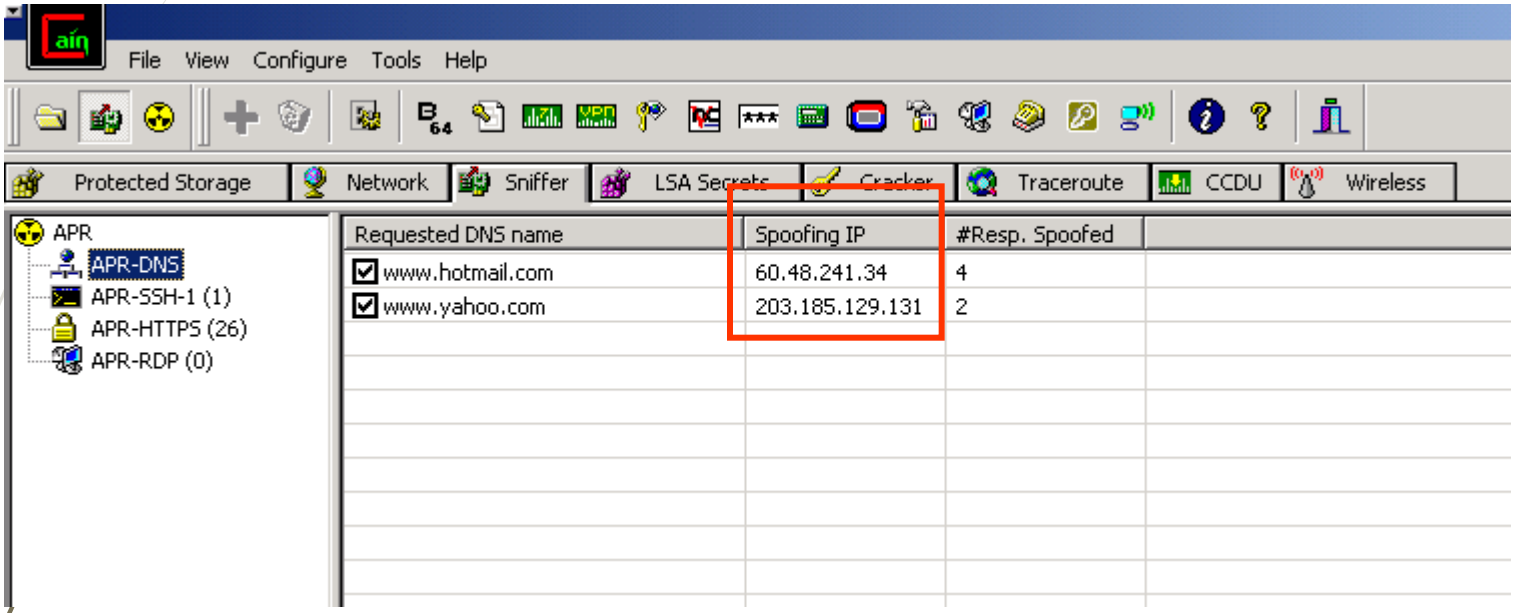




Disable and Enable Lan connection for refresh..

Hacking: IP Layer

DNS Spoofing



- Redirect Web Server which victim requests to Hacker Server(Spoofing IP)…

Hacking: TCP Layer

Example: Hacking TCP Layer

- Sync flood >Make many connection (sync) to victim for buffer overflow..

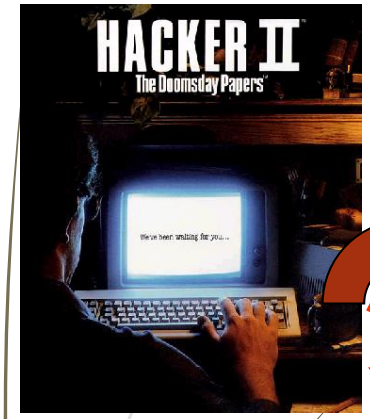
Example

```
root@kali:~# hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source www.hping3testsite.com

HPING www.hping3testsite.com (lo 127.0.0.1): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown

^C
--- www.hping3testsite.com hping statistic ---
1189112 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

Target is Attacked!!

Hacking: Application Layer

Hacking on HTTPS



CA Commercial

User	Private	Public
IE User	??	yellow
Webserver	??	Red
CA	??	Blue

=Red (Pub of Web)

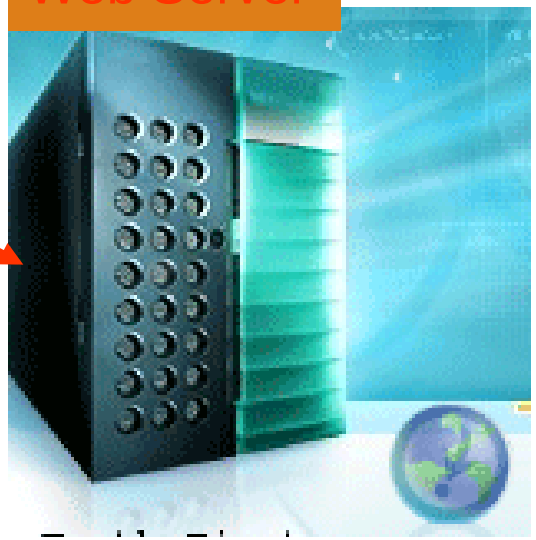
Fake Certificate!!

=Blue (Pub of CA)

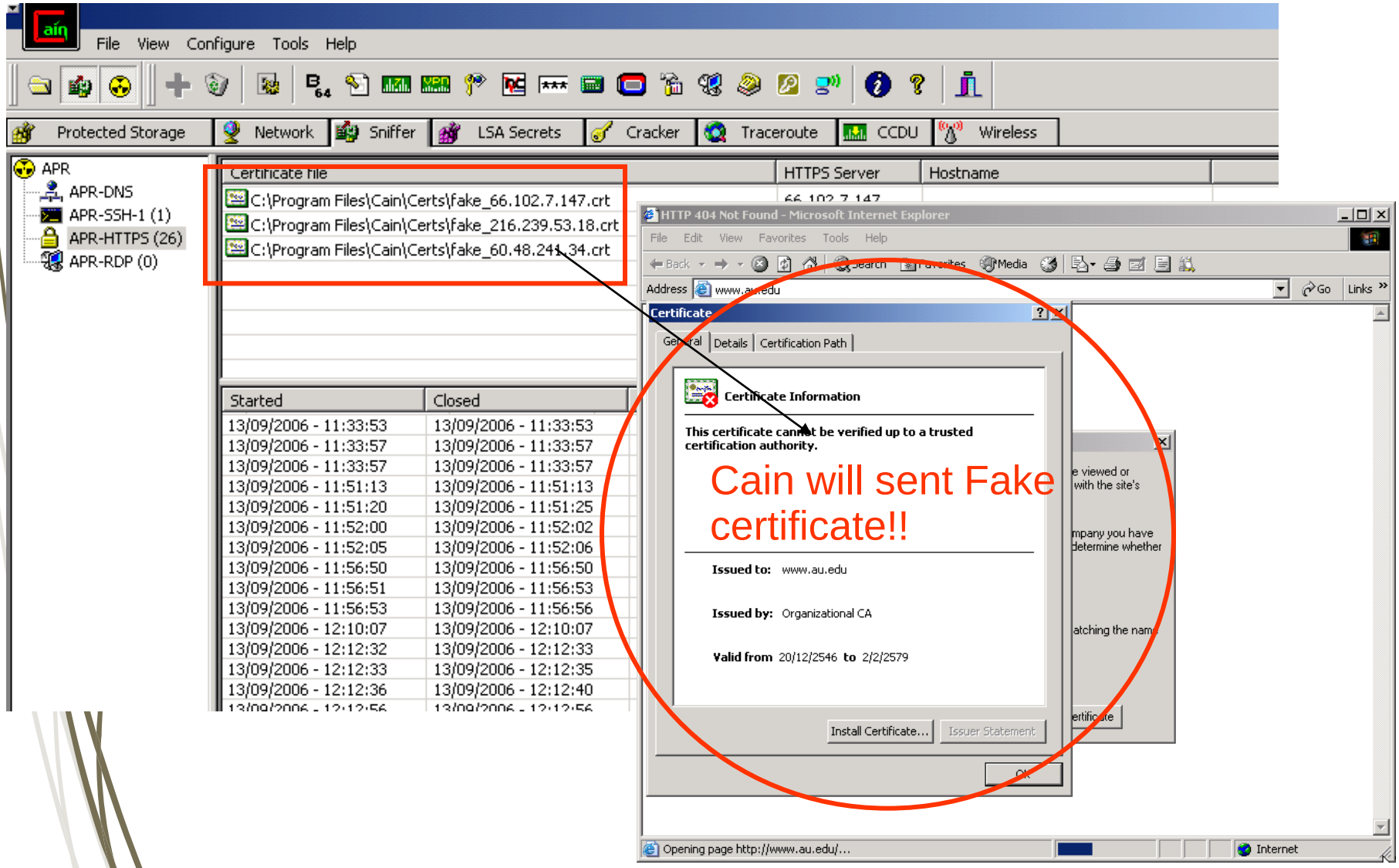
Computer

=Private of Web

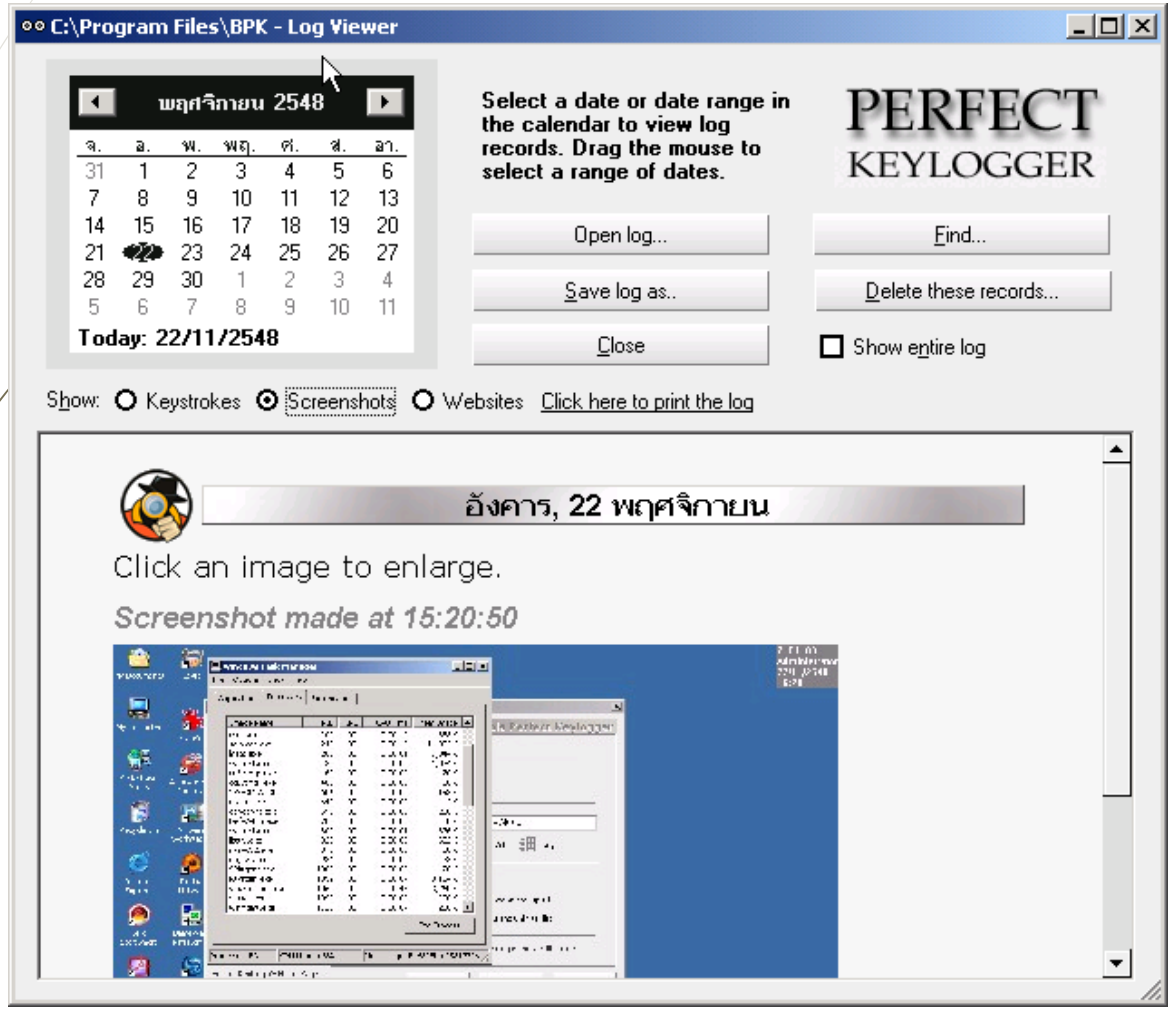
Web Server



Hacking on HTTPS



Perfect Keylogger



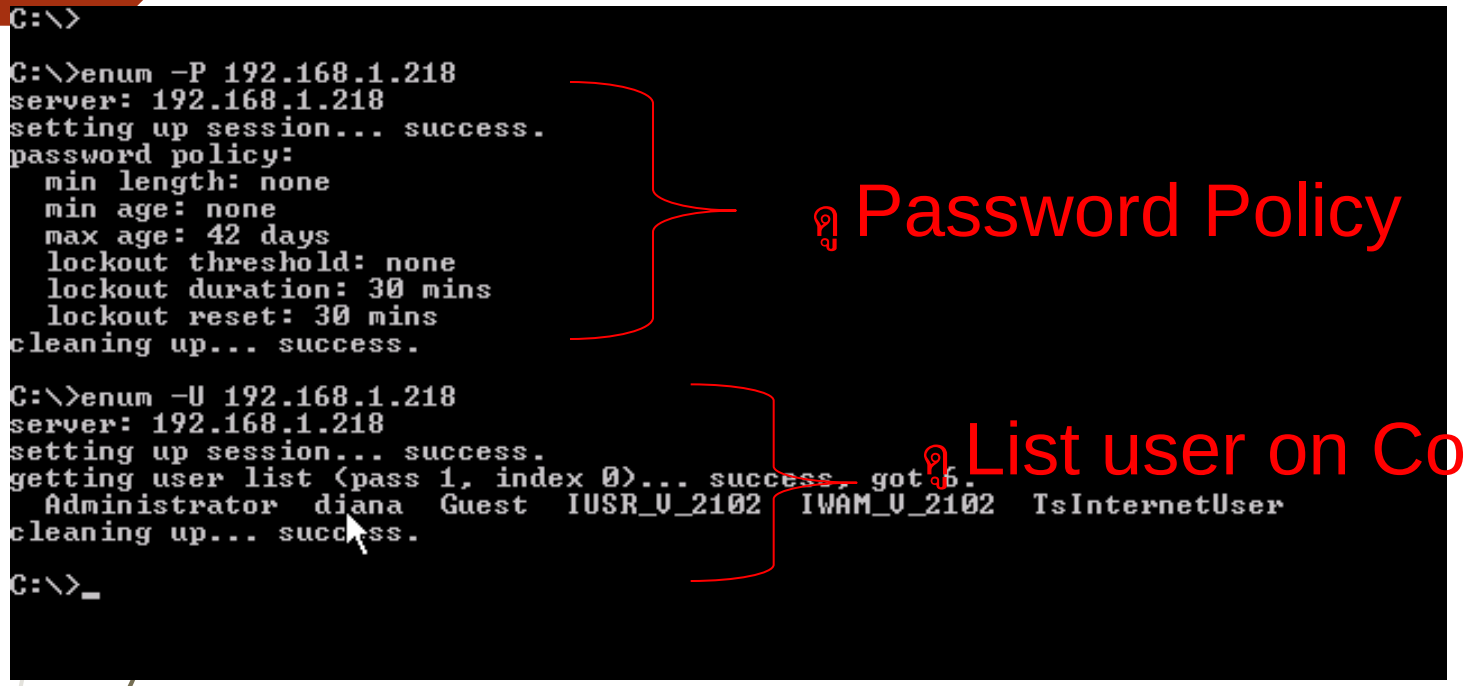
BackDoor

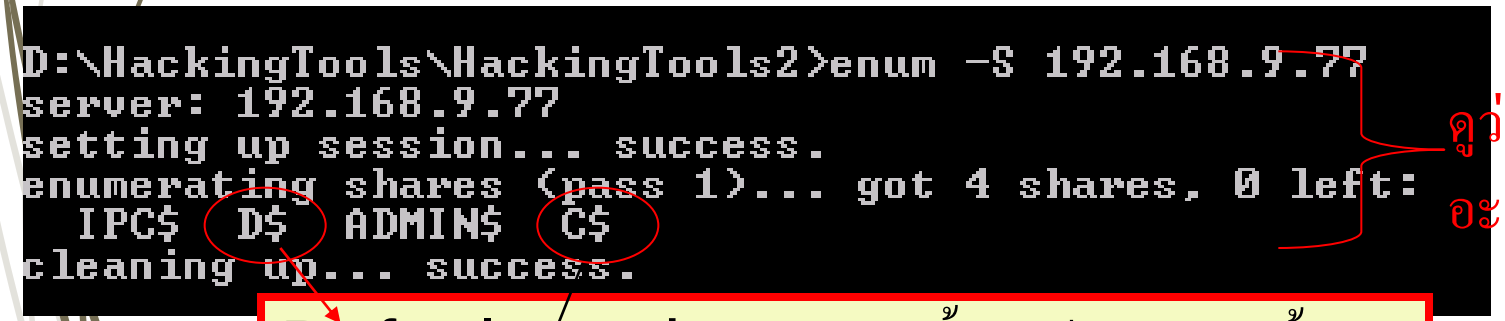
- เมื่อมีการติด เครื่องเหยื่อ จะถูกเปิดช่อง (**Back Door**) เพื่อให้เครื่อง **hacker** สามารถเข้าไป **control** ได้
- โดยพื้นฐานสามารถทำการ **check** ได้ว่าเรามีการเปิด **port** ไหนอยู่บ้างในเครื่องผ่านคำสั่ง

  netstat –a

```
C:\Documents and Settings\Administrator>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    SERVER01:epmap         SERVER01:0             LISTENING
  TCP    SERVER01:microsoft-ds  SERVER01:0             LISTENING
  TCP    SERVER01:912           SERVER01:0             LISTENING
  TCP    SERVER01:1025          SERVER01:0             LISTENING
  TCP    SERVER01:1026          SERVER01:0             LISTENING
  TCP    SERVER01:netbios-ssn   SERVER01:0             LISTENING
  TCP    SERVER01:netbios-ssn   SERVER01:0             LISTENING
  TCP    SERVER01:netbios-ssn   SERVER09:2332          TIME_WAIT
  TCP    SERVER01:netbios-ssn   SERVER5:1037           ESTABLISHED
  TCP    SERVER01:netbios-ssn   SERVER14:2141          ESTABLISHED
  TCP    SERVER01:microsoft-ds  SERVER06:1557          ESTABLISHED
  TCP    SERVER01:microsoft-ds  SERVER07:1272          ESTABLISHED
  TCP    SERVER01:microsoft-ds  SERVER08:1102          ESTABLISHED
  TCP    SERVER01:netbios-ssn   SERVER01:0             LISTENING
  UDP    SERVER01:microsoft-ds  *:*
```

Exam Enum cont.





Default จะมี share พวกนี้อยู่ให้ทำการปิดทิ้งซะ

www.virustotal.com

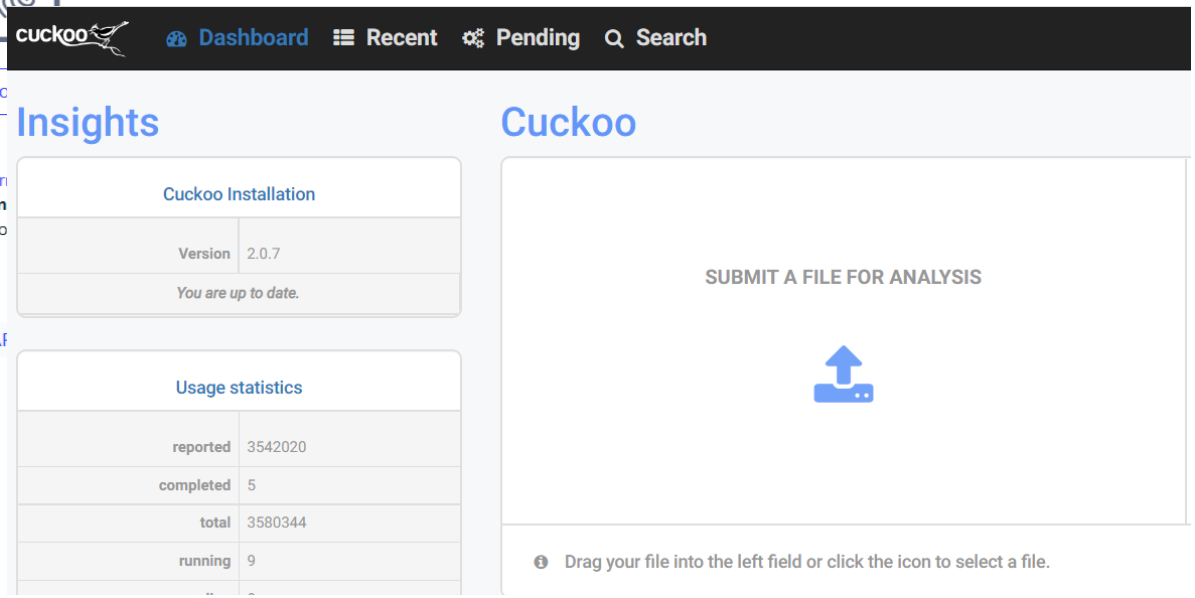
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE | URL | SEARCH

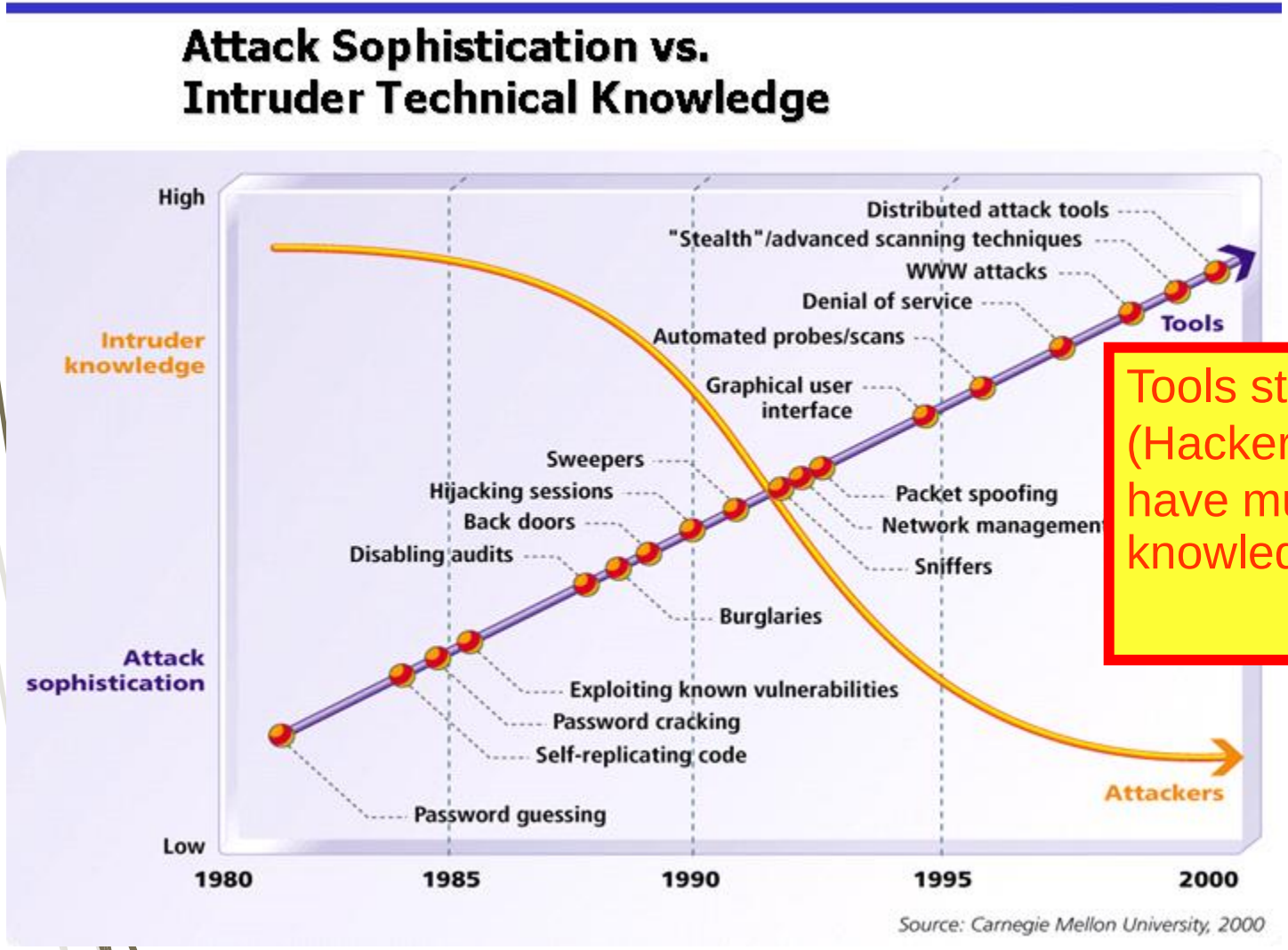
Choc

By submitting data above, you are agreeing to our Ter
your Sample submission with the security comm
VirusTotal is not responsible for the co

ⓘ Want to automate submissions? Check our AP



Trend of Hacker and Tools



Tools still improve.. (Hacker no need to have much more knowledge)

Chapter 4

Information Security Service

Sample

- ISO/IEC 27001 and BCM (Business Continuity Management) are booming in Public Sector (and Private sector also) because of "Government Requirement" and "Regulator Requirement"
  - ISO/IEC 27001 will be "Law Requirement (ETA M. 25)" Well-known IT Security Certification for Thailand IT professional
- ITIL V4 and ISO/IEC 27000 are upcoming trend.
- Over 10 Organizations in Thailand had been certified ISO/IEC 27001

Today Trend : “GRC”

About GRC

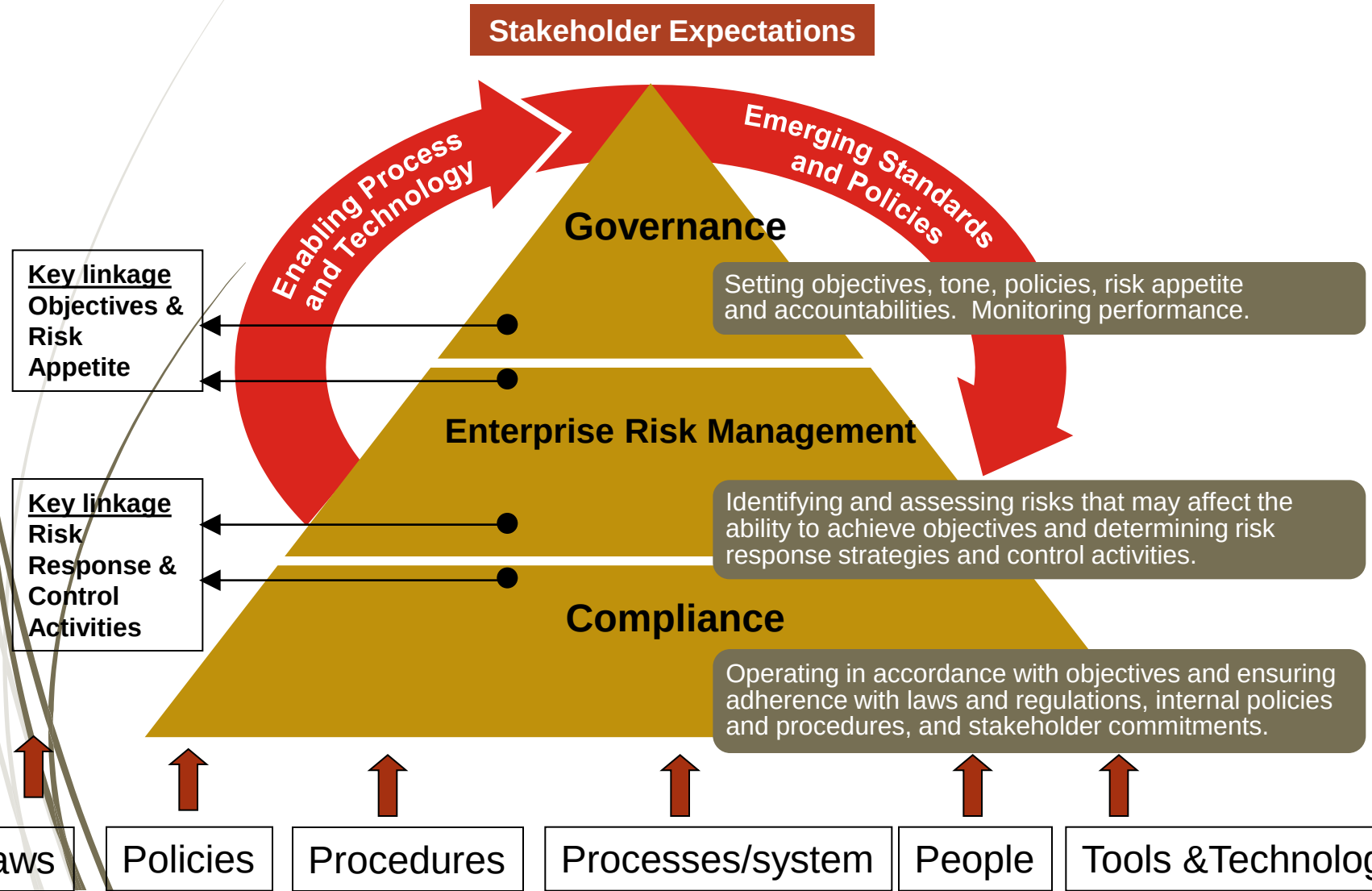
- แนวคิด “GRC”
  - **ทำให้องค์กรแสดงถึงความเป็น “Good Governance”**
  - **ทำให้องค์กรเกิดความสามารถในการแข่งขัน (Competitive Advantage) ในระยะยาว**
  - **เสริมภาพลักษณ์ที่ดีให้กับองค์กร ตลอดจนคณะผู้บริหารระดับสูง**
  - **สร้างจิตสำนึกในการปฏิบัติงานที่ดีให้กับพนักงานทุกคน**
  - **ส่งผลให้ลูกค้าเกิดความเชื่อถือ และมีความมั่นใจในการใช้บริการต่าง ๆ ขององค์กร**

About GRC

- เป็นทิศทางใหม่สำหรับผู้บริหารระดับสูงขององค์กร
  - **ไม่จำกัดเฉพาะผู้บริหารระบบสารสนเทศ หรือ CIO เท่านั้น**
  - **เป็นทิศทางของผู้บริหารในระดับ *C Level* ทั้งหมด จำเป็นต้องร่วมแรงร่วมใจกันในการผลักดันแนวคิด “GRC” ให้เป็นผลงานในเชิงปฏิบัติ**
- ภาวะผู้นำ หรือ “Leadership” เป็นปัจจัยสำคัญ
  - **งบประมาณ**
  - **ต้องมีบุคลากรที่ได้รับมอบหมายให้ทำตามแนวคิด “GRC” โดยเฉพาะ**
  - **ควรจัดจ้างที่ปรึกษา หรือผู้เชี่ยวชาญเฉพาะเพื่อให้คำแนะนำ และให้แนวทางปฏิบัติจาก Standard และ Best Practice ต่างๆ ได้อย่างถูกต้อง**

An Integrated Approach To Governance, Risk & Compliance

Source: A New Strategy for Success Through Integrated Governance, Risk and Compliance Management PWC white paper



GRC related best practices and compliance

SOX

ISO/IEC 38500

GLBA

HIPAA

ITSM

ISO/IEC 27001,27002

ITAF/GTAG

PCI DSS

Basel II

Corporate Governance

IT Governance

ISO 22301 (BCM)

ITIL & ISO/IEC 20000

ISO/IEC 27005,27006

CobiT 5

COSO (ERM)

CCA/ETA

Best Practices by using COBIT 5

isaca.org/resources/cobit/cobit-5

ISACA

Search

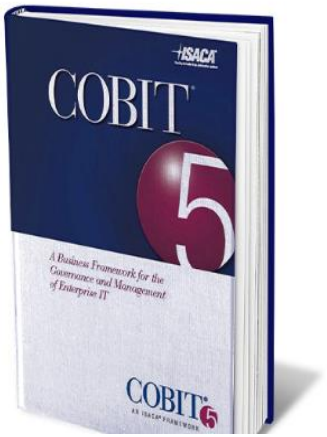
JOIN ABOUT US CAREERS SUPPORT STORE SIGN IN

CREDENTIALING MEMBERSHIP ENTERPRISE PARTNERSHIPS TRAINING & EVENTS RESOURCES

Home / Resources / COBIT / COBIT 5

COBIT 5 Publications

The Power of COBIT 5 is in its Breadth of Tools, Resources and Guidance. The value of COBIT 5 is in how it applies to your profession.



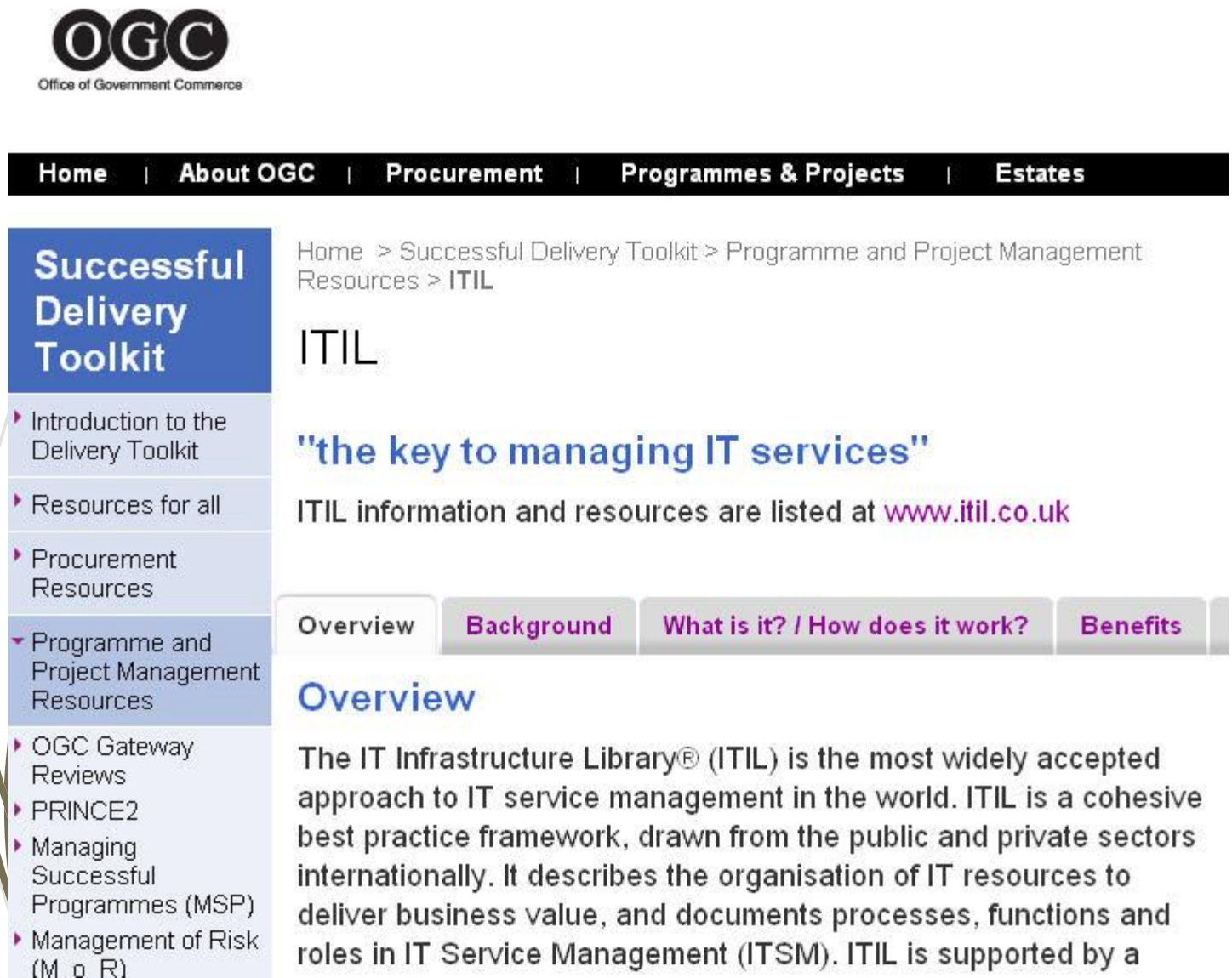
Featured COBIT 5

COBIT 5 Framework

COBIT 5 is the overarching business and management framework for governance and management of enterprise IT. This volume documents the 5 principles of COBIT 5 and defines the 7 supporting enablers.

LEARN MORE

Best Practices by using ITIL version 4



Best Practices by using PMP

Types of information security services

- They are 4 types of security services:

C – Confidentiality

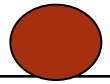
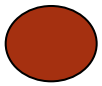
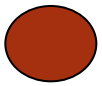
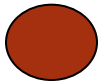
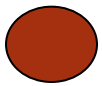
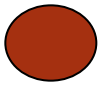
I – Integrity

A – Availability

A – Accountability

A – Authentication & Authorization

Overview of CIAA

	Access	Modify	DOS	Repudiation
Confidentiality				
Integrity				
Availability				
Accountability				

How to Implement Confidentiality

- EFS
- Hashing
- PKI, CA
- PGP > Pretty Good Privacy > S/MIME
- Steganography
- Access Control
- Data Classification

Etc..

What Is a Data Recovery Agent?

- A data recovery agent is a user account that can decrypt files that have been encrypted by other users

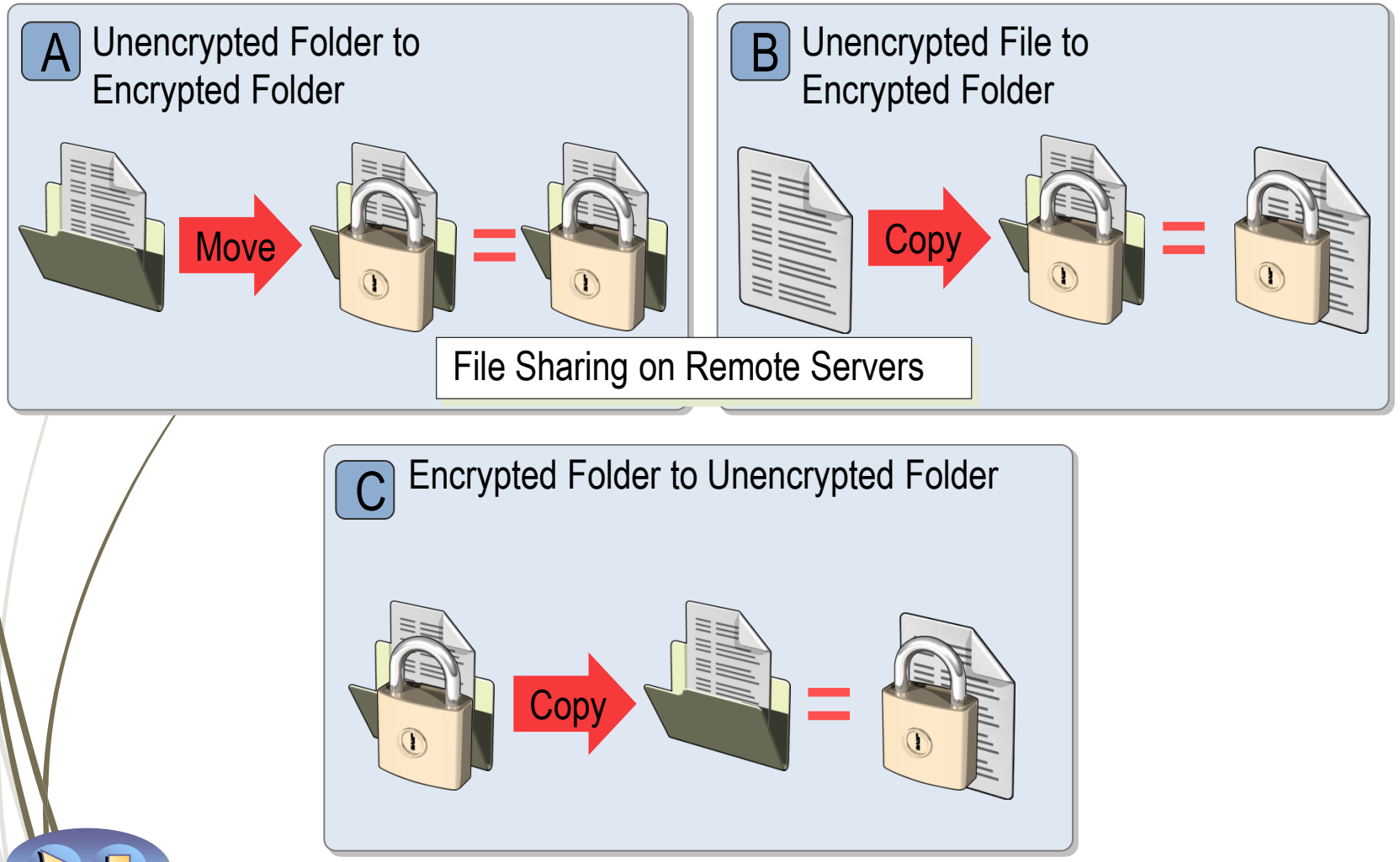
To implement a DRA on a stand-alone computer:

1. Use the cipher tool to create a DRA certificate and key pair
2. Add the user account as a DRA
3. To decrypt files, add the DRA certificate to the local certificate store

Best Practices for Implementing EFS in a Stand-Alone Environment

- Use as few DRAs as feasible and ensure that DRAs are highly trusted
- Implement a DRA for stand-alone computer.
- Delete the DRA private key after creation and after each use
- Configure encryption at the folder level to ensure that all contents are encrypted
- Overwrite de-allocated clusters by using the Cipher.exe program

Effects of Moving or Copying Encrypted Files Between Locations

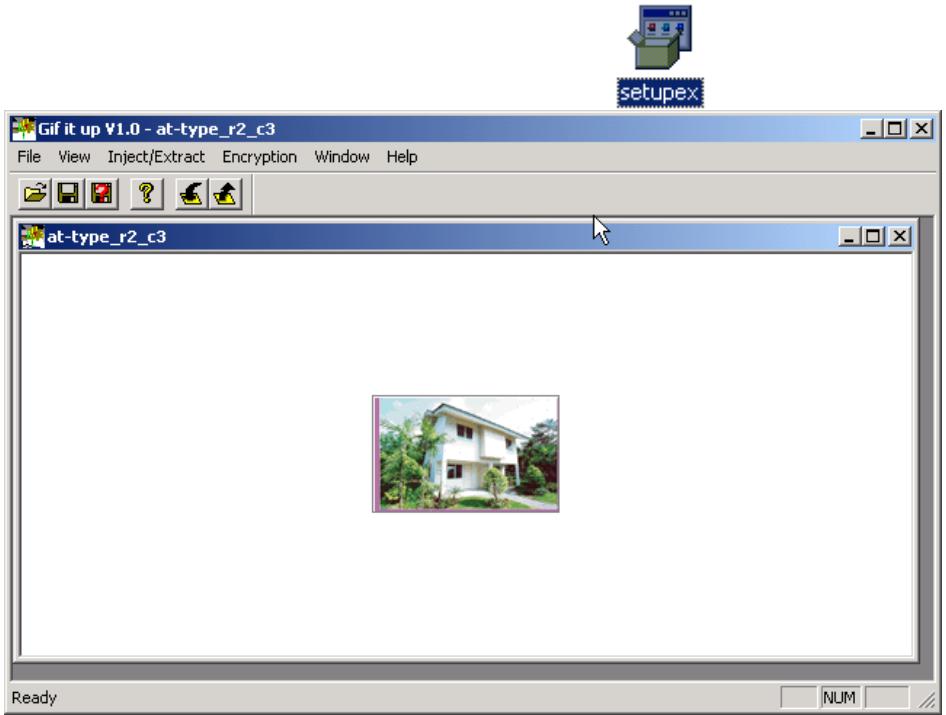


Gift it Up

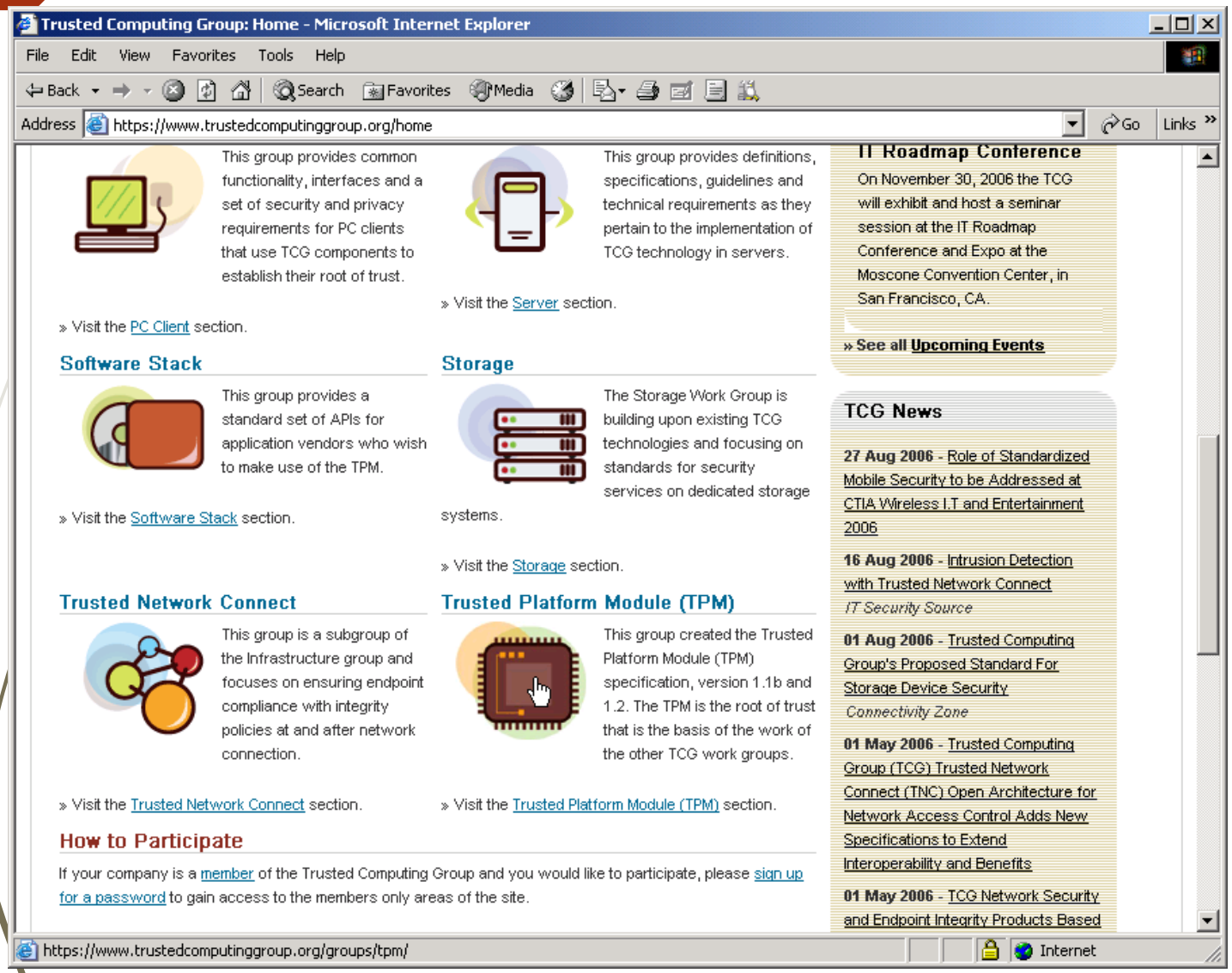
- Steganography is the art and science of writing hidden messages in such a way that

  Need to setup

- Steganography Tools



Trusted Platform Module

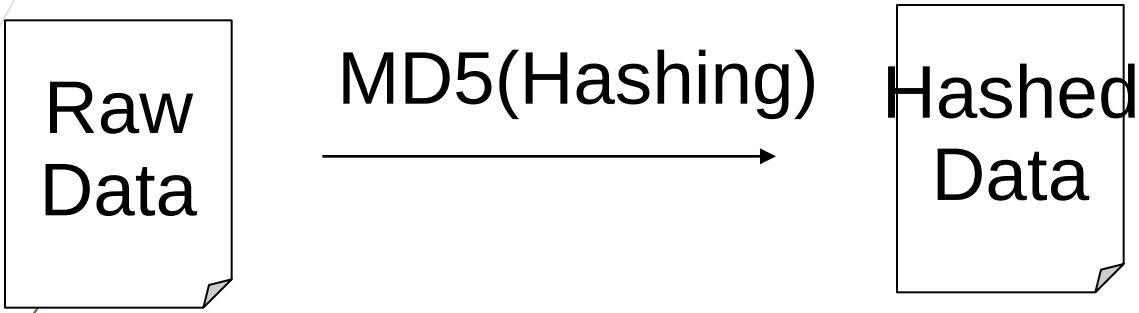


How to Implement Integrity

- **Hash**
- **Digital Signature**

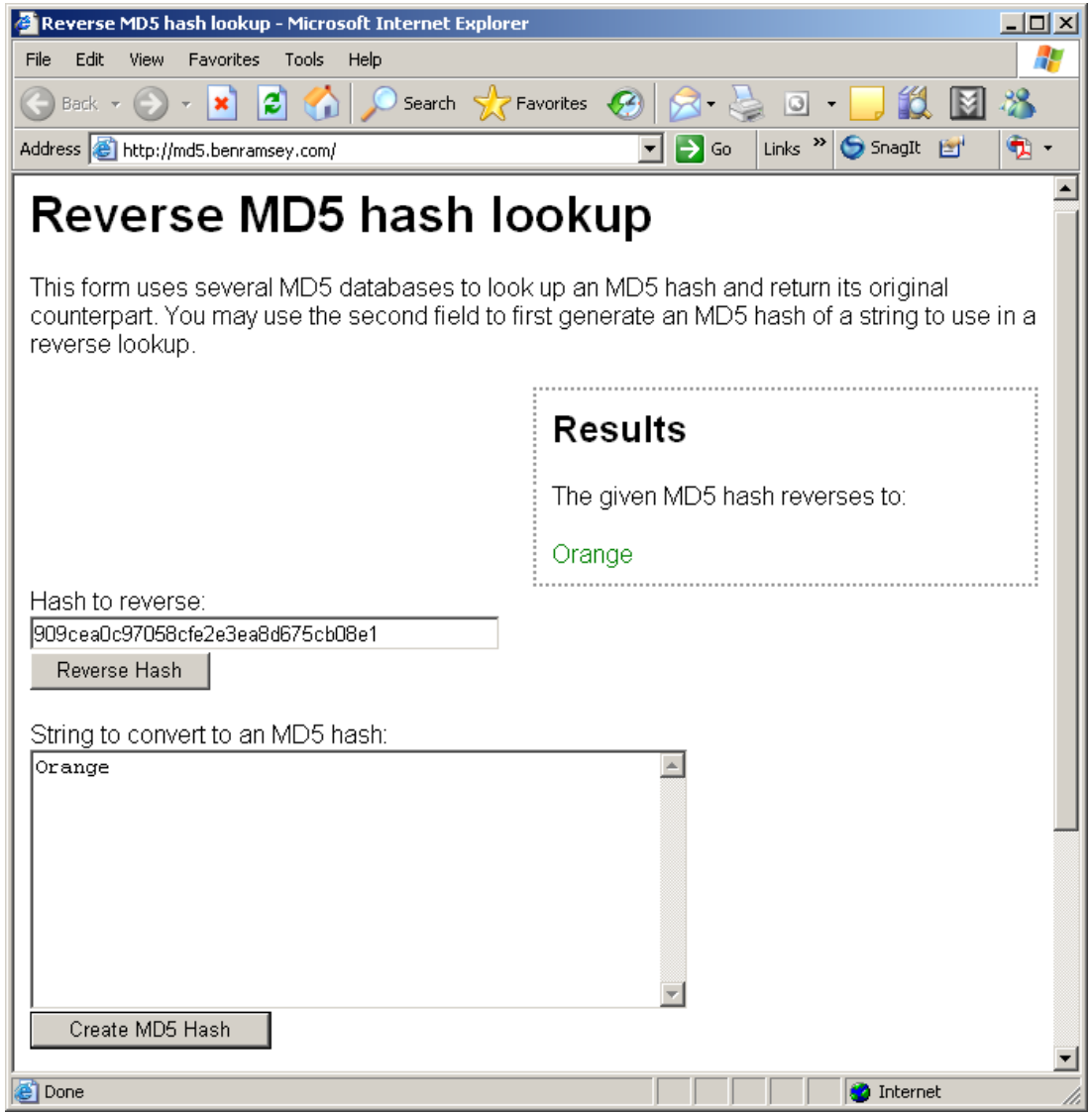
Etc…

MD5 REVERSE

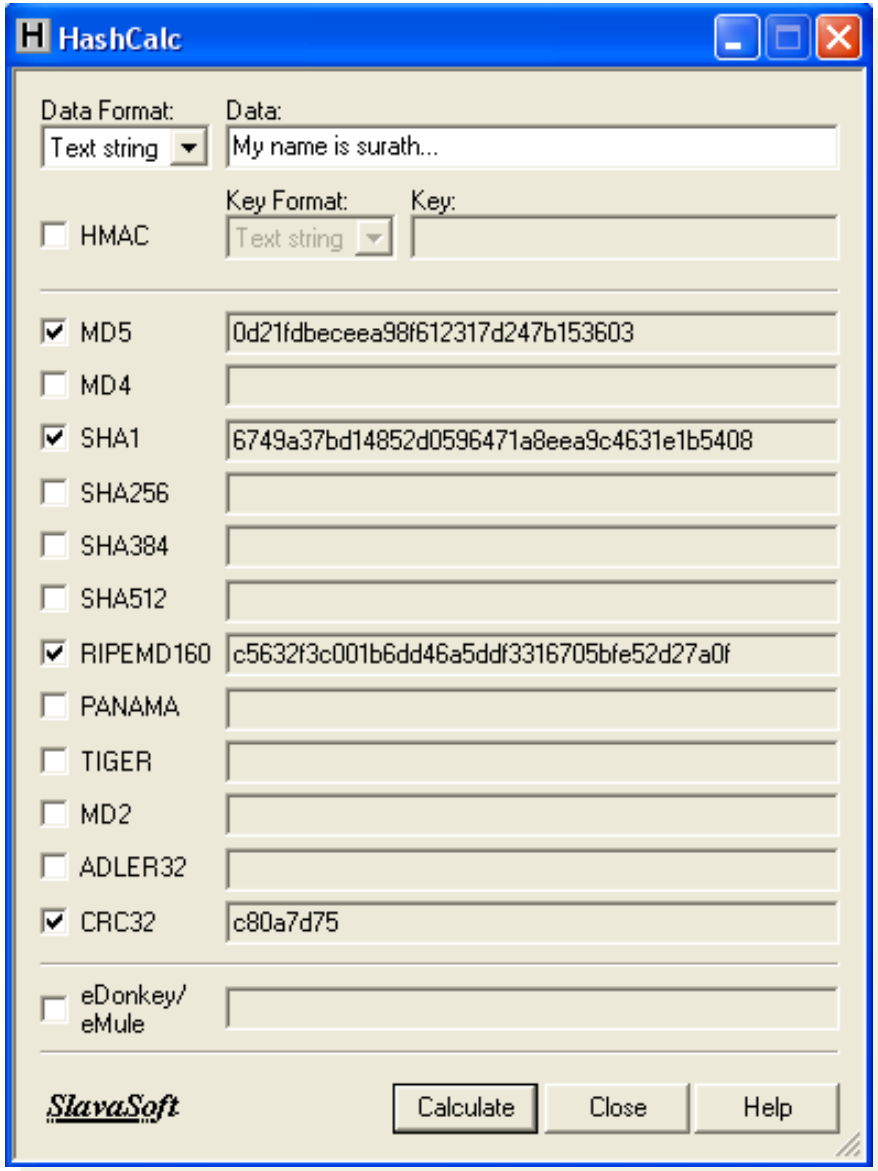


- Concept

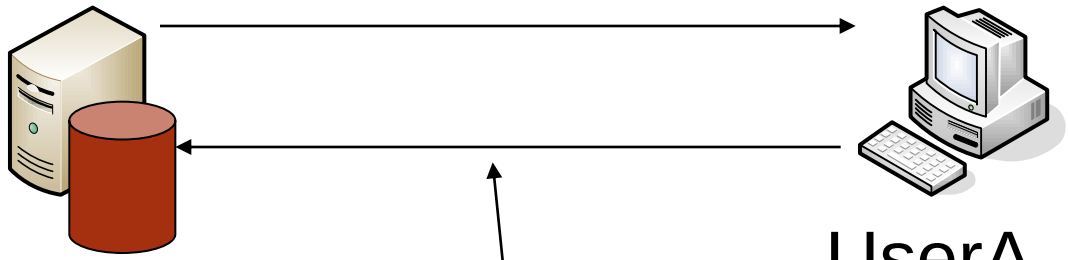
MD5 Reverse by Web



Hash Calculator



Password Authentication Protocol (PAP)



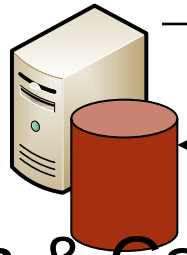
Challenge Handshake Authentication Protocol (CHAP)

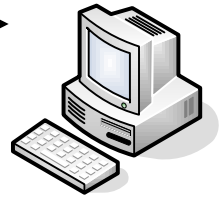
8. Response

4. UserA+PasswordA
> Hashing-C

3. Check challenge

2. Check





1. UserA

UserA
PasswordA

6. Search & Calc
Hashing-S

7. Hashing-C=Hashing-S

Hashing -C

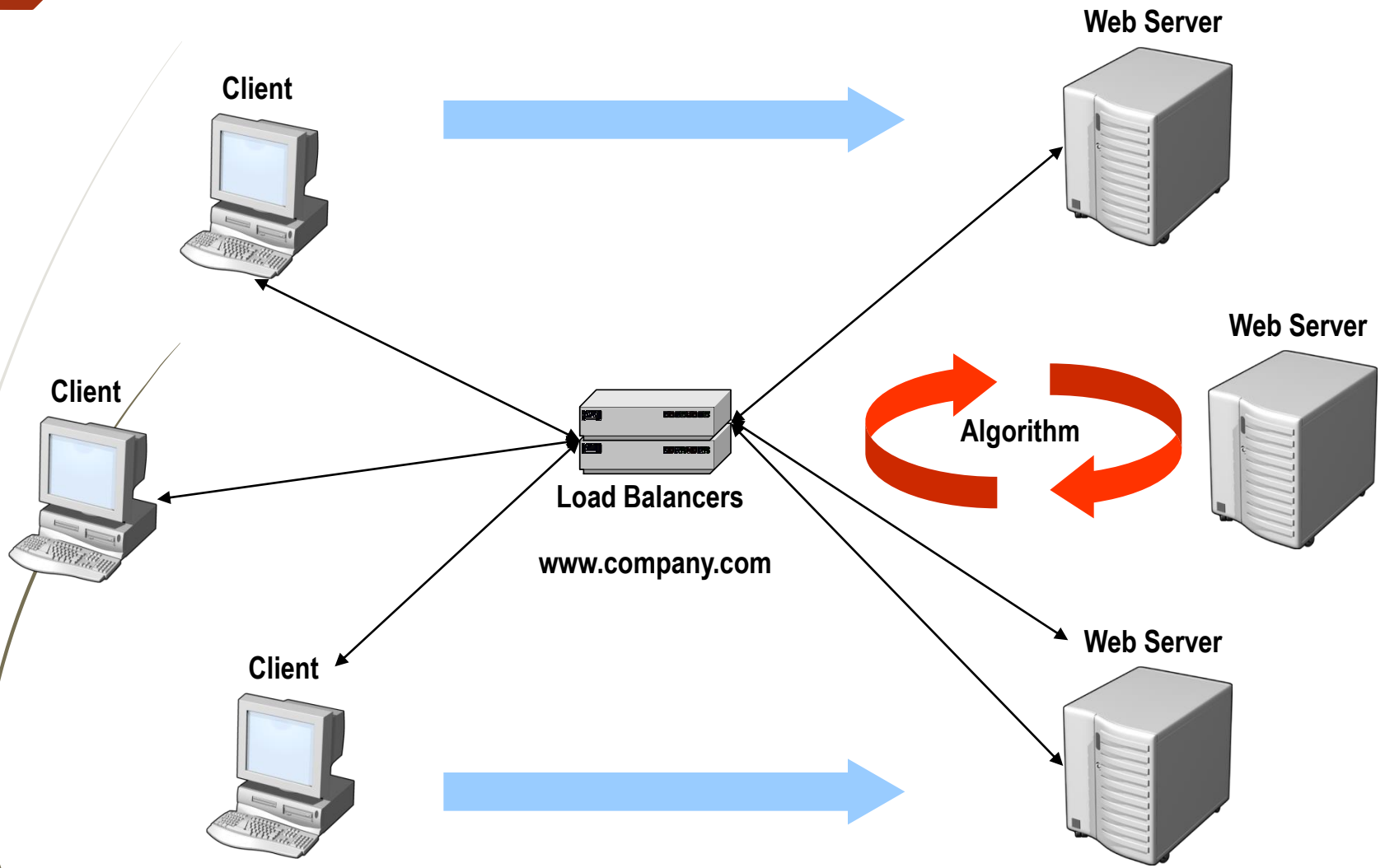
MSCHAP1 > Winnuke 98 > MSCHAP2 (Mutual)

How to Implement Availability

- Backup
- Network Load Balancing > NLB
- Cluster
- Access List

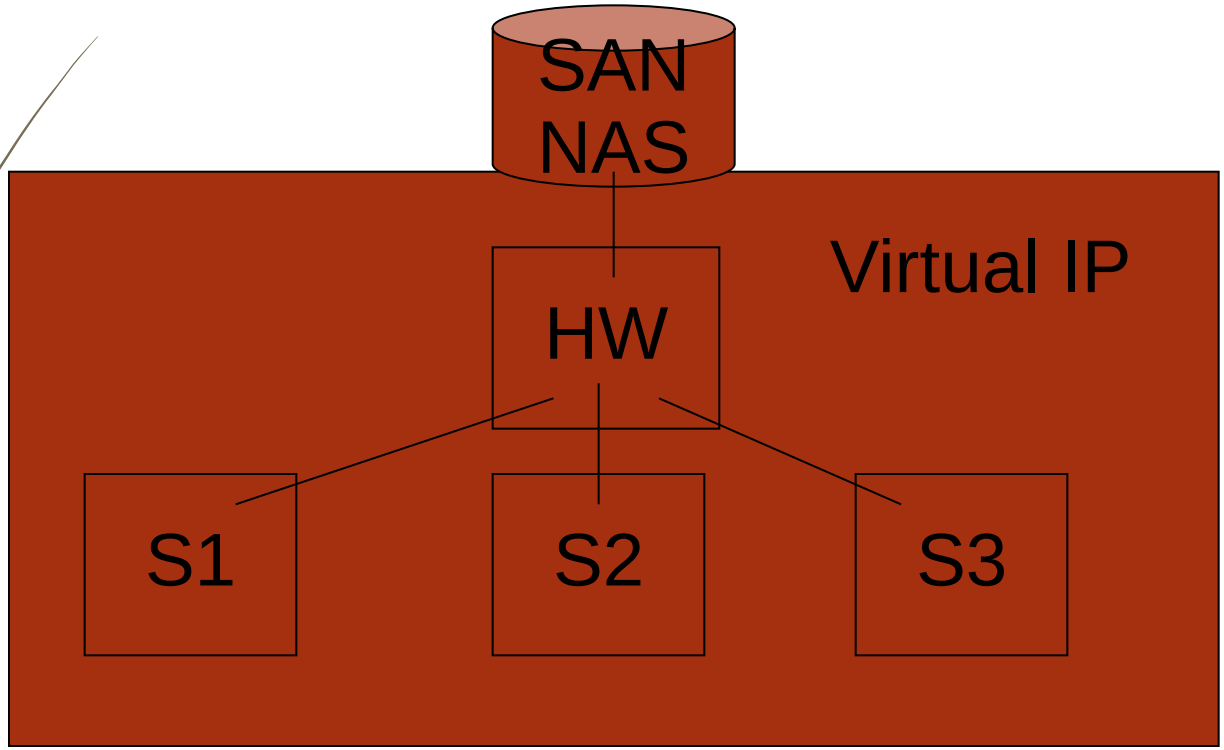
Etc...

Network Load Balancing



Cluster

- จุดประสงค์ คือ การนำเครื่องมากกว่า **1** เครื่องมาช่วยกันทำงาน ซึ่ง ต้องมี **Hardware** ที่ **support** ด้วย **>** ราคาแพง



How to Implement Accountability

- **Login**
  - **Secure ID, Token**
  - **Kerberos**
  - **Radius**
  - **Biometric**
  - **Card**

Etc…

แนวคิดความปลอดภัย

ส่วนประกอบความปลอดภัย	วิธีการดำเนินการ
People	จัดอบรมและกำหนดบทลงโทษ
Process	การทำแผน Information Security
Technique	จัดซื้ออุปกรณ์และเครื่องมือ

Website ที่เกี่ยวข้องกับ Information Security

- http://csrc.nist.gov
- http://www.cisa.gov
- http://www.sans.org
- http://www.securityfocus.com
- http://www.securiteam.com
- http://www.cisecurity.org
- http://www.owasp.org > Secure Coding

- http://www.isc2.org (CISSP > Security Admin)
- http://www.isaca.org (Cobit >CISA > audit IT)

OWASP Website

OWASP

PROJECTS CHAPTERS EVENTS ABOUT

Search OWASP.org

Store | Donate | Join

Who is the OWASP® Foundation?

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

For nearly two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. Donate, Join, or become a Corporate Member today.

Project Spotlight: OWASP Top 10

We are back again with yet another OWASP Spotlight series and this time we have a project which needs no introduction and I got the chance to interact with Andrew

OWASP 2022 Global AppSec APAC Virtual Event

Registration Open!

Join us virtually August 29 - September 1, for

Chapter 5

กฎหมายกับ INFORMATION SECURITY

Computer crime Law in Thailand

กฎหมายไทยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

- ธรรมเนียมทางอิเล็กทรอนิกส์
- ลายมือชื่ออิเล็กทรอนิกส์
- การโอนเงินทางอิเล็กทรอนิกส์
- การคุ้มครองข้อมูลส่วนบุคคล
- การกระทำผิดเกี่ยวกับคอมพิวเตอร์
- การพัฒนาโครงสร้างพื้นฐานสารสนเทศ

ตารางแสดงความหมายของสัญลักษณ์

สัญลักษณ์	ความหมาย
	ระดับ 1 คือ ระดับความมั่นคงปลอดภัยพื้นฐาน
	ระดับ 2 คือ ระดับความมั่นคงปลอดภัยปานกลาง
	ระดับ 3 คือ ระดับความมั่นคงปลอดภัยสูง
	มาตรการด้านการป้องกัน (preventive)
	มาตรการด้านการตรวจสอบ (detective)
	มาตรการด้านการแก้ไข (corrective)
	มาตรการที่เกี่ยวข้องกับบุคลากร (people)
	มาตรการที่เกี่ยวข้องกับกระบวนการ (process)
	มาตรการที่เกี่ยวข้องกับเทคโนโลยี (technology)

ตัวอย่างองค์กรที่มีความคาบเกี่ยวกับโครงสร้างพื้นฐานที่สำคัญของประเทศไทยและควรจัดจัดทำมาตรฐานนี้ในระดับความมั่นคงปลอดภัยสูงสุด (ระดับ 3)

สำหรับองค์กรที่มีความเกี่ยวข้องกับโครงสร้างพื้นฐานของประเทศนั้นจัดว่าเป็นองค์กรที่มีความเสี่ยงสูง จึงต้องเร่งดำเนินการจนถึงระดับความมั่นคงปลอดภัยสูงสุดแต่เนื่องจากบางองค์กรอาจไม่ได้จัดสรรงบประมาณในส่วนนี้ไว้ จึงสามารถเริ่มต้นดำเนินงานเฉพาะบางส่วนของระบบทั้งหมดที่มีอยู่ให้เข้ามาตรฐานปลอดภัยสูงสุดก่อน การดำเนินการบางระบบ เช่น ระบบประมวลผลหลัก ระบบที่เกี่ยวข้องกับการเงิน เป็นต้น ตัวอย่างองค์กรเหล่านั้น ได้แก่

1. กลุ่มไฟฟ้าและพลังงาน ประกอบด้วย
   - การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย
   - การไฟฟ้านครหลวง
   - การไฟฟ้าส่วนภูมิภาค
   - บริษัท ปตท. จำกัด (มหาชน)
   - กรมพัฒนาและส่งเสริมพลังงาน
   - เป็นต้น

2 . กลุ่มการเงิน การธนาคารและการประกันภัย

กระทรวงการคลัง
ธนาคารแห่งประเทศไทย
ตลาดหลักทรัพย์แห่งประเทศไทย
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
กรมการประกันภัย
สมาคมประกันชีวิตไทย
สมาคมประกันวินาศภัย
ธนาคาร
บริษัทหลักทรัพย์ต่างๆ
เป็นต้น

3. กลุ่มการสื่อสาร โทรคมนาคมและขนส่ง

บริษัท การบินไทย (มหาชน) จำกัด
บริษัท ทศท คอร์ปปอเรชั่น จำกัด (มหาชน)
บริษัท กสท คอร์ปปอเรชั่น จำกัด (มหาชน)
บริษัทวิทยุการบินแห่งประเทศไทย
การท่าอากาศยานแห่งประเทศไทย
การรถไฟแห่งประเทศไทย
กรมการบินพาณิชย์
การท่าเรือแห่งประเทศไทย
กระทรวงคมมนาคม
กรมอุตุนิยมวิทยา
เป็นต้น

4. กลุ่มความสงบสุขของสังคม

กระทรวงศึกษาธิการ
กระทรวงสาธาณสุข
กรุงเทพมหานคร
กระทรวงกลาโหม
สำนักงานตำรวจแห่งชาติ
กระทรวงเกษตรและสหกรณ์
การประปานครหลวง
การประปาส่วนภูมิภาค
เป็นต้น

Thailand ICT Related Law Latest Update

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

Computer Crime Law

เจตนารมณ์ของร่างกฎหมาย

เพื่อกำหนด.....

- ฐานความผิดและบทลงโทษ
- อำนาจหน้าที่ของพนักงานเจ้าหน้าที่
- หน้าที่ของผู้ให้บริการ

การกระทำความผิดซึ่งกระทบต่อหลักพื้นฐานด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security)

หลัก C.I.A

- **Confidentiality ความลับ**
- **Integrity ความครบถ้วน**
- **Availability สภาพพร้อมใช้งาน**

หมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์

ฐานความผิดและบทลงโทษสำหรับการกระทำโดยมิชอบ	
มาตรา ๕	การเข้าถึงระบบคอมพิวเตอร์
มาตรา ๖	การล่วงรู้มาตรการป้องกันการเข้าถึง
มาตรา ๗	การเข้าถึงข้อมูลคอมพิวเตอร์
มาตรา ๘	การดักข้อมูลคอมพิวเตอร์โดยมิชอบ
มาตรา ๙	การแก้ไข เปลี่ยนแปลง ข้อมูลคอมพิวเตอร์
มาตรา ๑๐	การรบกวน ขัดขวาง ระบบคอมพิวเตอร์
มาตรา ๑๑	สแปมเมล์ (Spam Mail)
มาตรา ๑๒	การกระทำความผิดต่อ ประชาชนโดยทั่วไป / ความมั่นคง
มาตรา ๑๓	การจำหน่าย/เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด
มาตรา ๑๔	นำเข้า ปลอม/ เท็จ /ภัยมั่นคง /ลามก/ ส่งต่อ ข้อมูลคอมพิวเตอร์
มาตรา ๑๕	ความรับผิดของผู้ให้บริการ
มาตรา ๑๖	การเผยแพร่ภาพ ตัดต่อ/ดัดแปลง
รวม ๑๒ มาตรา	

หมวดที่ ๒ พนักงานเจ้าหน้าที่

กำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่และหน้าที่ของผู้ให้บริการ	
มาตรา ๑๘	อำนาจของพนักงานเจ้าหน้าที่
มาตรา ๑๙	ข้อจำกัด/การตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่
มาตรา ๒๐	การใช้อำนาจในการ block เว็บไซต์ที่มีเนื้อหากระทบต่อความมั่นคงหรือขัดต่อความสงบเรียบร้อย
มาตรา ๒๑	การเผยแพร่/จำหน่ายชุดคำสั่งไม่พึงประสงค์
มาตรา ๒๒	ห้ามมิให้พนักงานเผยแพร่ข้อมูลที่ได้มาตามมาตรา ๑๘
มาตรา ๒๓	พนักงานเจ้าหน้าที่ประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูล
มาตรา ๒๔	ความรับผิดของผู้ล่วงรู้ข้อมูลที่พนักงาน เจ้าหน้าที่ได้มาตามมาตรา ๑๘
มาตรา ๒๕	ห้ามมิให้รับฟังพยานหลักฐานที่ได้มาโดยมิชอบ
มาตรา ๒๖ ถึง ๒๗	หน้าที่ผู้ให้บริการในการเก็บข้อมูลจราจรทางคอมพิวเตอร์และความรับผิด หากไม่ปฏิบัติตามหน้าที่
มาตรา ๒๘	การแต่งตั้งพนักงานเจ้าหน้าที่
มาตรา ๒๙	การรับคำร้องทุกข์กล่าวโทษ จับ ควบคุม ค้น & การกำหนดระเบียบ/แนวทางและวิธีปฏิบัติ
มาตรา ๓๐	การปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่
รวมทั้งสิ้น ๑๓ มาตรา	

Chapter 6

POLICY

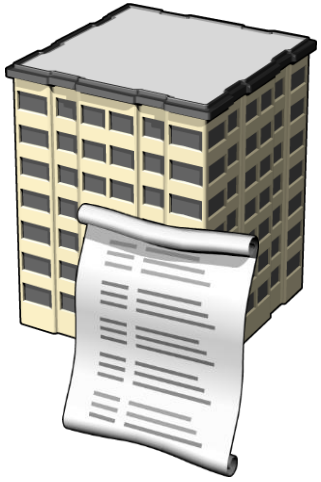
What Are Security Policies?

Security policies:

- **Are documents**
- **Explain how an organization implements security**

Administrative Policies

Technical Policies



Physical Policies

What is a policy ???

- Policy is the most boring job (really can be!)
- Policy is also the most important job for the information security department (IT professional)
- Policy setting takes little technical knowledge (more management)
- Few people like the result of the work ?

Why is policy so important?

- If define what security should be !!
- If puts everyone on the same page (same standard) !!

The Relationship Between Policies and Procedures

Policies describe what must be implemented to secure a network

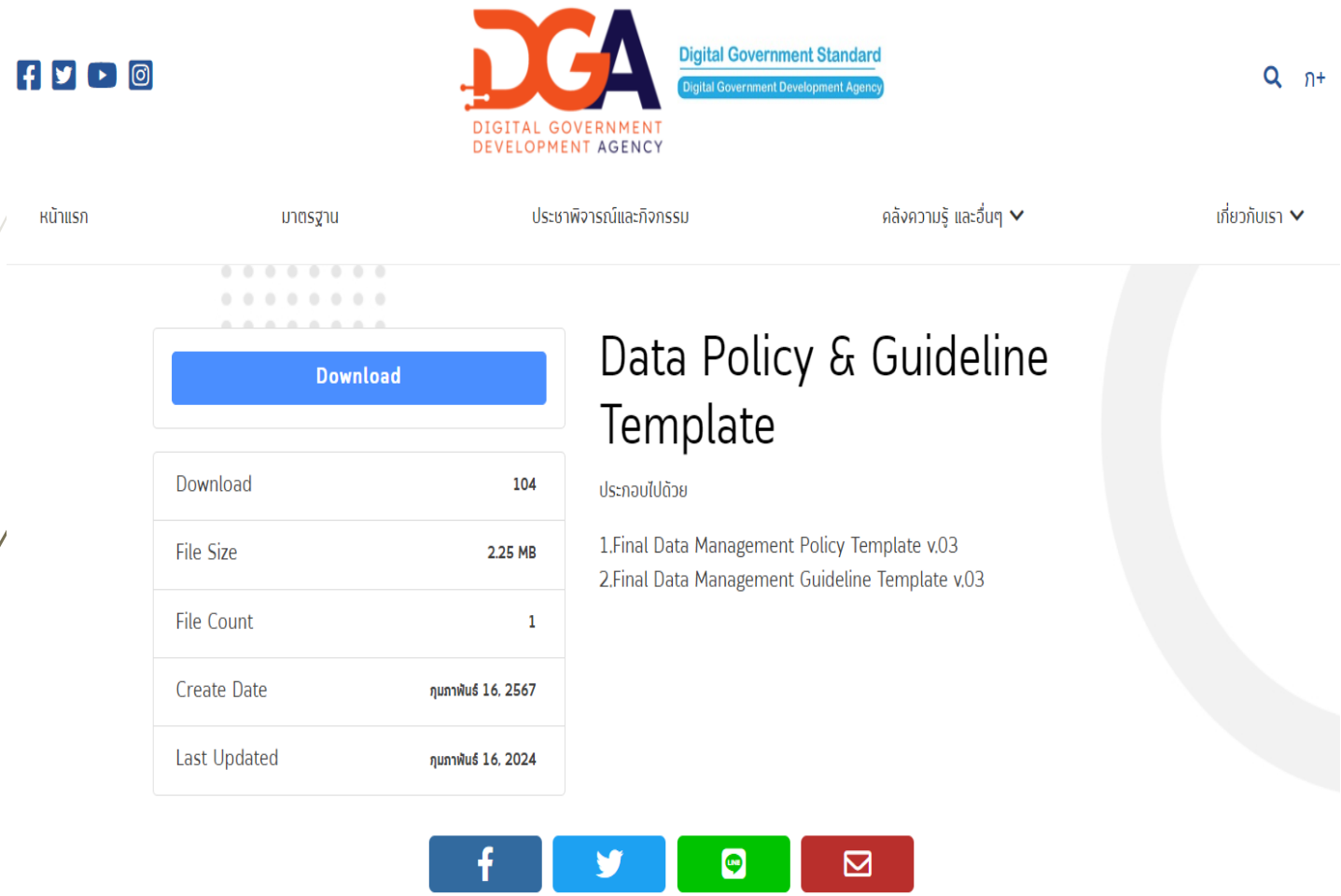
Procedures describe how to implement policies

Define various policies

- Purpose
- Scope
- Responsibility

(These are the 3 section of each policy)

Policy Template



- https://standard.dga.or.th/download/data-policy-guideline-template/

Example Antivirus Policy Template

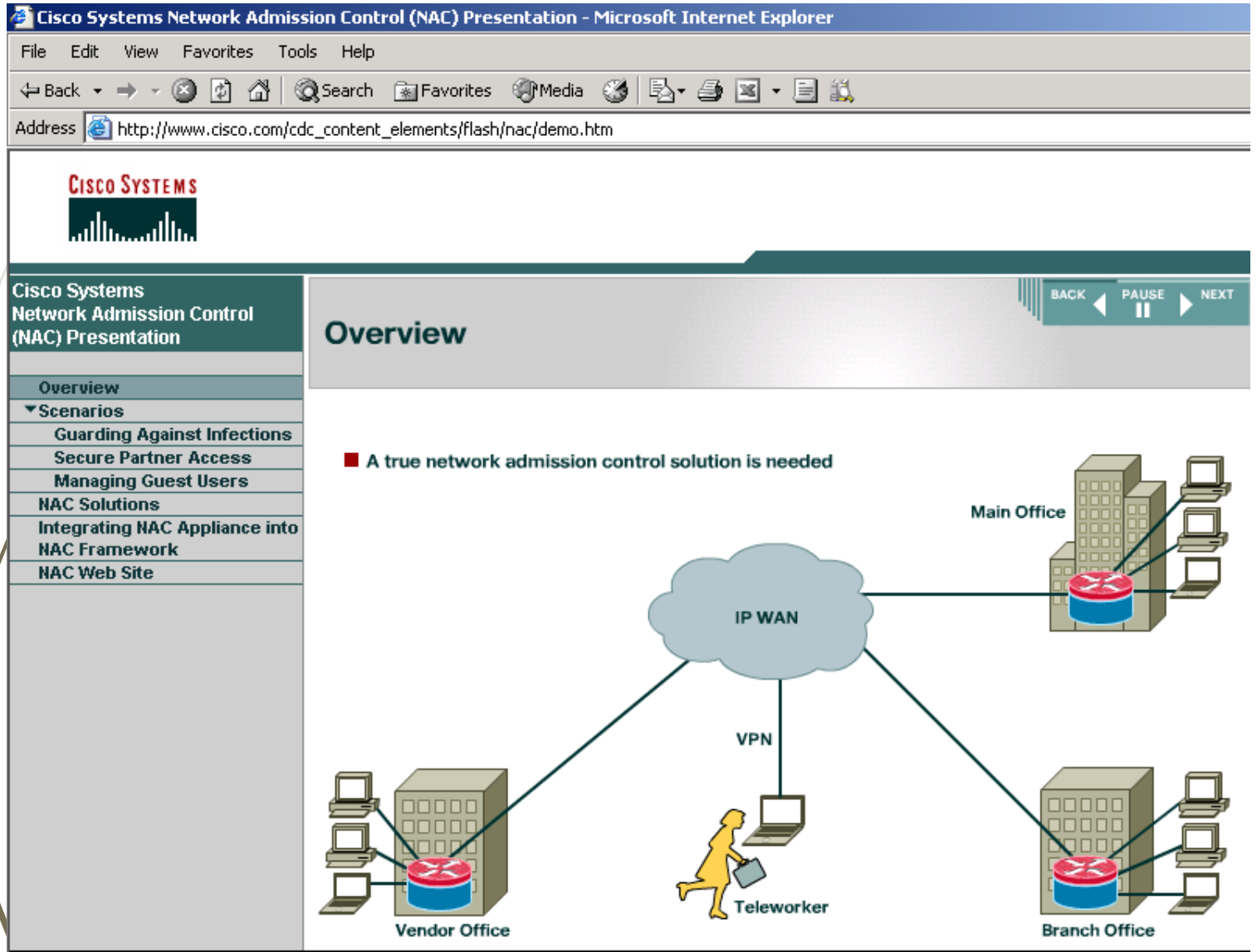
Guidelines on Anti-Virus Process

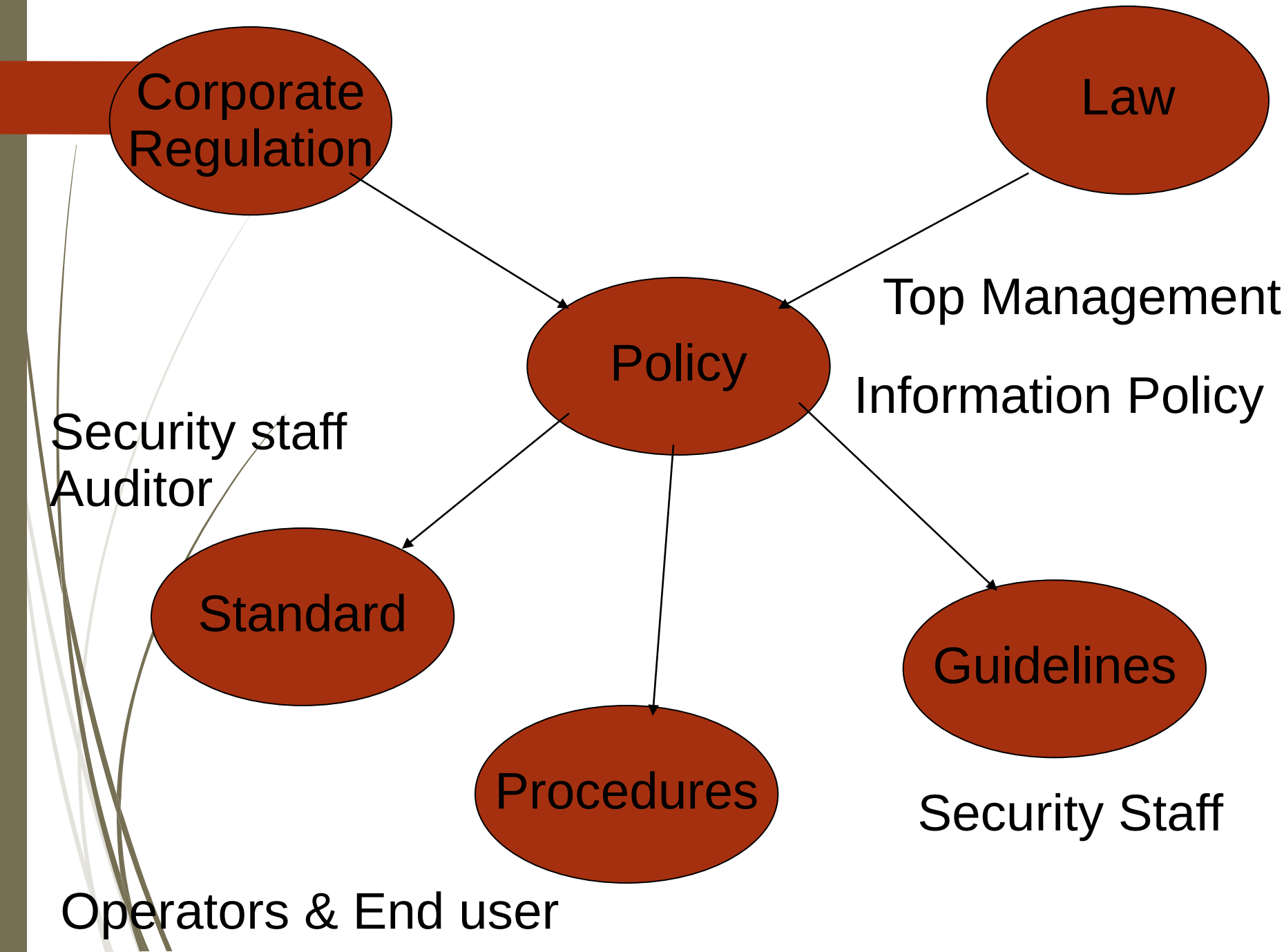
Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

Recommended processes to prevent virus problems:

- Always run the Corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in with <Company Name>'s *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe

Network Admission Control (NAC)




Corporate Regulation
Law
Top Management
Policy
Information Policy
Security staff
Auditor
Standard
Guidelines
Procedures
Security Staff
Operators & End user

Wireless Security

Policy

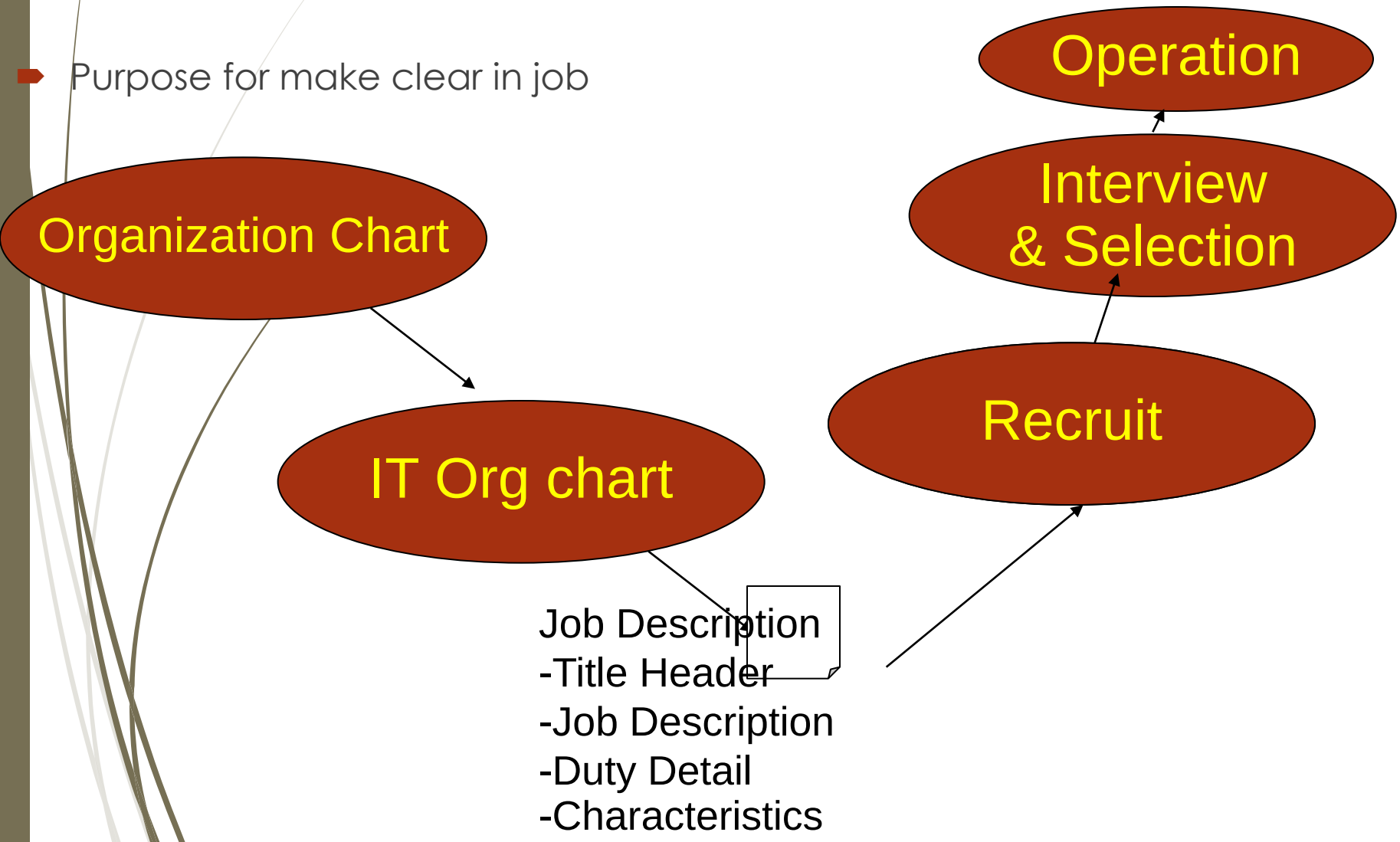
- อุปกรณ์เครือข่ายไร้สายทั้งหมดต้องผ่านความเห็นชอบจากทีมงานบริหารเครือข่าย
- พนักงานทุกคนที่จำเป็นต้องใช้งานในเครือข่ายไร้สายต้องขออนุมัติจากหน่วยหน้าฝ่ายทุกคน
- ห้ามไม่ให้พนักงานใช้เครื่องคอมพิวเตอร์ในเครือข่ายไร้สายในที่สาธารณะ
- ห้ามพนักงานบอกค่าติดตั้งของเครือข่ายไร้สายกับบุคคลภายนอก
- เลือกใช้เทคโนโลยี่ Authentication
- ให้ผู้ใช้ห้ามเปิดเผยรหัสผ่าน และ User account
- ผู้ใช้ต้องกำหนดรหัสผ่านยาวไม่น้อยกว่า 8 ตัวอักษร และสลับซับซ้อน
- รหัสผ่านต่างๆที่ใช้ในการ Authentication ห้ามบันทึกไว้ในที่มองเห็นได้
- ต้องมีการออกแบบเครือข่ายไร้สายแยกจากเครือข่ายที่ต้องการความปลอดภัยสูง

Penalty

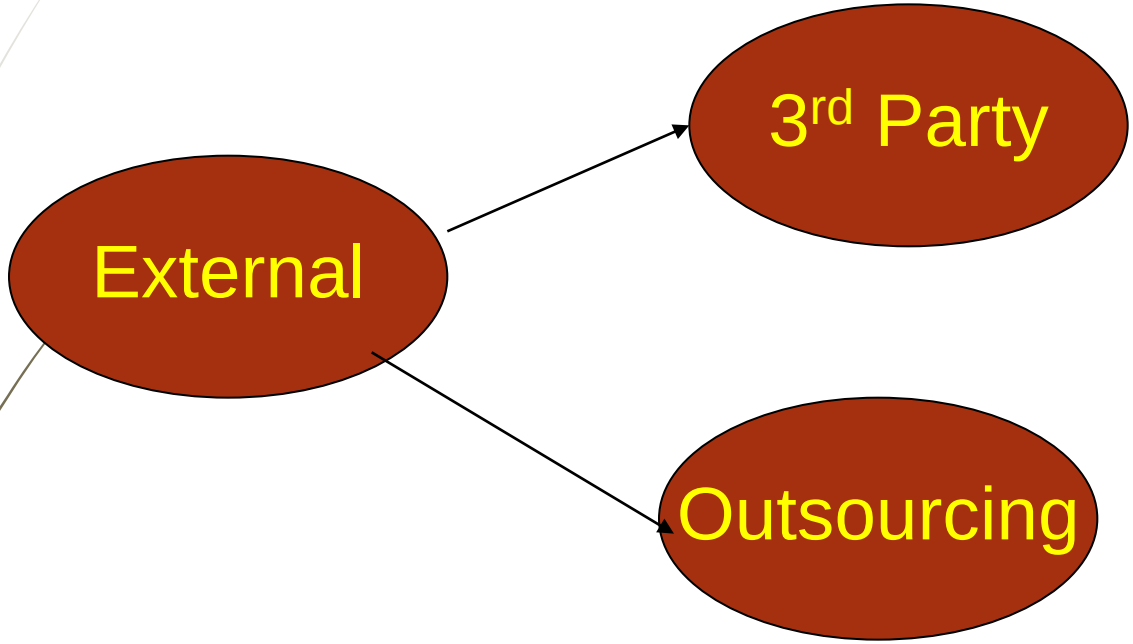
- ผู้ละเมิดนโยบายความปลอดภัยเครือข่ายไร้สายจะถูกระงับการใช้งาน
- กรณีที่มีการละเมิดซ้ำจะพิจารณาตามกฎลงโทษของบริษัทฯ

Segregation of Duties

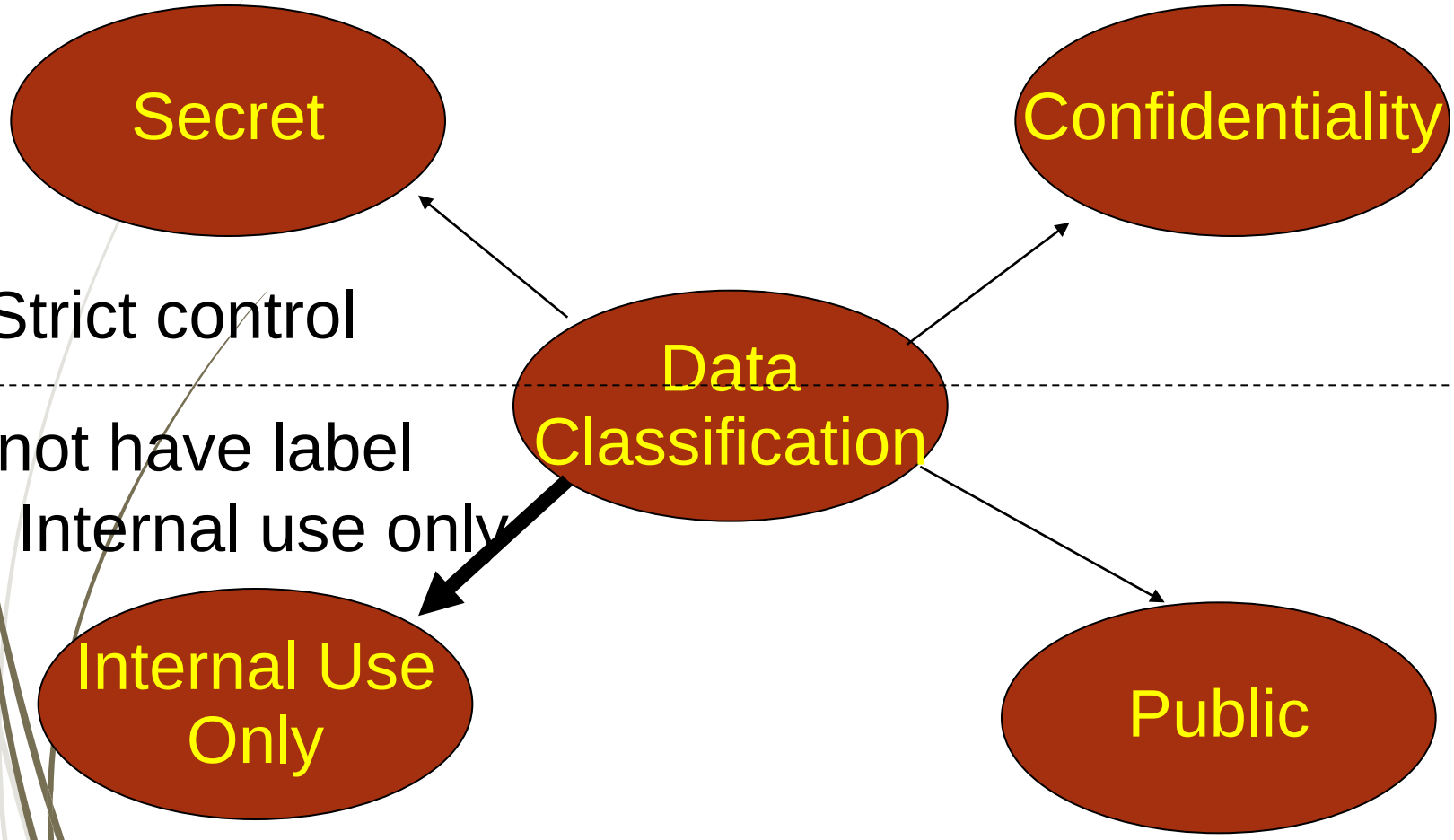
- Purpose for make clear in job



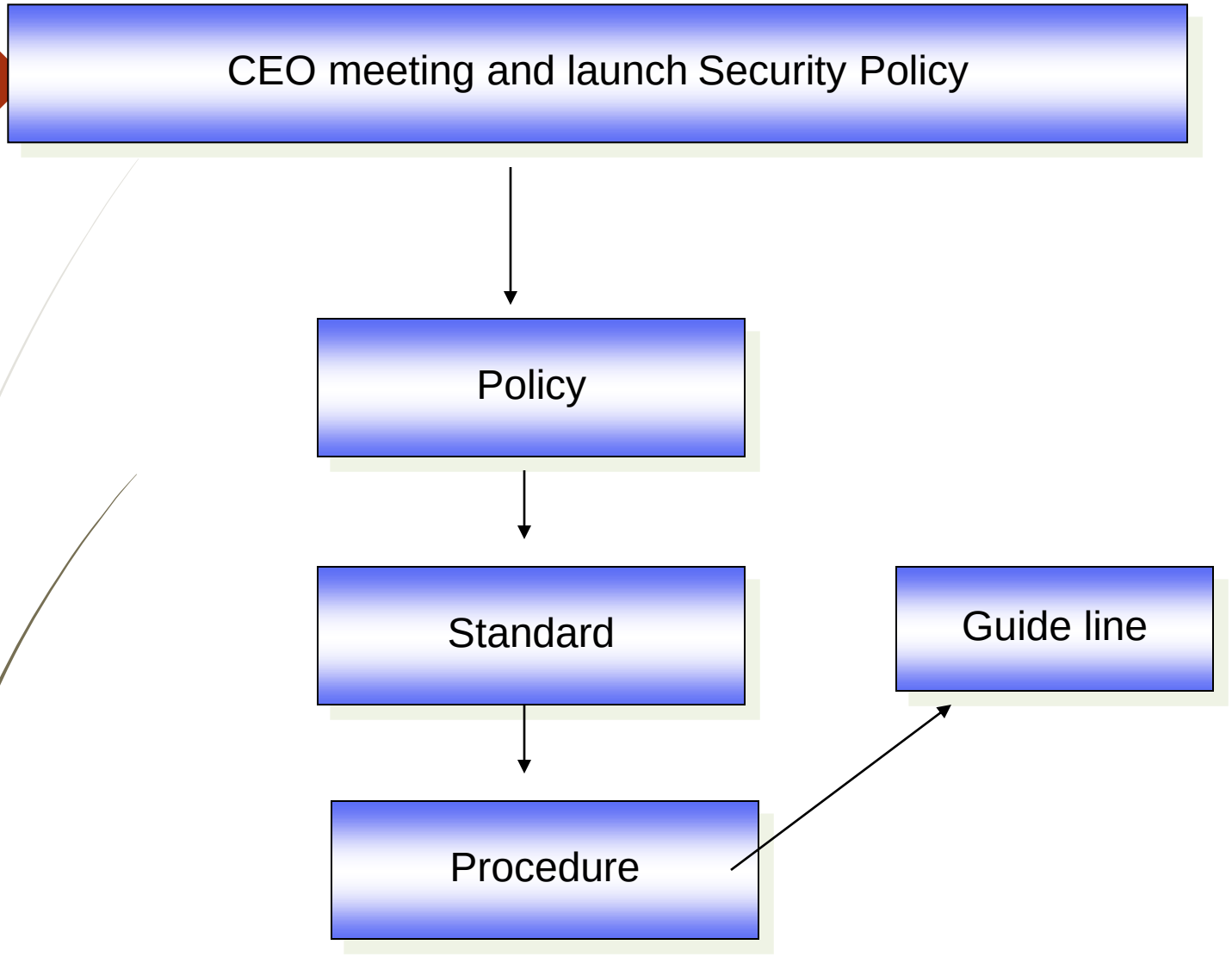
External



Separate level of Information



Move/Copy >> Disclosure >> Encryption >> Destruction


CEO meeting and launch Security Policy
Policy
Standard
Guide line
Procedure

Chapter 7

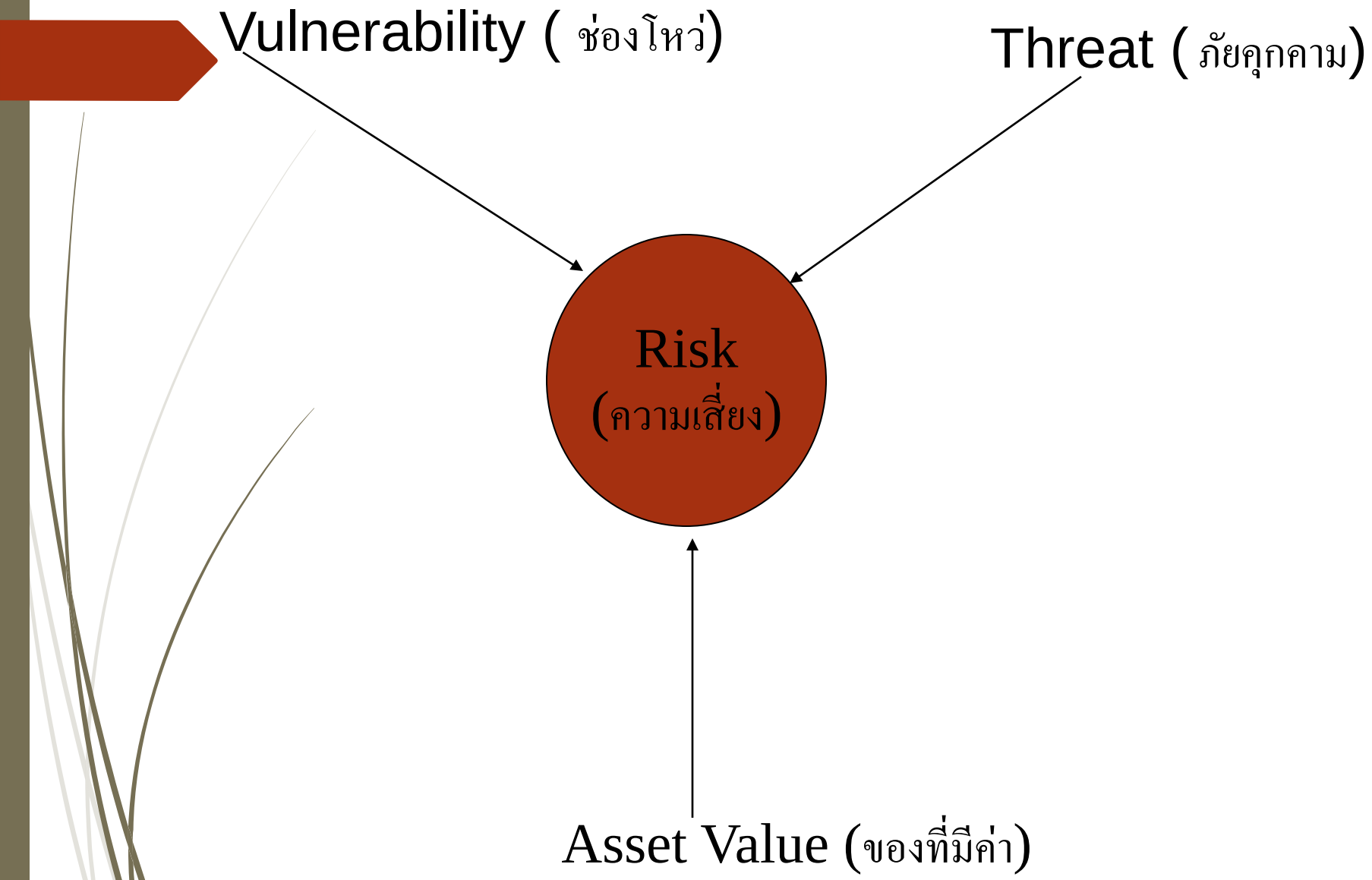
MANAGING RISK

What is Risk?

- **Risk is the potential for loss that requires protection.**
- **Risk have 2 component:**
  - **Vulnerability**
  - **Threat**

  Remark: Everything need to have value.

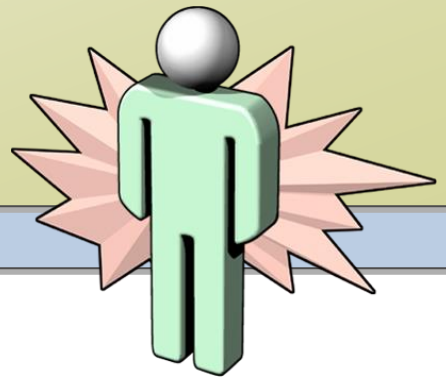
These two components form the basis for risk.


Vulnerability (ช่องโหว่)
Threat (ภัยคุกคาม)
Risk
(ความเสี่ยง)
Asset Value (ของที่มีค่า)

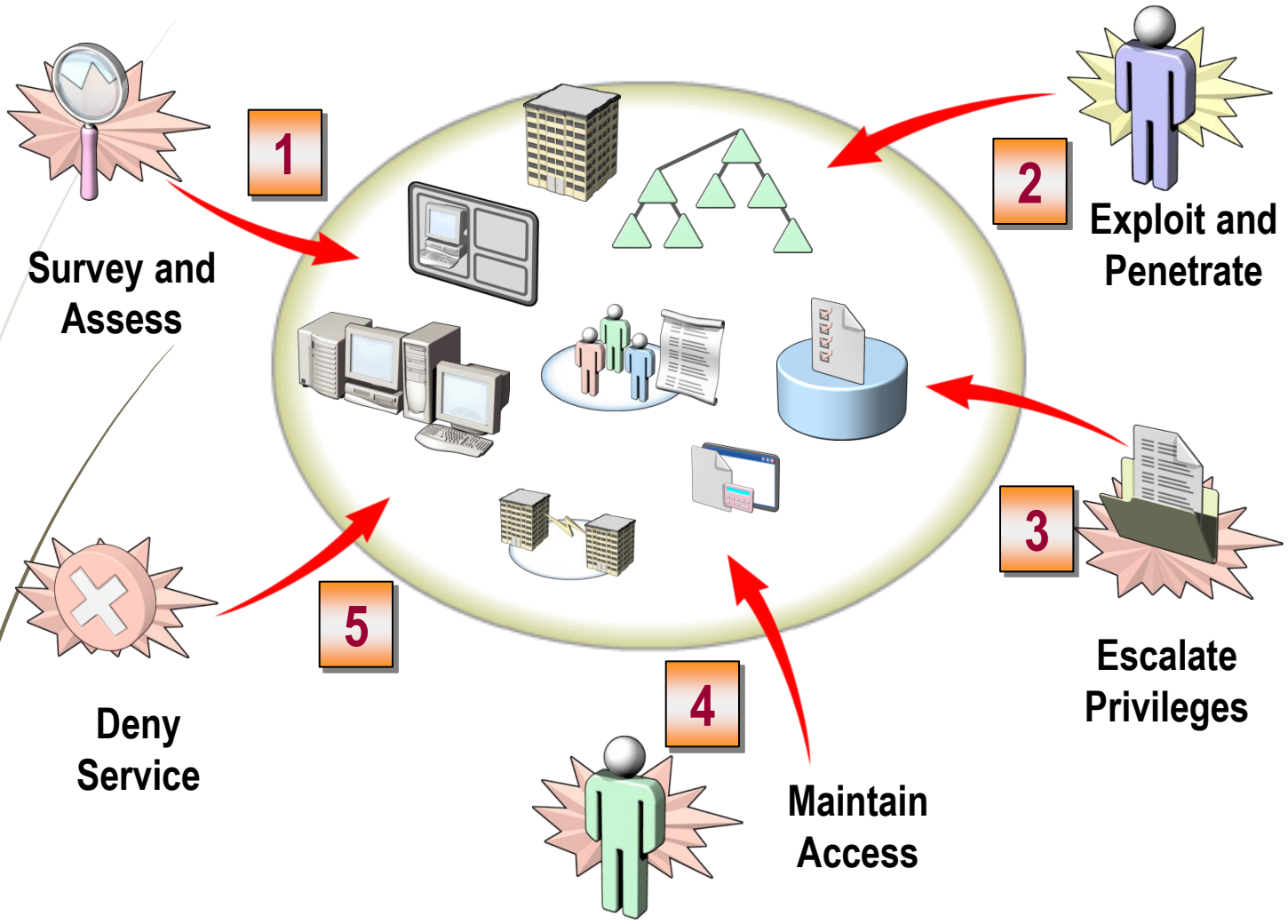
Why Network Attacks Occur

The reasons that network attacks occur include:

- Revenge
- Espionage
- Publicity
- Personal satisfaction
- Terrorism



Typical Anatomy of an Attack



Overview of the Risk Management Process

The stages of managing risks are:

1. Identify risks
2. Analyze risks
3. Plan for the management of risks
4. Develop methods to track changes to risks
5. Respond to risk management controls

Identify Risks to Assets

1 **Identify risks – For each risk create a risk statement**

Risk Statement Component	Example
Condition	**If a virus infects our website…**
Operations impact	**…it will take six hours to rebuild the Web server, which prevents customers from buying products…**
Financial and business impact	**…resulting in lost revenue, lost trust, and negative publicity**

Analyze Risks to Assets

2 **Analyze risks – Estimate the cost per year of the risk occurring**

Determine	Definition	Example
Single loss expectancy	**Total loss in the single instance of the risk**	**Financial impact: $12,000** **Business impact: $27,520** **Loss per instance: $39,520**
Annual rate of occurrence	**Number of times a year you expect the risk to occur**	**Twice a year**
Annual loss expectancy	**Amount of loss the risk can cause per year**	**Total Loss $39,520** **x2** **$79,040**

Manage Risks to Assets

3 **Plan for the management of risks – Create contingency plans and triggers**

Strategy	Definition	Example
Accept	**Acknowledge that the risk exists**	**Do nothing proactive**
Mitigate	**Proactively change the asset's exposure to the risk**	**Use virus protection software**
Transfer	**Partially shift the responsibility for the risk to a third-party**	**Use an external vendor to host the Web site**
Avoid	**Eliminate the source of risk or exposure to the risk**	**Remove the Web site from the Internet**

Track Changes to a Risk

4 **Develop methods to track changes to risks – Develop a process for monitoring risks**

Monitoring time frame	Example
Real-time	**Application that monitors the Web site continuously**
Periodic	**Scheduled quarterly review of risk management plan**
Ad-hoc	**Review the plan after each major security incident**

What Are Risk Management Controls?

5 **Respond to risk management controls**

Create controls to update:

- **Risk statements**
- **Risk analysis**
- **Management strategies and contingency plans**
- **Processes for monitoring security**

Guidelines for Creating a Risk Management Plan

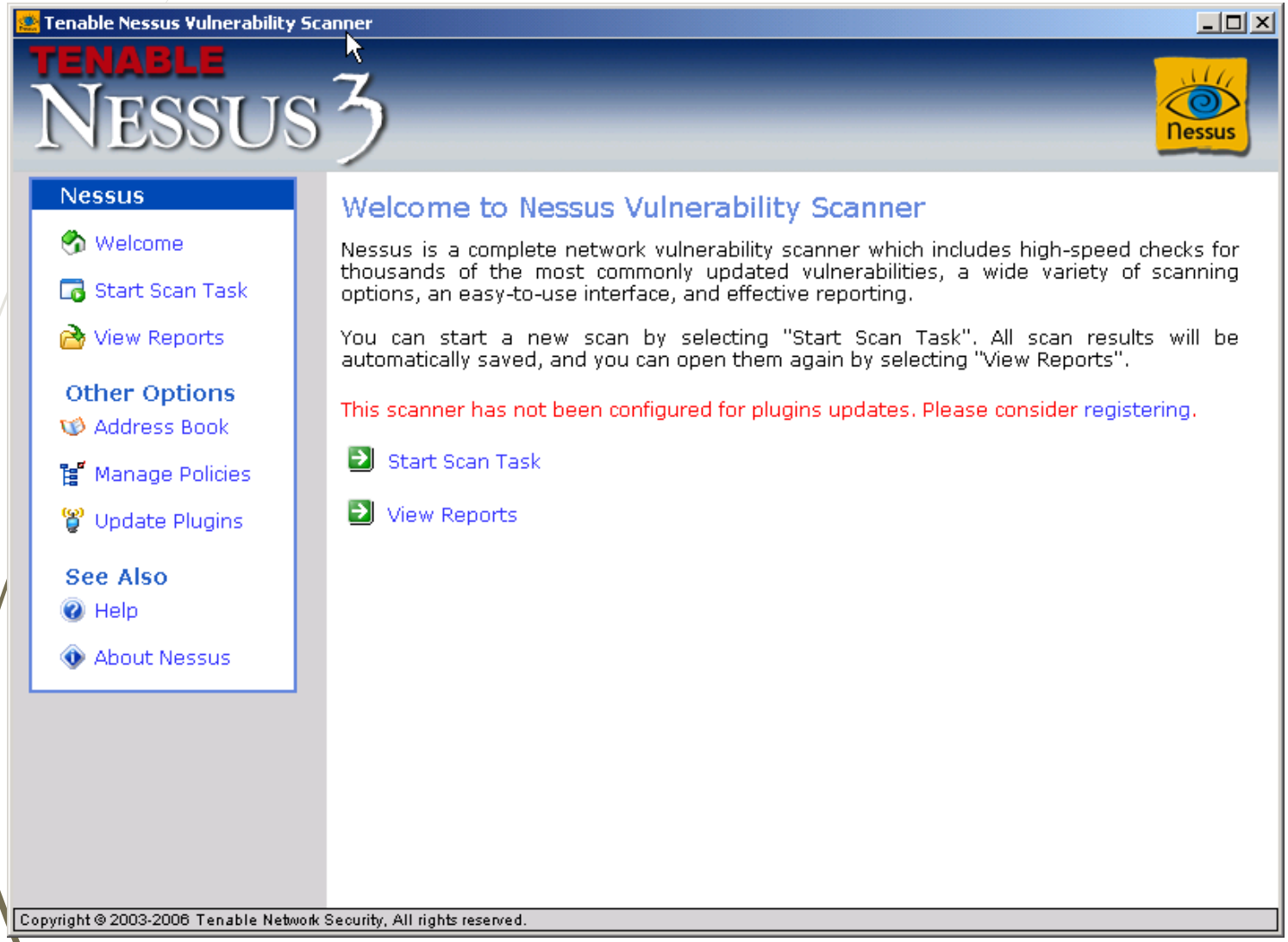
For a successful risk management plan, consider the following:

- ✓ **Obtain approval and support from upper management**
- ✓ **Determine the scope of the risk management plan**
- ✓ **Implement actions in a timely manner**
- ✓ **Update the risk management plan as changes occur**
- ✓ **Use the risk management plan to assign ownership and allocate resources**

LANguard


GFi
www.gfi.com
GFiLANguard
Network Security Scanner
Copyright © 2005 GFI Software Ltd.
Downloading updated missing patch detection files ... 8%
This program is protected by US and international copyright laws.

: Nessus Number one of Security Scanner



Chapter 8

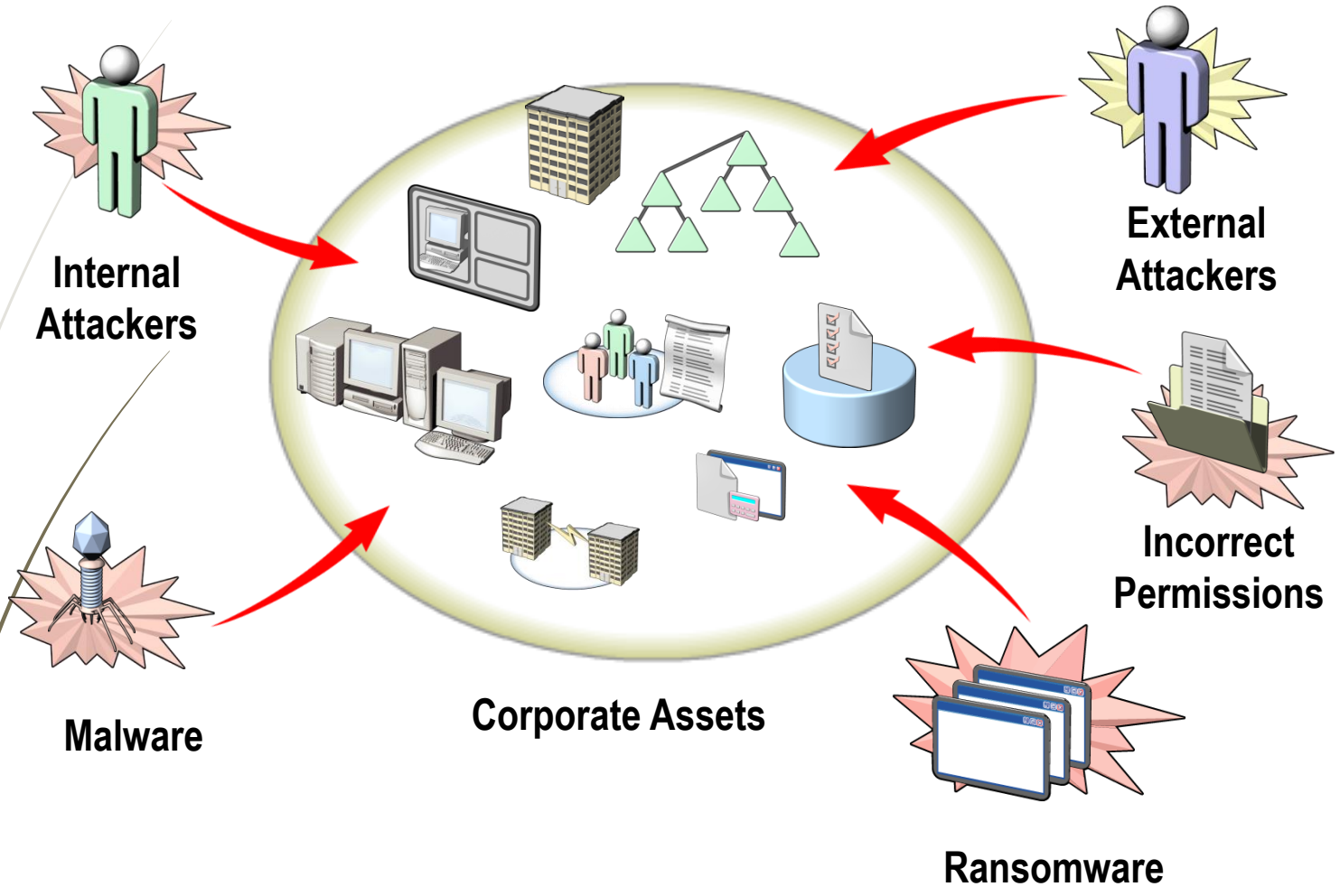
INFORMATION SECURITY PROCESS

PPT Concept

Suitable set of controls

Policies, Organizational structures
Processes, Procedures
Hardware, and Software

Why Invest in Network Security?



What Are the Key Principles of Security?

Principle	Definition
Defense in Depth	**Provide multiple layers of protection**
Least Privilege	**Grant the least amount of privilege or permissions necessary to perform the required task**
Minimized Attack Surface	**Reduce vulnerable points on a network**

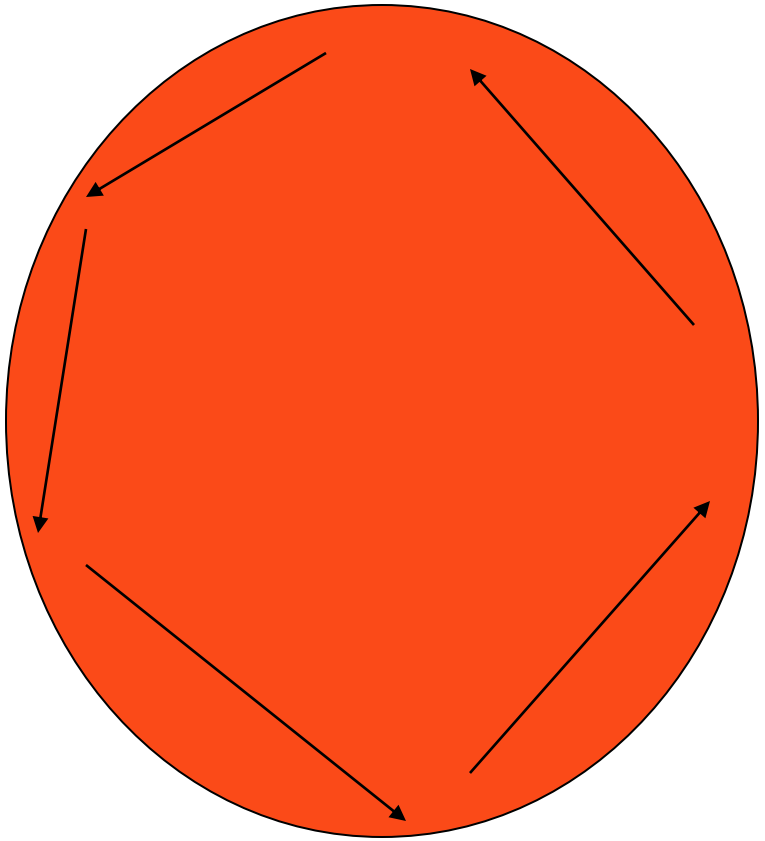
Accessing Security Risks

Information Security Process

1. Assessment (risk also)
2. Policy
3. Implementation
4. Training
5. Audit

Assessment

Policy



Audit

Implementation

Training

Assessment

- การสำรวจช่องโหว่ในระบบ
  - ใช้เครื่องมือในการตรวจสอบ เช่น **Retina, Nessus, NStealth, Languard** เป็นต้น
- การสำรวจช่องโหว่ในขั้นตอนปฏิบัติ
  - ใช้ **Gap analysis** พิจารณารายละเอียดดังต่อไปนี้
    - มูลค่าในทรัพย์สินสารสนเทศ
    - พิจาณาความเสี่ยงต่อทรัพย์สิน
    - แนะนำแผนปฏิบัติและสร้างแผนงานให้เหมาะสม

นโยบาย (Policy)

- นำผลสำรวจที่ได้มาจัดทำแผนงานในระดับนโยบาย ซึ่งผู้ปฏิบัติควรจะมีความรู้เกี่ยวกับความปลอดภัยเป็นอย่างดี เพื่อที่จะรู้ถึงผลที่ดำเนินการ ถ้าไม่ปฏิบัติตามแผนที่วางไว้จะเกิดอะไรขึ้นน่ากลัวอย่างไร

การนำไปใช้ (Implementation)

- การใช้งานเราจะพบปัญหาว่าต้องมีการปรับเปลี่ยนแผนให้ทันสมัยอยู่เสมอ บางทีอาจต้องมีการเปลี่ยนแผนทุก 3 เดือนและมีการกำหนดระดับความสำคัญ ผู้รับผิดชอบ รวมถึงมีรอบในการตรวจสอบทบทวนอยู่เสมอ

การจัดการอบรม (Awareness Training)

- **เป็นการอบรมให้ผู้ปฏิบัติงานมีความเข้าใจในเรื่องความปลอดภัยเป็นอย่างดี เพราะทุกๆคนเป็นส่วนหนึ่งในระบบ**

Audit

- มีรอบในการ **Audit** ทุกๆปี เพื่อทำการตรวจเช็ค ว่าทุกๆอย่างเป็นไปตามที่วางไว้ โดยการประเมินผล เป็นแบบ **scoring** และ **grade**

Chapter 9

FIREWALL

FIREWALL

แบ่งเป็น 2 ประเภทใหญ่คือ

1. Personal Firewall (Host-based) คือ Firewall ที่มีอยู่และป้องกันเฉพาะเครื่องที่ทำการติดตั้ง ยกตัวอย่างเช่น Zone Alarm หรืออาจจะมาจากระบบปฏิบัติการอยู่แล้ว เช่น windows เป็นต้น

2. Network Firewall (Network-based) เป็น Firewall ประเภทที่มีการป้องกันทั้ง Network ยกตัวอย่างเช่น

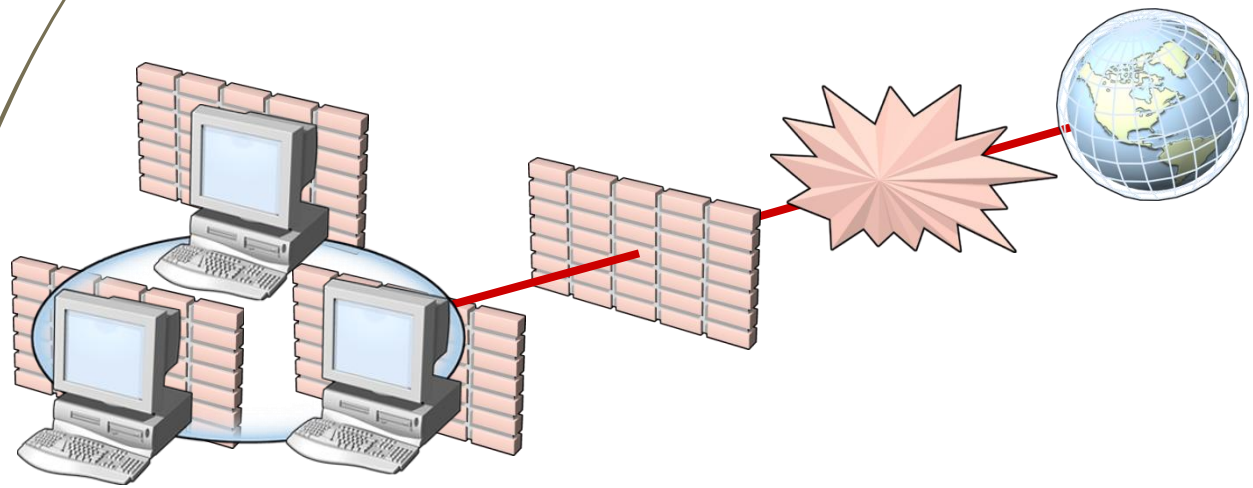
Software: IPCOP (Linux), Ubuntu, CentOS

Hardware: IRONPort, Juniper, Radware, Fortigate เป็นต้น

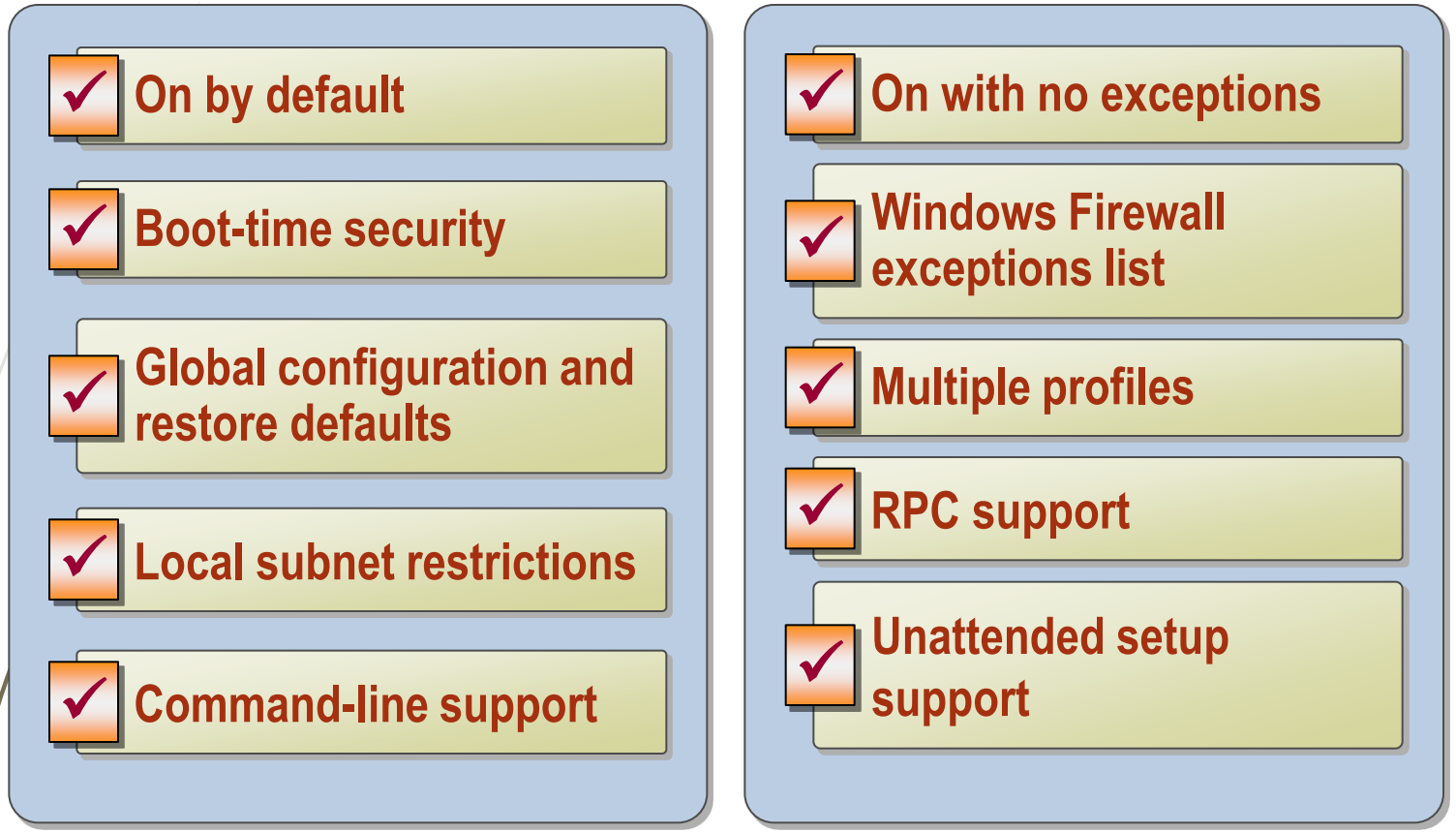
The Need for Client Firewalls

Which clients need firewalls?

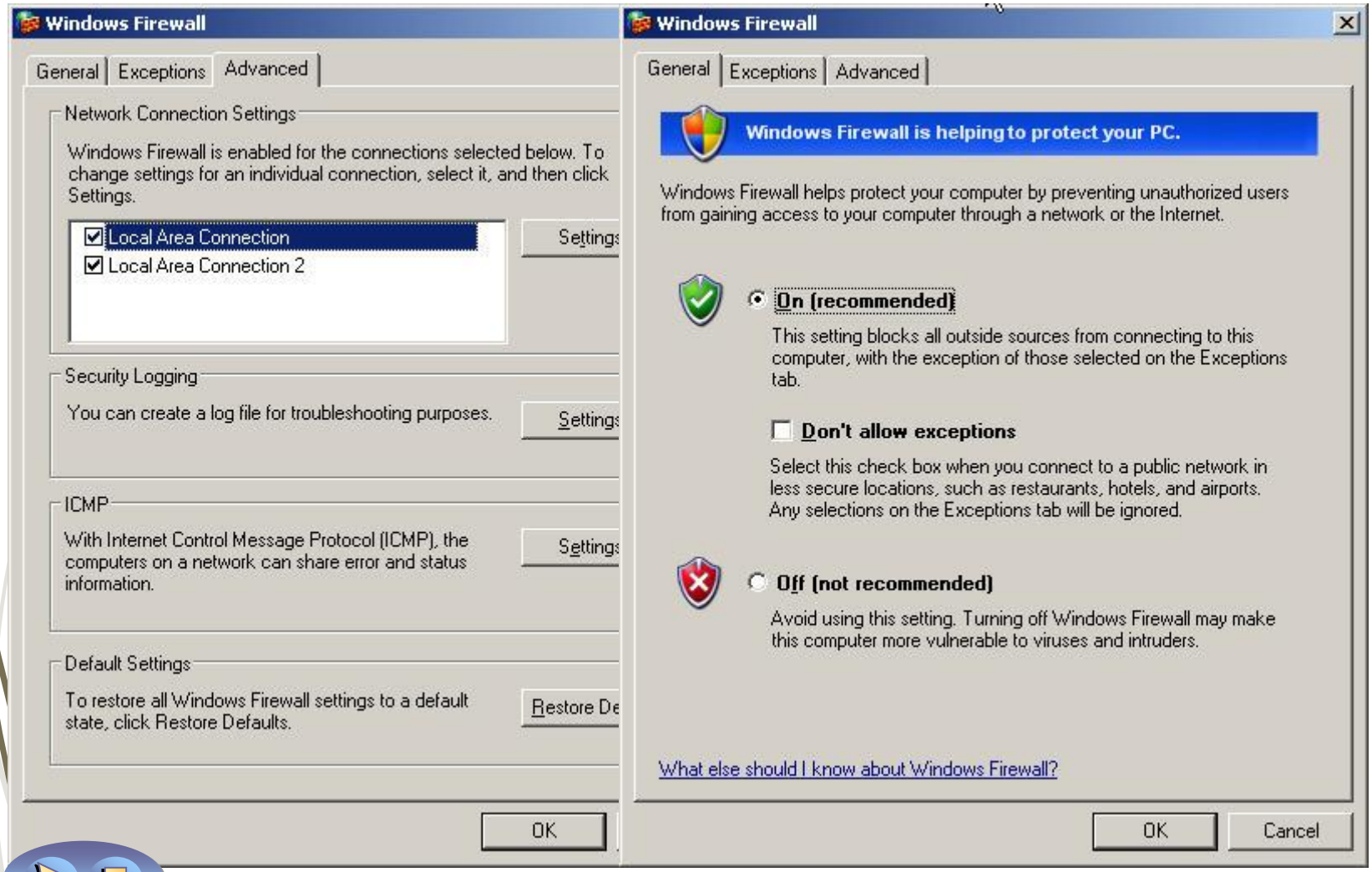
- LAN clients
- Desktops with modem connections
- Mobile clients



Windows Firewall



Windows Firewall Configuration Options



Type of Network Firewall

- **Packet Filtering**

  - Work on Layer 3(OSI)

  - Complicated to setup

  - Work directly Example if set deny to use web, everyone can not use.

- **Stateful Filtering**

  - Work on Layer 4(OSI)

  - Easier setting more than Packet Filtering

  - Decide about behavior of attacking and lock.

- **Application Filtering**

  - Work on Layer 7(OSI)

  - Easily to setup

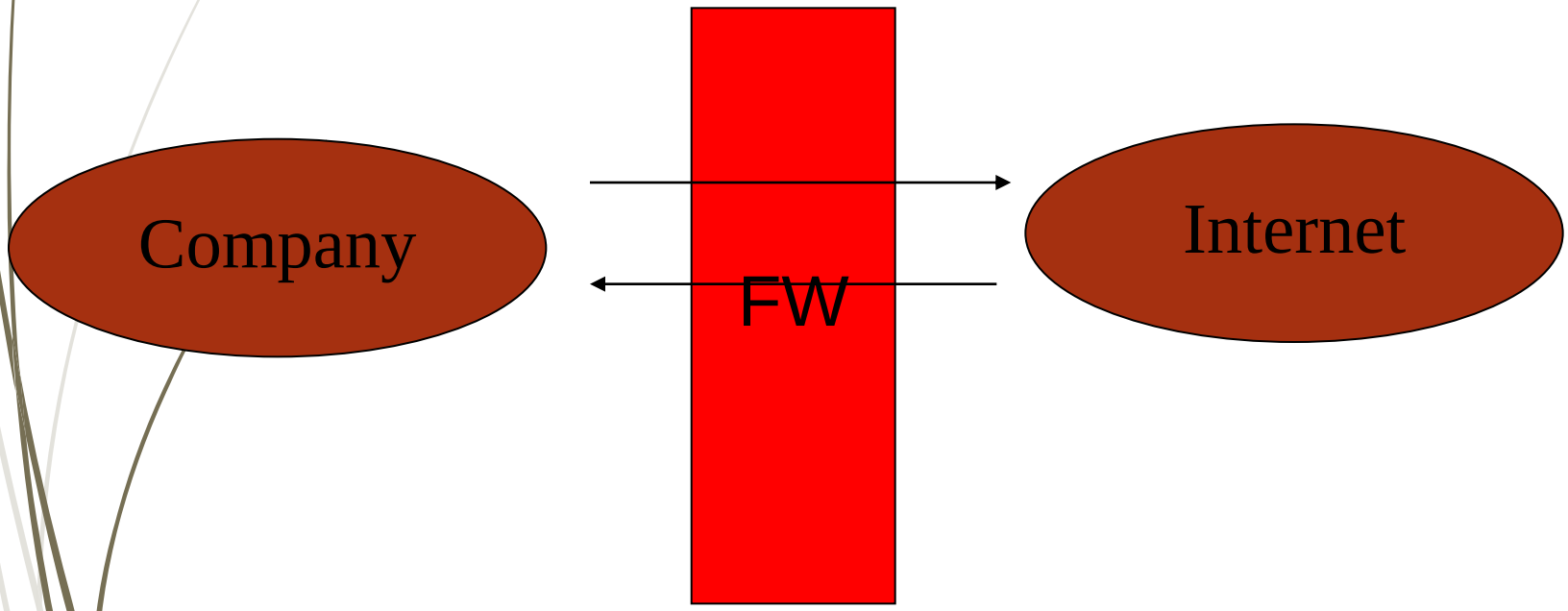
  - Intelligent working Example we can set someone allow access web and someone cannot.

Remark: IDS and IPS work on Layer7

TOPOLOGY OF FIREWALL

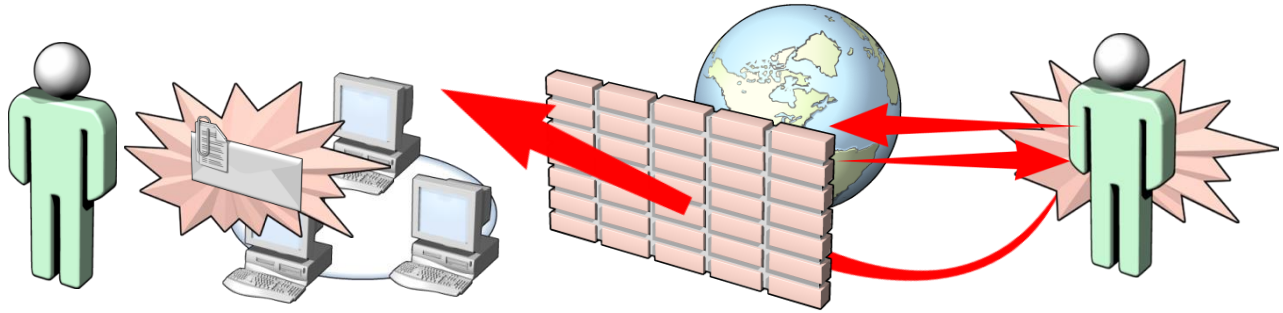
- Edge Firewall (Bastion Host)
- 3 Legs Firewall
- Front Firewall
- Back Firewall

Edge Firewall (Bastion Host)

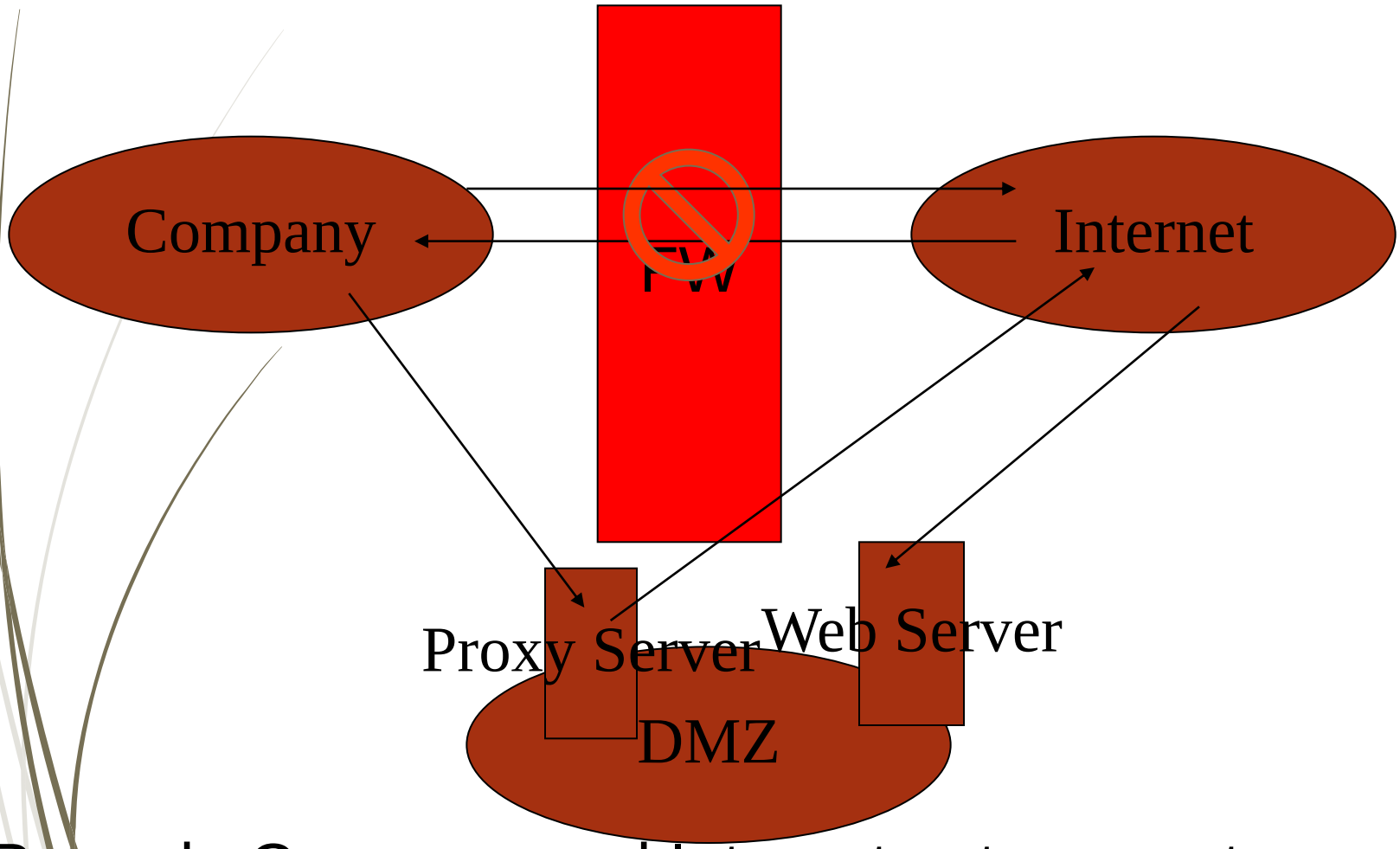


Resources to Protect with Network Perimeters Security

Attacker	Threat	Example
External	**Information disclosure**	**An attacker runs a series of port scans on a network and creates a network diagram and vulnerability list.** **The attacker uses this information to systematically attack the network.**
Internal	**Denial of service**	**An employee opens an e-mail from an external Web-based e-mail account that contains a new worm virus.** **The virus infects the internal network from inside the perimeter.**

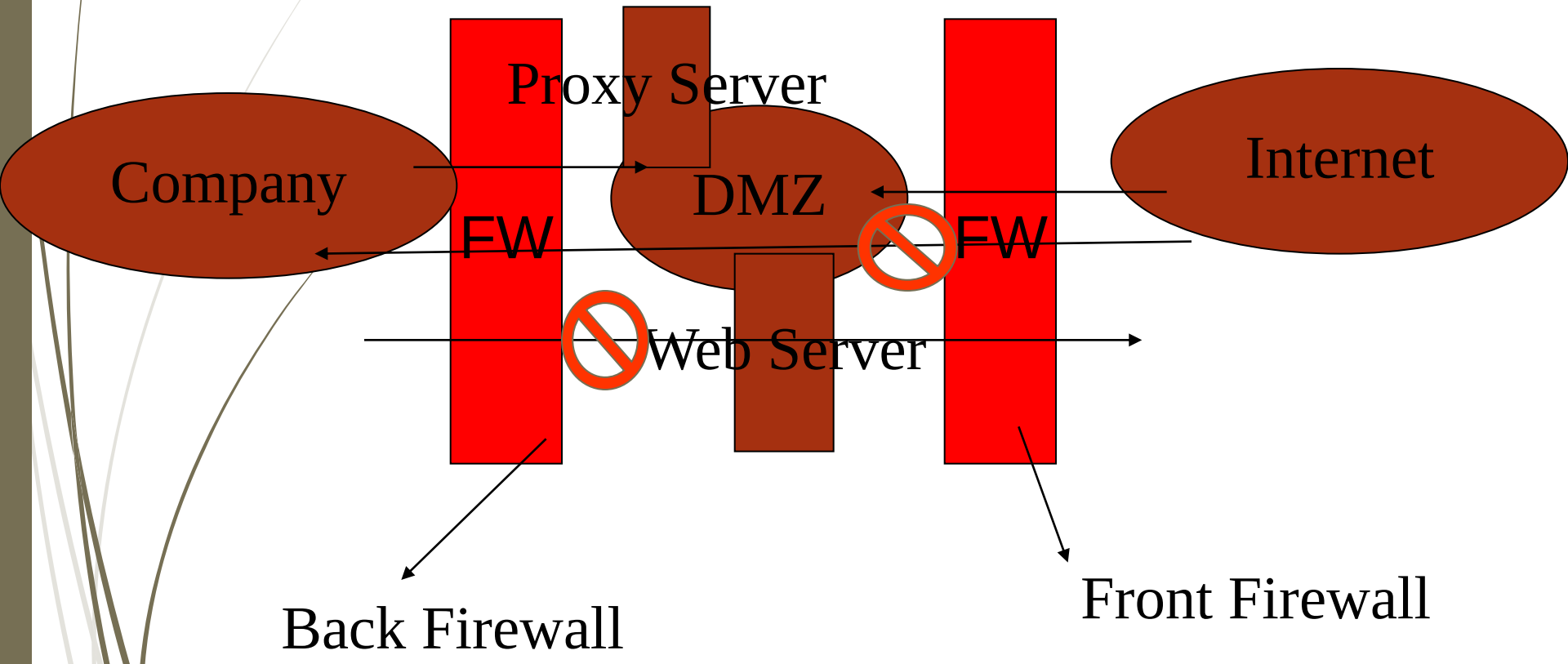


3 Legs Firewall



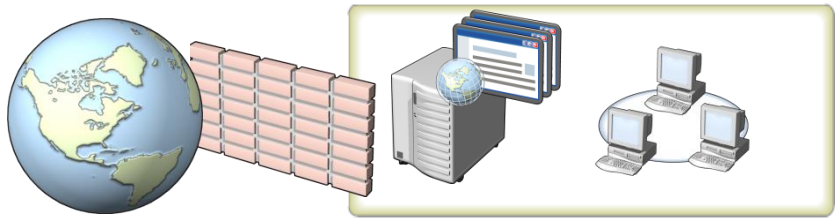
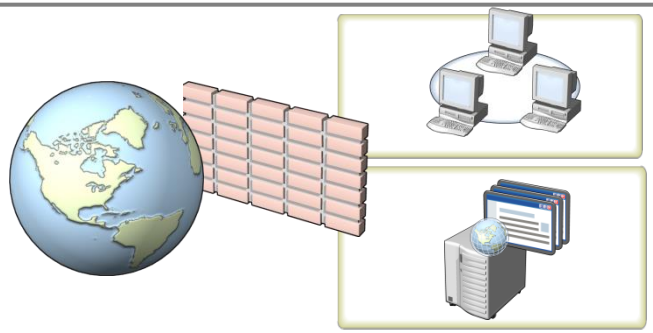
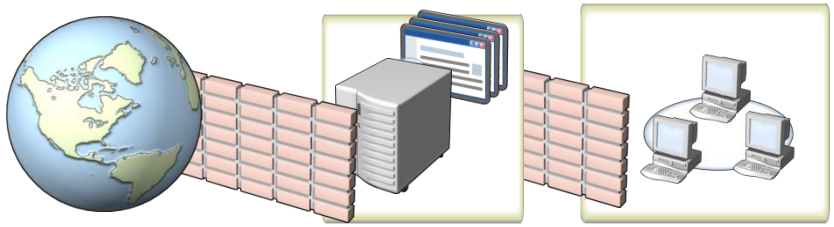
Remark: Company and Internet not connect directly. But we use DMZ as buffer..

BackFirewall & Front Firewall

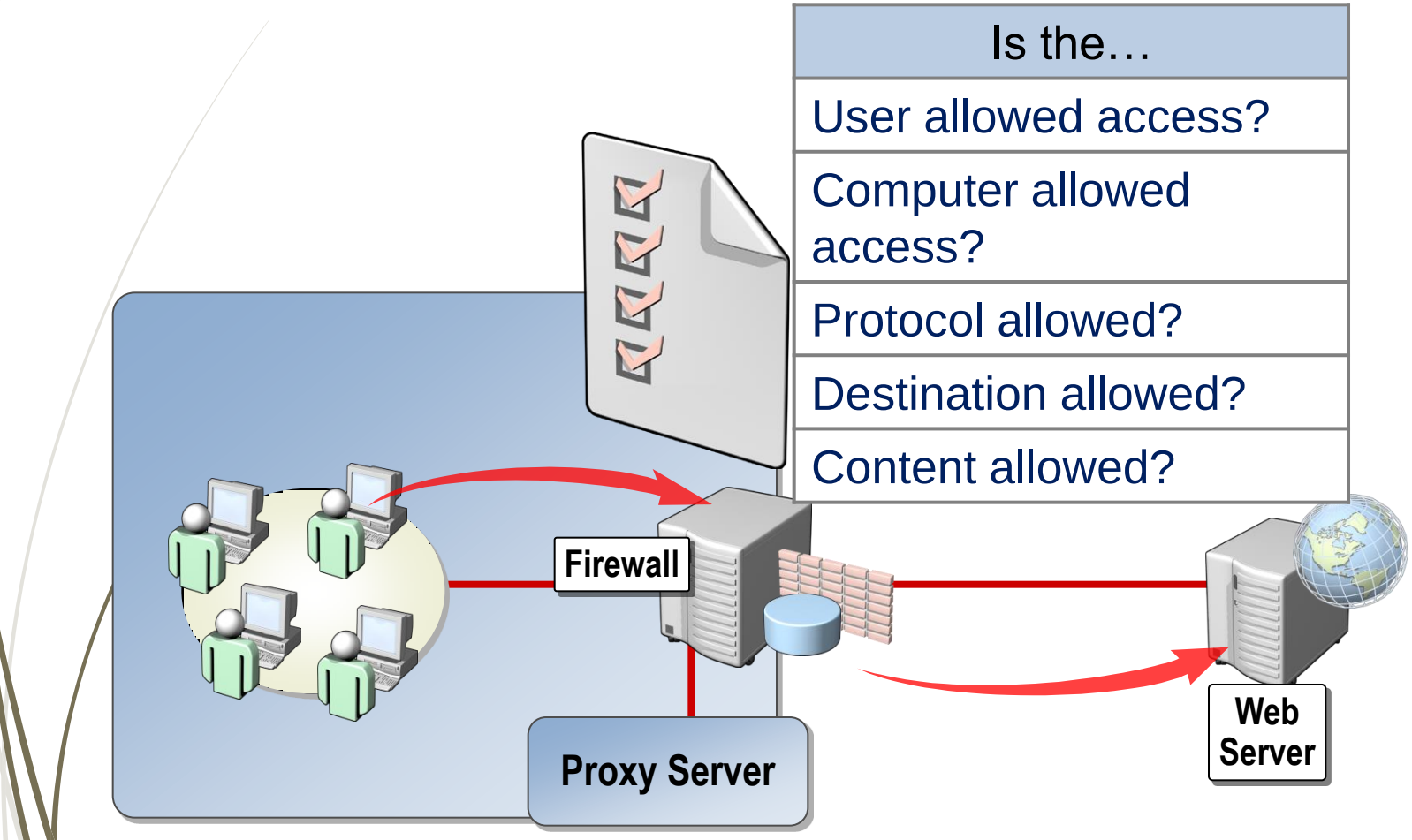


Remark: Company and Internet not connect directly. But we use DMZ as buffer..

Methods for Securing Network Perimeters

Type	Description
Bastion host	
Three-pronged configuration	
Back-to-back configuration	

Firewall Configuration Options for Internet Access

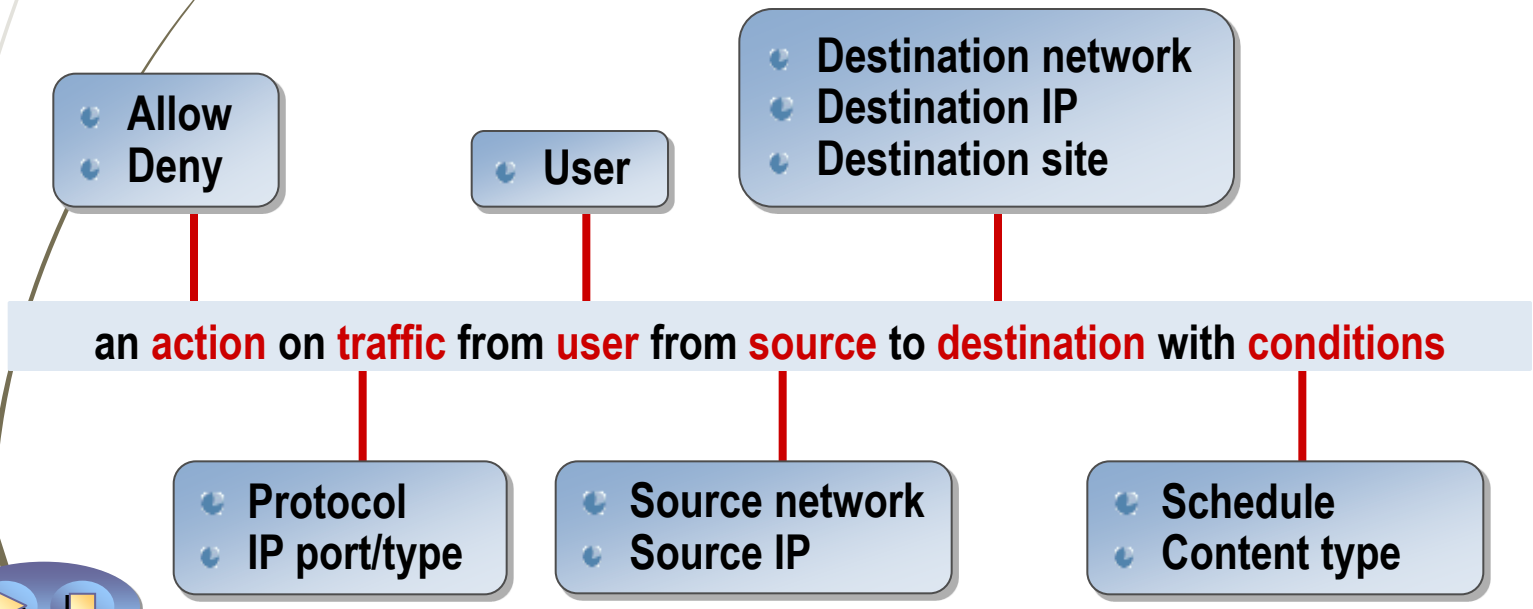


Firewall Access Rules

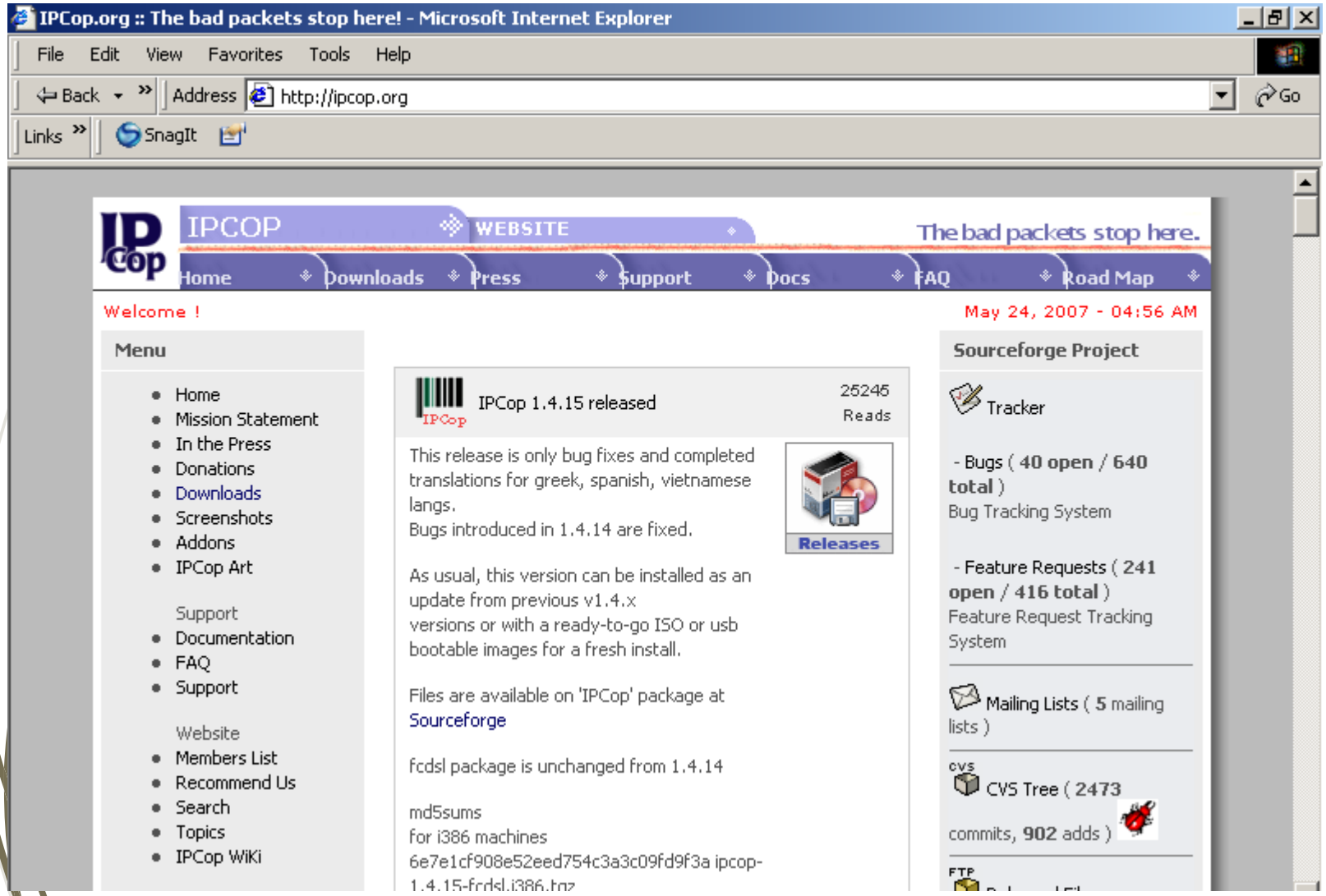
Types of access rule elements used to create access rules are:

- Protocols
- User sets
- Content types
- Schedules
- Network objects

Access rules always define:



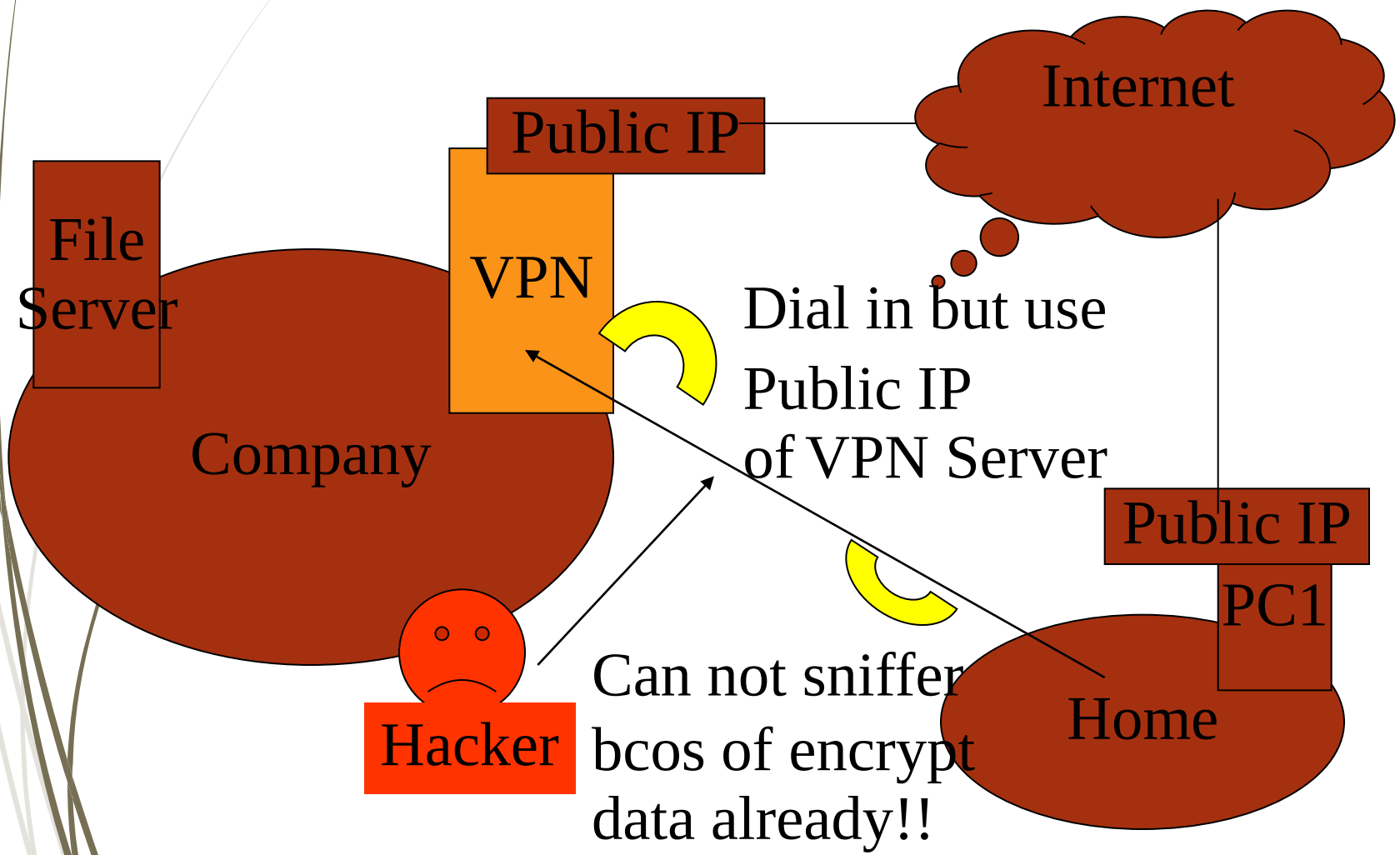
: IPCOP


IPCop.org :: The bad packets stop here! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Address http://ipcop.org Go
Links SnagIt
IPCOP WEBSITE
The bad packets stop here.
Home Downloads Press Support Docs FAQ Road Map
Welcome !
May 24, 2007 - 04:56 AM
Menu
Home
Mission Statement
In the Press
Donations
Downloads
Screenshots
Addons
IPCop Art
Support
Documentation
FAQ
Support
Website
Members List
Recommend Us
Search
Topics
IPCop WiKi
IPCop 1.4.15 released
25245 Reads
This release is only bug fixes and completed translations for greek, spanish, vietnamese langs.
Bugs introduced in 1.4.14 are fixed.
As usual, this version can be installed as an update from previous v1.4.x versions or with a ready-to-go ISO or usb bootable images for a fresh install.
Files are available on 'IPCop' package at Sourceforge
fcdsl package is unchanged from 1.4.14
md5sums
for i386 machines
6e7e1cf908e52eed754c3a3c09fd9f3a ipcop-1.4.15-fcdsl.i386.tgz
Releases
Sourceforge Project
Tracker
- Bugs (40 open / 640 total)
Bug Tracking System
- Feature Requests (241 open / 416 total)
Feature Request Tracking System
Mailing Lists (5 mailing lists)
CVS Tree (2473 commits, 902 adds)
FTP

Chapter 10

VIRTUAL PRIVATE NETWORK

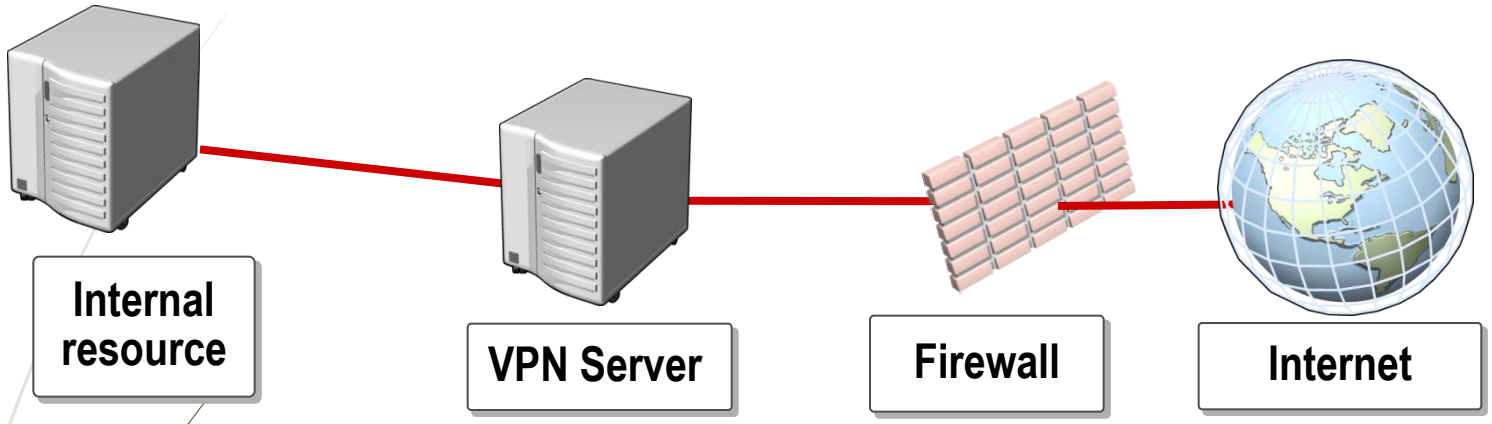
Why we need to use VPN!!!



Guidelines for Determining Hardware Requirements for Remote Access

Component	Guidelines
Dial-up networking	• **A dial-up remote access server must have a modem or a multiport adapter, and it must have access to an analog telephone line or lines**
VPN	• **For interfaces on the public network, use IPSec accelerator network cards**
CPU	• **Increase the available processing power to increase throughput**
RAM	• **If you do not need to handle more than 1,000 concurrent calls from remote access users, 512 MB of RAM is adequate**

VPN Server Placement



To allow PPTP connections, enable:

- TCP Port: 1723
- Protocol ID: 47

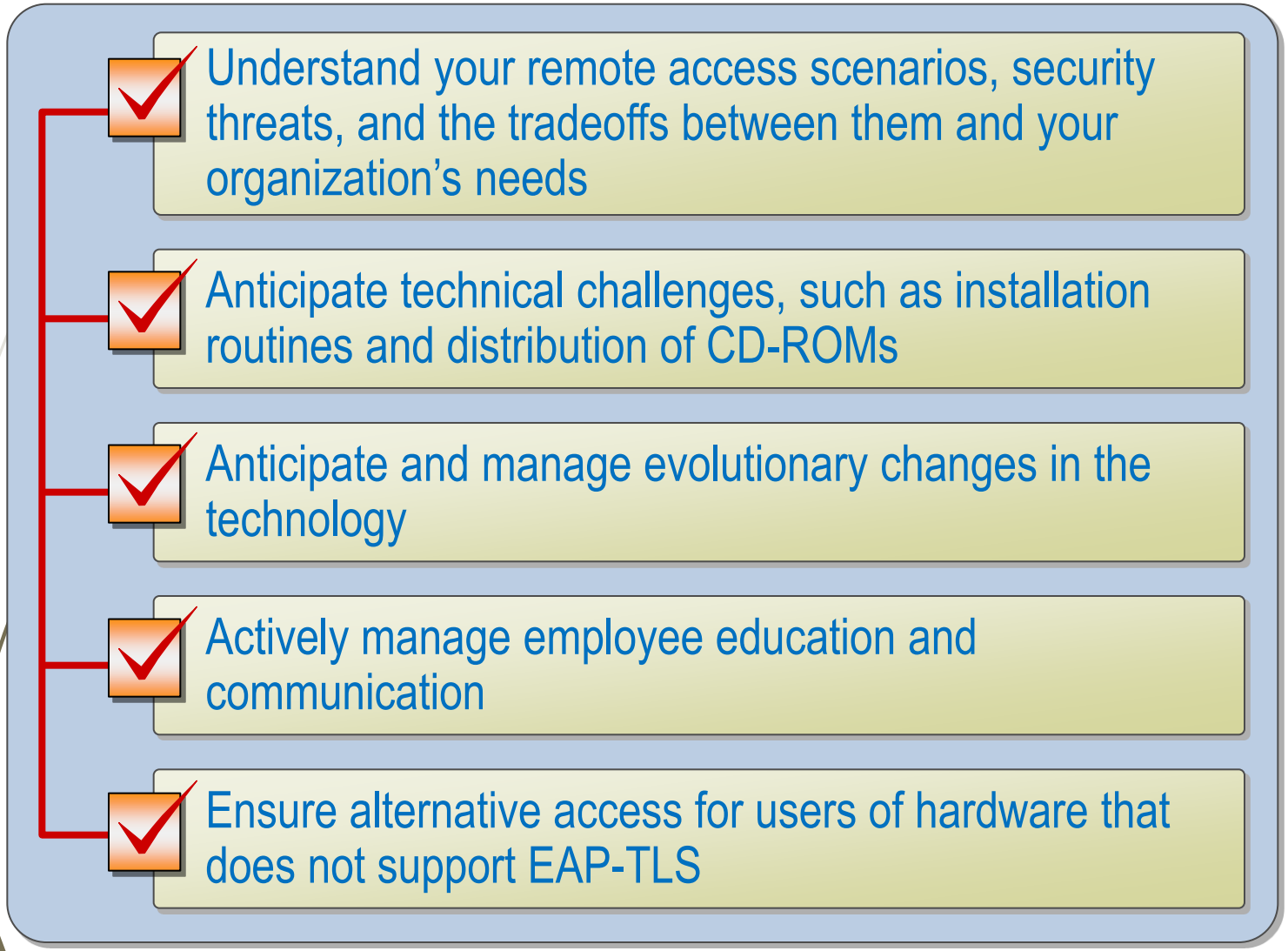
To allow L2TP/IPSec connections, enable:

- UDP Port: 500
- UDP Port: 4500
- Protocol ID: 50

VPN

- PPTP encrypt in TCP Layer but not secure 100 % because of hacker can see IP of VPN server
- L2TP/IPSec encrypt in IP Layer but need to use together with IPSec
- SSTP
- IKE

Guidelines for Resolving Remote Access Deployment Challenges



What Is Network Access Quarantine Control?

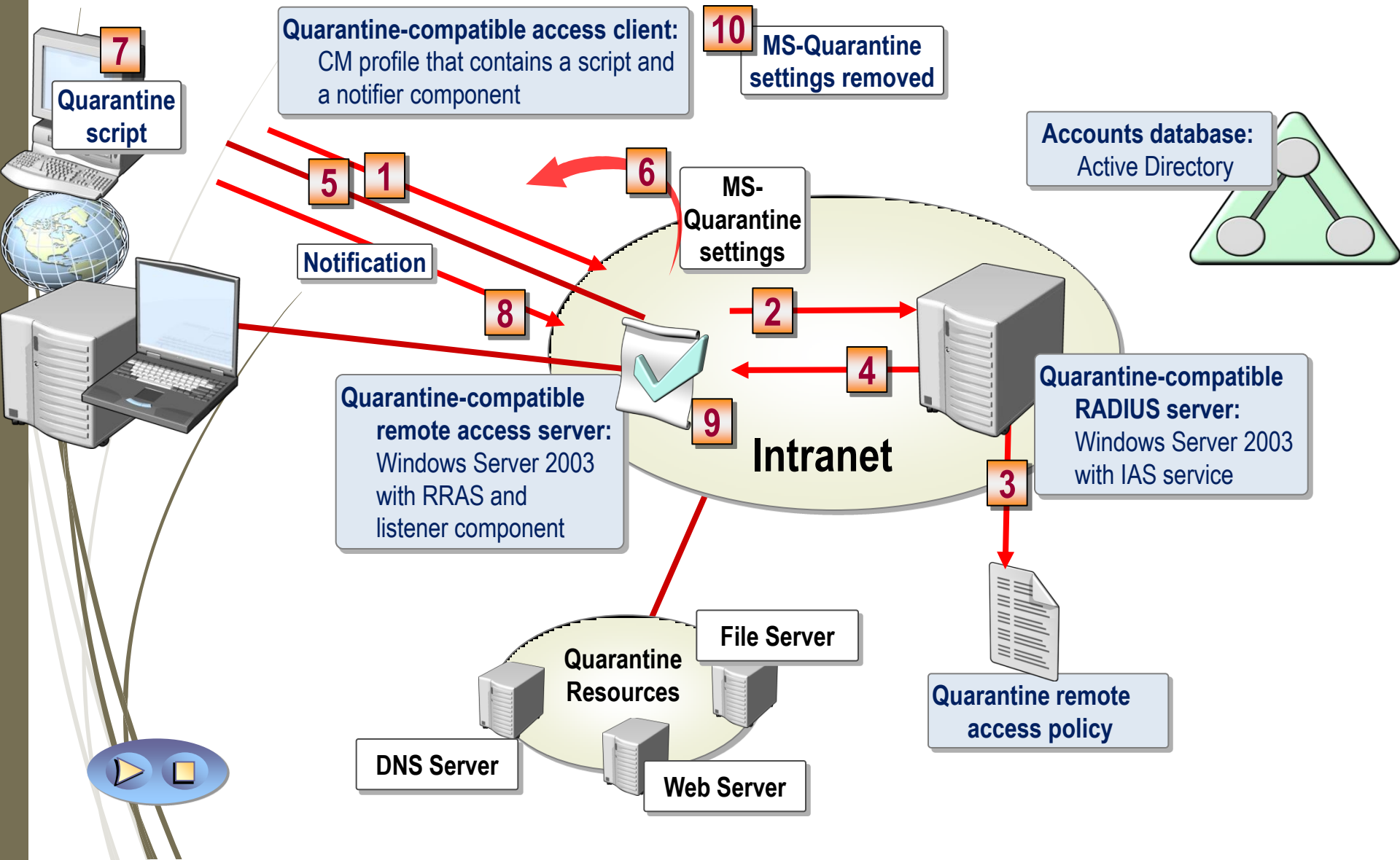
Network Access Quarantine Control

- Provides protection when users in your organization accidentally reconfigure key settings and do not restore them before connecting to your network

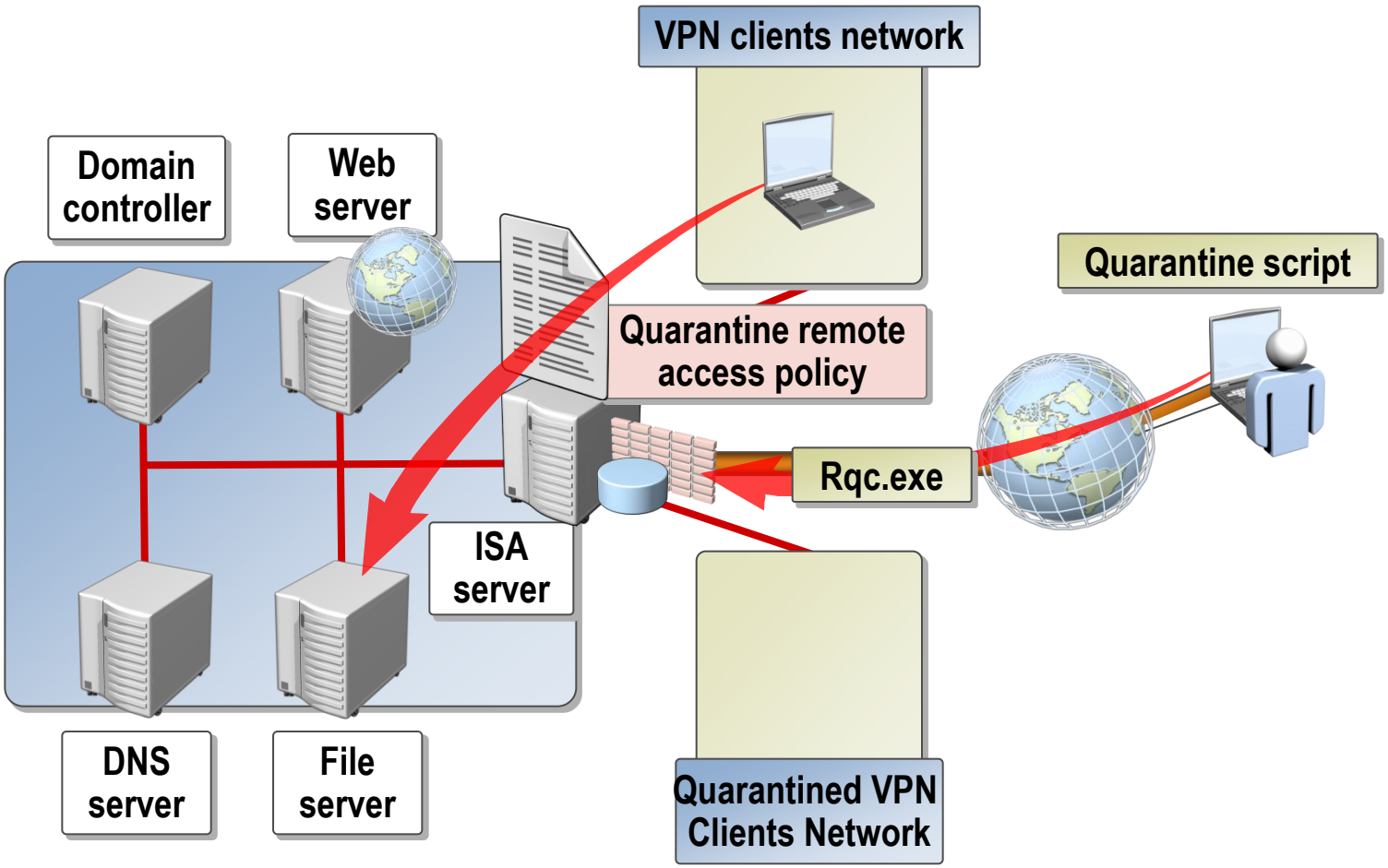
Quarantine mode

- A set of network restrictions that are configured in IAS and implemented by the remote access server for each connection

How Network Access Quarantine Control Works



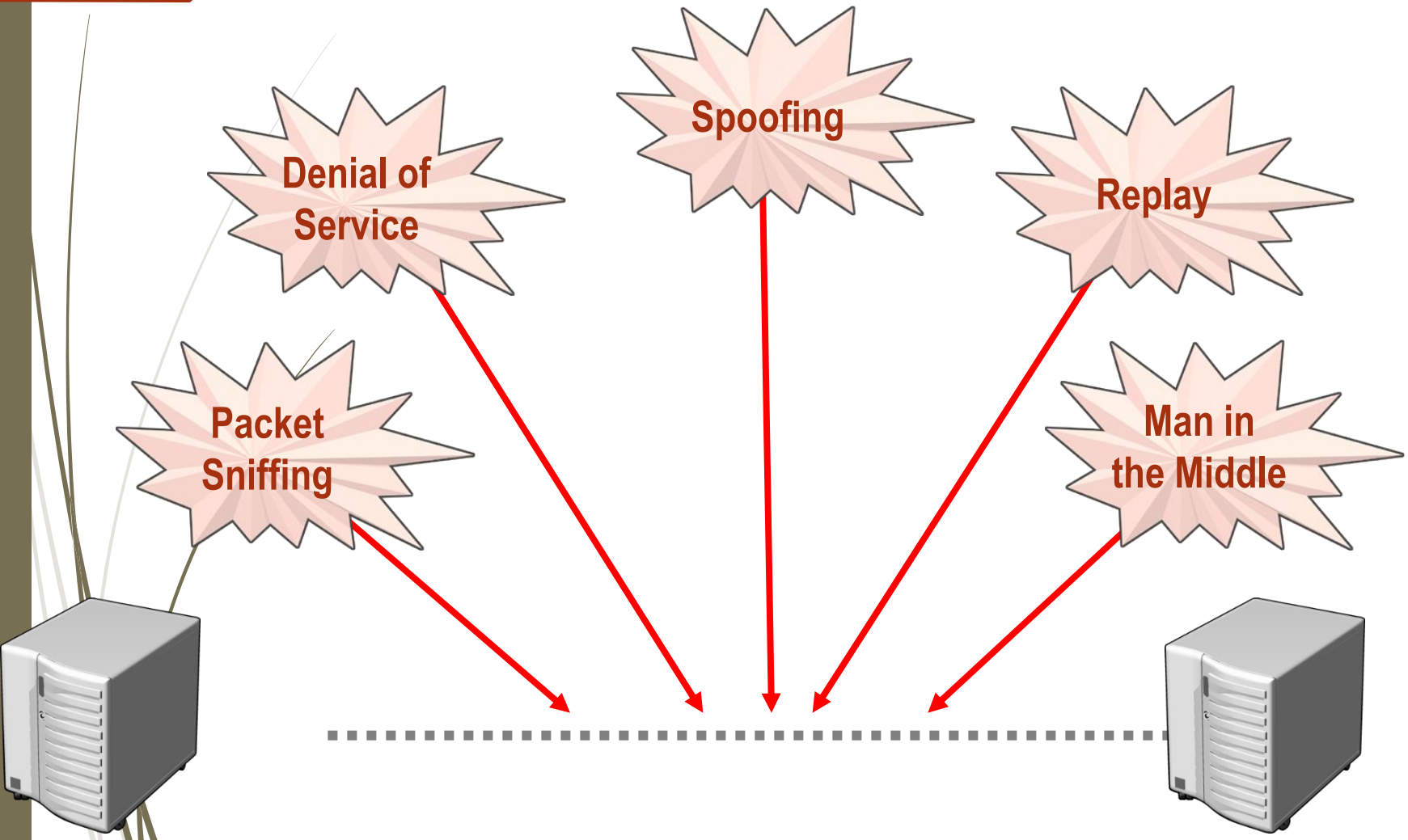
How VPN Quarantine Work?



Chapter 11

การเข้ารหัส ENCRYPTION

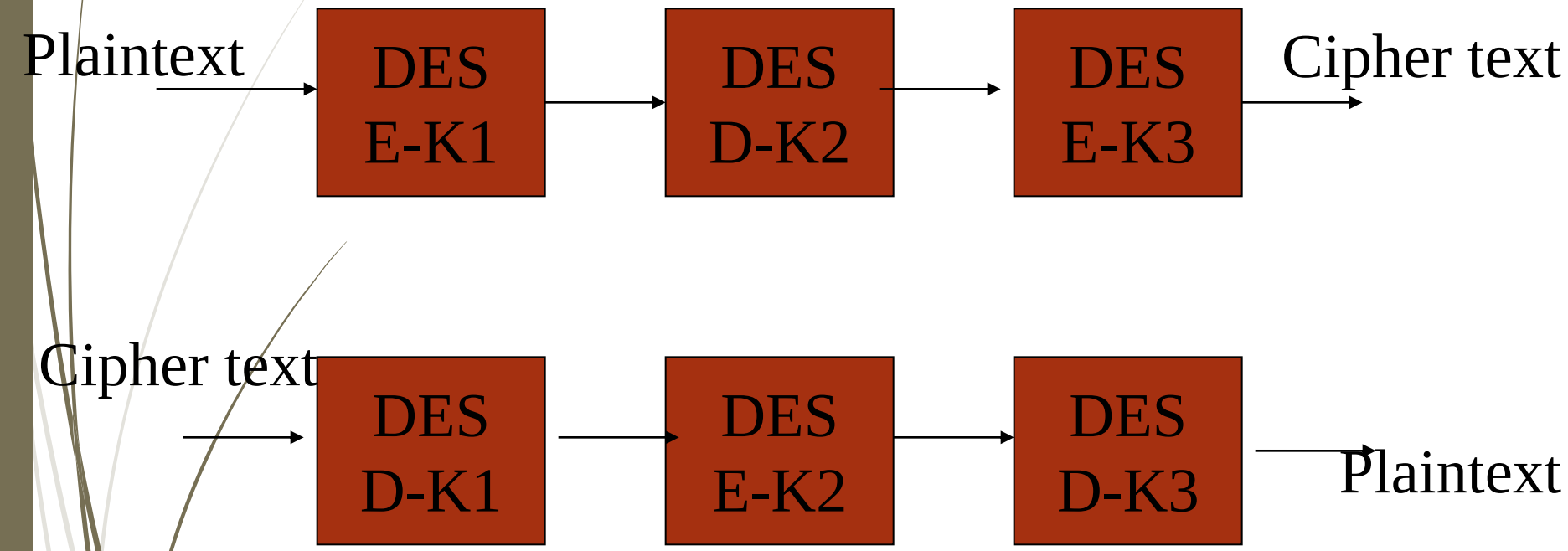
Threats to Secure Data Transmission



คำศัพท์ที่ควรรู้เกี่ยวกับการเข้ารหัส

Plaintext	ข้อมูลที่ไม่มีการเข้ารหัส ส่งตรงๆ
Ciphertext	ข้อมูลที่มีการเข้ารหัส เช่นใช้เทคนิคแบบ - Dynamic เช่น RSA, MD5 - Static เช่น DES, 3DES
Algorithm	คือการแปลงข้อมูลจากที่ไม่มีการเข้ารหัสให้มีการเข้ารหัส หนึ่งแนวคิดอาจจะมีหลายเทคนิค
Key	คือข้อมูลชุดที่ใช้ในการถอดรหัสจากข้อมูลที่เข้ารหัสเป็นข้อมูลที่ไม่เข้ารหัส รวมถึงการเข้ารหัส
Encryption	คือกระบวนการในการเข้ารหัสข้อมูลที่ไม่เข้ารหัส
Decryption	ตรงข้ามกับ Encryption
Cryptography	เป็นศิลปะที่ทำการปิดบังข้อมูลด้วยการเข้ารหัส
Cryptograher	คือบุคคลที่ที่ใช้ Cryptography
Cryptanalysis	ผู้วิเคราะห์ว่า Cryptography ได้ใช้ Algorithm ที่เหมาะสมหรือไม่
Cryptanalyst	เป็นผู้แบ่ง และระบุว่า Cryptography ใดที่มีความอ่อนแอ หรือเข้มแข็ง

การเข้าและถอดรหัสแบบ 3 DES



What Is SSL/TLS?

SSL and TLS

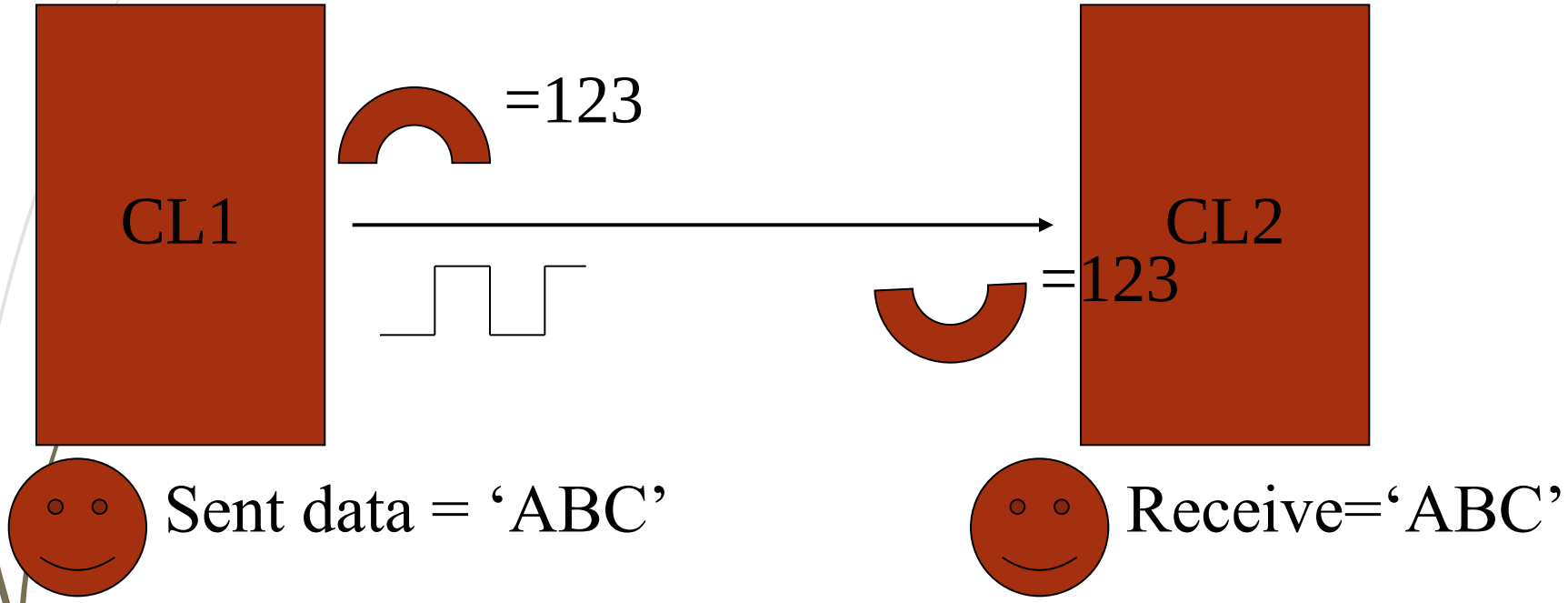
- Provide session encryption and integrity and server authentication
- Enable clients and servers to communicate in a way that prevents successful eavesdropping, tampering, or message forgery
- Reside at the transport layer of the OSI model

Cryptographic features

- Authentication
- Confidentiality
- Message integrity

Symmetric Key

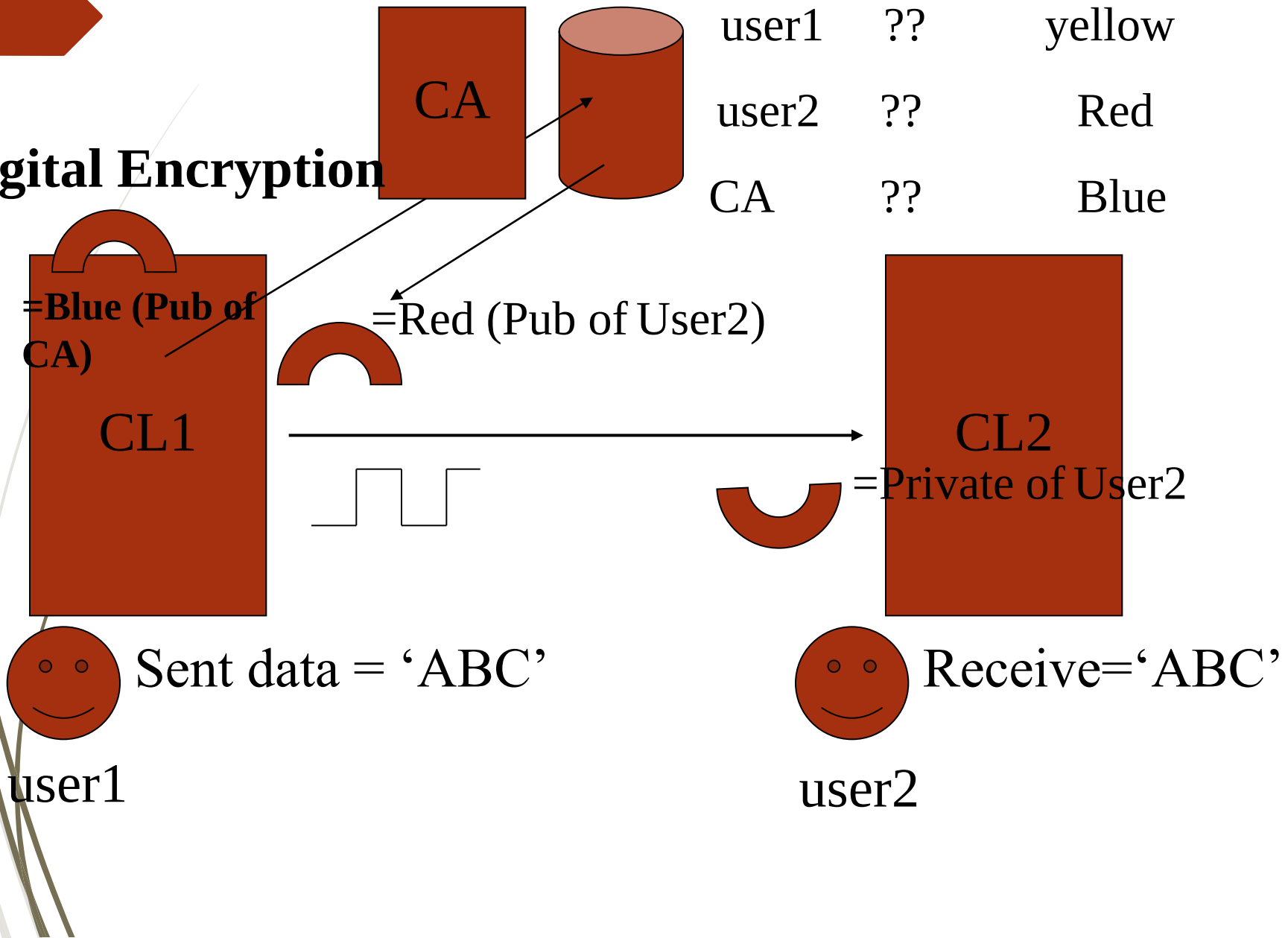
Look like Preshare- Key…



Asymmetric Key

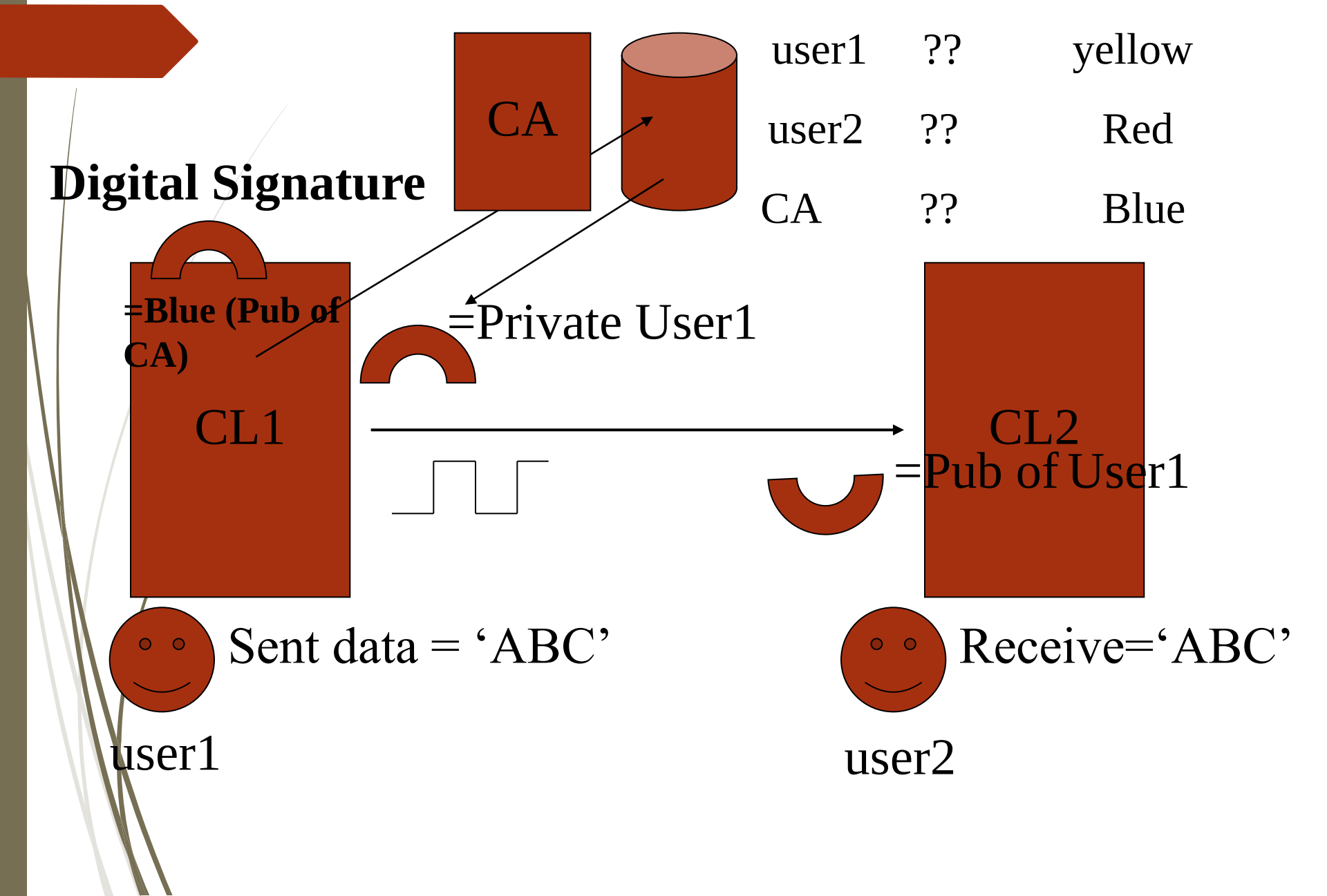
User	Private	Public
user1	??	yellow
user2	??	Red
CA	??	Blue

Digital Encryption



Asymmetric Key

User	Private	Public
user1	??	yellow
user2	??	Red
CA	??	Blue

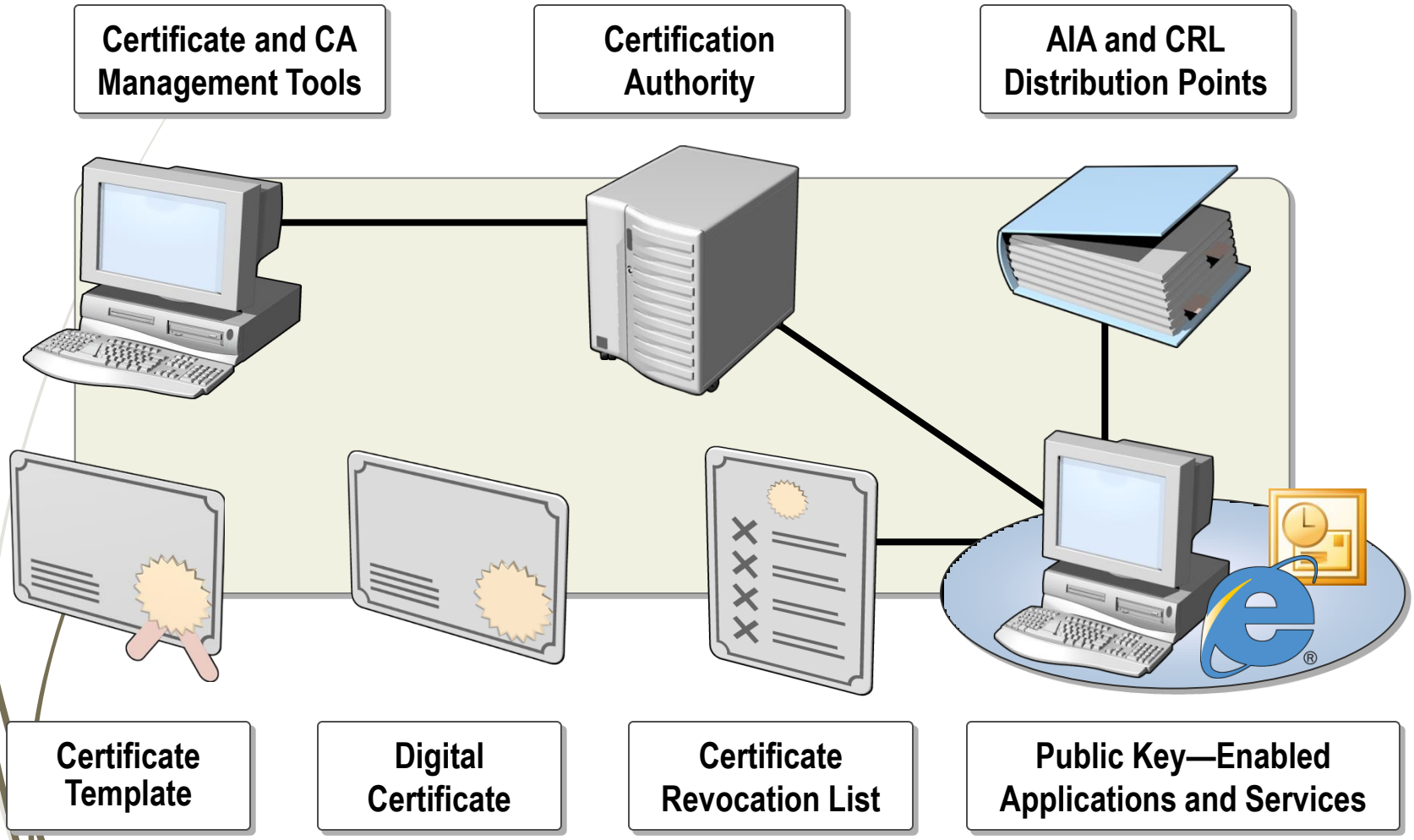


What Is a PKI?

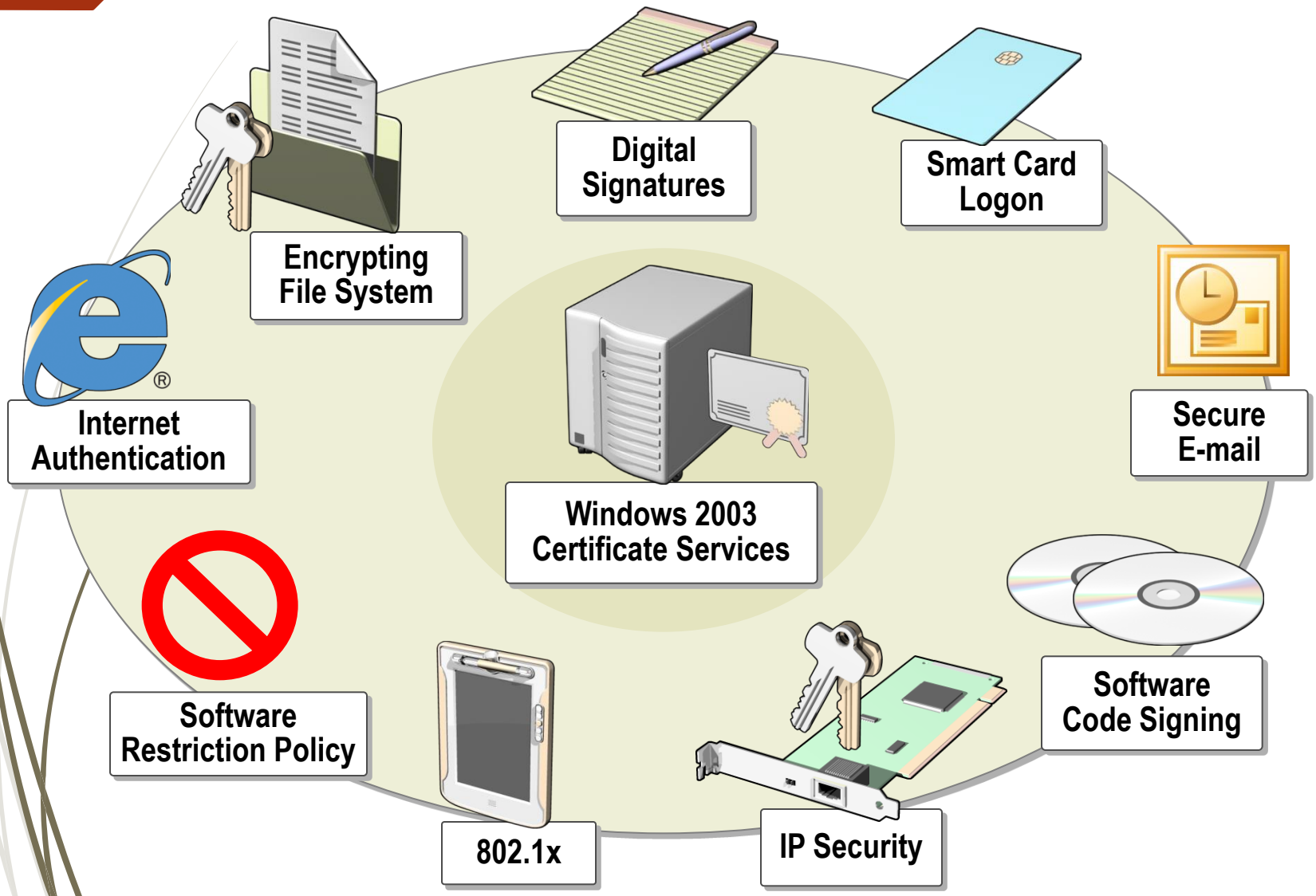
The combination of software and encryption technologies that helps to secure communication and business transactions

Requirement	PKI solutions
Confidentiality	**Data encryption**
Integrity	**Digital signatures**
Authenticity	**Hash algorithms, message digests, digital signatures**
Nonrepudiation	**Digital signatures, audit logs**
Availability	**Redundancy**

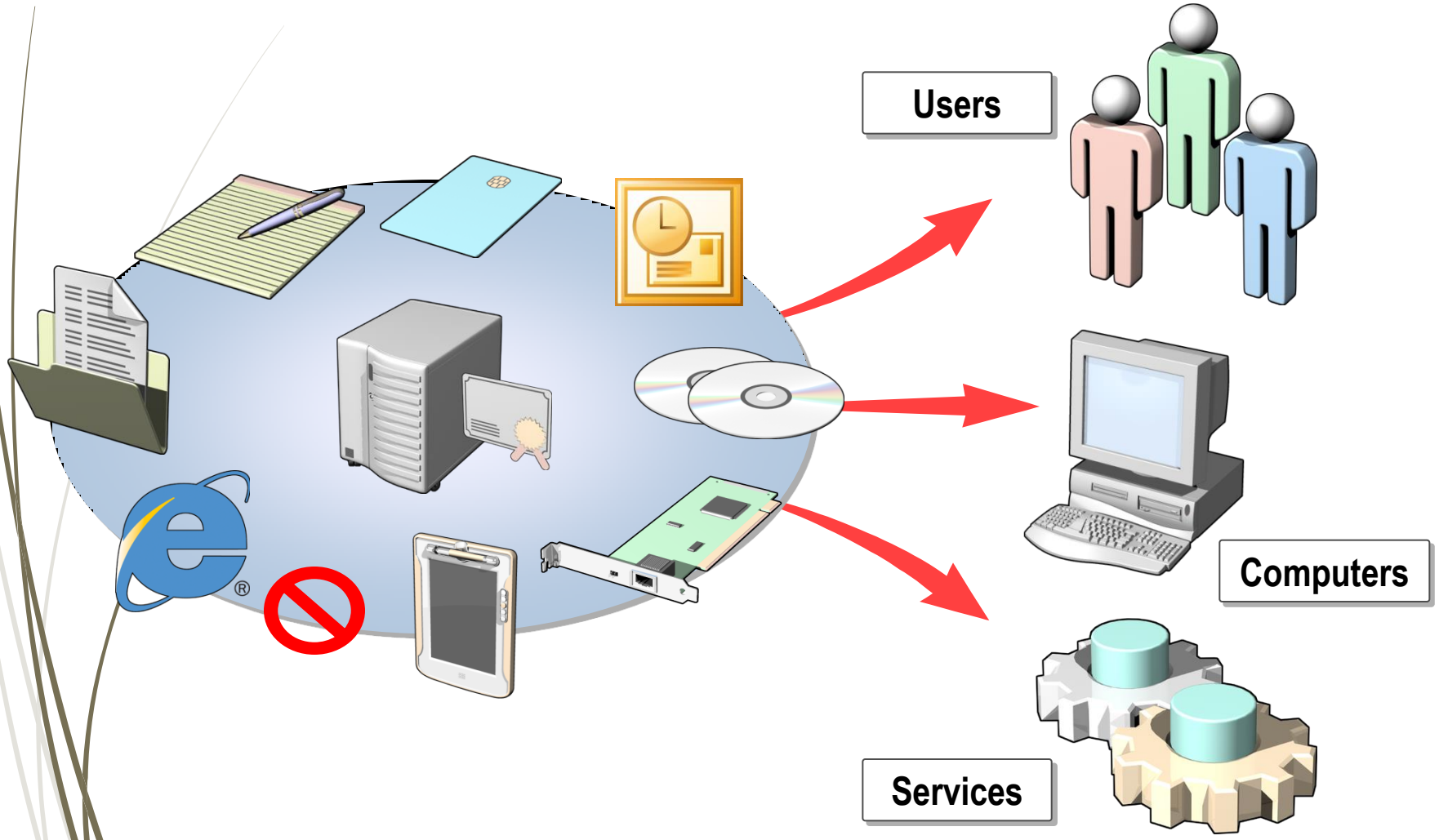
Components of a PKI



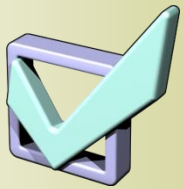
Applications That Use a PKI



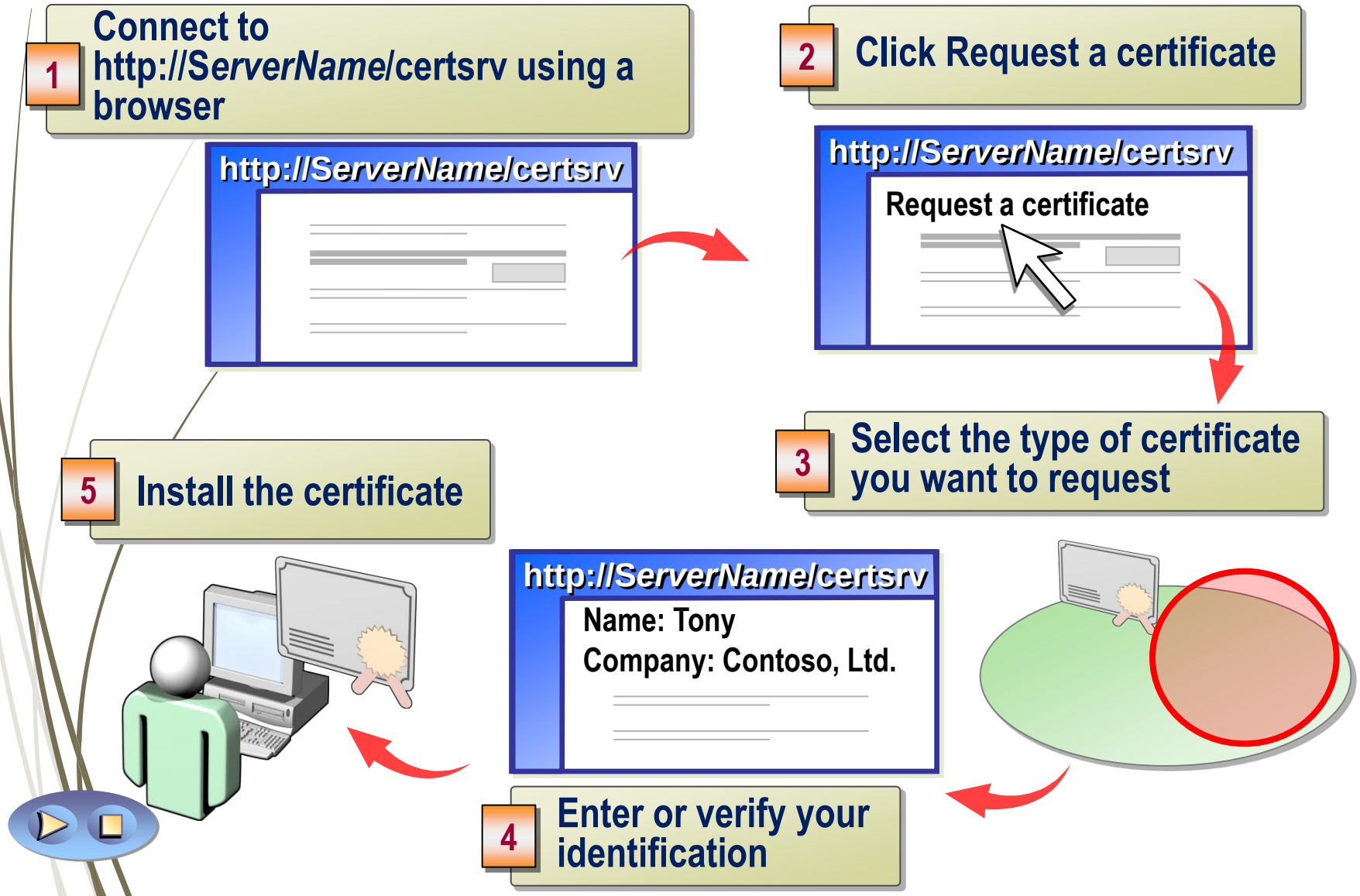
Accounts That Use PKI-Enabled Applications



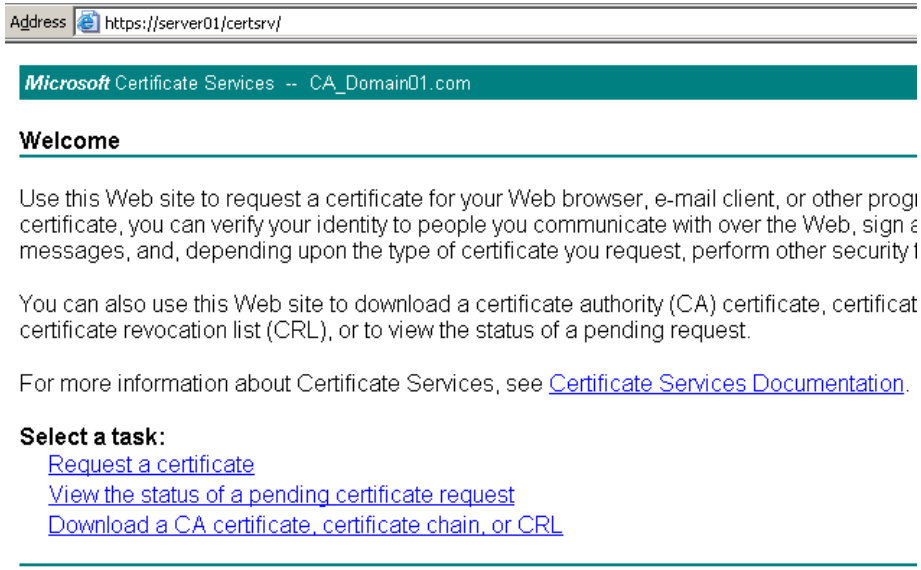
How Applications Check Certificate Status

Process	Action
 Certificate discovery	1 **Collects CA certificates from cache, Group Policy, enterprise policy, applications, and AIA URLs**
 Path validation	2 **Validates the certificates in a certificate chain until the certificate chain terminates at a trusted, self-signed certificate**
 Revocation checking	3 **Ensures that no certificates have been revoked**

Certificate Enrollment Using a Web-Based Interface

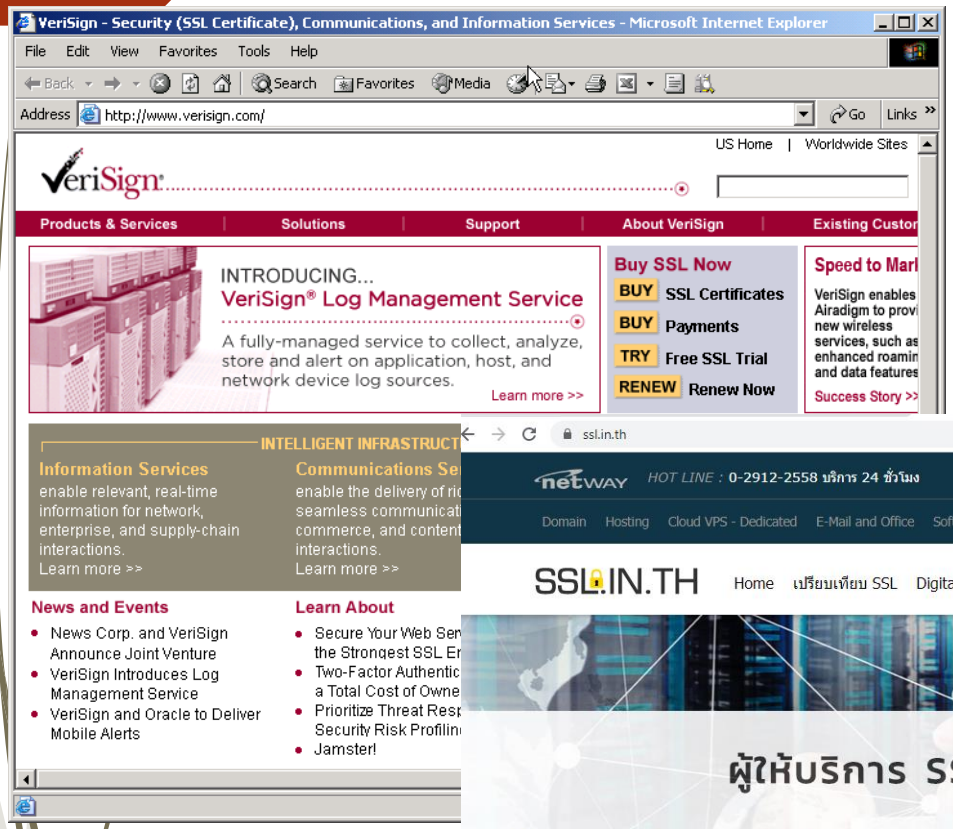


Client Certificate Enroll

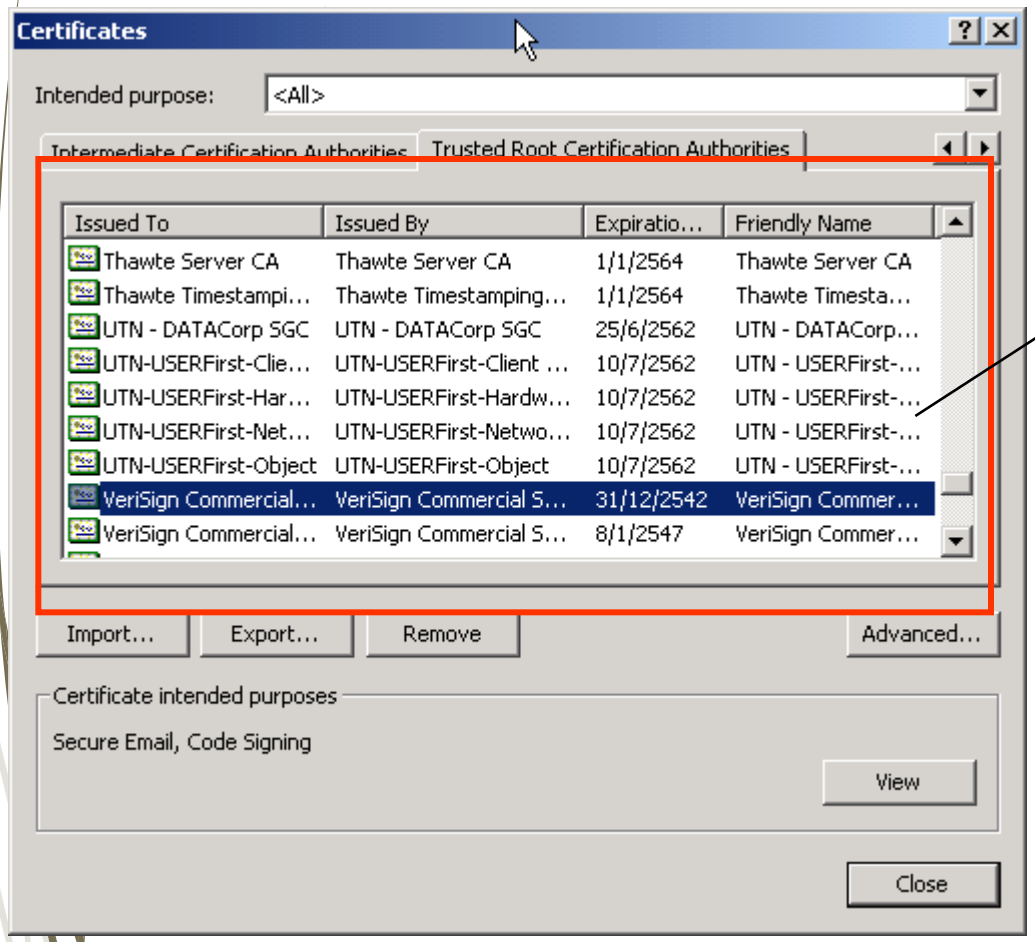


- By Use IE > http or https:\\CAServerName\certsrv
- Log in ต้องการให้ user คนไหนลงทะเบียน
- Request Register > Next ไปเรื่อย จะให้ติดตั้ง

CA Commercial



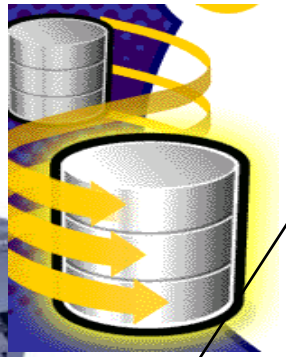
Why we use HTTPS automatic..



Certification installs already when u install windows….

Overview: CA Commercial

CA Commercial



User	Private	Public
IE User	??	yellow
Webserver	??	Red
CA	??	Blue

Session Key

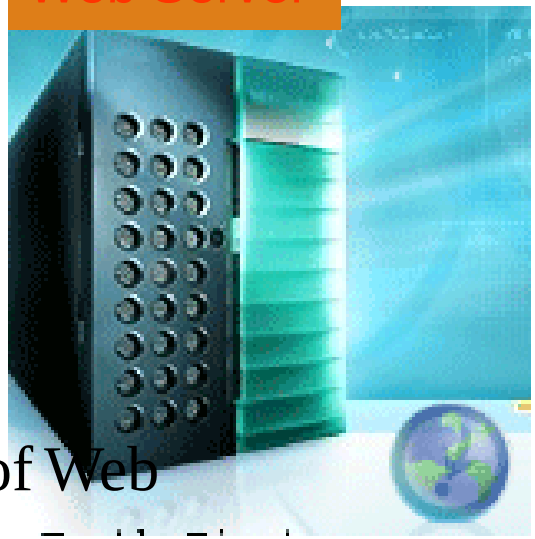
Computer

=Blue (Pub of CA)

=Red (Pub of Web)

=Private of Web

Web Server



Chapter 12

IDS & IPS

IDS & IPS

- เปรียบเสมือน เป็น รปภ ที่ทำการตรวจตราดูเหตุการณ์ผิดปกติที่อยู่ภายใน ซึ่ง กรณีที่เป็น **IDS** จะทำการตรวจตา และทำการแจ้งเตือนเท่านั้น แต่ถ้าเป็น **IPS** จะทำการตรวจตา และ ทำการบล็อก หรือขจัดปัญหา ทันที.....

IDS > Intrusion Detection System
IPS > Intrusion Prevention System

Mode ของ IDS

- **Notification >** ทำการแจ้งเตือน
- **Shunning >** ไม่แจ้งเตือน เพราะรู้ว่าโจมตีไปก็เท่านั้น
- **Deception >** ล่อให้ไป **Honey Pot**

  (ดูพฤติกรรมของ Hacker ว่าจะทำอย่างไรต่อไป)

Mode ของ IPS

- **Session Termination > ยกเลิก Session ที่โจมตี**
- **Network Configuration > ทำการปรับเปลี่ยนค่า Network Config (Firewall etc.)**
- **Deception > ล่อไปที่ Honey Pot**

ชนิดของ IDS & IPS

- มีทั้ง software based และ hardware based
- Network Base/Host Base
- ชนิดของ IDS/IPS
  - Signature-base IDS/IPS
  - Anomaly/Statistically IDS/IPS
  - Artificial Intelligence IDS/IPS

การทำงานของ IDS & IPS

- จะทำการตรวจสอบ **Packet** ที่มีการวิ่งผ่านเครื่อง โดยจะทำการอ่านเป็น **pattern** หรือ **signature** ว่าตรงกับเงื่อนไขที่ระบุเข้าข่ายผิดปกติ

  - ระบบเครือข่ายทำงานช้าลง

- **IDS** ต้องทำงานรวดเร็วเพราะต้องดู **Packet** ทั้งหมด

- **Harddisk** ต้องขนาดใหญ่เพื่อทำการเก็บ **Log**

  - ต้องมีกฎในการกรอง และหมั่น **update** อยู่เสมอ

Example IDS (Software)

OSSEC

SNORT®

Example IDS (Hardware)

Chapter 13

WINDOWS BEST PRACTICE

Components of Client Computer Security

Client Security Defense In Depth	
Software Updates	Apply software updates to keep systems current
Password Best Practices	Use strong passwords across systems to restrict access
Data Protection	Back up, encrypt, and restrict access to data
Application Security	Deploy, configure, and restrict application software installation
Client Management	Use Active Directory, templates, and policies to enforce security
Mobile Computing	Implement policies and technologies to secure remote and wireless access
Antivirus / Anti-spyware	Install and maintain antivirus software to help protect against malicious code
Personal Firewalls	Configure hardware devices and/or software to help protect perimeter

Hot Fixes, Service Pack, Patches

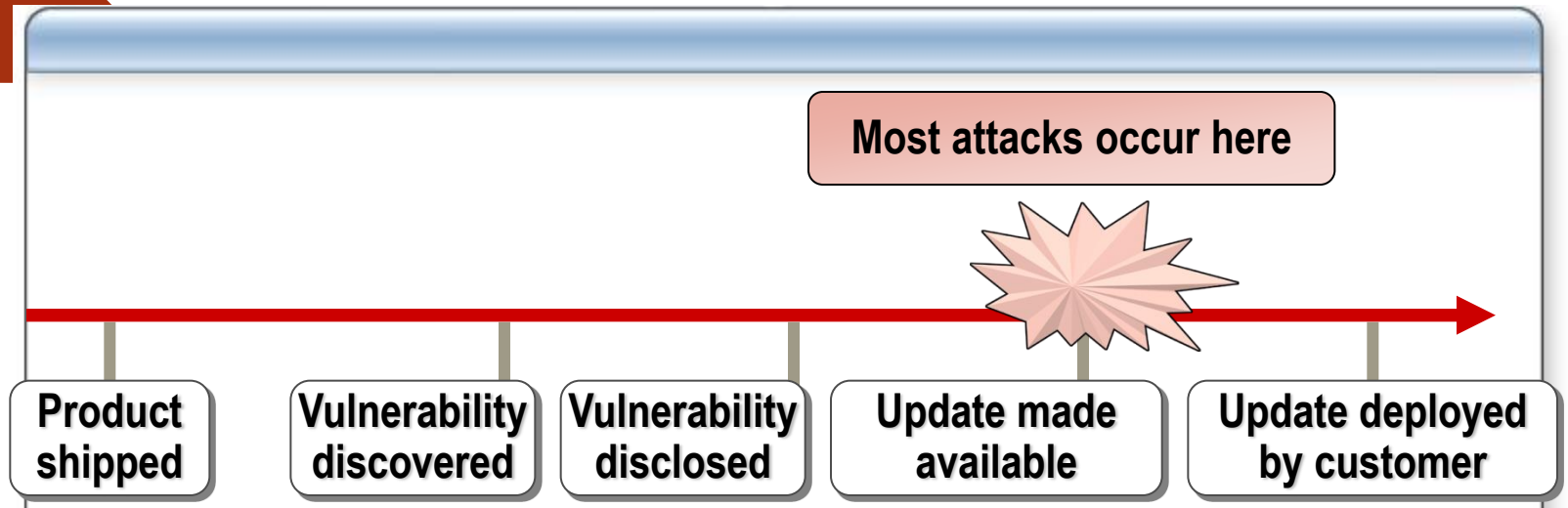
- **Hot Fixes >** ออกมา **Realtime Order** เพื่อแก้ไขหรือ **repair** อุดช่องโหว่ที่เกิดขึ้น
- **Service Pack > Set of Hot Fixes**
- **Patches > Temporary Quick Fixes > Skip MalFunction**

Benefits of Update Management

Benefits of effective update management include:

- Reduced down time
- Reduced cost
- Reduced data loss
- Increased protection of intellectual property

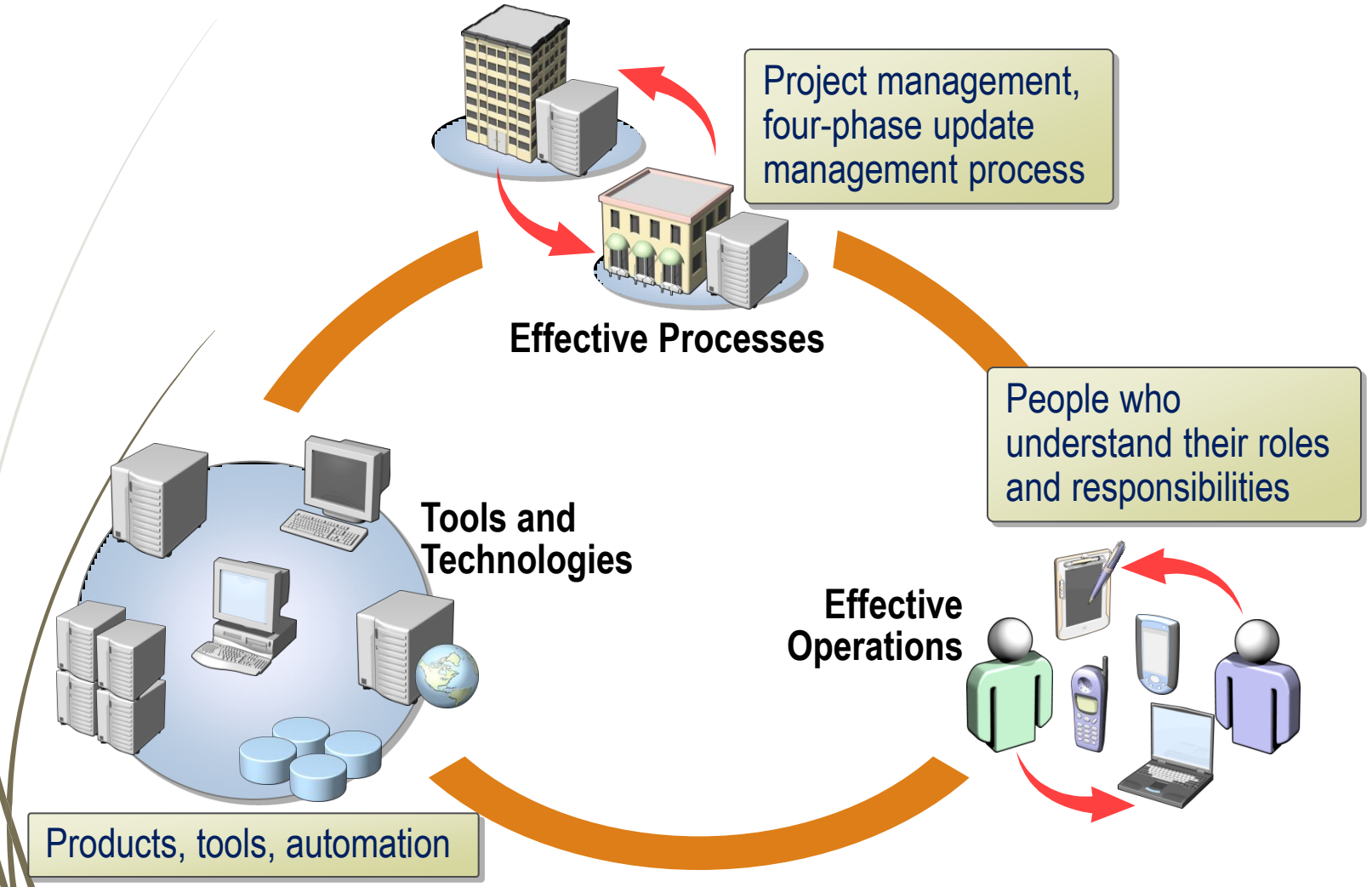
Software Vulnerability and Exploit Timelines



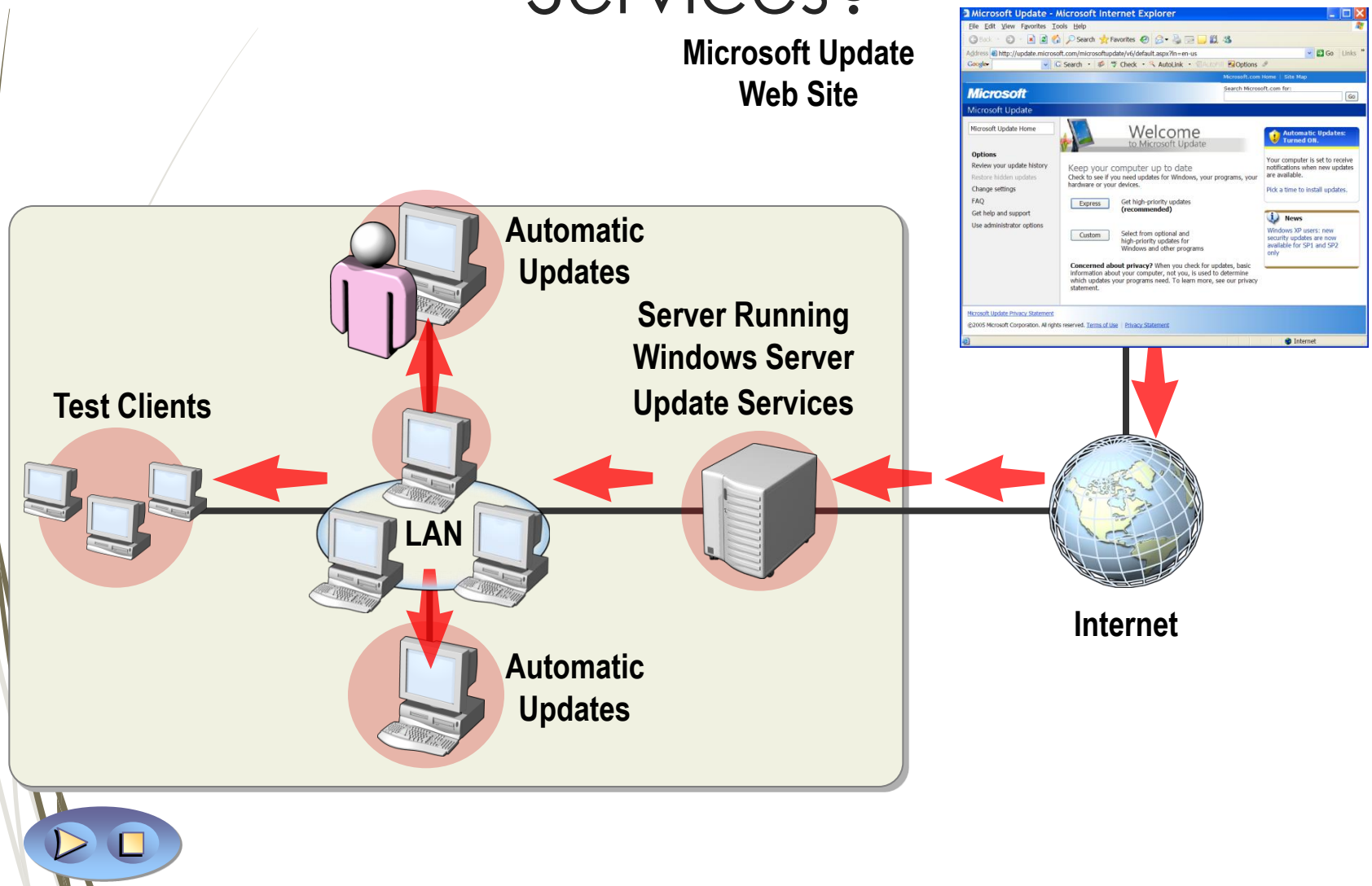
Malicious software attack	Days between update and exploit
Nimda	331
SQL Slammer	180
Welchia/Nachi	151
Blaster	25
Sasser	14

Days between update and exploit have decreased

Components for Successful Update Management



What Is Windows Server Update Services?



What Is Automatic Updates?

Automatic Updates is client software that:

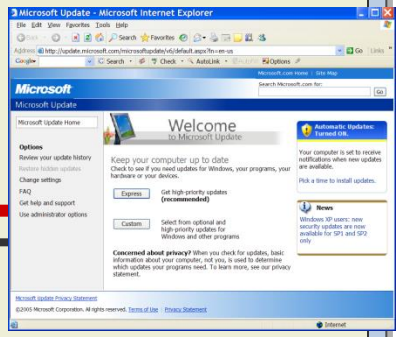
- **Communicates with Microsoft Update or WSUS**
- **Downloads and installs updates**

Configuration option	Description
Notify for download and notify for install	User is notified when updates are ready to be downloaded
Auto download and notify for install	User is notified when updates are ready to be installed
Auto download and schedule the install	Provides the ability to schedule the install

WSUS Process

Server-Side Process

1. WSUS runs scheduled synch



2. Testing?

Yes?

Test new packages

No?

3. Admin approves new packages

Client-Side Process

1. Automatic Updates on client checks WSUS

2. Is Administrator logged on?

Yes? Administrator sees status balloon, can defer installation

No?

3. Scheduled install job begins

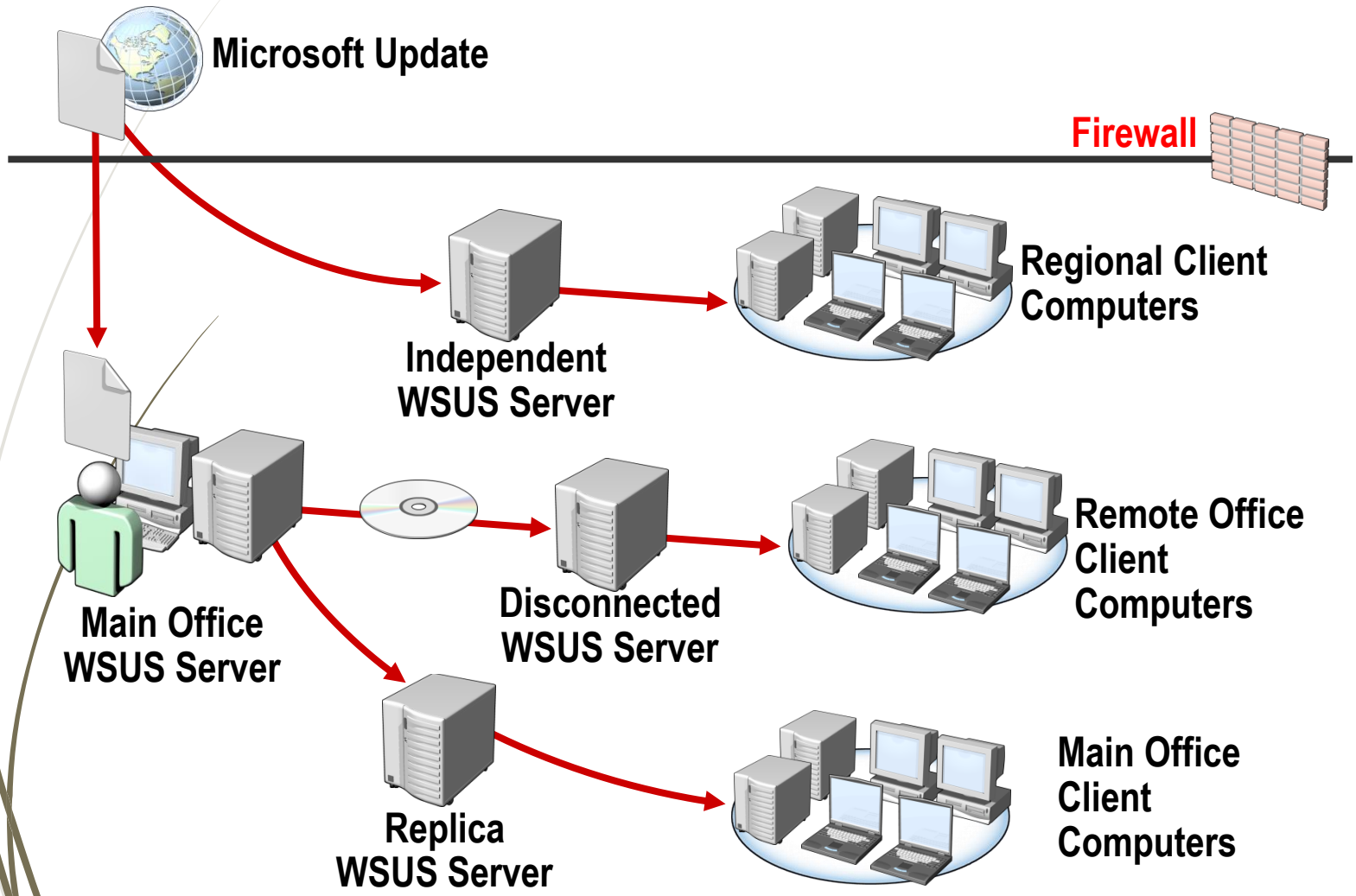
4. Do any packages require a restart?

Yes? System restart

No?

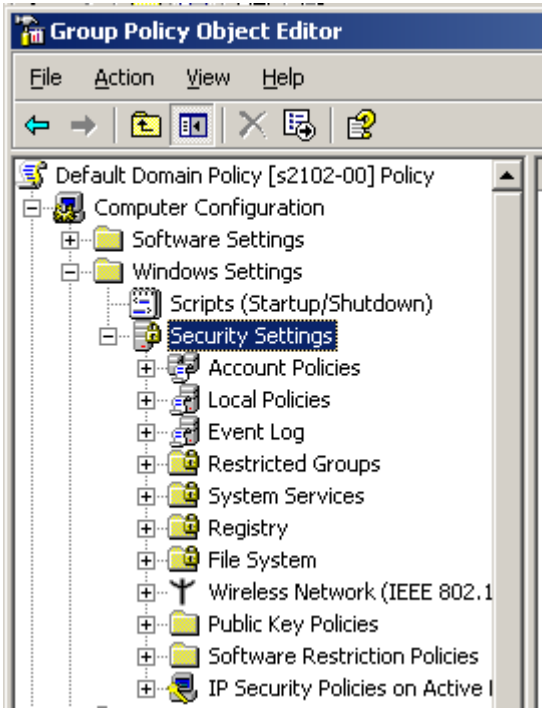
5. Automatic Updates waits for next scheduled check

WSUS Deployment Scenarios

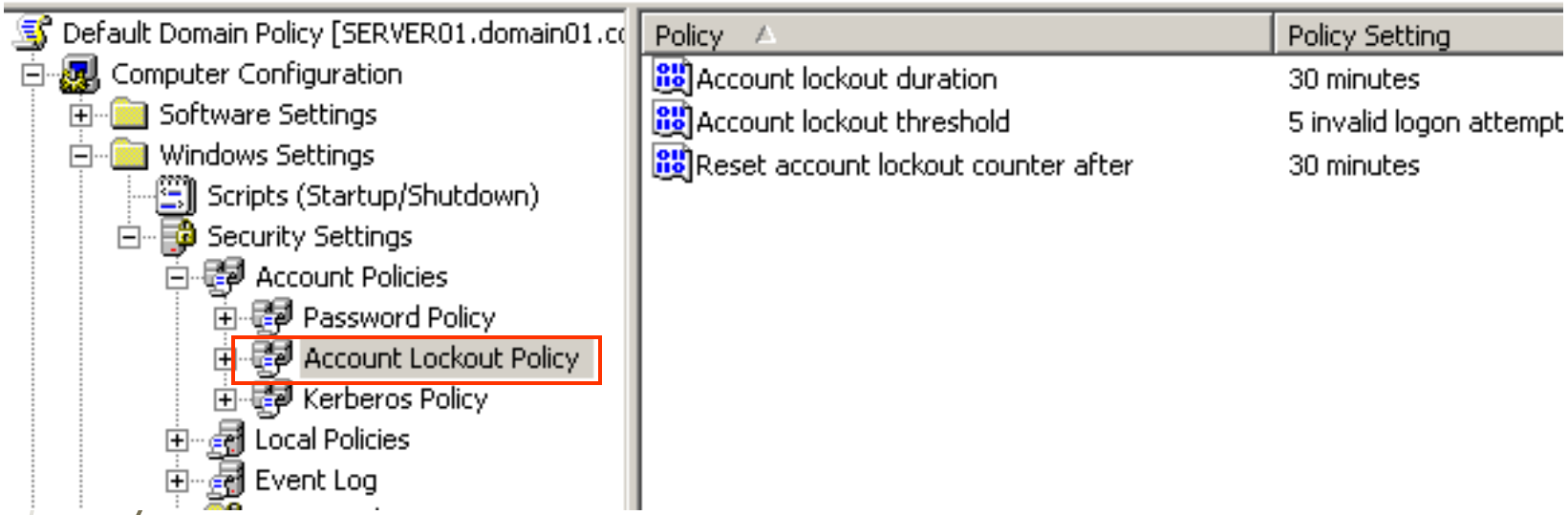


Security Settings

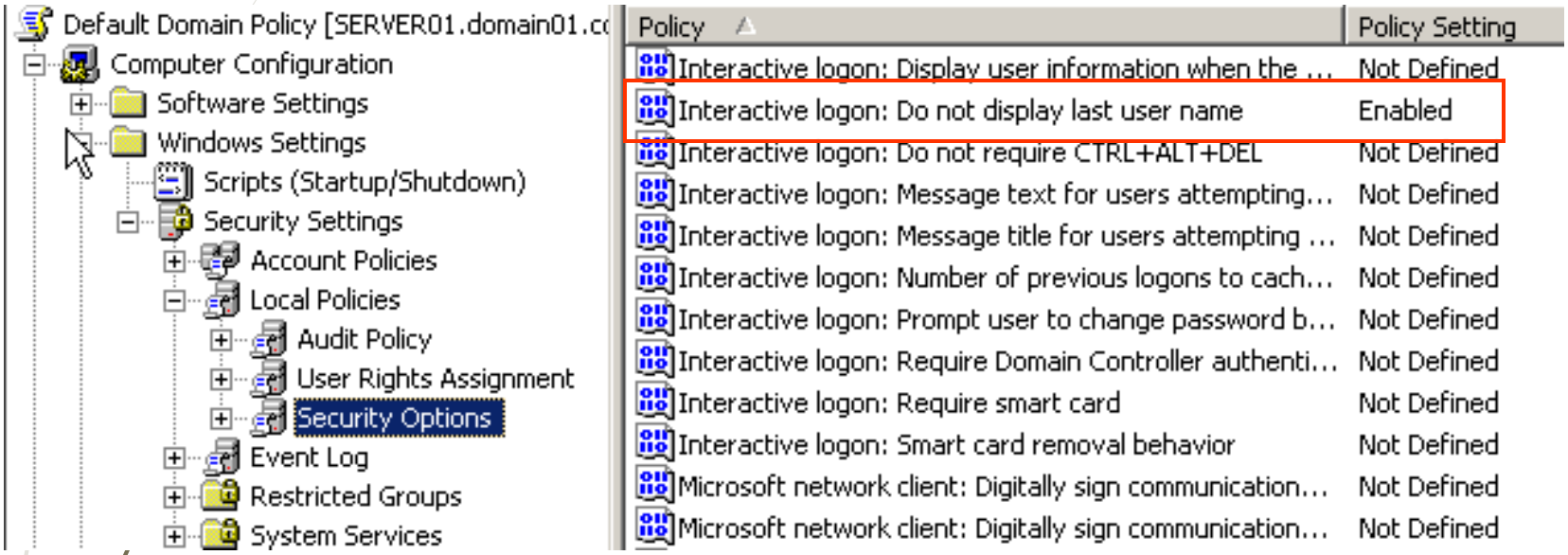
- มีการกำหนดสิ่งต่างๆดังนี้
  - Account Policies
  - Local Policies
  - Event Log
  - Restricted Groups
  - System Services
  - Registry
  - File System
  - Wireless Network (IEEE 802.11) Policies
  - Public key policies
  - Software Restriction Policies
  - IP Security Policies



Example Policy: Set Account Lockout



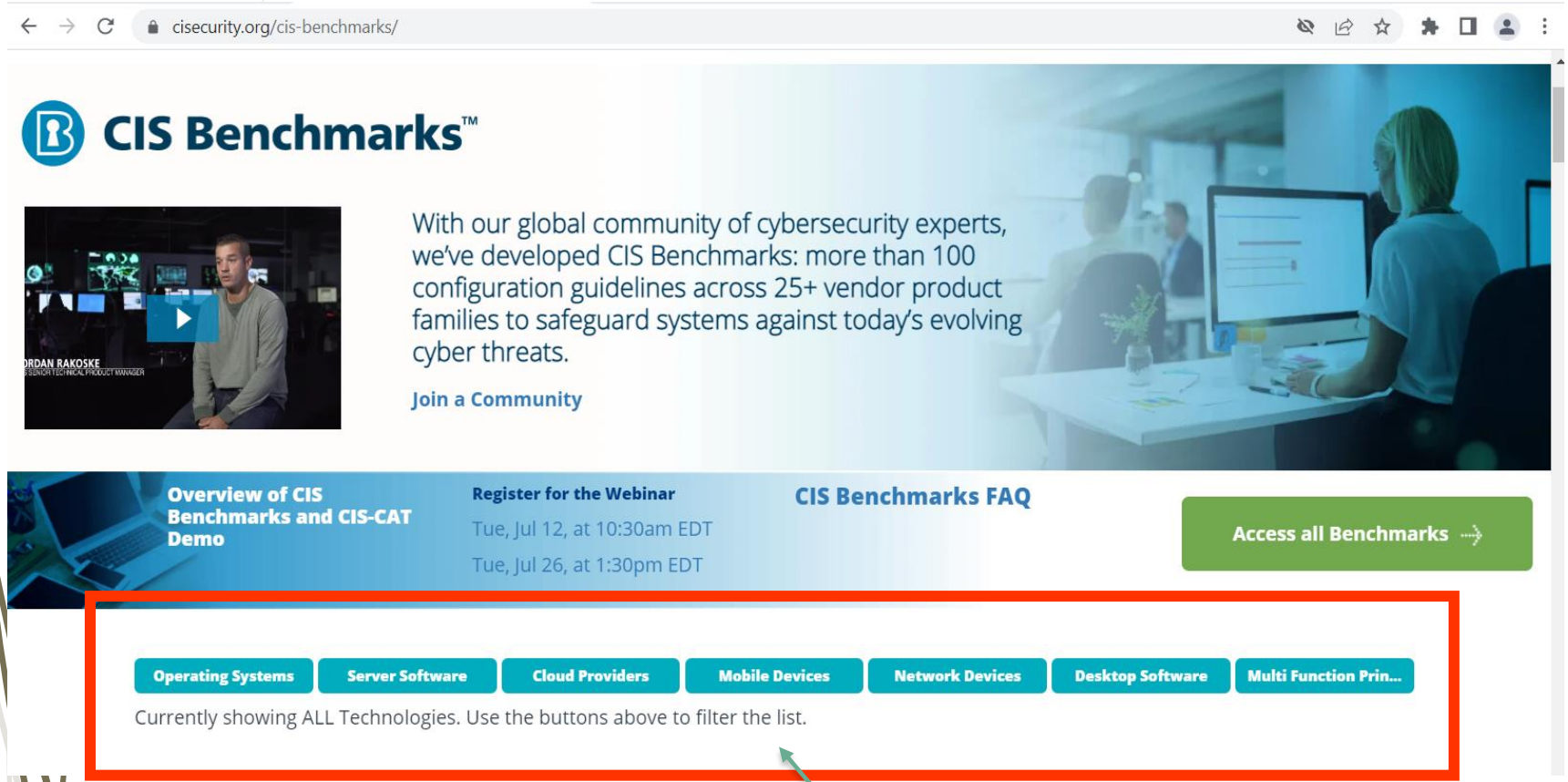
Example Policy: Don’t Display Last username



สิ่งที่ควรปฏิบัติสำหรับ Software Restriction Policies

- สร้าง GPO แยกสำหรับ Software Restriction Policies
- ทดสอบ Software Restriction policy ก่อนที่กำหนดในคอมพิวเตอร์อื่นๆ
- ถ้าต้องการแก้ไข Software restriction policy ให้กำหนดไม่อนุญาตก่อน
- ถ้ามีปัญหาในการกำหนดนโยบายให้บูตเลือกเป็น Safe mode
- ถ้าเกิดมีการล็อคเครื่องทำงานกับ Software Restriction Policies ให้เลือกบูตเป็น Safe mode และล็อกออนด้วย Administrator ที่เครื่องแก้ไขนโยบาย และรัน Gpupdate.exe, รีบูต และล็อกออนใหม่
- ใช้ Software restriction policies ในจุดต่อกับการกำหนด Access Control settings
- ใช้ Caution เมื่อมีการกำหนด Default setting เป็น Disallowed

www.cisecurity.org/benchmark.html



Benchmark

Chapter 14

WIRELESS BEST PRACTICE

What Are the Benefits of Wireless Networks?

Business benefits

- Mobile users save time and effort a with transparent connection to the corporate network
- Users can use e-mail, electronic calendars, and chat technologies when away from their desks

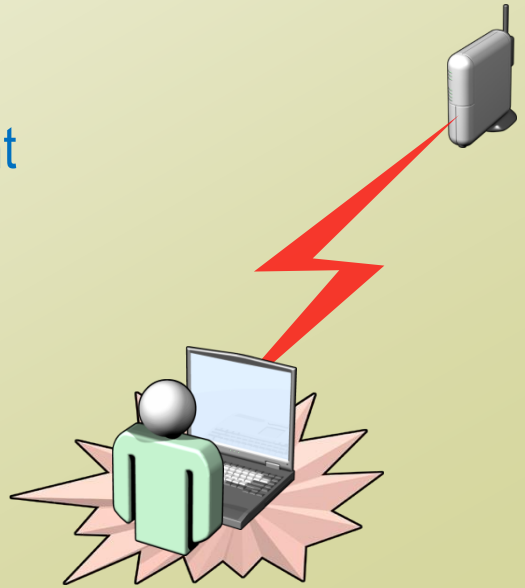
Operational benefits

- The cost of provisioning network access to buildings is substantially lowered
- The network can be easily scaled to respond to different levels of demand when the organization changes

Threats to Wireless Network Security

Security threats include:

- Disclosure of confidential information
- Unauthorized access to data
- Impersonation of an authorized client
- Interruption of the wireless service
- Unauthorized access to the Internet
- Accidental threats
- Unsecured home wireless setups
- Unauthorized WLAN implementations



Wireless Network Standards

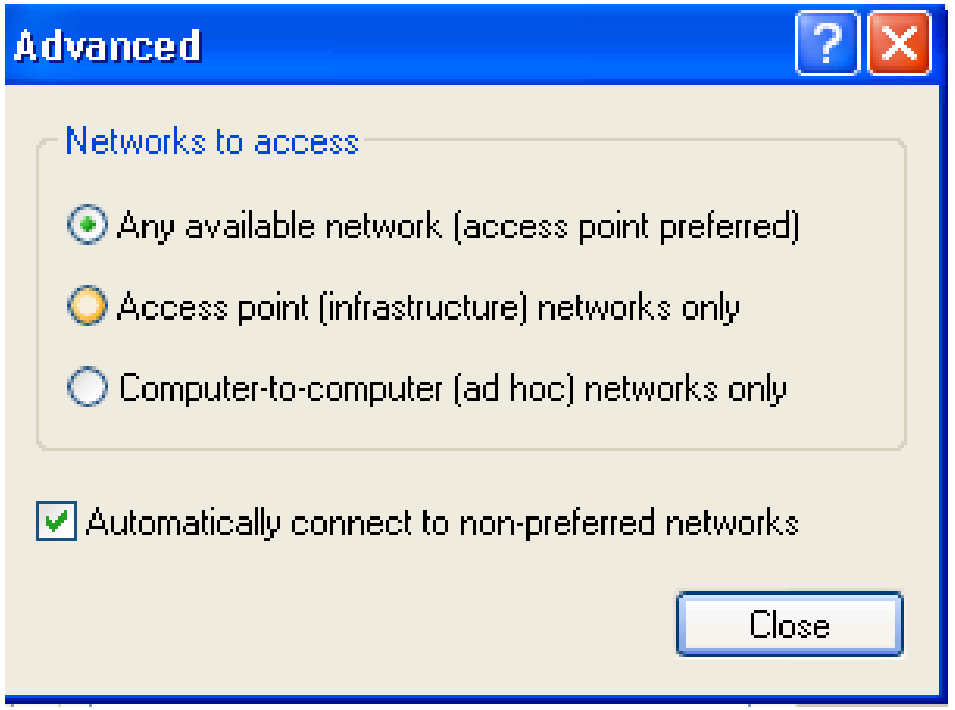
IEEE Standard	Frequency	Maximum Bandwidth
802.11a	5 GHz	54 Mb/s
802.11b	2.4 GHz	11 Mb/s
802.11g	2.4 GHz	54 Mb/s
802.11n	2.4 GHz & 5 GHz	600 Mb/s
802.11ac	5 GHz	7 Gb/s

802.1X*:* Defines a port-based access control mechanism of authenticating access to a network and for managing keys used to protect traffic

IEEE 802.11

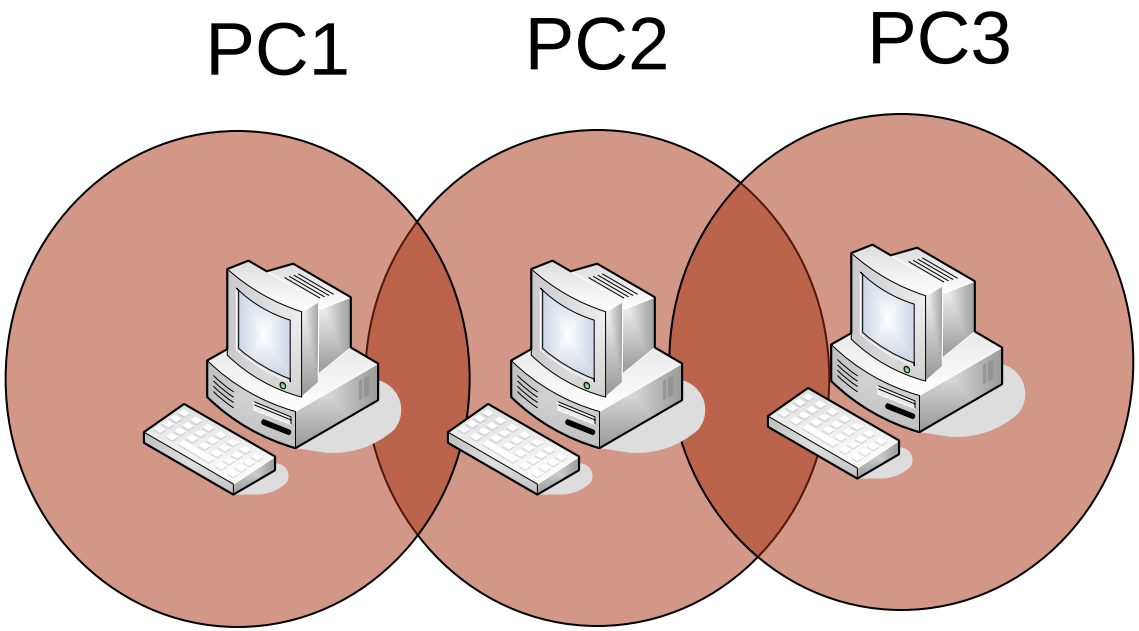
- 802.11 ติดต่อที่ 2 MBps ที่ 2.4GH
- 802.11a ติดต่อที่ 54 MBps ที่ 5 GH
- 802.11b ติดต่อที่ 11 MBps ที่ 2.4GH
- 802.11g ติดต่อที่ 54 Mbps ที่ 2.4 GH
- 802.11n > 600 Mbps
- 802.11AC >>
- 802.11AX >>

802.11 > WiFi

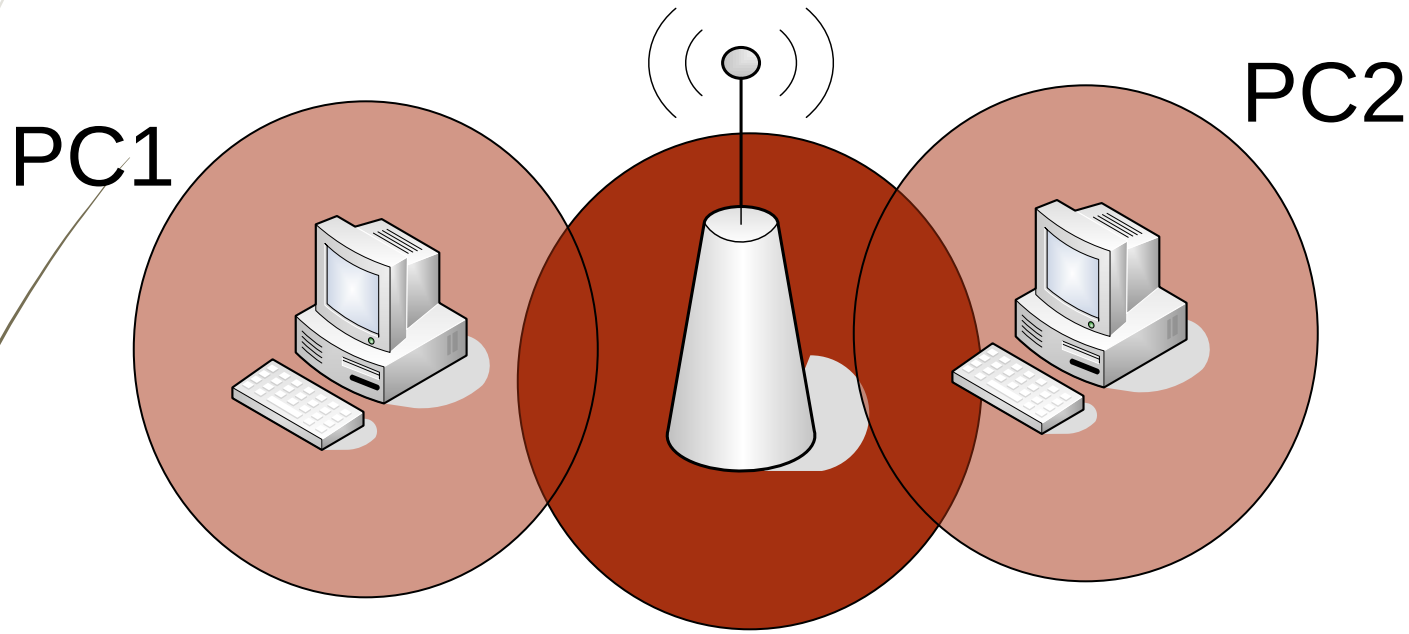


- มีอยู่สองโหมด
  - Adhoc
  - Infrastructure
- สิ่งที่จำเป็นสำหรับการติดตั้ง
  - SSID
  - Network Key (Security) > WEP (Wired Equivalent Protocol)
  - Authentication
  - Encryption

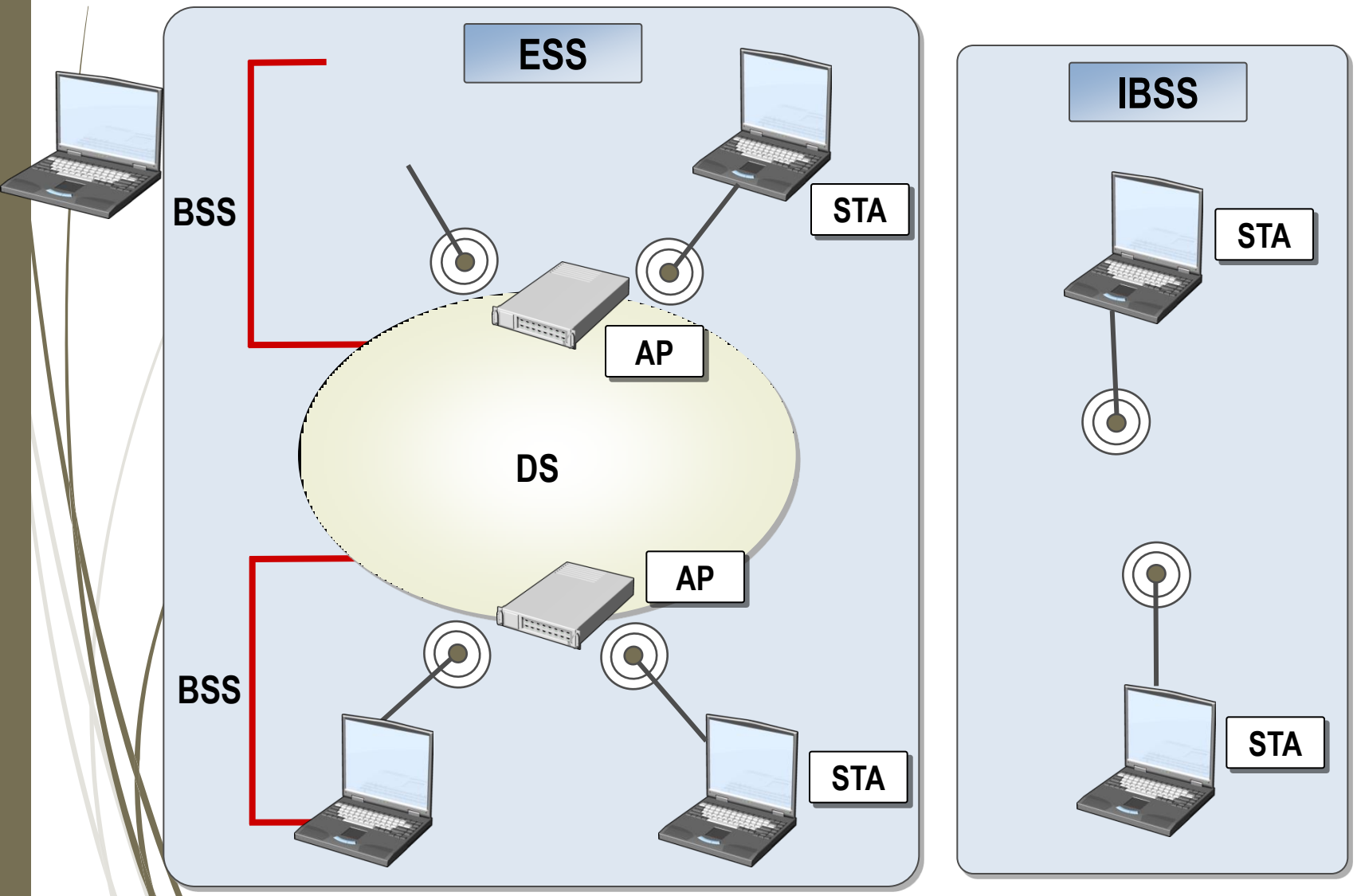
Adhoc



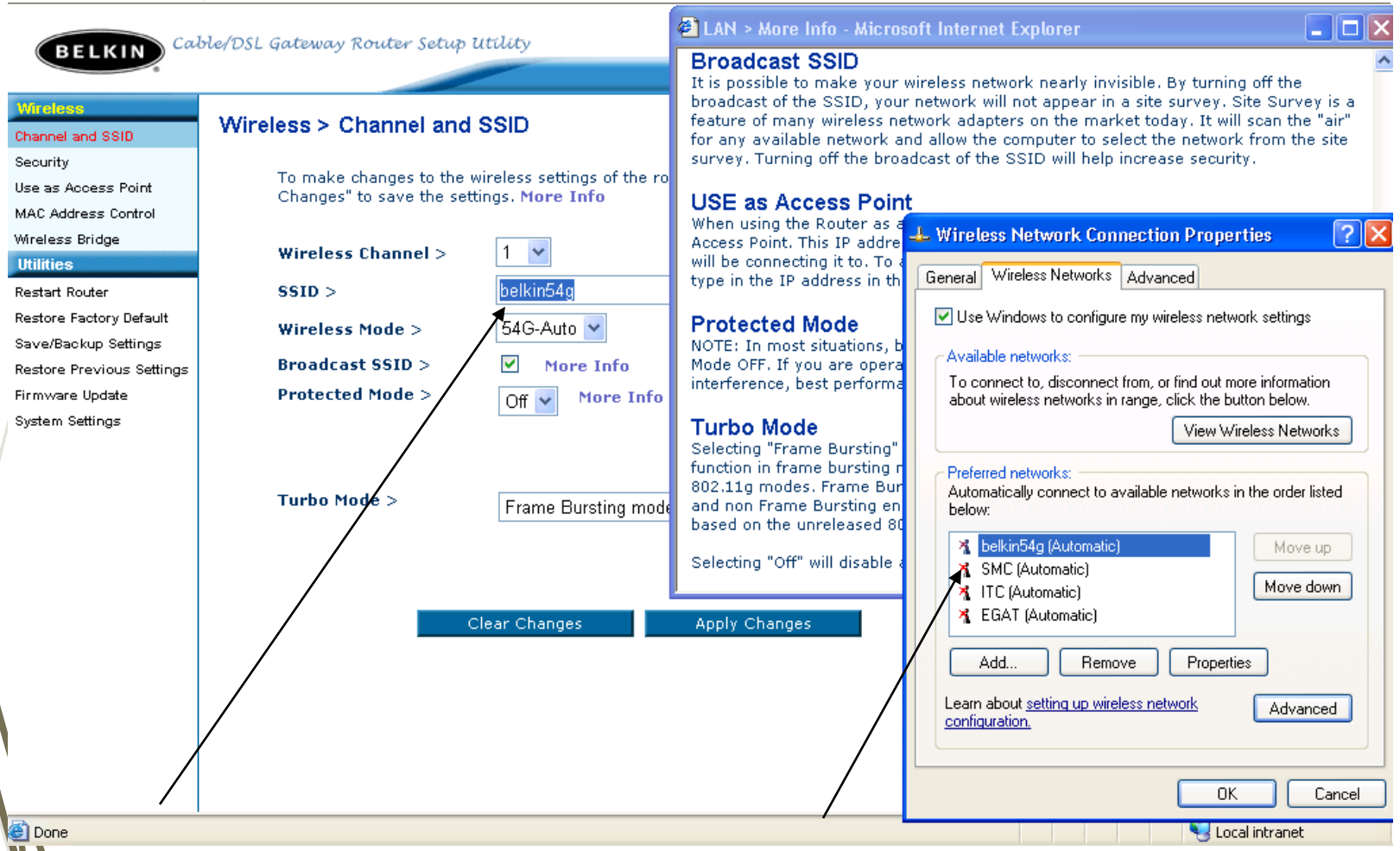
Infrastructure



Wireless Network Architecture

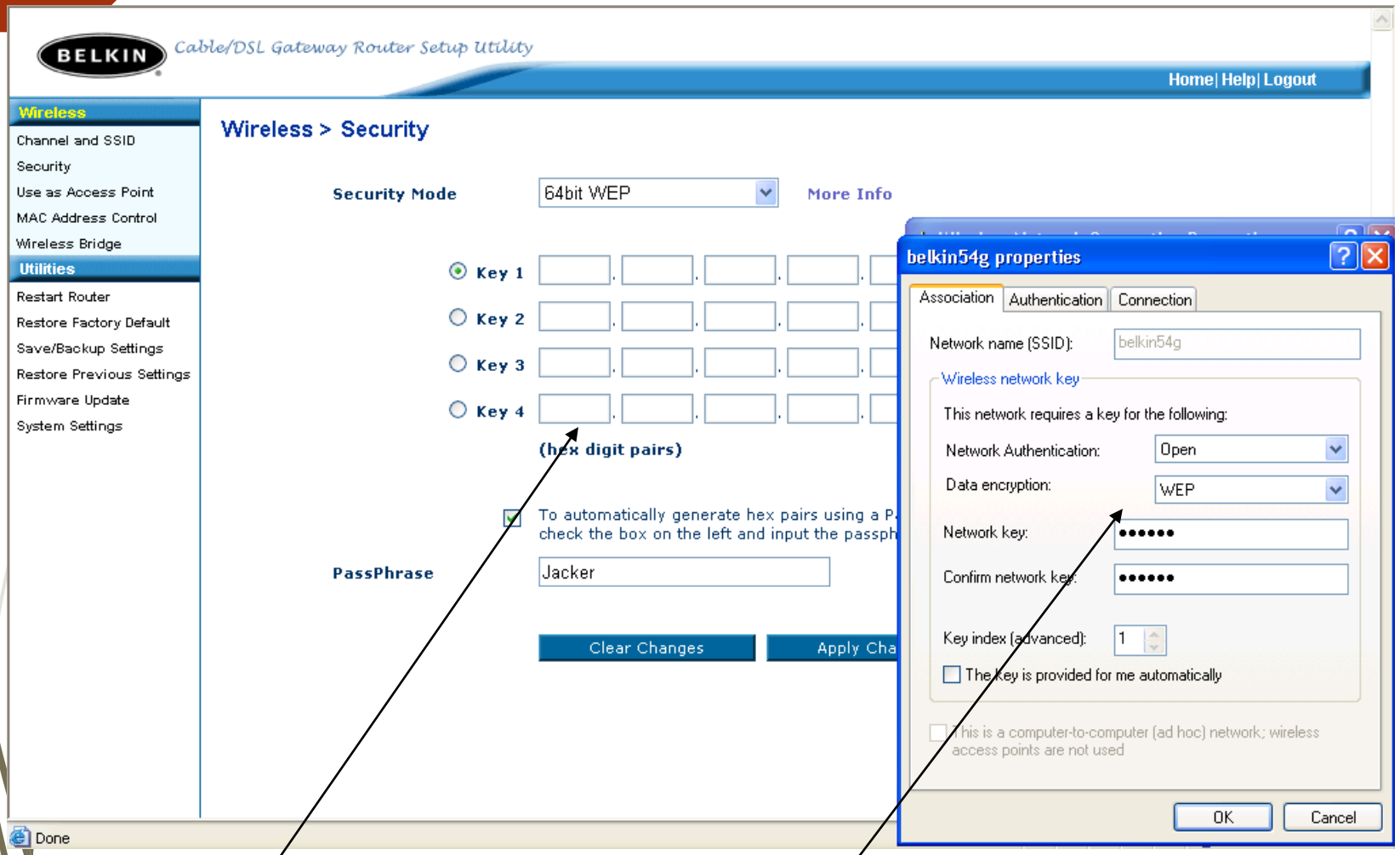


SSID



Access Point Computer

WEP

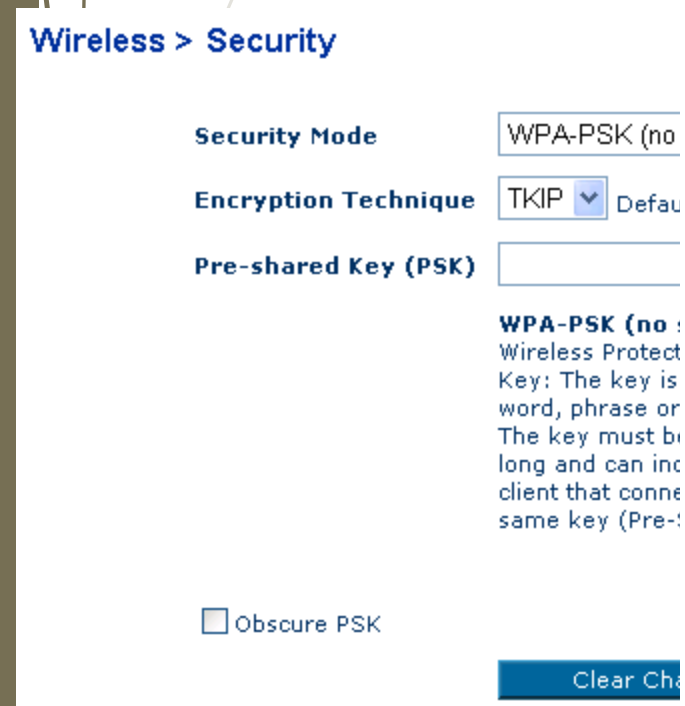


Access Point

Computer

WPA

ปลอดภัยผู้ใช้ต้องล็อกออนผ่าน RADIUS Server หรือ No RADIUS



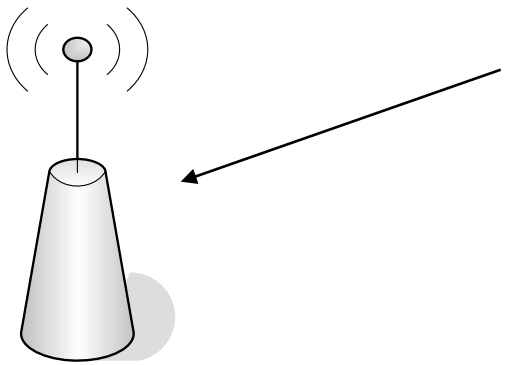
เพิ่มความปลอดภัยใน Wireless ด้วย MAC Address List

Wireless > MAC address control

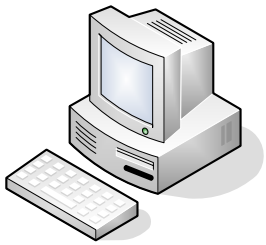
Mac Address Control is the ability to set up a list of clients that you want to allow or deny access to the wireless network.

◉ Allow ○ Deny ○ Disable

00:10:11:15:55



เข้าใช้งานได้เพราะมีค่าในรายการ



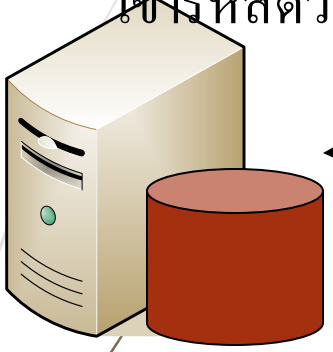
00:10:11:15:55

RADIUS Concept

Port 1812

ระบุหมาย IP Address (C>S, S>C)

เข้ารหัสด้วย Radius key

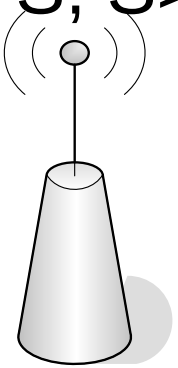


A

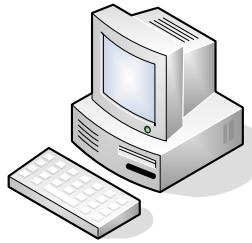
B

C

RADIUS Server

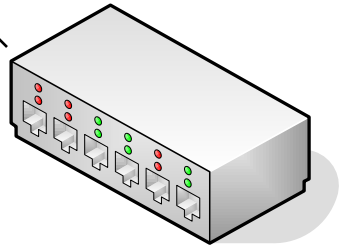


RADIUS Client

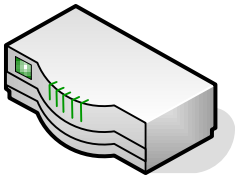


ระบุ User A

และรหัสผ่าน



RADIUS Client



RADIUS Client

Wireless Security..

- การไม่ **broad cast SSID**
- การใช้ **WPA v.2 (AES)** เพื่อนำมาทำการ **encryption**
- จำเป็นต้องมีการ **authentication** คือ ระบุ **user** และ **password** เพื่อทำการเข้าใช้

remark: ส่วนนี้ทาง **microsoft** กับ **Cisco** ตกลงกันเพื่อออก มาตรฐานกลาง **>>> Radius (microsoft** จะเปิด บริการที่ชื่อว่า **Radius server)**

>>>> จะเป็นในส่วนของการใช้ **standard >802.1X**

THANK YOU
Q & A