Security in Mind
(IT Security Awareness)

Kitisak Jirawannakool

E-Government Agency (Public Organization)

kitisak.jirawannakool@ega.or.th

Agenda

- What is EGA?
- ICT Law
- Trend 2016

Agreement

- Turn off your mobile phone or keep silent
- Stop me anytime, if you want to ask or share something
- Relax and feel free to discuss
- Keep in touch and keep sharing after class
- Be aware, but do not panic

Contact me

Name : Kitisak Jirawannakool

Facebook : http://www.facebook.com/kitisak.note

Email : kitisak.jirawannakool@ega.or.th

jkitisak@gmail.com

Weblog : http://foh9.blogspot.com

Twitter : @kitisak

#whoami

- Information Security Specialist at EGA
- OWASP Thailand Chapter Leader
- Certification and Award
  - COMTIA Security+
  - Asia Pacific Information Security Leader Achievements 2011 (ISLA) by (ISC)2
- Membership
  - APWG, ShadowServer, OWASP, MSCP, CSAThailand Chapter, MedSec

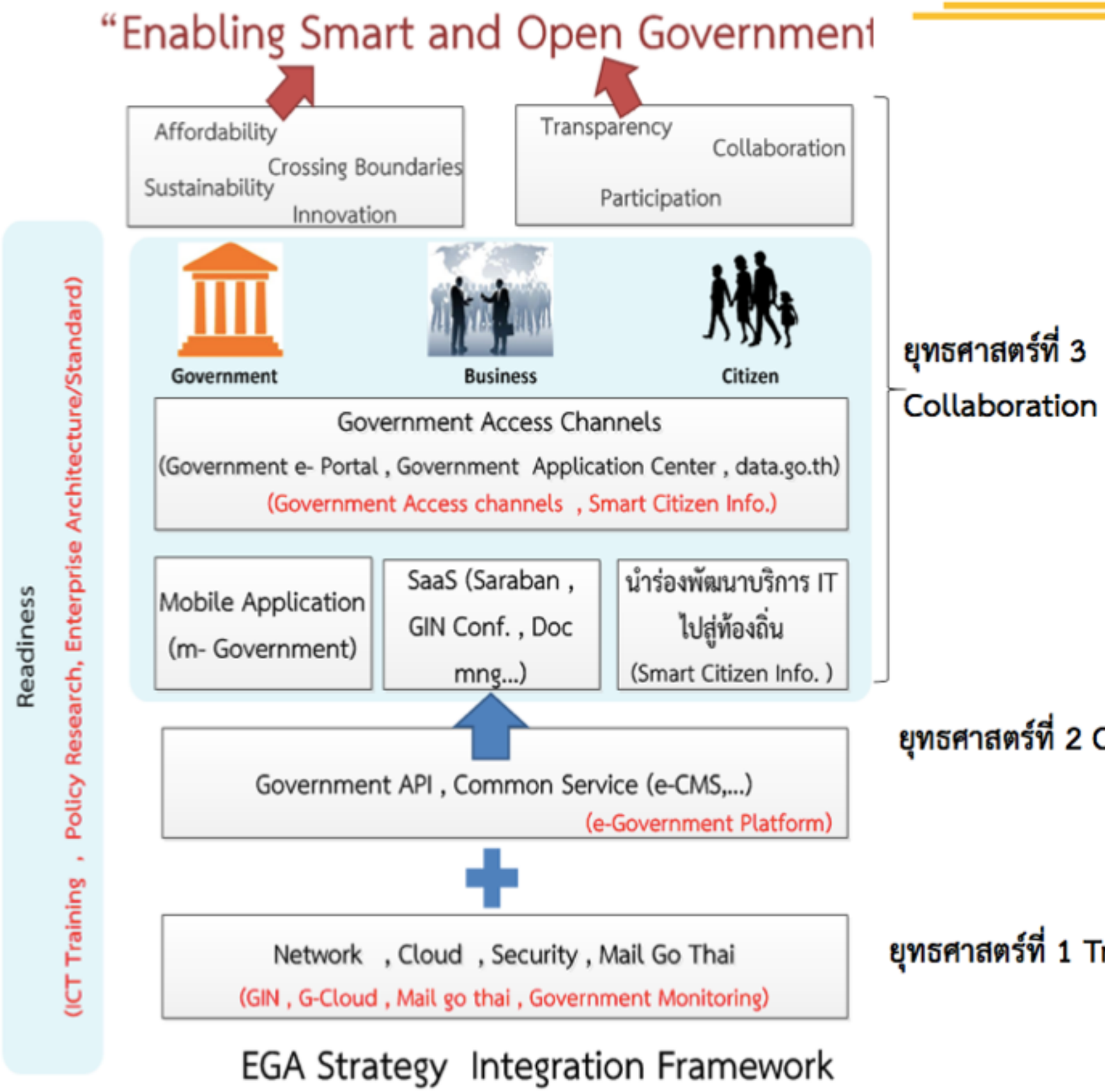
Of course, I am an anonymous cyclist, not hacker !!!!

About EGA

- First established in 1997 as Government Information Technology Services (GITS)
- ~ 200 staffs
- Services
  - Government Information Network (GIN)
  - Government Cloud Services (G-Cloud)
  - MailgoThai service
  - Government Computer Emergency and Readiness Team (G-CERT)
- More details : http://www.ega.or.th

EGA
e-Government Agency

G-CERT by EGA


"Enabling Smart and Open Government
Affordability
Crossing Boundaries
Sustainability
Innovation
Transparency
Collaboration
Participation
Government
Business
Citizen
Government Access Channels
(Government e- Portal , Government Application Center , data.go.th)
(Government Access channels , Smart Citizen Info.)
Mobile Application (m- Government)
SaaS (Saraban , GIN Conf. , Doc mng...)
นำร่องพัฒนาบริการ IT ไปสู่ท้องถิ่น
(Smart Citizen Info.)
Government API , Common Service (e-CMS,...)
(e-Government Platform)
Network , Cloud , Security , Mail Go Thai
(GIN , G-Cloud , Mail go thai , Government Monitoring)
Readiness
(ICT Training , Policy Research, Enterprise Architecture/Standard)
ยุทธศาสตร์ที่ 3
Collaboration
ยุทธศาสตร์ที่ 2 Connecting
ยุทธศาสตร์ที่ 1 Transformation
ยุทธศาสตร์ที่ 4
Readiness
EGA Strategy Integration Framework

G-CERT by EGA

Government Computer Emergency and Readiness Team (G-CERT)

- Risk Assessment
- Incident Monitoring
- Information Analysis
- Response Team
- Awareness Raising

E-

Services

M@il.Go.th
ระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ

Other Government's services

G-Cloud
Government Cloud Service

Cloud Provider

Inter Cloud

Cloud Provider

Cloud Provider

SaaS

PaaS

IaaS

GIN 2.0

GIN

Government Agency

Government Agency

EGA Contact Center
24x7 Helpdesk and Contact Center

IT Security Policy

นโยบายความปลอดภัยสารสนเทศ

- ข้อกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล
- การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ
- การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
- การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ
- การสำรองและกู้คืนข้อมูลระบบสารสนเทศ
- การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
- การปฏิบัติตามข้อกำหนด

นโยบายการเข้าถึงและการใช้งานระบบสารสนเทศ

- การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ
- การบริหารจัดการการเข้าถึงของผู้ใช้งาน
- การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
- การควบคุมการเข้าถึงเครือข่าย
- การควบคุมการเข้าถึงระบบปฏิบัติการ
- การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
- การบริหารจัดการการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
- การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

นโยบายการเข้าถึงและการใช้งานระบบสารสนเทศ

- การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่
- การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
- การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์
- การใช้งานระบบอินเทอร์เน็ต
- การใช้งานเครือข่ายสังคมออนไลน์

Computer Crime Law

Kitisak Jirawannakool

เหตุที่มาของพ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

- ลักษณะการกระทำความผิดที่ไม่ครอบคลุม
- พยานหลักฐานที่ต้องการจากเดิม
- พยานหลักฐานและแนวทางปฏิบัติในการรวบรวมพยานหลักฐาน

พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

- ความผิดใหม่ที่ถูกบัญญัติเพิ่ม
- พยานหลักฐาน และบุคคลที่เกี่ยวข้อง
- เจ้าหน้าที่และอำนาจดำเนินการ

ลักษณะความผิดที่ถูกบัญญัติไว้ตาม พ.ร.บ.

- ความผิดที่เกี่ยวกับระบบคอมพิวเตอร์และสารสนเทศ
- ความผิดที่เกี่ยวกับการเผยแพร่เนื้อหา
- ความผิดเกี่ยวกับผู้ให้บริการ
- ความผิดเกี่ยวกับการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่

ความผิดที่เกี่ยวข้องโดยตรงกับระบบสารสนเทศ

- การเข้าถึงระบบและข้อมูลคอมพิวเตอร์โดยมิชอบ
- การเปิดเผยมาตรการป้องกันระบบ
- การแก้ไข เปลี่ยนแปลง ข้อมูลคอมพิวเตอร์โดยมิชอบ
- การดักรับข้อมูลทางอิเลคทรอนิคส์
- การรบกวนระบบคอมพิวเตอร์
- การส่งข้อมูลอิเลคทรอนิคส์รบกวนการใช้งาน

นิยาม : ระบบคอมพิวเตอร์

“ระบบคอมพิวเตอร์”

อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

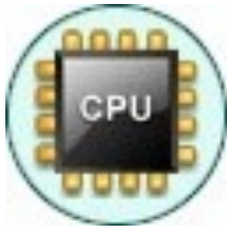
อะไรบ้างที่เป็นระบบคอมพิวเตอร์ (1)

อะไรบ้างที่เป็นระบบคอมพิวเตอร์ (2)

อะไรบ้างที่เป็นระบบคอมพิวเตอร์ (3)

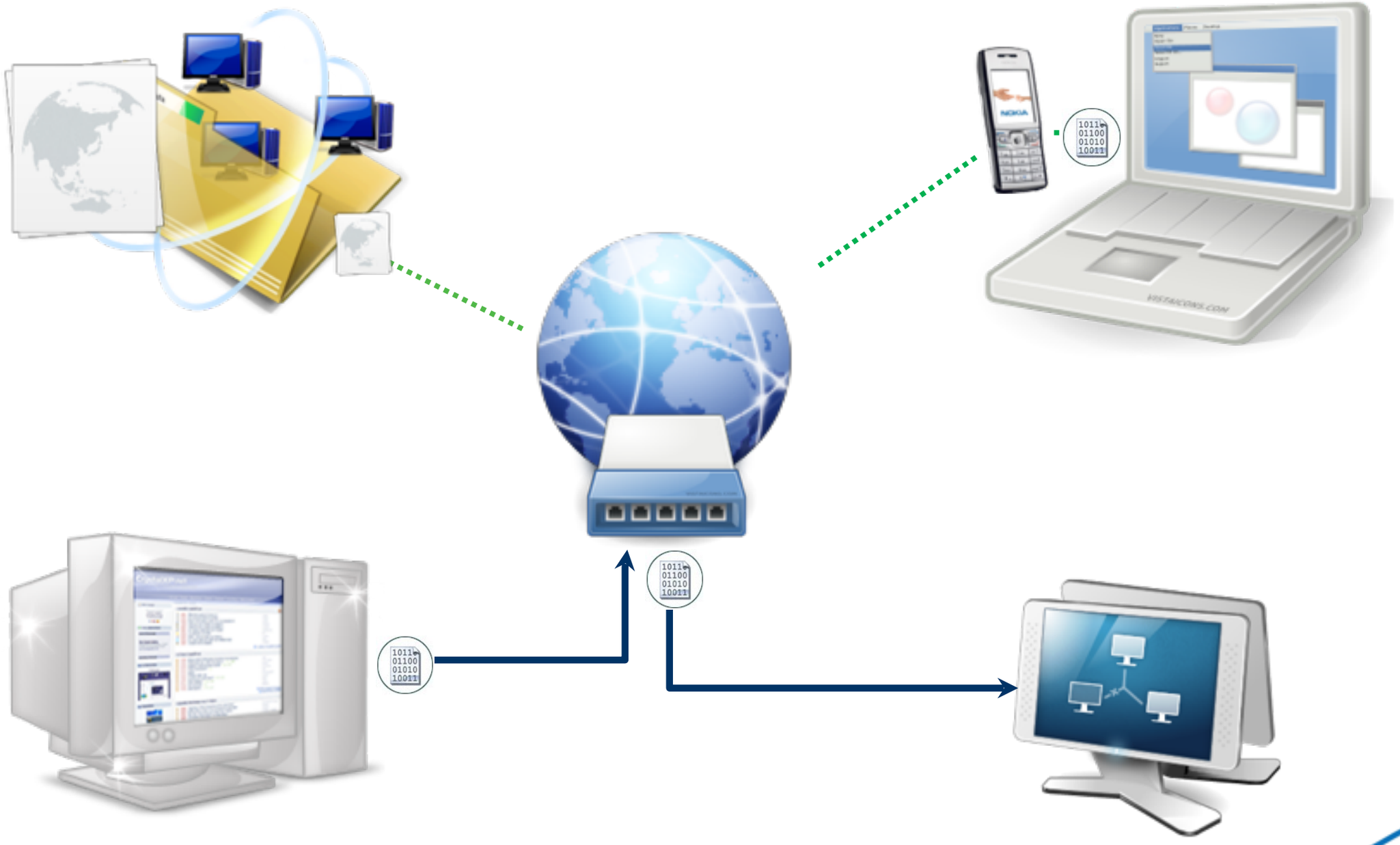
นิยาม : ระบบคอมพิวเตอร์

Computer System



- Input Device
- Output Device
- Memory
- Processor

นิยาม : ระบบคอมพิวเตอร์



การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ

- มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

องค์ประกอบฐานความผิด

การเข้าถึง

การเข้าถึงทางกายภาพ

การเข้าถึงผ่านทางระบบเครือข่าย

ระบบคอมพิวเตอร์มีลักษณะที่เป็น Live

โดยมิชอบ

ไม่มีอำนาจ หรือไม่มีสิทธิในการเข้าถึงในส่วนนั้นๆ

หรือเคยมีสิทธิ แต่ปัจจุบันไม่มีสิทธิ

ต้องรู้ว่าตนเองไม่มีสิทธิ

ไม่จำเป็นต้องมีเจตนาทุจริต

มาตรการป้องกัน

ความหมายของมาตรการป้องกัน

การรับทราบเรื่องมาตรการป้องกัน

การรองรับมาตรการป้องกันของระบบคอมพิวเตอร์บางประเภท

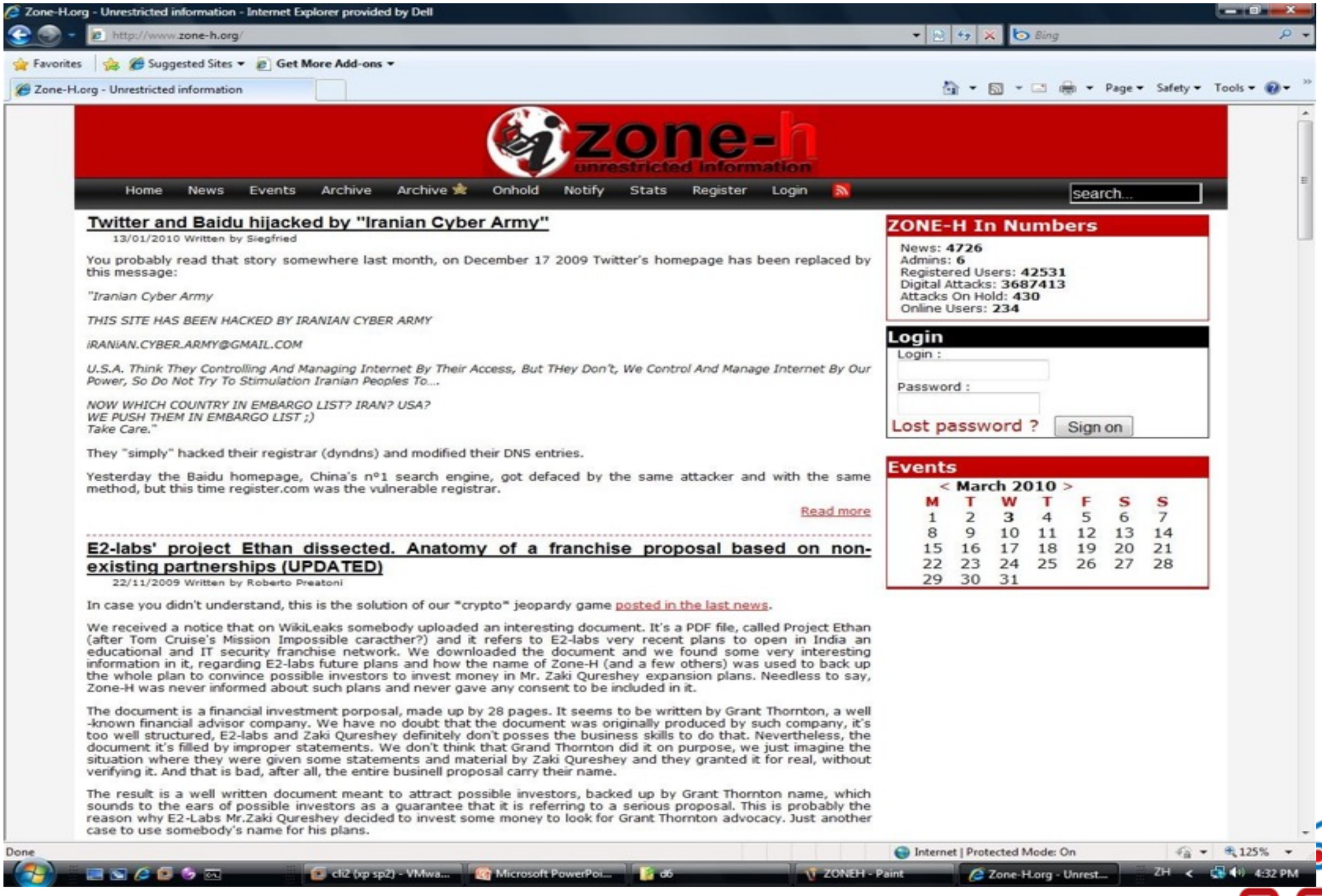
ตัวอย่างเทคนิค การเข้าถึงระบบโดยมิชอบ

- การคาดเดารหัสผ่านของบุคคล
- การใช้เทคนิค SQL Injection
- การทำหน้า Log in ปลอมเพื่อให้หลงเชื่อ
- การดักรับข้อมูลคอมพิวเตอร์จากระบบเครือข่าย
- การเจาะระบบโดยอาศัยช่องโหว่ของซอฟต์แวร์

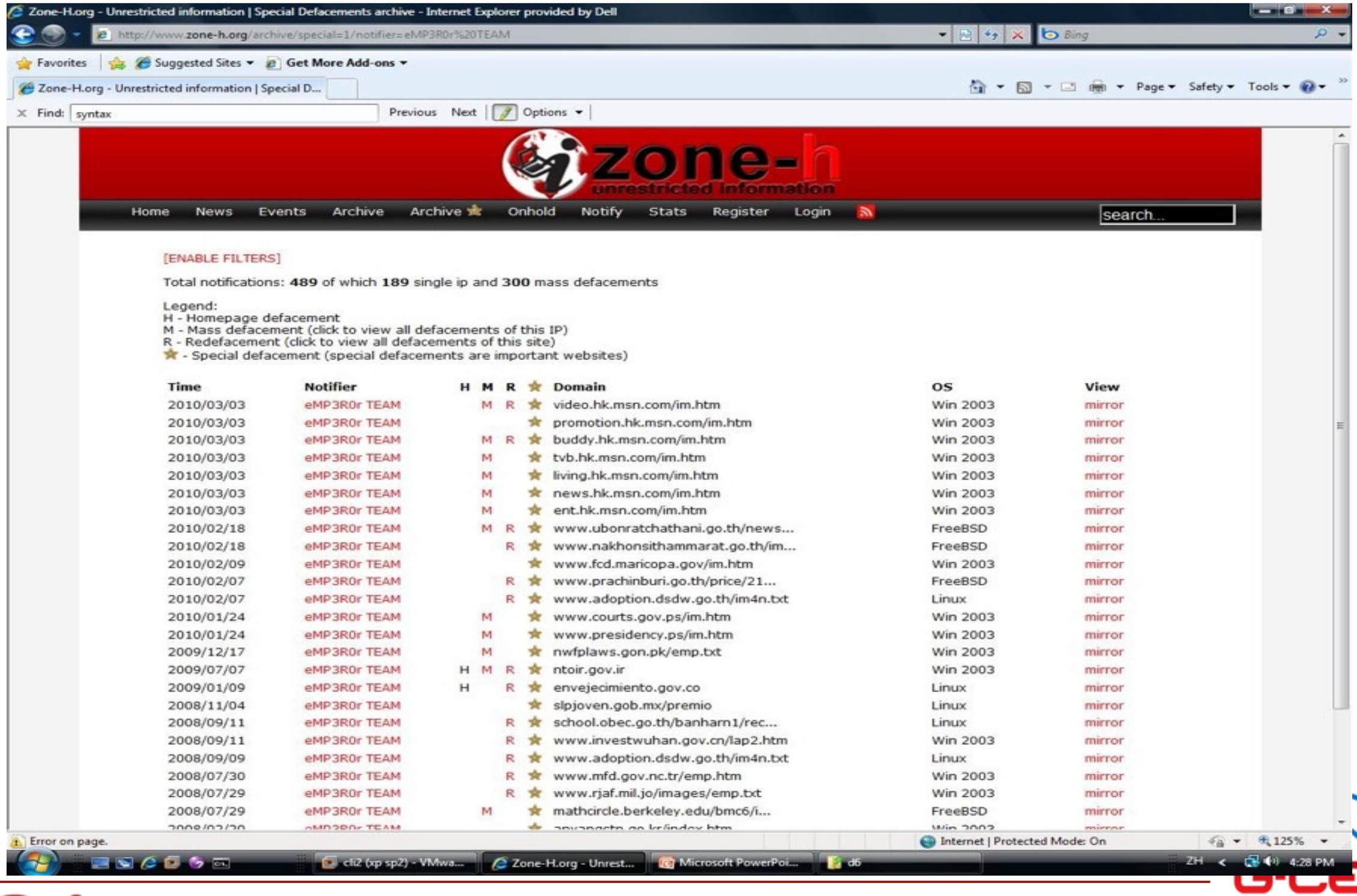
เป้าหมายของการเข้าถึงระบบคอมพิวเตอร์

- ต้องการทำให้เกิดความเสียหายภายในระบบ
- ต้องการใช้งานทรัพยากรของระบบ
- ต้องการข้อมูลที่อยู่ภายในระบบ
- ต้องการชื่อเสียง หรือประกอบอาชญากรรม

Page Defacement



Page Defacement



ent.hk.msn.com hacked by eMP3R0r TEAM - Internet Explorer provided by Dell

http://www.zone-h.org/mirror/id/10314139

Favorites | Suggested Sites | Get More Add-ons

ent.hk.msn.com hacked by eMP3R0r TEAM

Page | Safety | Tools

zone-h unrestricted information

Home News Events Archive Archive Onhold Notify Stats Register Login search...

Mirror saved on: 2010-03-02 23:07:42

Notified by: eMP3R0r TEAM
System: Win 2003

Domain: http://ent.hk.msn.com/im.htm
Web server: IIS/6.0

IP address: 202.67.153.73
Notifier stats

Hacked By Emperor

We Are: iM4n - Spyn3t - h4x21

Special TnX 2 Ciph3r

Home News Events Archive Archive Onhold Notify Stats Register Login Disclaimer Contact

Attribution-NonCommercial-NoDerivs 3.0 Unported License

Done | Internet | Protected Mode: On | 125%

cli2 (xp sp2) - VMwa... | Microsoft PowerPoi... | d6 | ZONEH-2 - Paint | ent.hk.msn.com ha... | ZH | 4:33 PM

EGA e-Government Agency

G-CERT by EGA

Zone-H.org - Unrestricted information | Defacements archive - Internet Explorer provided by Dell

http://www.zone-h.org/archive

Favorites | Suggested Sites | Get More Add-ons

Zone-H.org - Unrestricted information | Defacem...

Page | Safety | Tools

zone-h unrestricted information

Home | News | Events | Archive | Archive ★ | Onhold | Notify | Stats | Register | Login | search...

NOTIFIER | DOMAIN CO.TH | Fulltext ☑

Date : ALL | 01 | January | 1998 | Apply filter

Total notifications: **2244** of which **747** single ip and **1497** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
★ - Special defacement (special defacements are important websites)

Time	Notifier	H	M	R	★	Domain	OS	View
2010/03/02	xinplysz	H				www.premat.co.th	Win 2003	mirror
2010/02/26	mdx		M	R		www.itag.co.th/bymdx.html	Win 2003	mirror
2010/02/26	mdx		M	R		www.malca-amit.co.th/bymdx.html	Win 2003	mirror
2010/02/26	mdx		M	R		www.alternet.co.th/bymdx.html	Win 2003	mirror
2010/02/25	Azerbaijan Attacker					www.fuzion.co.th/news/	Linux	mirror
2010/02/18	LatinHackTeaM	H			★	www.zyxel.co.th	Linux	mirror
2010/02/17	DrAeX			R		www.sbox.co.th/adanali.htm	Win 2003	mirror
2010/02/16	DrAeX			R		www.bioc.co.th/01.htm	Win 2003	mirror
2010/02/16	MadNet					www.topliner.co.th/new/index.php	FreeBSD	mirror
2010/02/14	By_aGReSiF		M			lavanille.co.th/default.htm	Win 2003	mirror
2010/02/14	By_aGReSiF		M			lavanille.co.th/default.htm	Win 2003	mirror
2010/02/14	By_aGReSiF		M			lavanille.co.th/default.htm	Win 2003	mirror
2010/02/09	G00g!3 W@rr!0r					ateducation.co.th/flash_images...	Linux	mirror
2010/02/09	v4 Team	H				amani.co.th	Linux	mirror
2010/02/09	v4 Team	H				dsfutures.co.th	Linux	mirror
2010/02/09	v4 Team	H	M			online.dsfutures.co.th	Linux	mirror
2010/02/09	v4 Team	H	M			prstation.co.th	Linux	mirror
2010/02/09	v4 Team	H	M	R		pakfood.co.th	Linux	mirror
2010/02/09	v4 Team	H	M			ifc.co.th	Linux	mirror
2010/02/09	v4 Team	H	M			ampelite.co.th	Linux	mirror
2010/02/09	v4 Team	H	M			pine.co.th	Linux	mirror
2010/02/09	v4 Team	H	M			ommas.co.th	Linux	mirror
2010/02/09	v4 Team	H	M			trinergy.co.th	Linux	mirror
2010/02/09	v4 Team	H	M			pacificfreight.co.th	Linux	mirror
2010/02/09	v4 Team	H	M			superblack.studio.co.th	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Done | Internet | Protected Mode: On | 125%

cli2 (xp sp2) - VMwa... | Microsoft PowerPoi... | d6 | Zone-H.org - Unrest... | ZH | 4:37 PM

War Driving

151.120.11.39

151.120.11.35

151.120.11.39

151.120.11.40

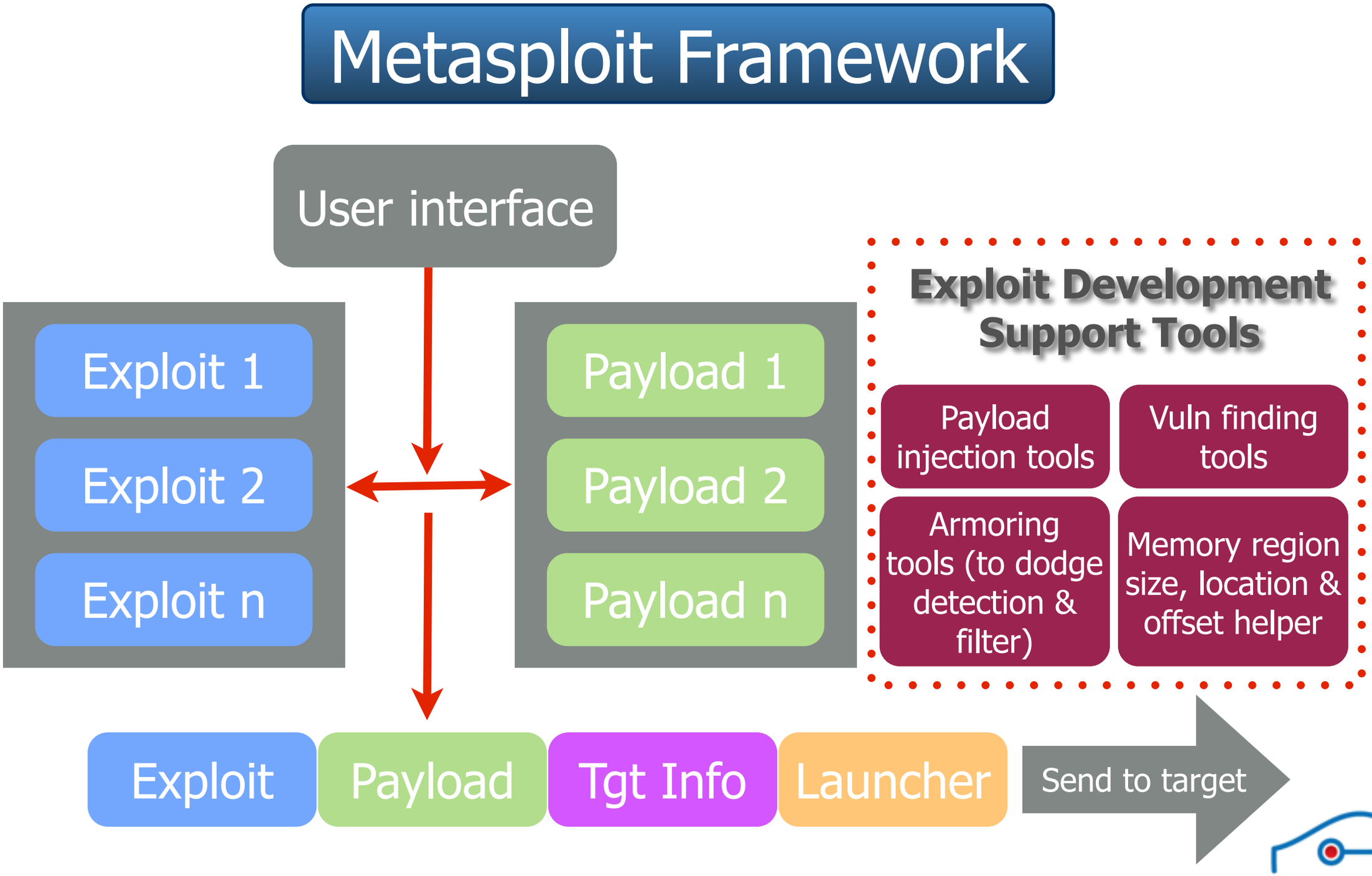
151.120.11.40

151.120.11.35

EGA
e-Government Agency

G-CERT by EGA

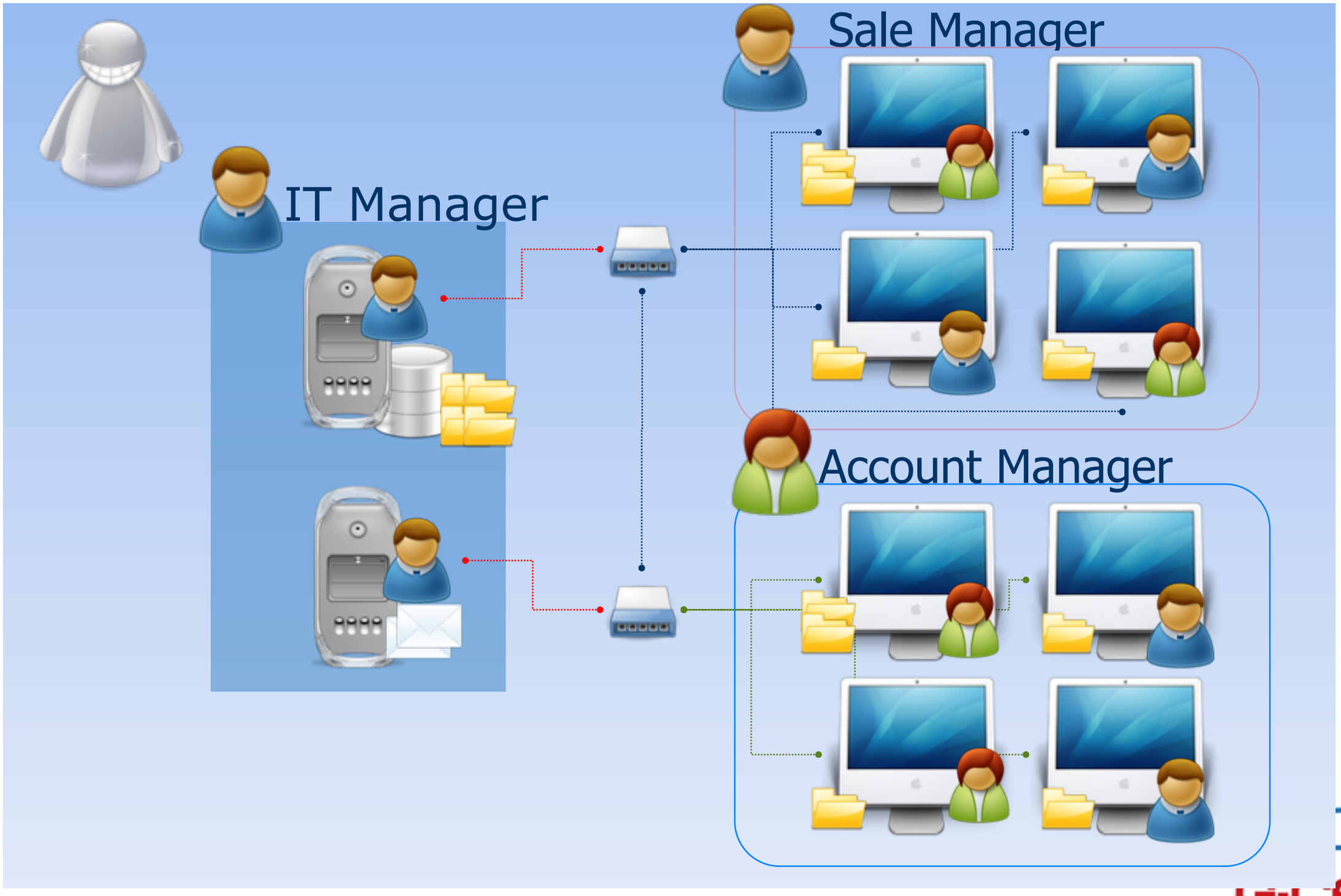
ตัวอย่างเทคนิค การเข้าถึงระบบโดยมิชอบ



เข้าถึงข้อมูลของบุคคลอื่นโดยมิชอบ

- มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

เข้าถึงข้อมูลของบุคคลอื่นโดยมิชอบ



การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ

- การพิจารณาว่าเป็นการเข้าถึงระบบ หรือการเข้าถึงข้อมูลจะพิจารณาอย่างไร
- การเข้าถึงสื่อสำหรับจัดเก็บข้อมูล (Storage Media) ที่ยังมิได้นำไปเชื่อมต่อกับระบบคอมพิวเตอร์
- การพิจารณาเรื่อง การเป็นเจ้าของระบบคอมพิวเตอร์และเจ้าของข้อมูลคอมพิวเตอร์

การป้องกันข้อมูลโดยการตั้งรหัสผ่าน

- ไม่ควรตั้งรหัสผ่านน้อยกว่า 8 ตัวอักษร
- ไม่ควรเลือกคำที่มีอยู่ในพจนานุกรม
- ไม่ควรเลือกข้อมูลส่วนตัวมาเป็นรหัสผ่าน
- ควรประกอบไปด้วยตัวอักษรใหญ่ เล็ก และอักขระพิเศษ
- มีการเปลี่ยนรหัสผ่านอยู่เสมอ

การแก้ไข เปลี่ยนแปลง หรือทำลายข้อมูล

- มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือ บางส่วน ซึ่งข้อมูลคอมพิวเตอร์ ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

การเปิดเผยมาตรการป้องกันระบบคอมพิวเตอร์โดยมิชอบ

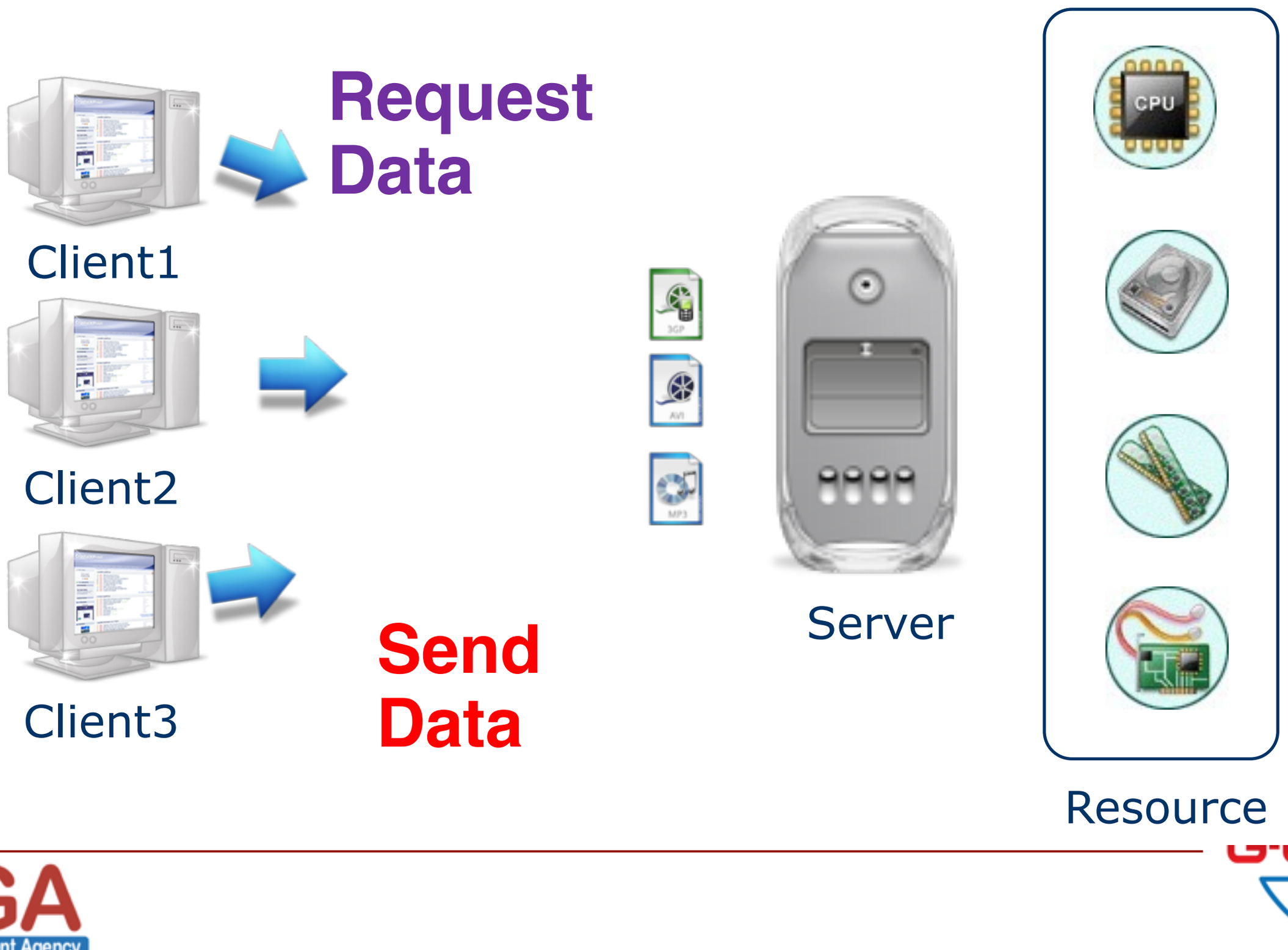
- มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ

ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุก ไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

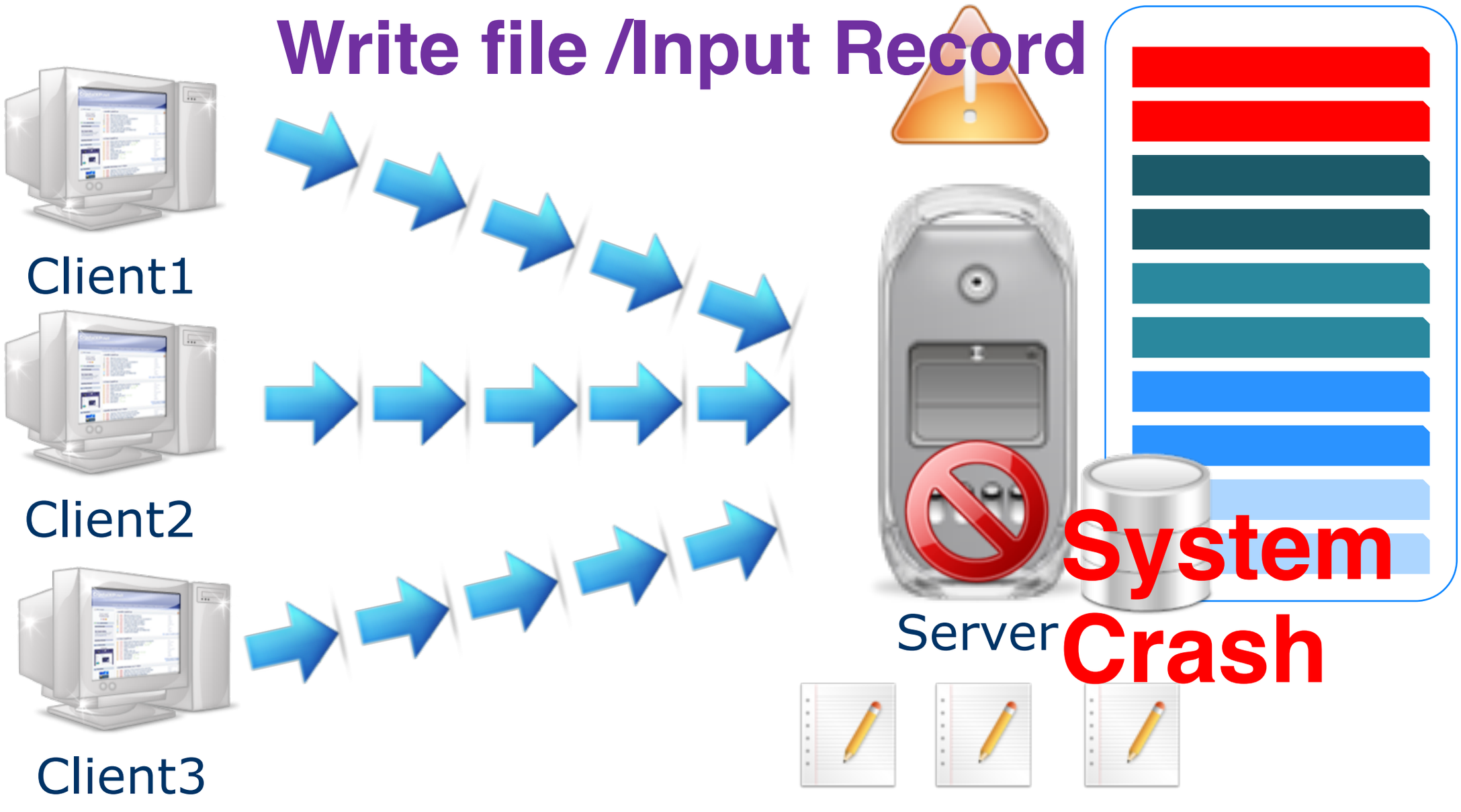
รบกวนการทำงานของเครื่องคอมพิวเตอร์

❖ มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุก ไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

Client-Server Service



Server Overload



E-Mail Bomb

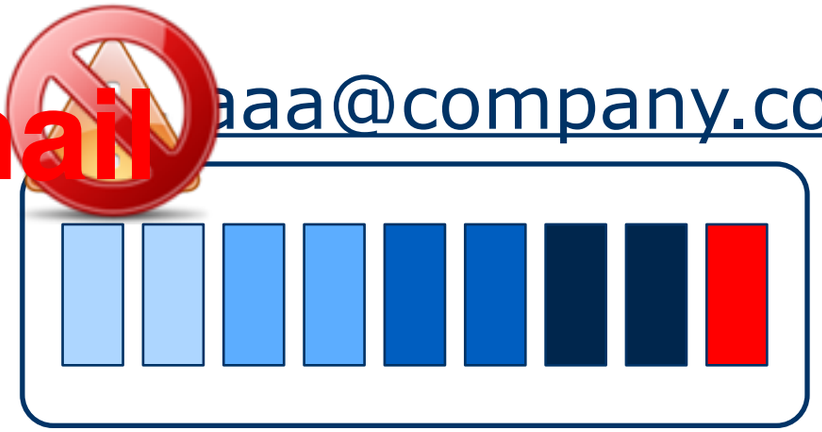
Client 1

Client 2

Client 3

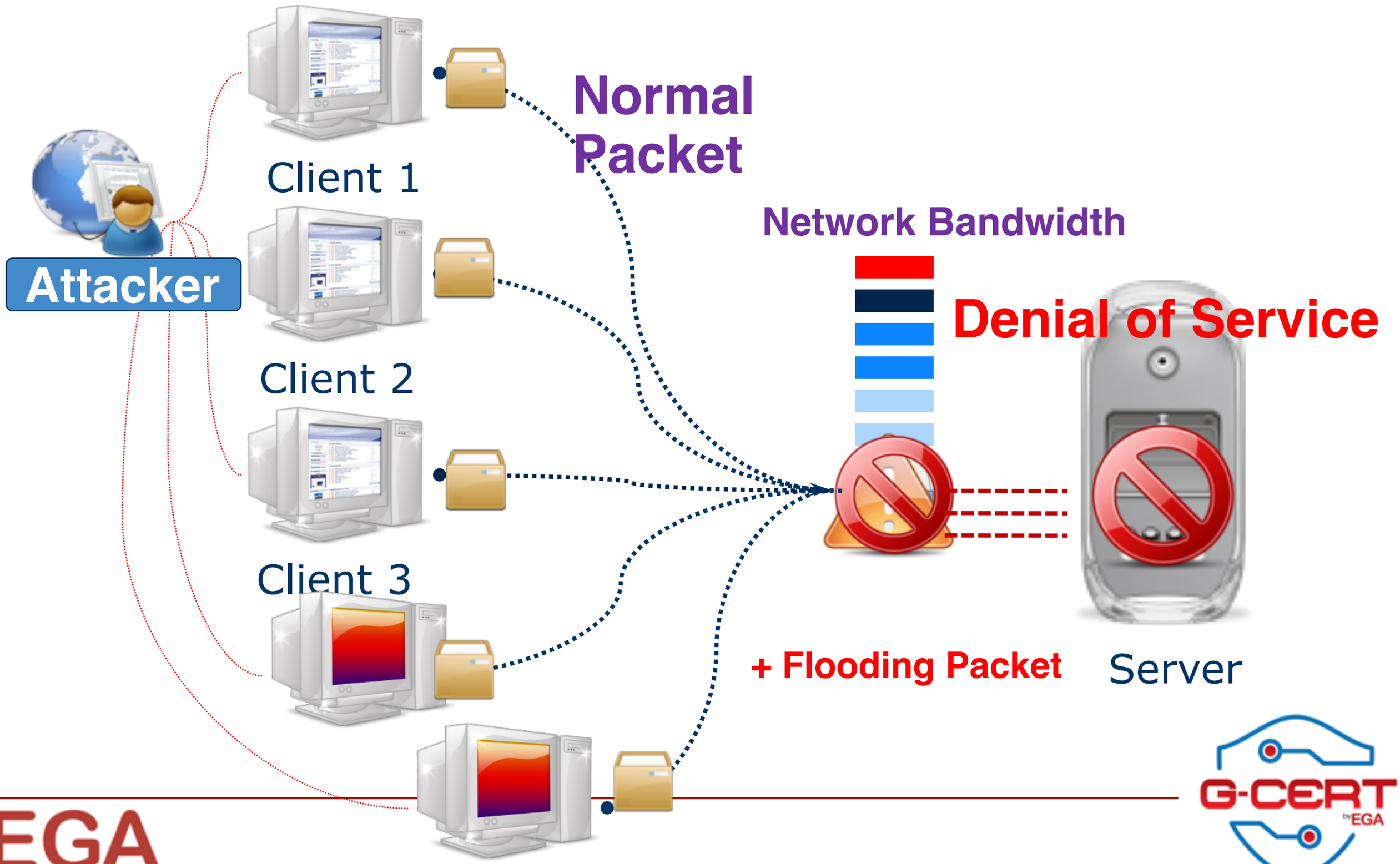
Sending E-mail

Mail Server



E-mail Account Storage

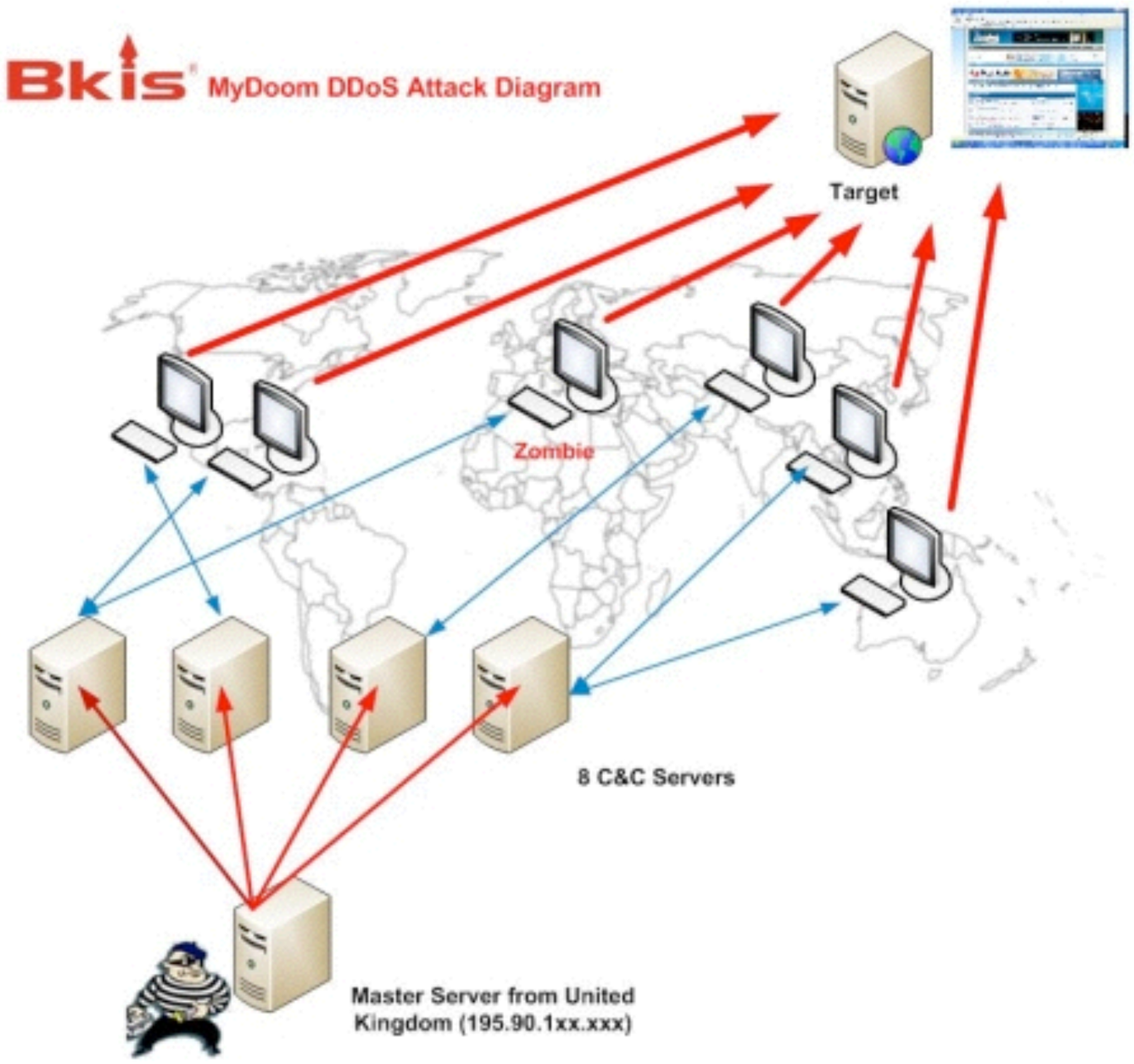
Packet Flooding Attack



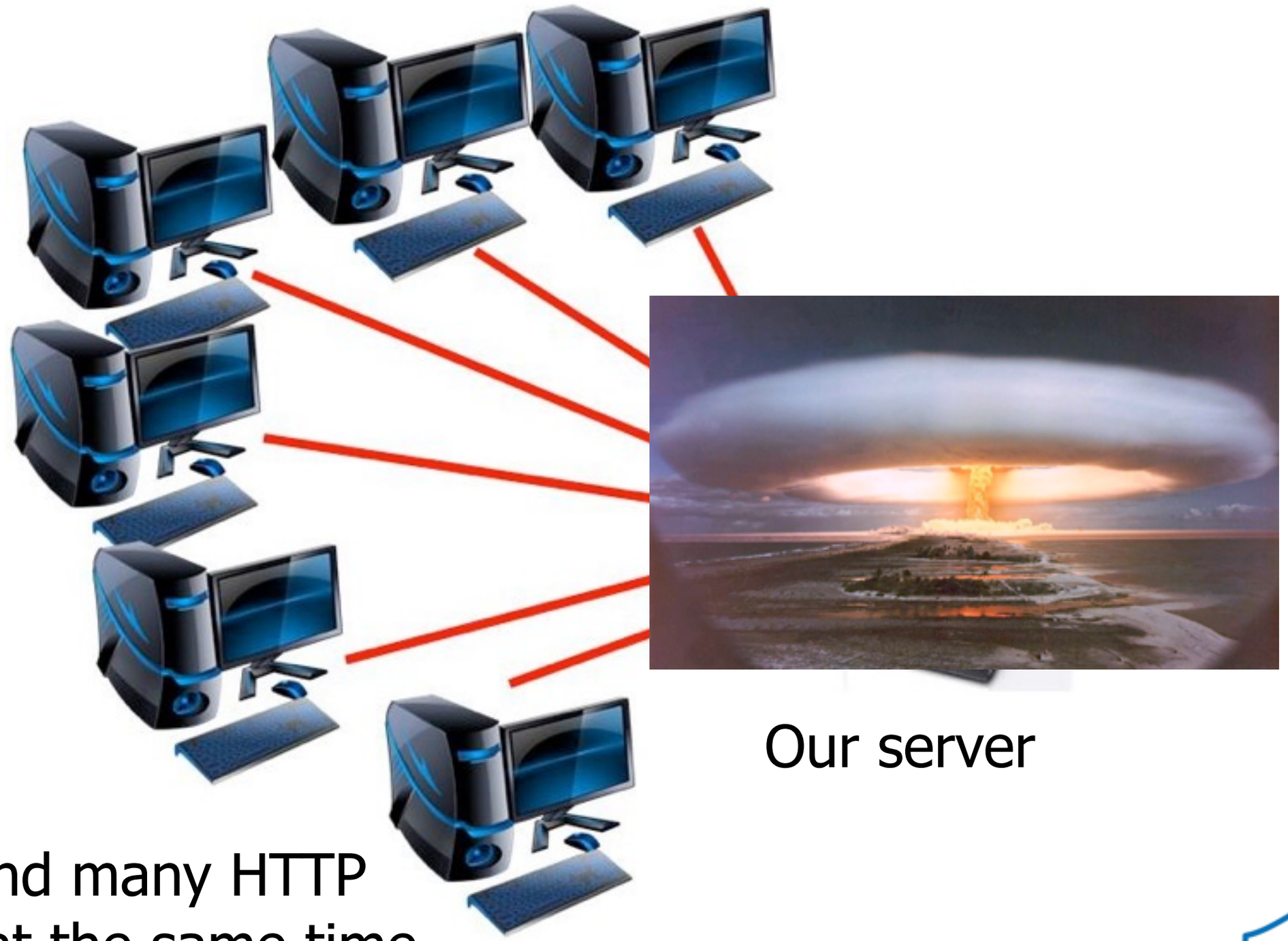
DoS (Denial of Service)

Ping of Dead

Distributed Denial of Service (DDoS)



Distributed Denial of Service (DDoS) - Flooding



Our server

Botnet send many HTTP requests at the same time

Over consuming

Your server is like the donkey,
and no, it’s not the donkey’s fault.

Hello Single Gateway !!!!!!!!

Impacts

LOG IN SIGN UP WEB SEARCH

MENU Bangkok Post NEWS

NEWS HOMEPAGE | MOST RECENT | TOP STORIES | POLITICS | CRIME | GENERAL | ASEAN

NEWS > GENERAL

ICT website down ahead planned attack

30 Sep 2015 at 21:30 5,398 viewed 5 comments

WRITER: ONLINE REPORTERS

telecomasia.net

BLOGS RSS

Don Sambandaraksa

Thai govt website DDoSed as CAT customer data leaked

October 26, 2015

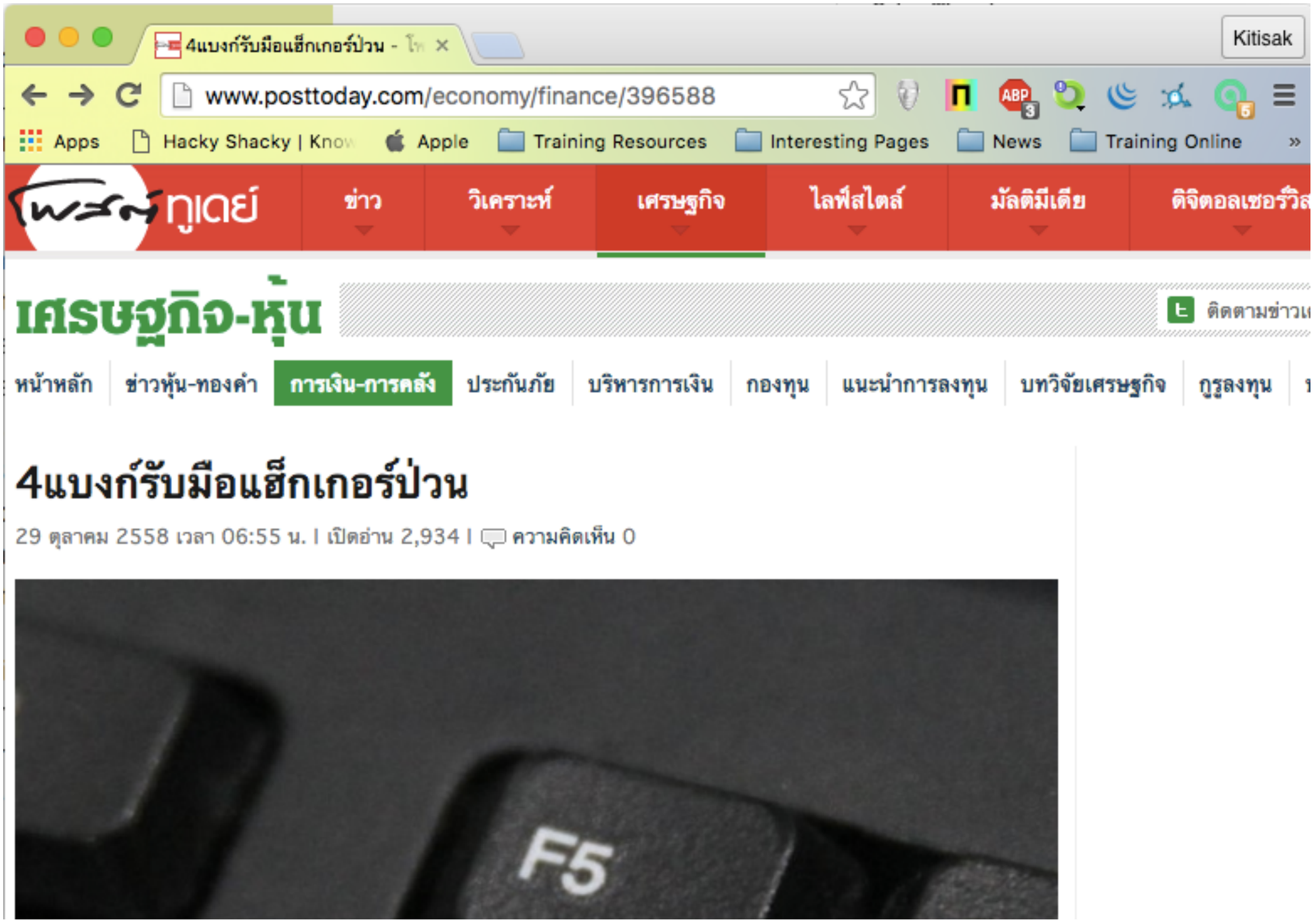
Share G+1 4 Like 21 Tweet 22 share Print Email

Faced with a wave of DDoS attacks, a horde of hackers claiming to be Anonymous and major data leaks from state-owned CAT Telecom all in protest of Thailand's Single Gateway surveillance program, ICT Minister Uttama Savanayana took to Twitter to reassure people that everything was in order and that we had nothing to fear because we have regular data backups.

EGA e-Government Agency

G-CERT by EGA

Ransom DDoS



EGA
e-Government Agency

G-CERT by EGA

Three Security Characteristics

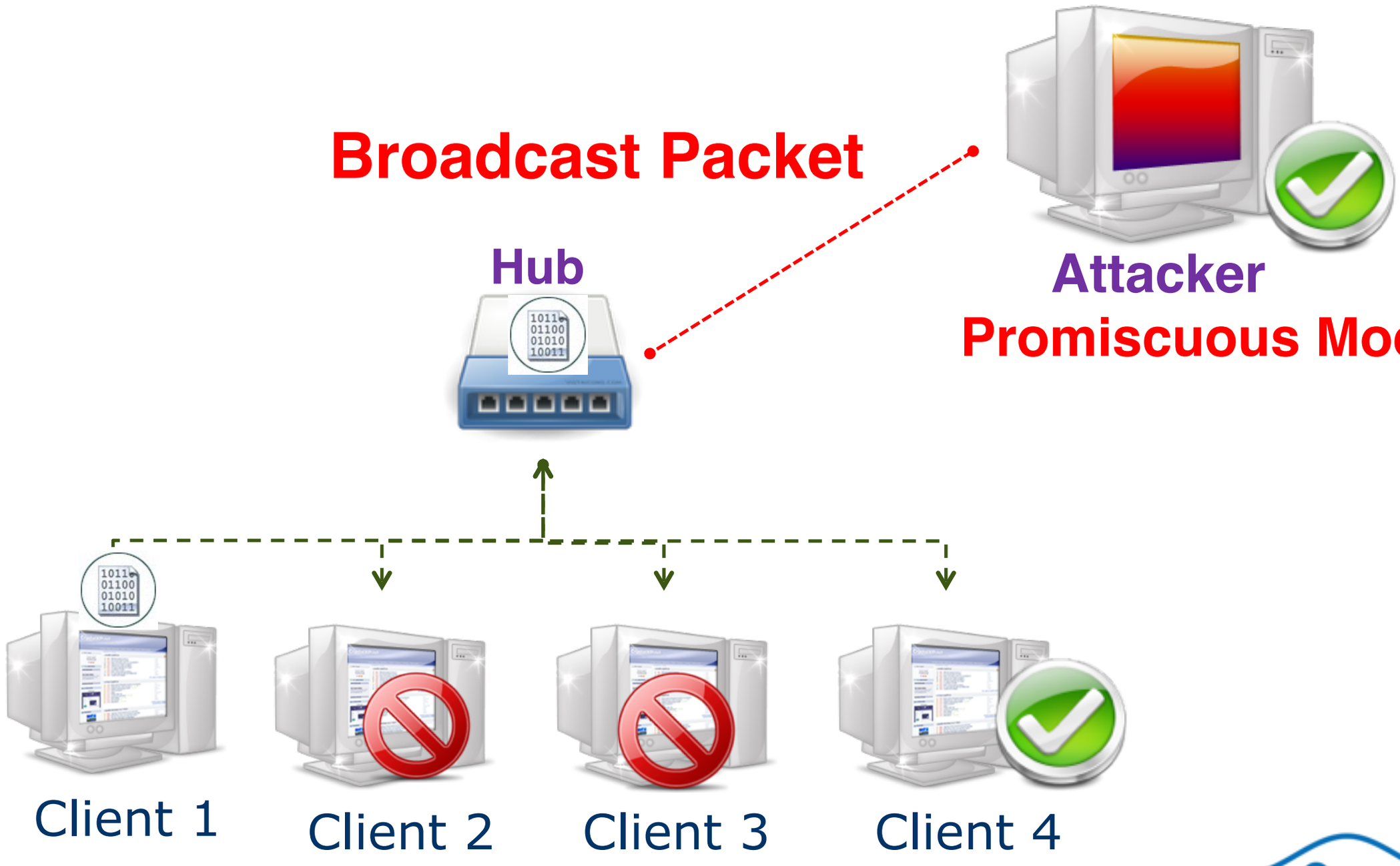
- The primary goal of DDoS defense is maintaining availability in the face of attack

Source Pic:http://www.aptugo.com/uploads/images/description/security_pillars_aptugo.png

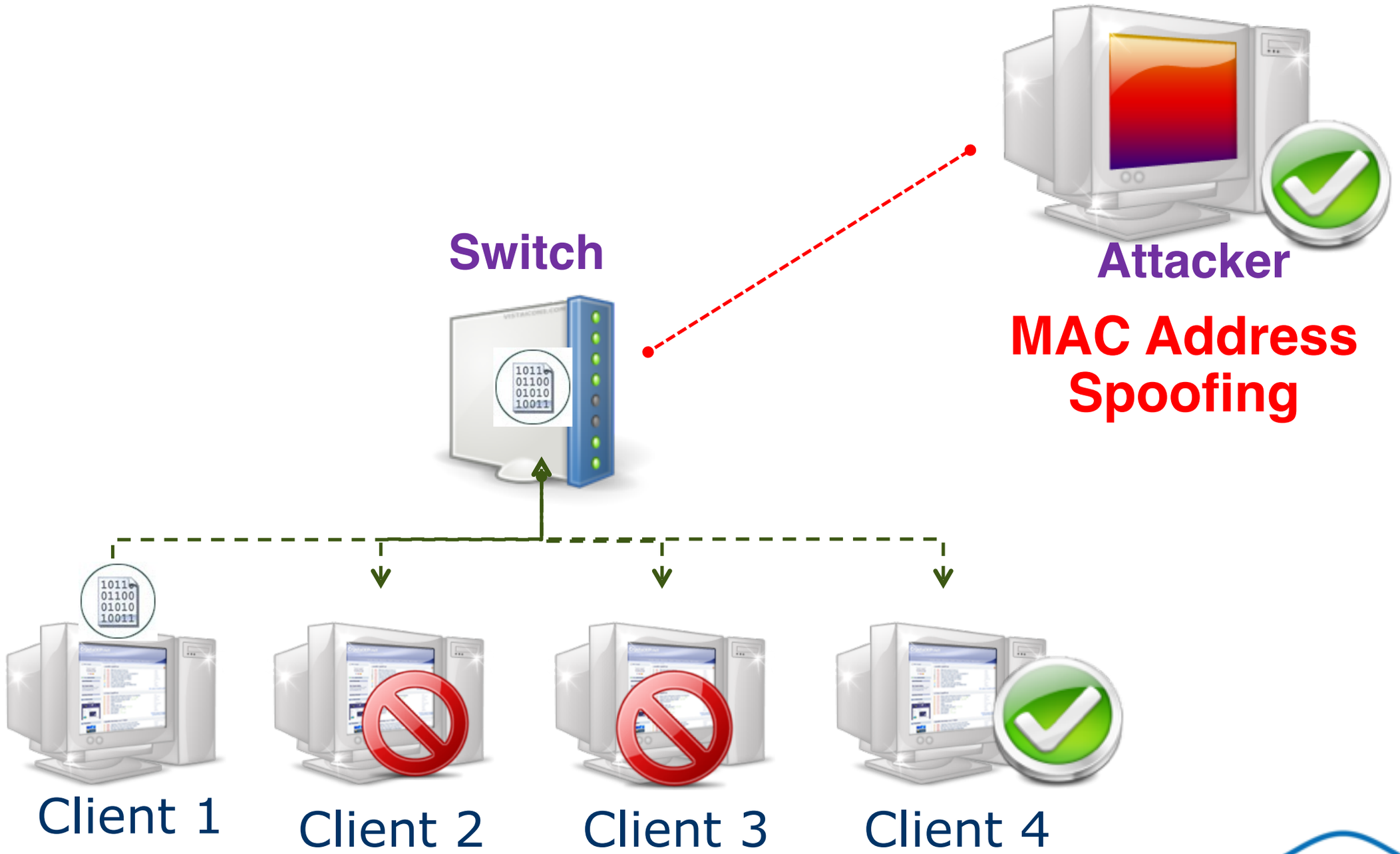
การดักรับข้อมูลคอมพิวเตอร์

❖ มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้น มิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคกไม่เกิน สามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

Packet Sniffering 1



Packet Sniffering 2



Packet Sniffer Test

Wireshark

ความผิดในลักษณะของการเผยแพร่ข้อมูล

- นำข้อมูลที่ต้องห้ามตาม พ.ร.บ.นี้ เข้าสู่ระบบคอมพิวเตอร์
- เผยแพร่หรือส่งต่อข้อมูล ต้องห้ามตาม พ.ร.บ.นี้
- ให้การสนับสนุน ในการเผยแพร่ข้อมูลต้องห้ามตาม พ.ร.บ.นี้

Spam Mail

- มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

เผยแพร่เครื่องมือที่สามารถมุ่งร้ายต่อระบบได้

❖ มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือ ในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือ มาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

ความผิดในลักษณะของการเผยแพร่ข้อมูลที่ไม่เหมาะสม

❖ มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

ความผิดในลักษณะของการเผยแพร่ข้อมูลที่ไม่เหมาะสม

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็น ข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

ภาพตัดต่อ

- มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูล คอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้น เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือ ปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ความผิดเกี่ยวกับผู้ให้บริการ

- ผู้ให้บริการในการเชื่อมต่อสู่ระบบอินเทอร์เน็ต
- ผู้ให้บริการในการดำเนินการเกี่ยวกับข้อมูล

นิยาม : ผู้ให้บริการ

ผู้ให้บริการ

ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเตอร์เน็ต หรือให้สามารถติดต่อถึงกันได้โดยประการอื่น ทั้งนี้โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามตนเอง หรือเพื่อประโยชน์ของบุคคลอื่น

ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม (1)

ผู้ใช้บริการ

ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้จ่ายหรือไม่ก็ตาม

บทบาทและหน้าที่ของผู้ให้บริการ

- ดูแลมิให้มีข้อมูลที่ขัดต่อกฎหมาย
- จัดเก็บข้อมูลคอมพิวเตอร์และข้อมูลจราจรทางคอมพิวเตอร์
- จัดเก็บข้อมูลของผู้ใช้บริการ (ในลักษณะที่ระบุตัวบุคคลได้)
- ประสานงานและดำเนินการตามคำสั่งของพนักงานเจ้าหน้าที่

นิยาม : ข้อมูลจราจรทางคอมพิวเตอร์

- ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของการบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

- เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง
- ระบุ ตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้
- มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ
- จัดให้มีผู้ประสานงานและให้ข้อมลกับพนักงานเจ้าหน้าที่

การจัดเก็บข้อมูลของผู้ให้บริการ (1)

❖การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้วิธีการที่มั่นคง ปลอดภัย ดังต่อไปนี้

(๑)เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุ ตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

(๒) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึง ข้อมลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archiving หรือทำ Data Hashing เป็นต้น เว้นแต่ ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้บริหารองค์กร กำหนดให้สามารถเข้าถึง ข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กร มอบหมาย เป็นต้น รวมทั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้

การจัดเก็บข้อมูลของผู้ให้บริการ (2)

- (๓) จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อให้การส่งมอบข้อมูลนั้น เป็นไปด้วยความรวดเร็ว

(๔) ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้(Identification and Authentication) เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือ บริการ Free Internet หรือ บริการ 1222 หรือ Wi-Fi Hotspot ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง

การกำหนดเวลาของเครื่องที่ให้บริการ

- ข้อ ๙ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกา

ของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

ความรับผิดของผู้ให้บริการ

❖ มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตาม มาตรา ๑๔

พนักงานเจ้าหน้าที่ ตาม พ.ร.บ. ฯ

บุคคลที่เป็นพนักงานเจ้าหน้าที่

อำนาจของพนักงานเจ้าหน้าที่

แนวทางการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่

อำนาจหน้าที่ของพนักงานเจ้าหน้าที่

1. มีหนังสือเรียก/สอบถาม บุคคลที่เกี่ยวข้อง
2. เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ใช้บริการ
3. สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการ

อำนาจของพนักงานเจ้าหน้าที่ (หมายศาล)

4 ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์

5 สั่งให้ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์

6 ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์

7 ถอดรหัสลับของข้อมูลคอมพิวเตอร์

8 ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็น

EGA e-Government Agency

G-CERT by EGA

อำนาจของพนักงานเจ้าหน้าที่

9 การสั่งให้ระงับการเผยแพร่ข้อมูลคอมพิวเตอร์

10 การสั่งให้ระงับการใช้ ทำลาย หรือ แก้ไขข้อมูลคอมพิวเตอร์

การเปรียบเทียบอำนาจของพนักงานเจ้าหน้าที่กับพนักงานสอบสวน

Q& A

Security in Mind
(IT Security Trends 2016)

Kitisak Jirawannakool

E-Government Agency (Public Organization)

kitisak.jirawannakool@ega.or.th

Agenda

- What is EGA?
- Interesting Attack and trends
  - Ransomeware
  - Cloud Security
  - Mobile Security
  - Social Media
  - Internet of Things

How it used to be?

Board

Accountability

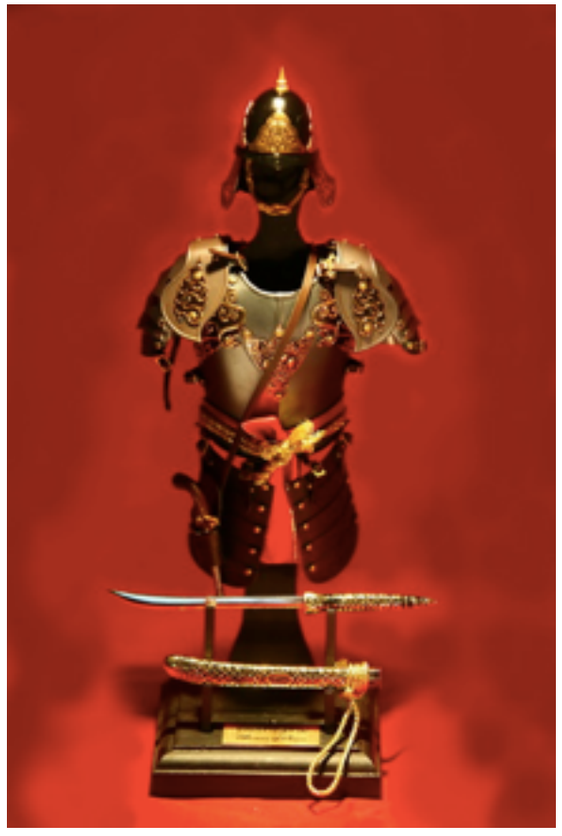
Physical Security

IT & Security

… and How it is growing to be?

What are we protecting?

- What is there to protect ?
  - Primary process
  - Customers, Employees, Identities
  - Products, Contracts
  - Supporting processes
  - Reputation
  - Information, infrastructure
  - Critical infrastructures
  - Health, lives



EGA
e-Government Agency

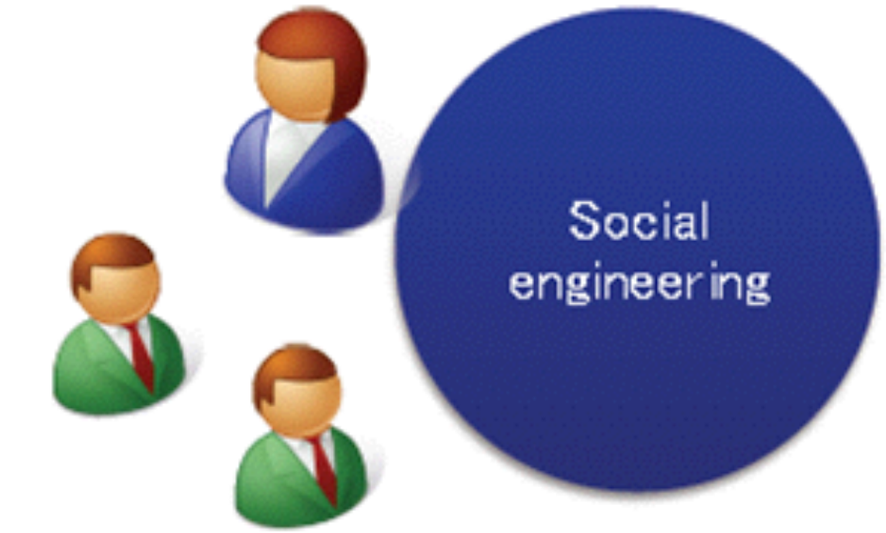
G-CERT by EGA

Situation is changing

* More network devices and users
* More communication opportunity
* More socializing

More chance for attackers
to do their business

Attackers point of view



Technically

Sophisticated
attack

Reach to
information
asset

Important points

Awareness Training

Collaboration

Technical Training

Incident Response

EVER SINCE WE BOUGHT TIMMY A COMPUTER, WE HAVEN'T HAD TO WORRY ABOUT HIM WATCHING ALL THAT JUNK ON TV...

Timmy's Room Keep out!

Internet Porn

What is Security?

Security Goals

- C (Confidentiality)
- I (Integrity)
- A (Availability)

Security Mechanisms

- Authentication
- Access Control
- Encryption
- Signatures

How to attack our servers?

- Systems
  - OS
  - Software installed
- Network
  - Sniffer
  - Spoofing
  - Flooding / DDoS
- Applications
- Data
- Operation

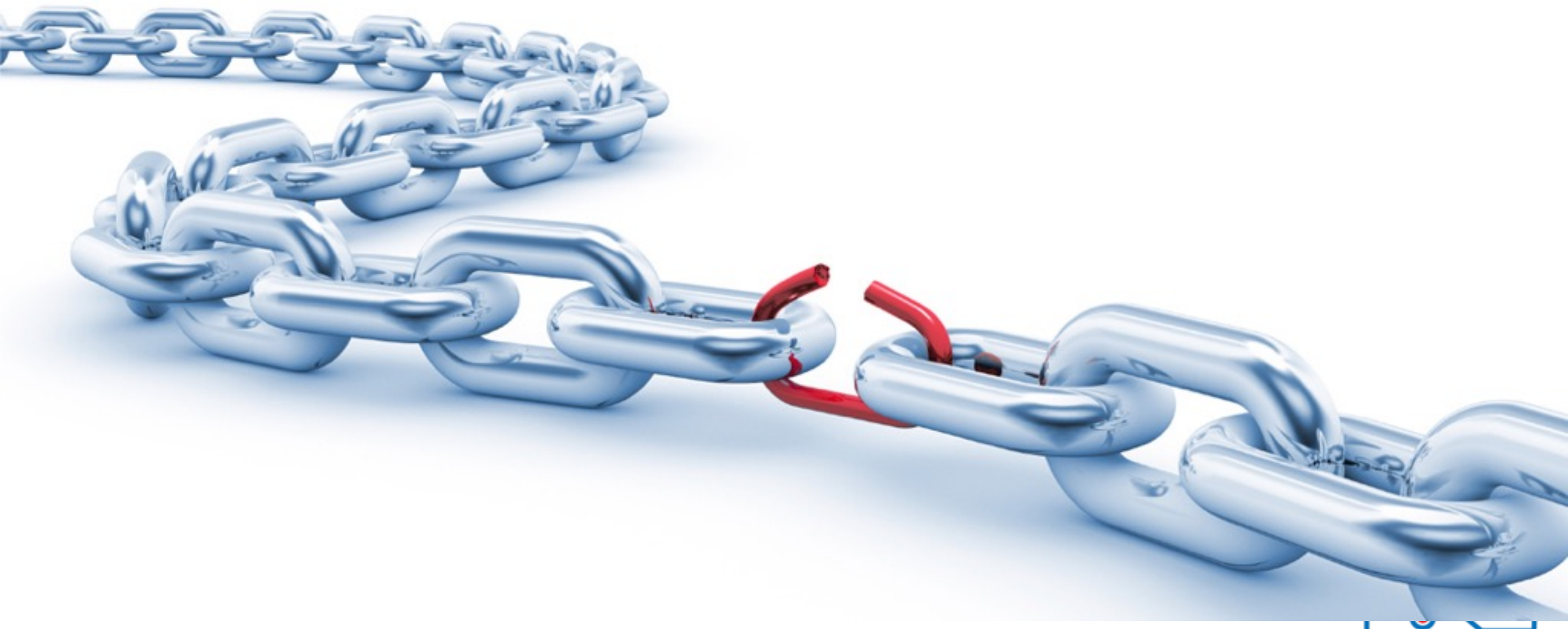
Security myths: We are not a target

Security Myths : We are not a target

- "Mostly I hear it from victims. They think they aren't worth hacking. Some say it's not worthwhile because they're a small business – not on anybody's radar. Others contend they don't collect Social Security numbers, credit card data or other 'valuable' information. They are usually wrong."

Alan Brill, senior managing director for the cybersecurity and information assurance practice at Kroll

Source: Ellen Messmer, 13 security myths you'll hear -- but should you believe? http://www.networkworld.com/news/2012/021412-security-myths-256109.html



Spear Phishing

http://www.terrapapers.com/wp-content/uploads/2013/10/Spear-phishing-1.png

Example

Gmail by Google

Dale Peterson <peterson@digitalbond.com>

(no subject)

1 message

Dale Peterson <dale.peterson111@yahoo.com> Thu, Jun 7, 2012 at 7:48 AM
Reply-To: Dale Peterson <dale.peterson111@yahoo.com>
To: "rvpasupuleti@yahoo.com" <rvpasupuleti@yahoo.com>

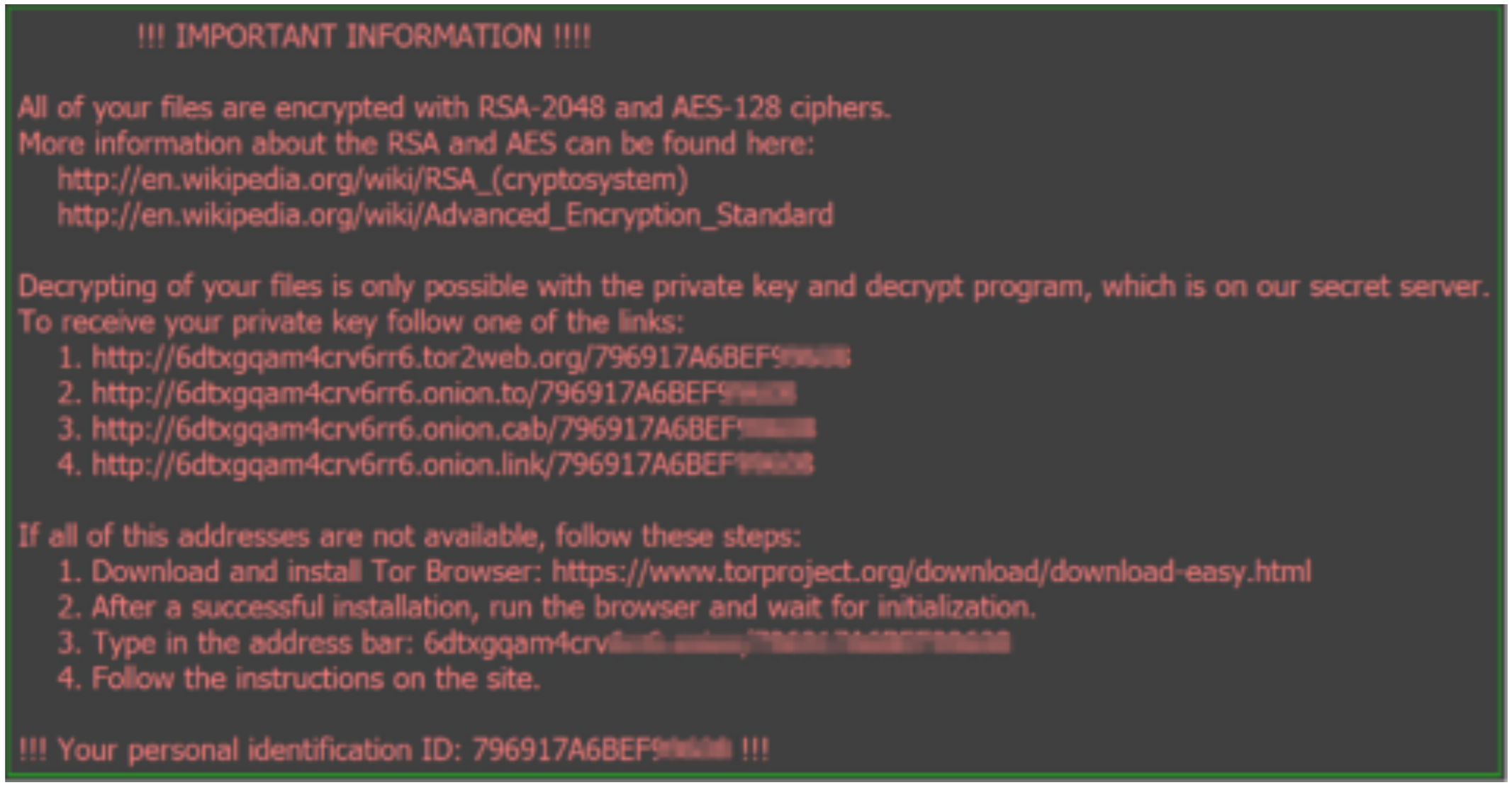
Dear All:
Field devices essential for the monitoring and control in DCS and SCADA systems are increasingly being deployed with Ethernet cards to connect these devices to local and wide area IP networks. Many of the Ethernet cards have their own CPU, memory, operating system and applications. Field device vendors are also providing the capability to upgrade or replace the firmware in these Ethernet cards. Unfortunately in most cases there is no effective security on the firmware upload to the field device Ethernet cards.
Details are available at: Leveraging_Ethernet_Card_Vulnerabilities_in_Field_Devices.pdf
Download it and have a look.
Regards,
Peterson

Ransomware

- Several companies were infected
- All important and document files are encrypted by RSA-4096 (No way to decrypt)
- Need much better backup process

CryptoLocker

Locky (need to enable macro)



!!! IMPORTANT INFORMATION !!!!

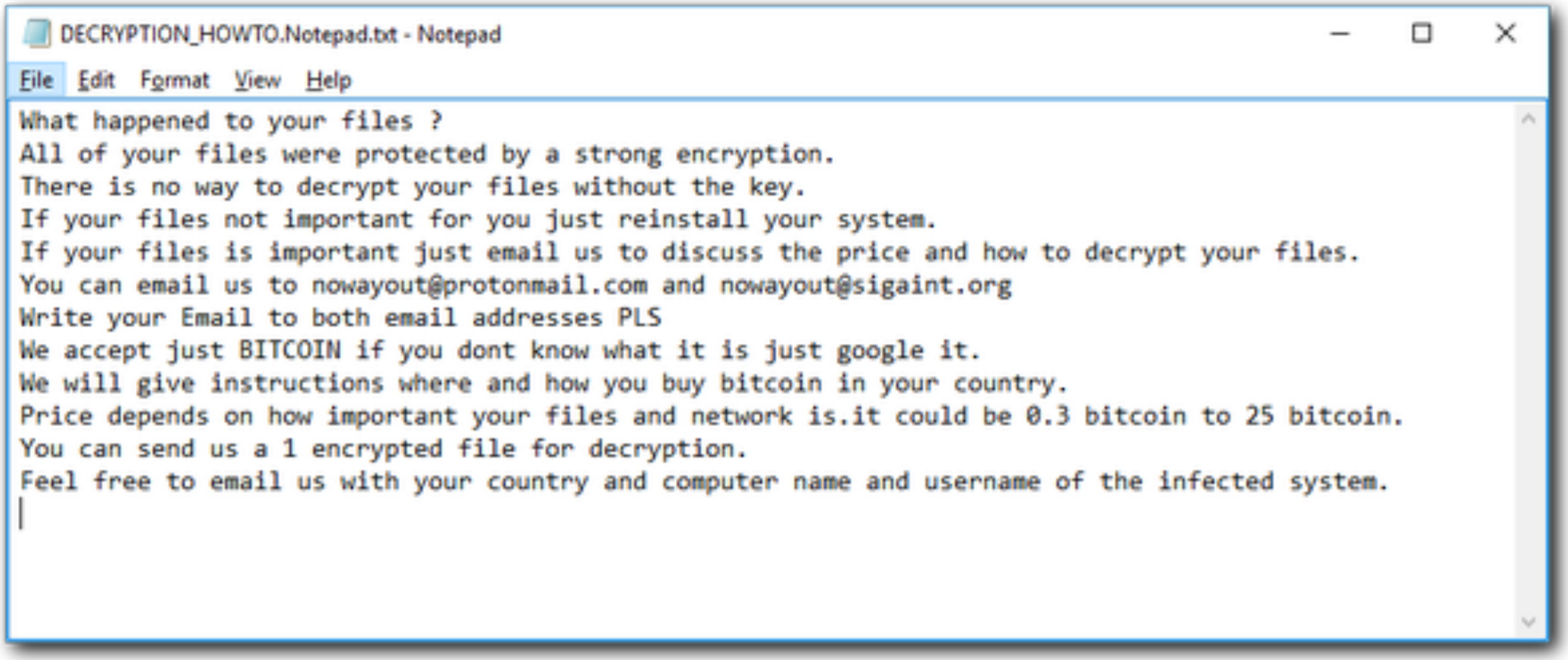
All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://6dtxgqam4crv6rr6.tor2web.org/796917A6BEF
2. http://6dtxgqam4crv6rr6.onion.to/796917A6BEF
3. http://6dtxgqam4crv6rr6.onion.cab/796917A6BEF
4. http://6dtxgqam4crv6rr6.onion.link/796917A6BEF

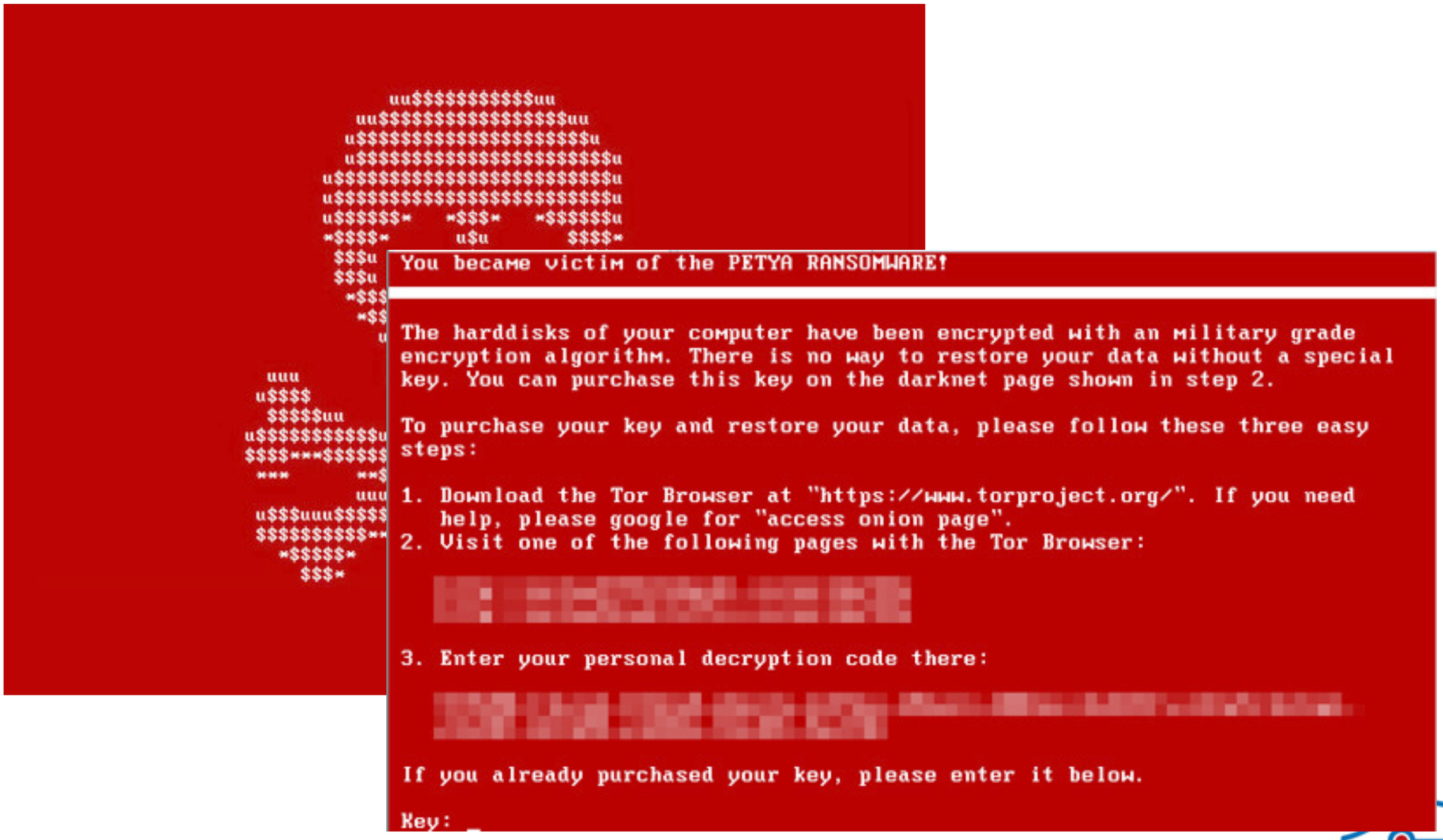
If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 6dtxgqam4crv
4. Follow the instructions on the site.

!!! Your personal identification ID: 796917A6BEF !!!

Surprise (Spread via TeamViewer)



Petya (MBR infected)

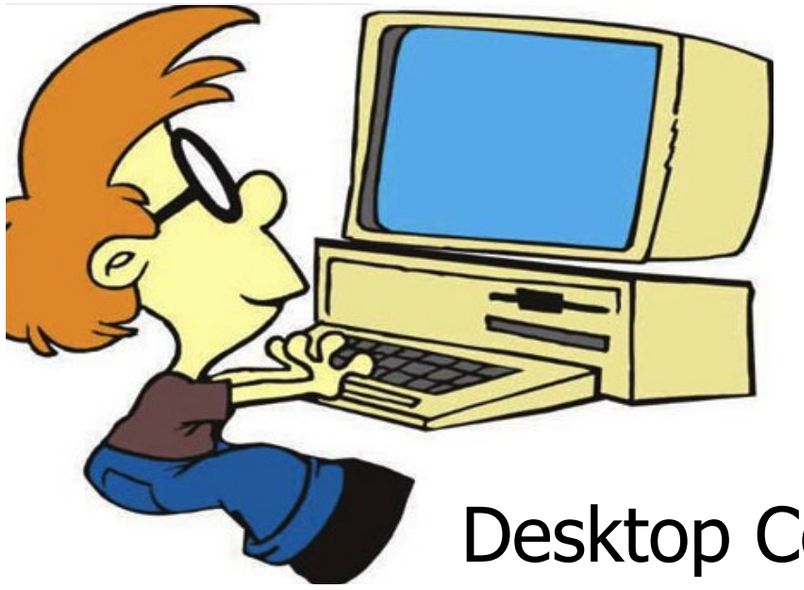


Facts

- Ransomware is not too difficult to remove
- Challenge is how to decrypt files
  - only 5% if you are lucky enough
- Need much better backup policy and technology

Clouds Security

The Evolution of Technology

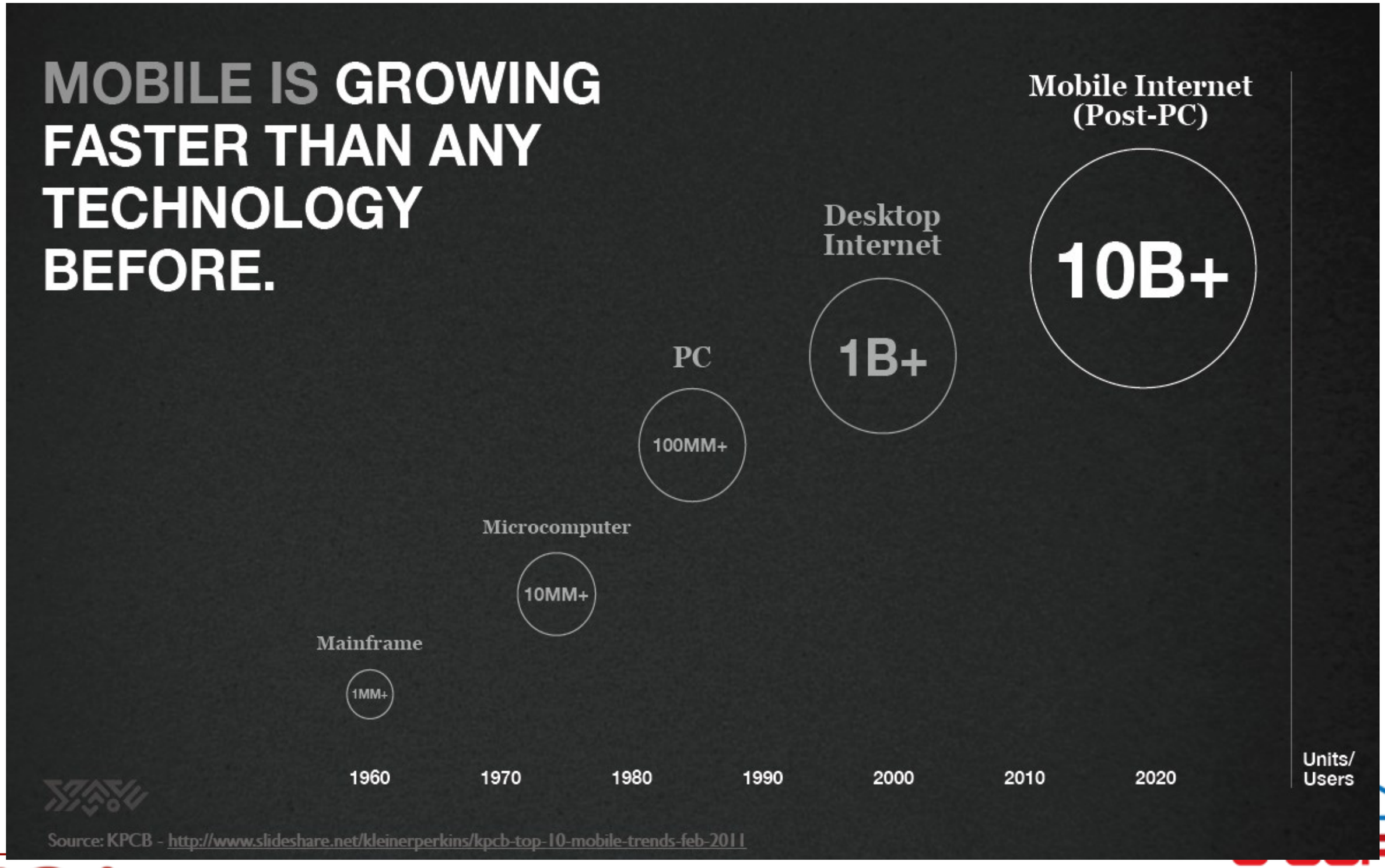


Desktop Computer

Internet Computer

Mobile Devices

Mobile devices will be used to connect



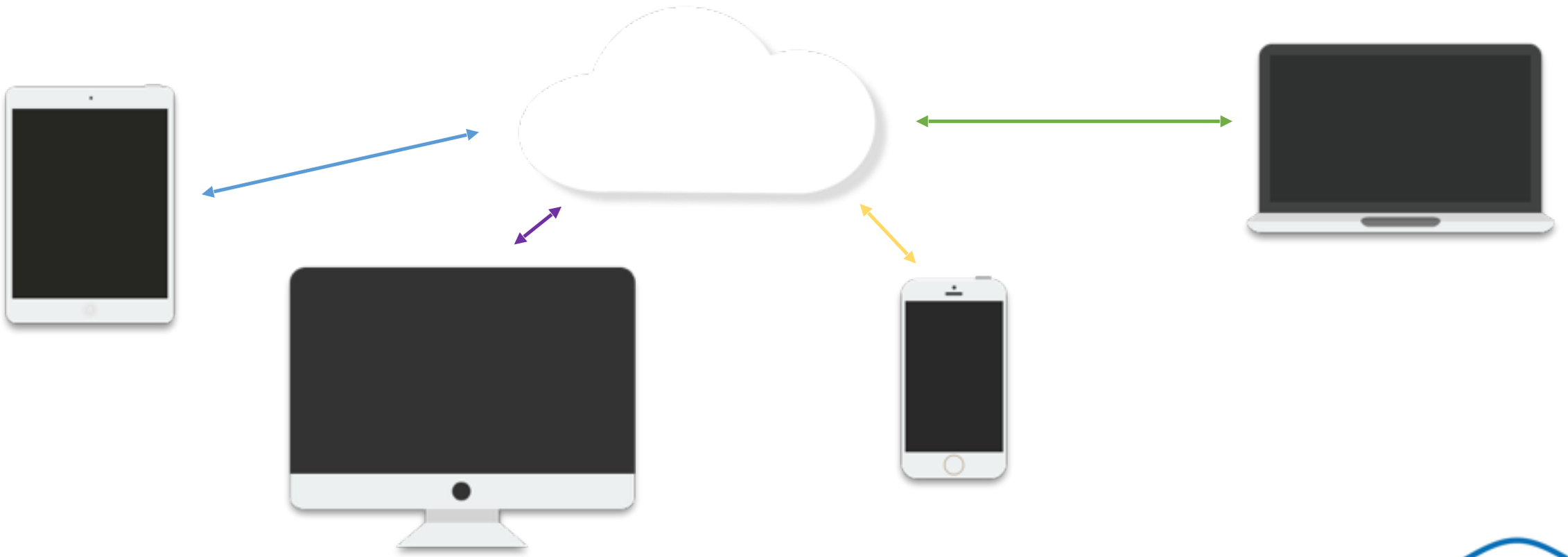
Our Organizations nowadays

- Mobile Workers
- Global (Customers, Partners, Alliances)
- Anywhere & Anytime
- Business Continuity
- Digital Life Convergence

Source : http://www.rickscloud.com/

Cloud Computing?

- Cloud Computing คือ ระบบที่ให้บริการทรัพยากรด้านคอมพิวเตอร์ ที่ทุกคนสามารถเข้าถึงได้
- ไม่ว่าจะอยู่ที่ใดก็ตาม หรือ อุปกรณ์ใดก็ตาม และสามารถแชร์ข้อมูลระหว่างผู้ใช้ได้



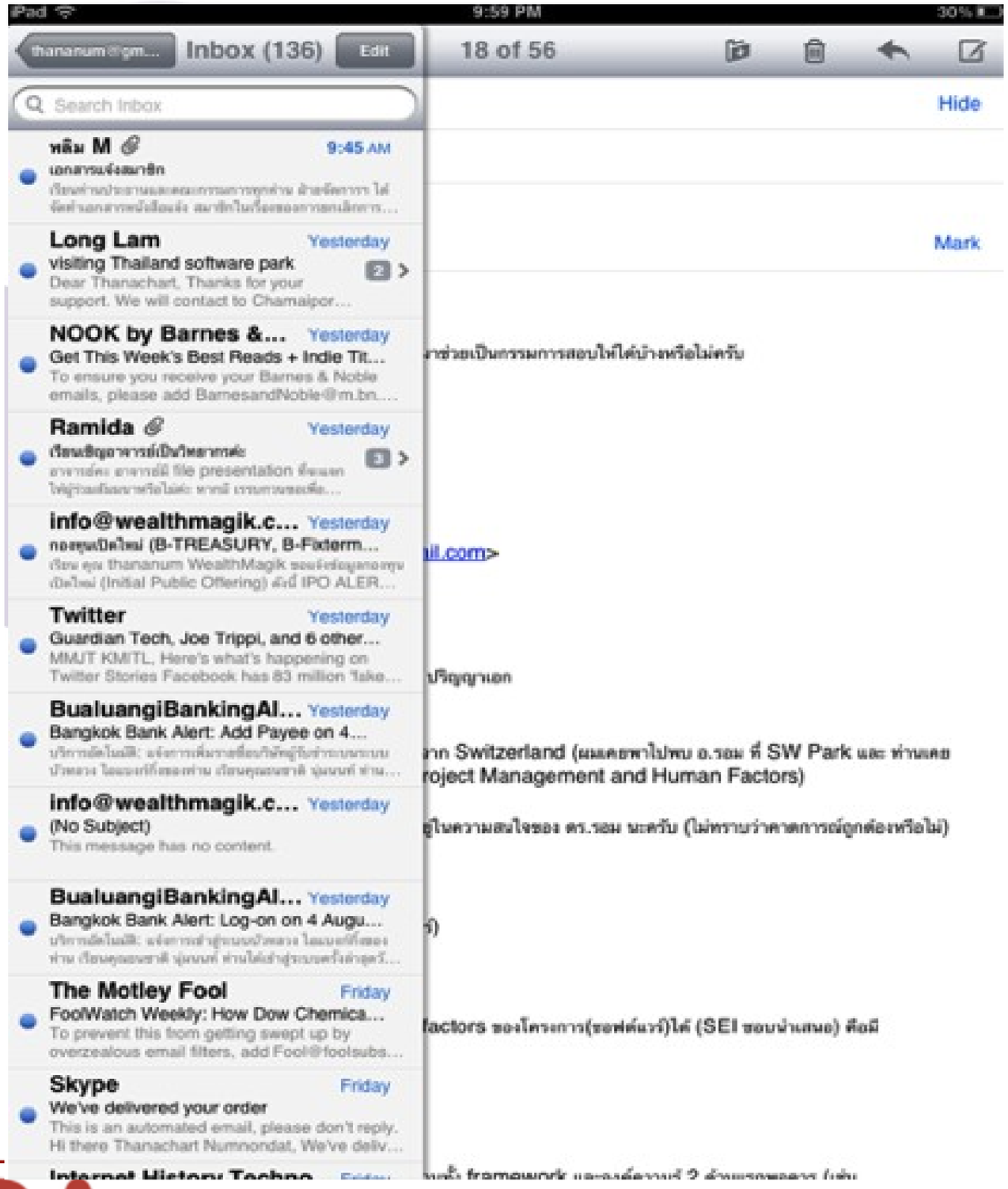
Cloud components

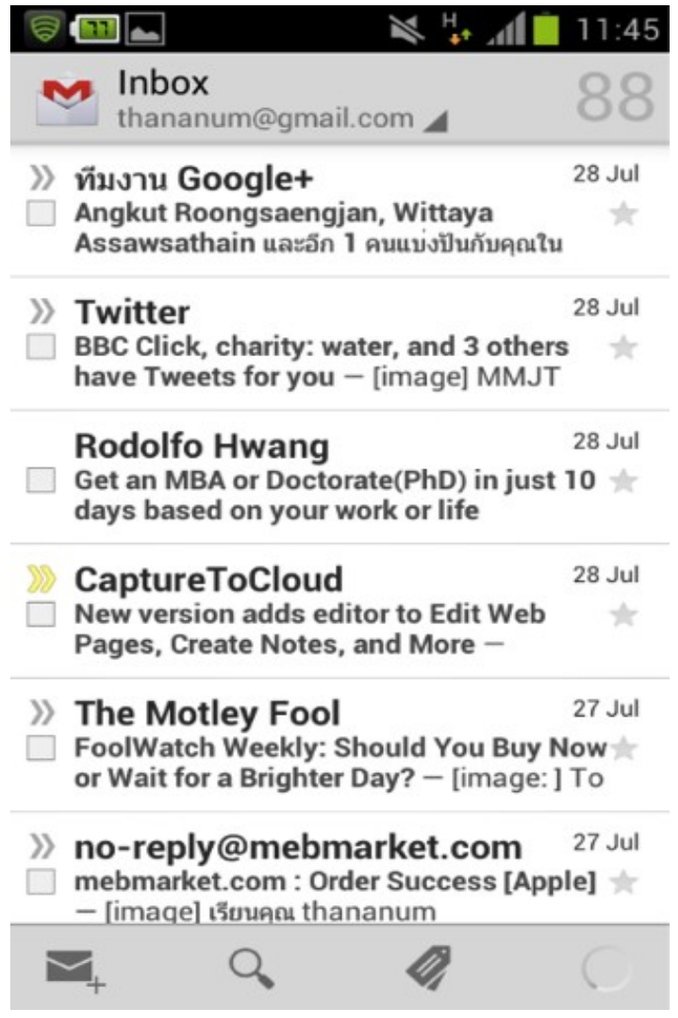
Server Storage Network Application Service

Software usage trends

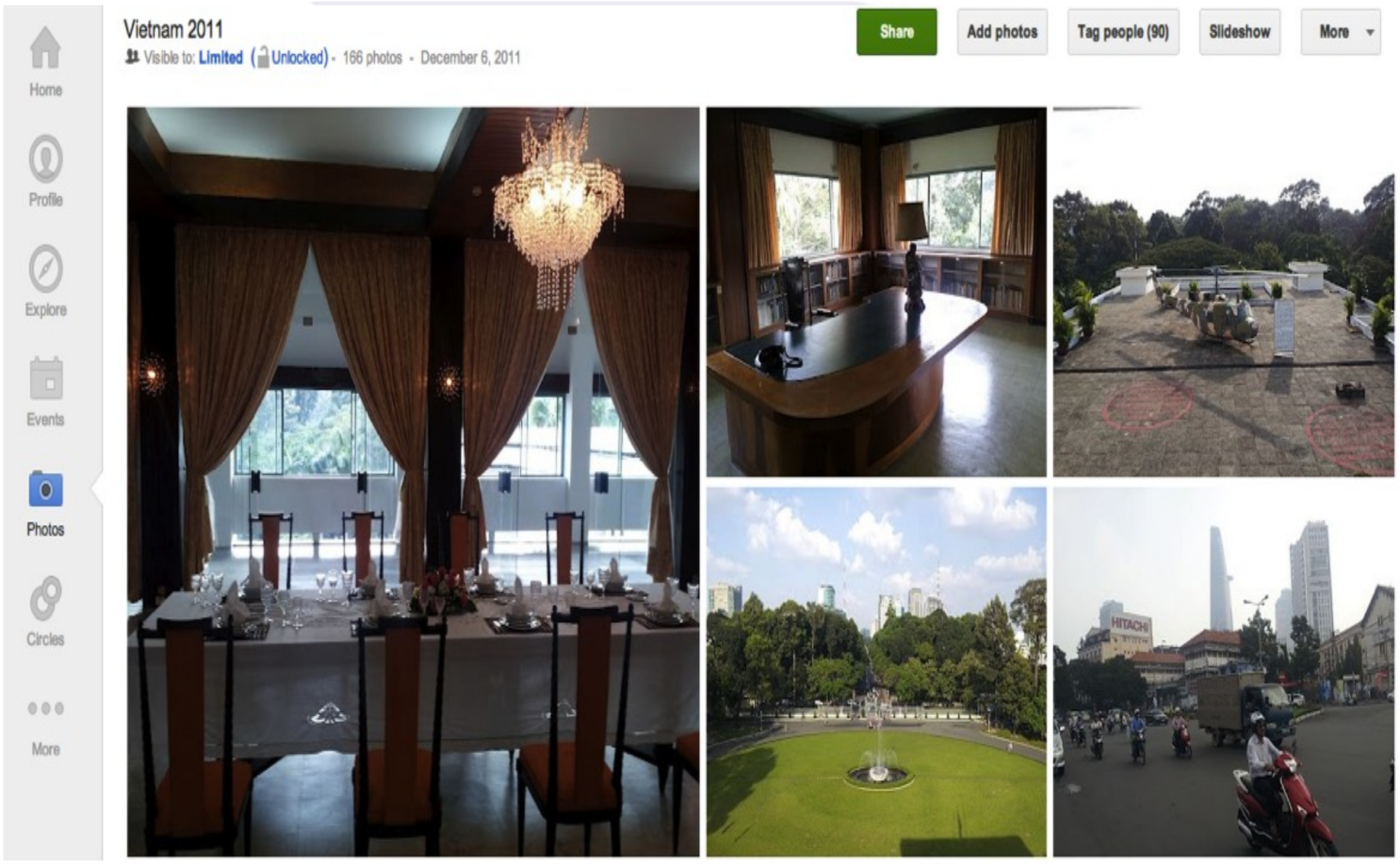
- Able to be executed on Computers, Tablets and Smartphones
- Able to access the data/information in Anywhere, Anytime and Any devices
- Run continuously (No crash, No loss)
- Pay by OPEX, not CAPEX
- Service (not Product)

Gmail


iPad
9:59 PM
30%
thananum@gm...
Inbox (136)
Edit
18 of 56
Search Inbox
Hide
Mark
หลิม M
9:45 AM
เอกสารประกอบการสมัครสมาชิก
Long Lam
Yesterday
visiting Thailand software park
Dear Thanachart, Thanks for your support. We will contact to Chamaipor...
NOOK by Barnes &...
Yesterday
Get This Week's Best Reads + Indie Tit...
To ensure you receive your Barnes & Noble emails, please add BarnesandNoble@m.bn....
Ramida
Yesterday
info@wealthmagik.c...
Yesterday
Twitter
Yesterday
Guardian Tech, Joe Trippi, and 6 other...
MMJT KMITL, Here's what's happening on Twitter Stories Facebook has 83 million 'fake...
BualuangiBankingAl...
Yesterday
Bangkok Bank Alert: Add Payee on 4...
info@wealthmagik.c...
Yesterday
(No Subject)
This message has no content.
BualuangiBankingAl...
Yesterday
Bangkok Bank Alert: Log-on on 4 Augu...
The Motley Fool
Friday
FoolWatch Weekly: How Dow Chemica...
To prevent this from getting swept up by overzealous email filters, add Fool@foolsubs...
Skype
Friday
We've delivered your order
This is an automated email, please don't reply.
Hi there Thanachart Numnondat, We've deliv...

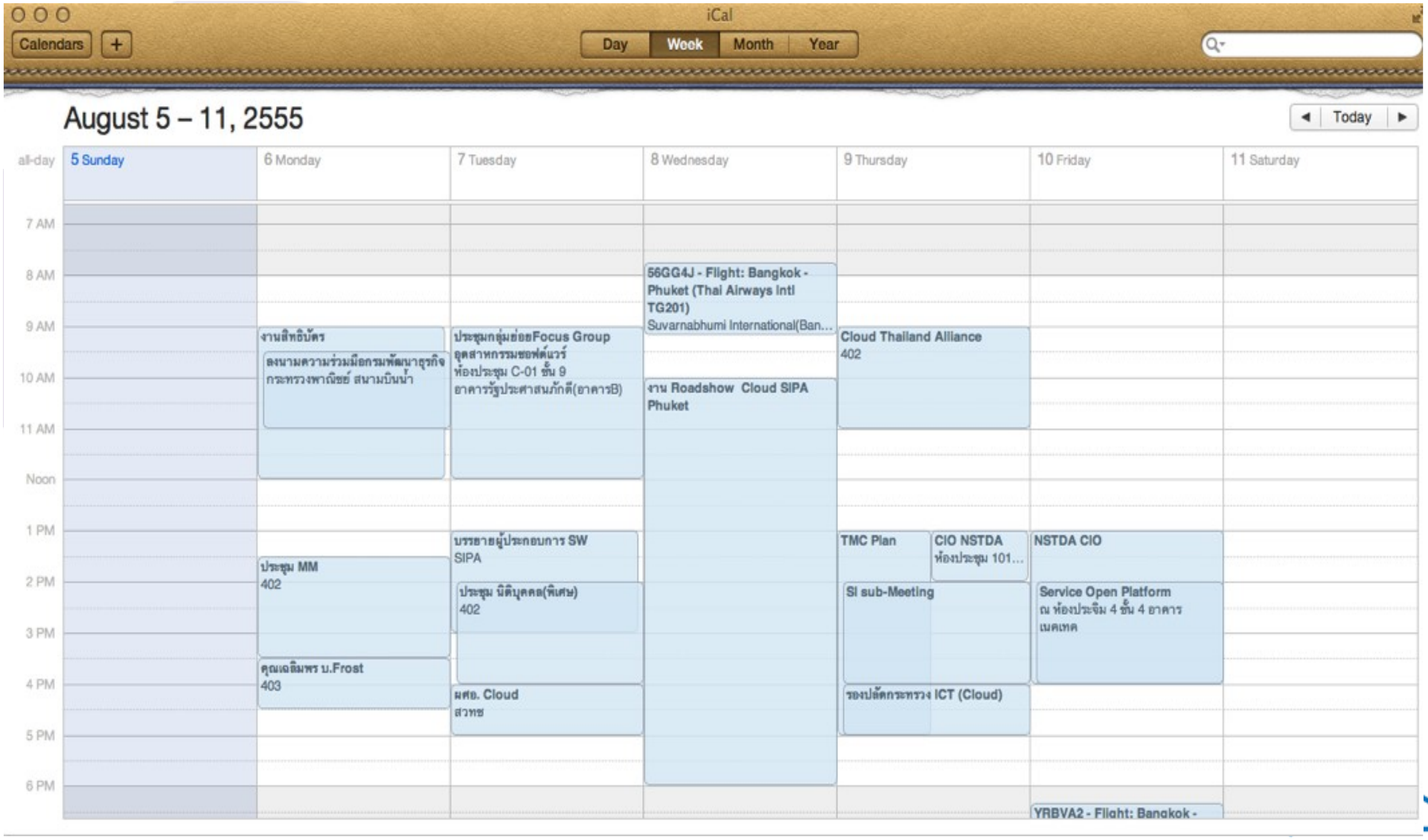

11:45
Inbox
thananum@gmail.com
88
ทีมงาน Google+
28 Jul
Angkut Roongsaengjan, Wittaya Assawsathain และอีก 1 คนแบ่งปันกับคุณใน
Twitter
28 Jul
BBC Click, charity: water, and 3 others have Tweets for you — [image] MMJT
Rodolfo Hwang
28 Jul
Get an MBA or Doctorate(PhD) in just 10 days based on your work or life
CaptureToCloud
28 Jul
New version adds editor to Edit Web Pages, Create Notes, and More —
The Motley Fool
27 Jul
FoolWatch Weekly: Should You Buy Now or Wait for a Brighter Day? — [image:] To
no-reply@mebmarket.com
27 Jul
mebmarket.com : Order Success [Apple]
— [image] เรียนคุณ thananum

Picasa


Home
Profile
Explore
Events
Photos
Circles
More
Vietnam 2011
Visible to: Limited (Unlocked) - 166 photos - December 6, 2011
Share
Add photos
Tag people (90)
Slideshow
More

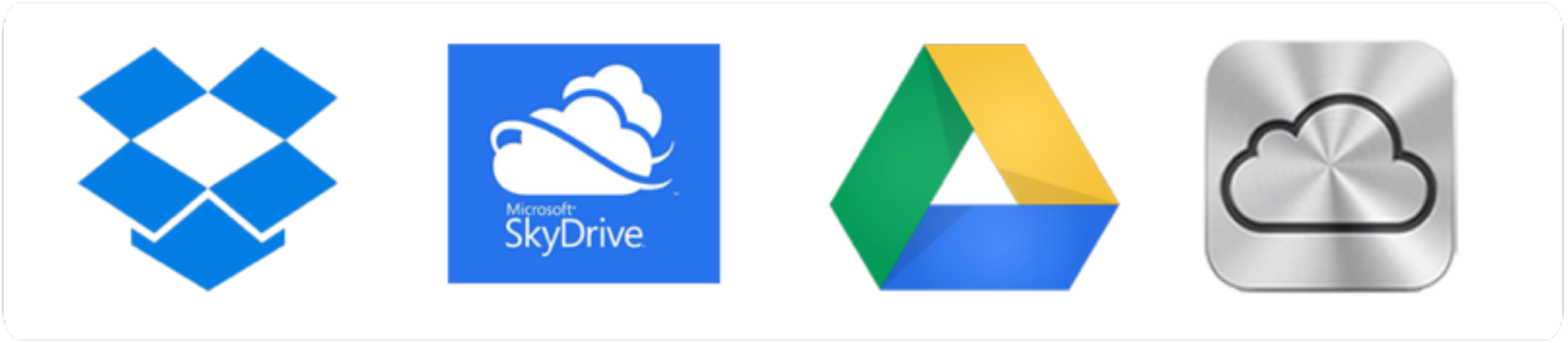

11:55
Vietnam 2011
Next
1/12
10,000++ Galaxy S II Games for download!

Google Calendar

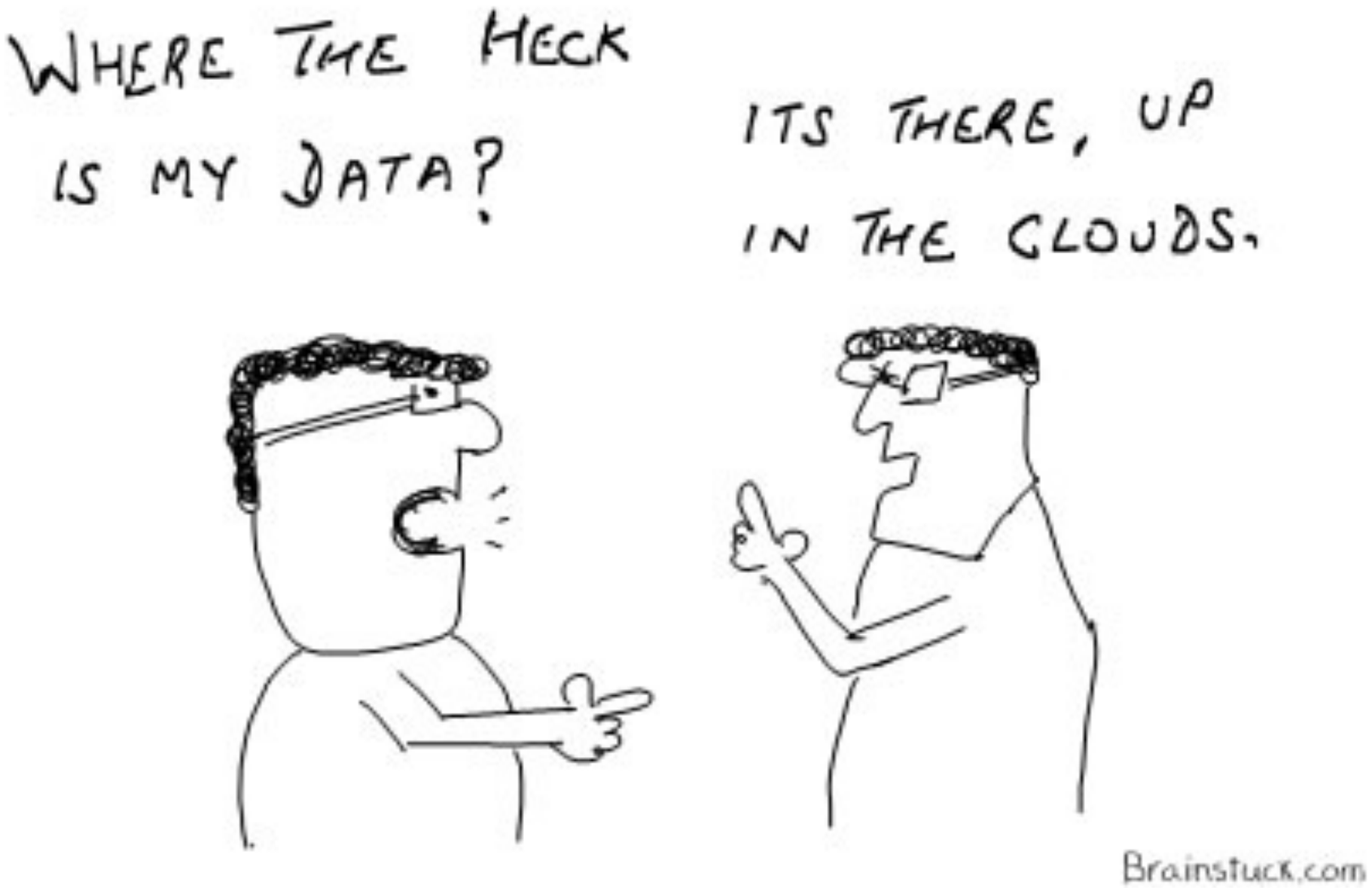


Google docs

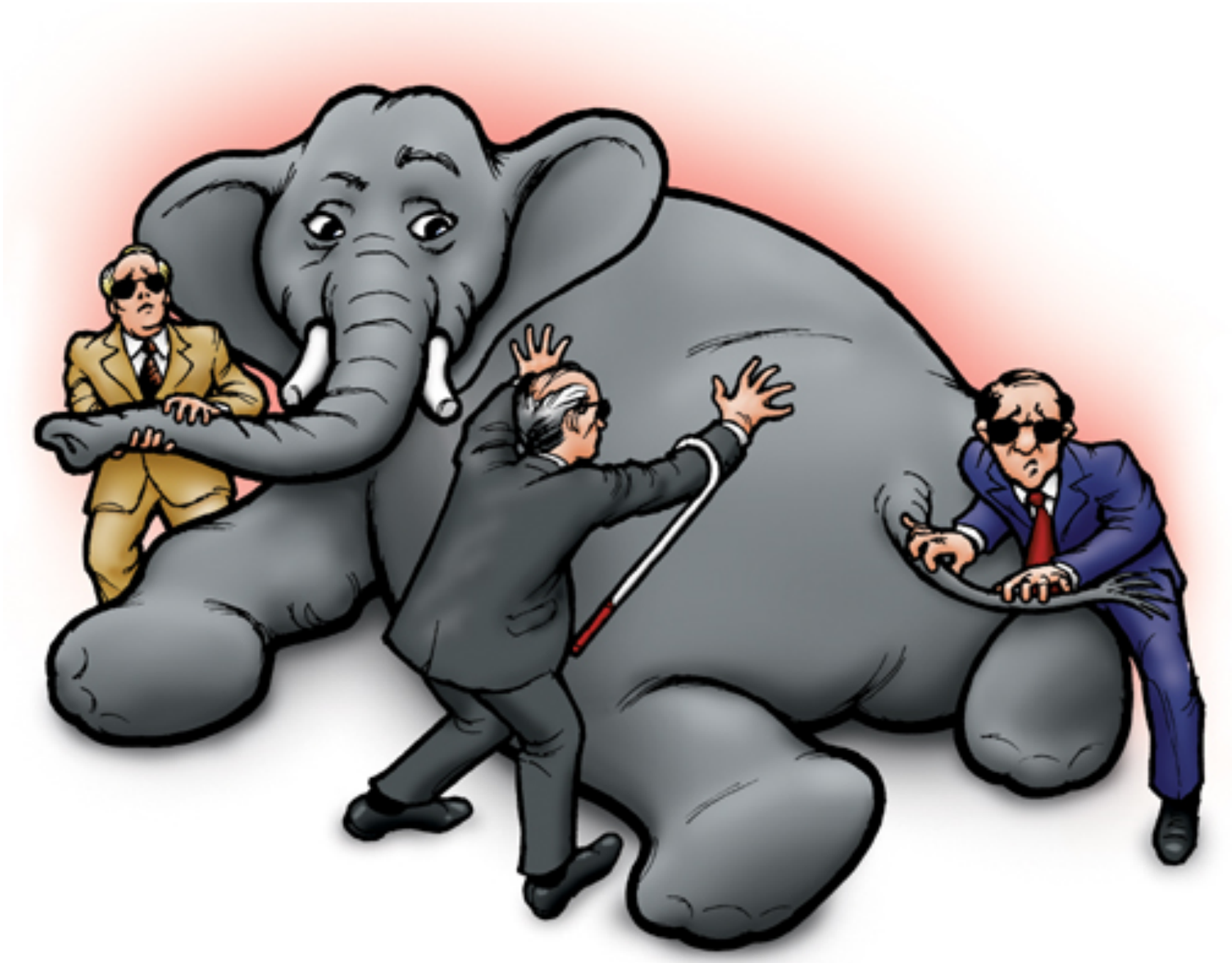
Cloud Storage



Do you know what does he say?



What is Cloud?



Cloud security Risks & Challenges

- Conflicts with international privacy laws
- Data ownership
- Service guarantees
- Securing virtual machines
- Massive outages
- Encryption needs & Standards
- Storing sensitive & personal information in clouds
- Contingency planning / disaster recovery for clouds

CSA Top Threats

- Data Breaches
- Data Loss
- Account of Service Traffic Hijacking
- Insecure Interfaces and APIs
- Denial of Service
- Malicious Insiders
- Abuse of Cloud Services
- Insufficient Due Diligence
- Shared Technology Vulnerabilities

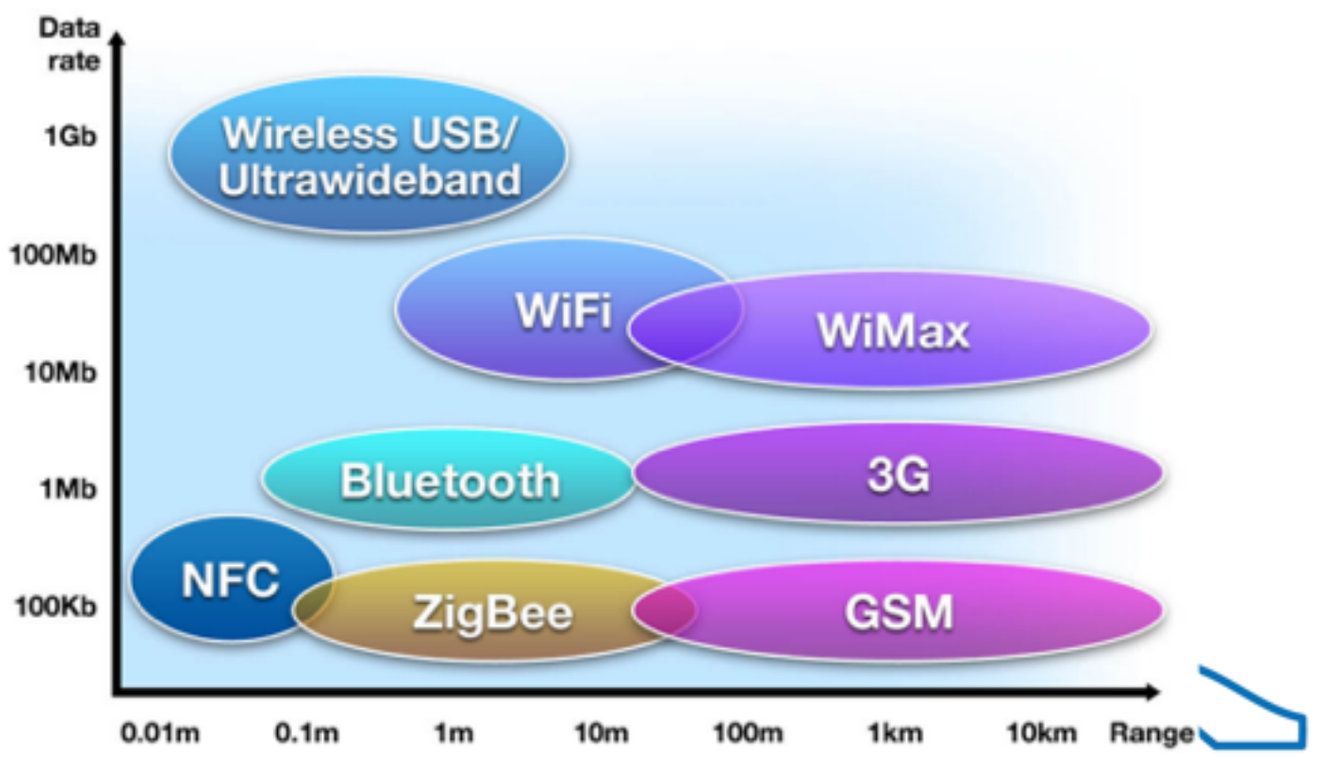
Mobile devices

Windows phone android iPhone BlackBerry. palm webOS

Mobile devices

Connection technology

- 3G, 4G or EDGE
- Wifi, WiMax
- NFC - Near Field Communication
- DLNA - Digital Living Network Alliance
- Bluetooth



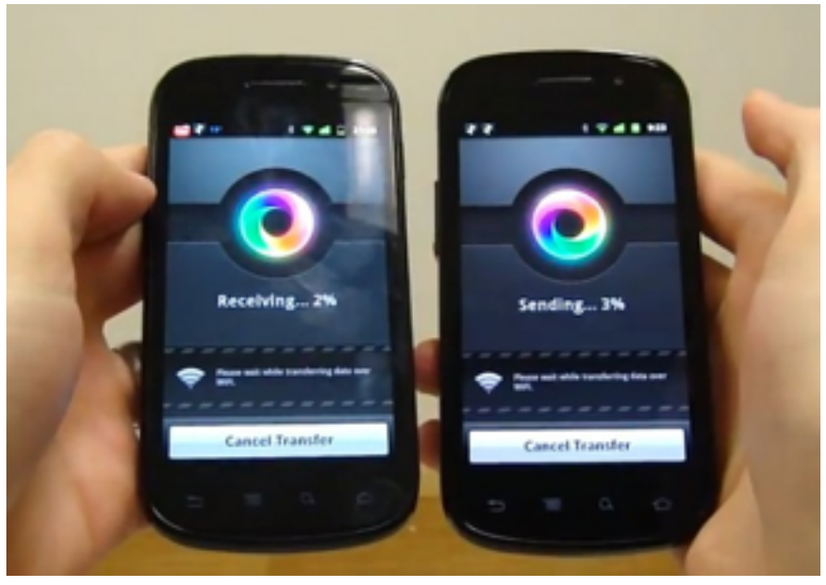
NFC


SAMSUNG


simplicity


Suica
Suicaを
ふれてください


Special offer
€ 2,00
LetsGoMobile


Receiving... 2%
Cancel Transfer
Sending... 3%
Cancel Transfer

Recent mobile devices

- Truly handheld computer
- Connectivity everywhere
- Apps for everything
- Cheap

Simple Questions

- Do you Lock your mobile device?
- Do you have Anti-malware installed?
- How many Apps in your device?
- Are them all Trustworthy?
- Have you ROOTED/Jail-broken your device?

The Common Fails!

- Lost
- Stolen
- Free WiFi lovers
- Lots of apps (Trusted/Untrusted)
- No passcode protected
- Location services
- Left unattended
- Just click
- Full time WiFi on and with “Auto connect”

Threats (1/2)

- Malware
  - Zeus
  - Spyphone
- Phishing - SMS (Already talked)
- WiFi attacks
  - War Driving and WiFi Sniffing
  - Rouge Access points
  - Man in the Middle Attacks
- Theft and Loss
- Violation of Privacy (EXIF)

Threats (2/2)

- QR Code
- SPIM : Spam on Instant Messaging
- Credential stolen

Theft / Loss

Data is the most important thing in our mobile.

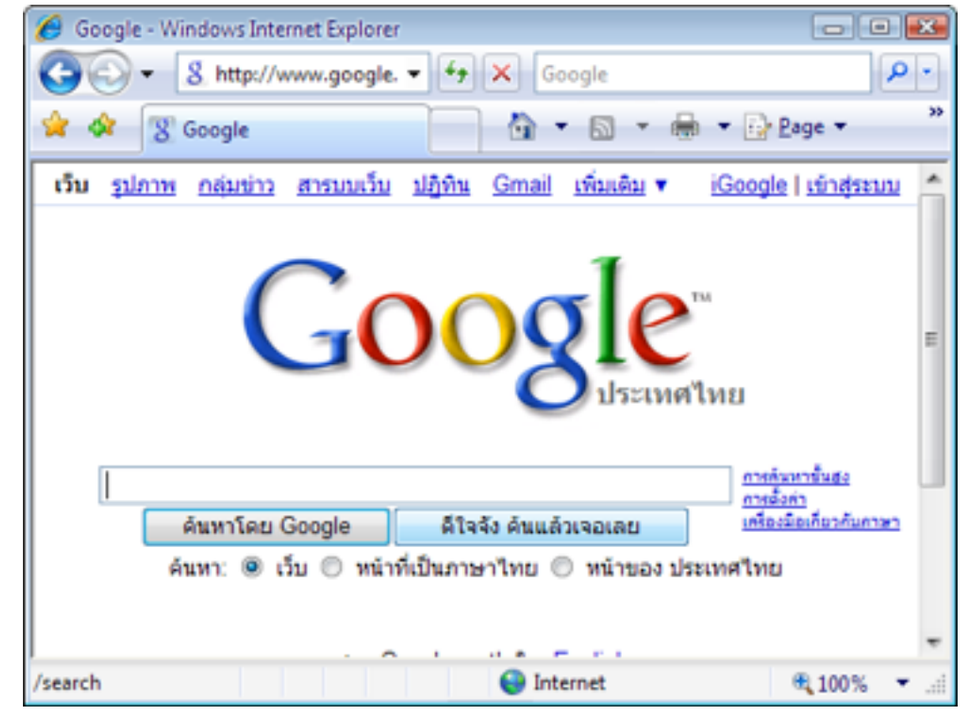
Information Leaks

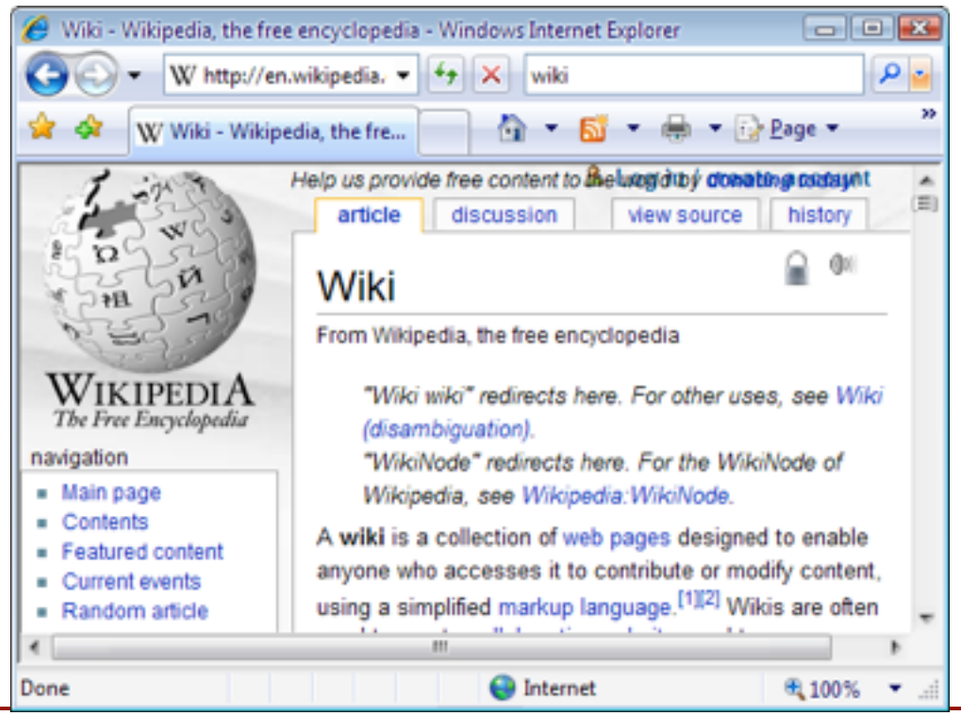
Information Leakage

- Confidential Report
- New campaign/project
- Sensitive information

- Organization may lose customers and profit
- May destroy reputation of organization
- May affect the national security of Thailand

3 Jedi Master





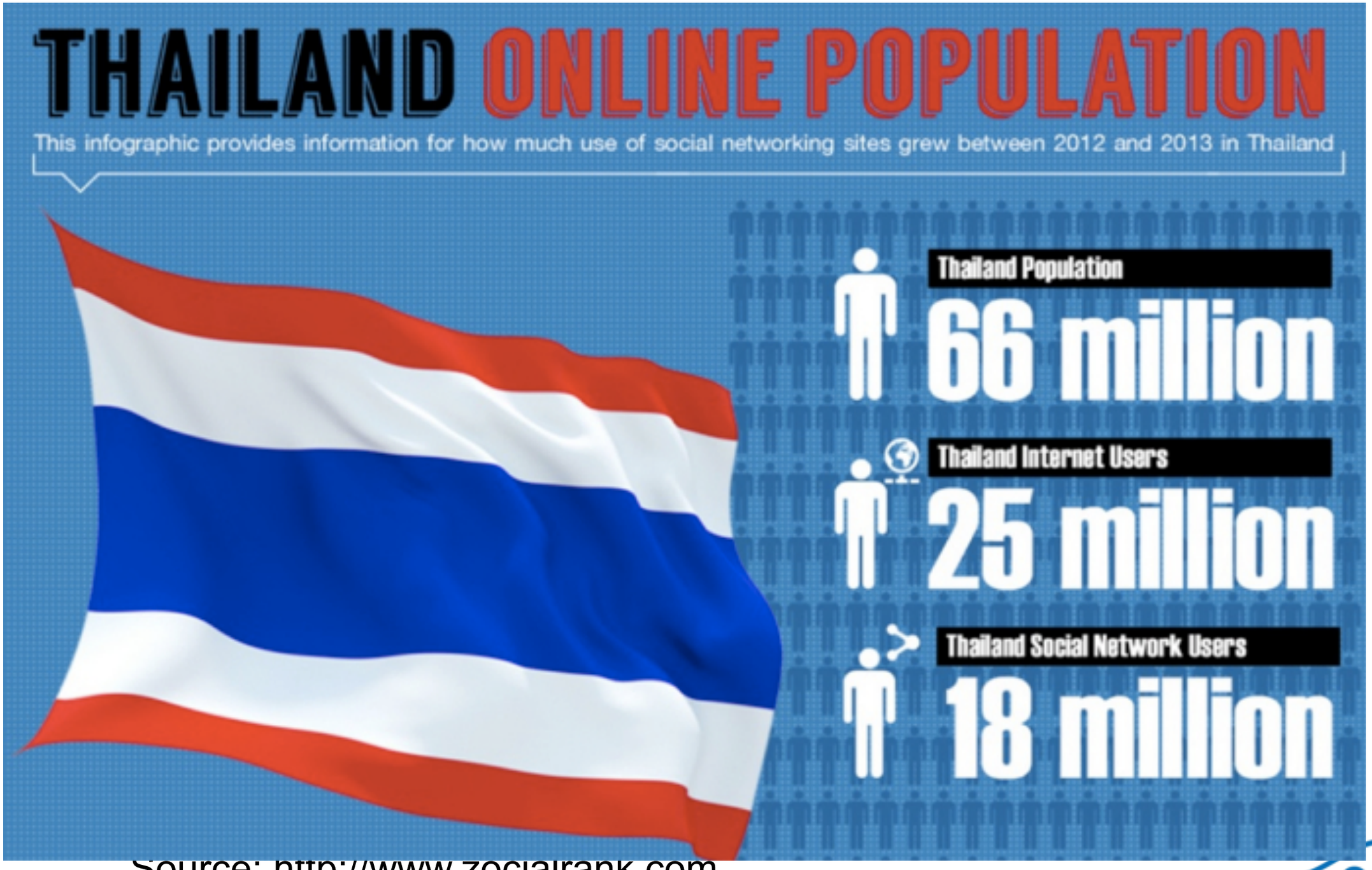
Google : Best Friend of Hacker

http://www.linuxexposed.com/Articles/Hacking/Google-A-Hackers-Best-Friend.html

Google can find

- Personal information
- Email addresses
- Confidential data
- Insecure database

Facebook users statistics



Source: http://www.zocialrank.com

TOTAL THAILAND FACEBOOK USER

18.5 MILLION

9.3 million user

9.0 million user

Other 0.2 million user

#ZocialAward Data from ZocialRank.com

Zocial inc. Online Analysis

EGA e-Government Agency

G-CERT by EGA

TOTAL THAILAND TWITTER USER

2 MILLION

Average

> 5.5 Tweet/Day

> 0.4 RT / Tweet

> 200,000 active user/day

#ZocialAward Data from ZocialRank.com

Zocial inc.
Online Analysis

Total Video in Youtube by Thai People

5.3 million

Average New

2,500 Upload Viedo/day

#ZocialAward Data from ZocialRank.com

Zocial inc.
Online Analysis

EGA
e-Government Agency

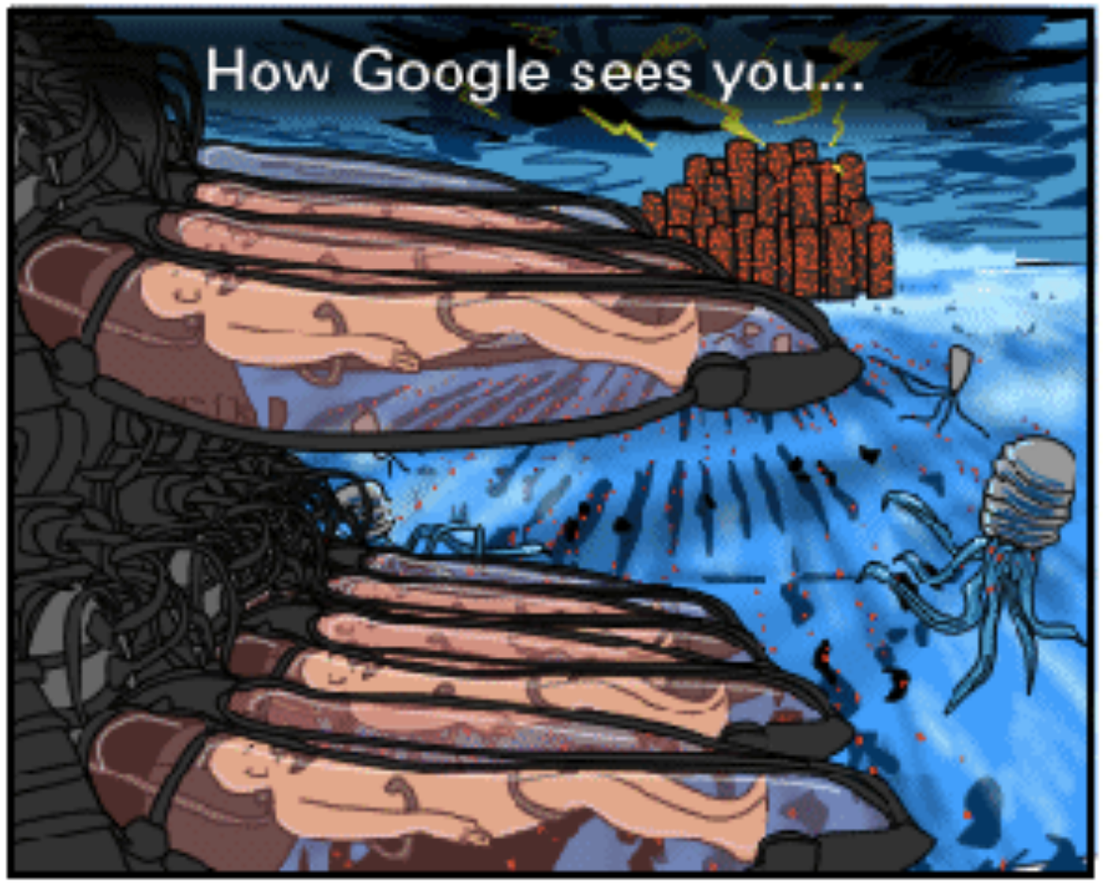
G-CERT by EGA

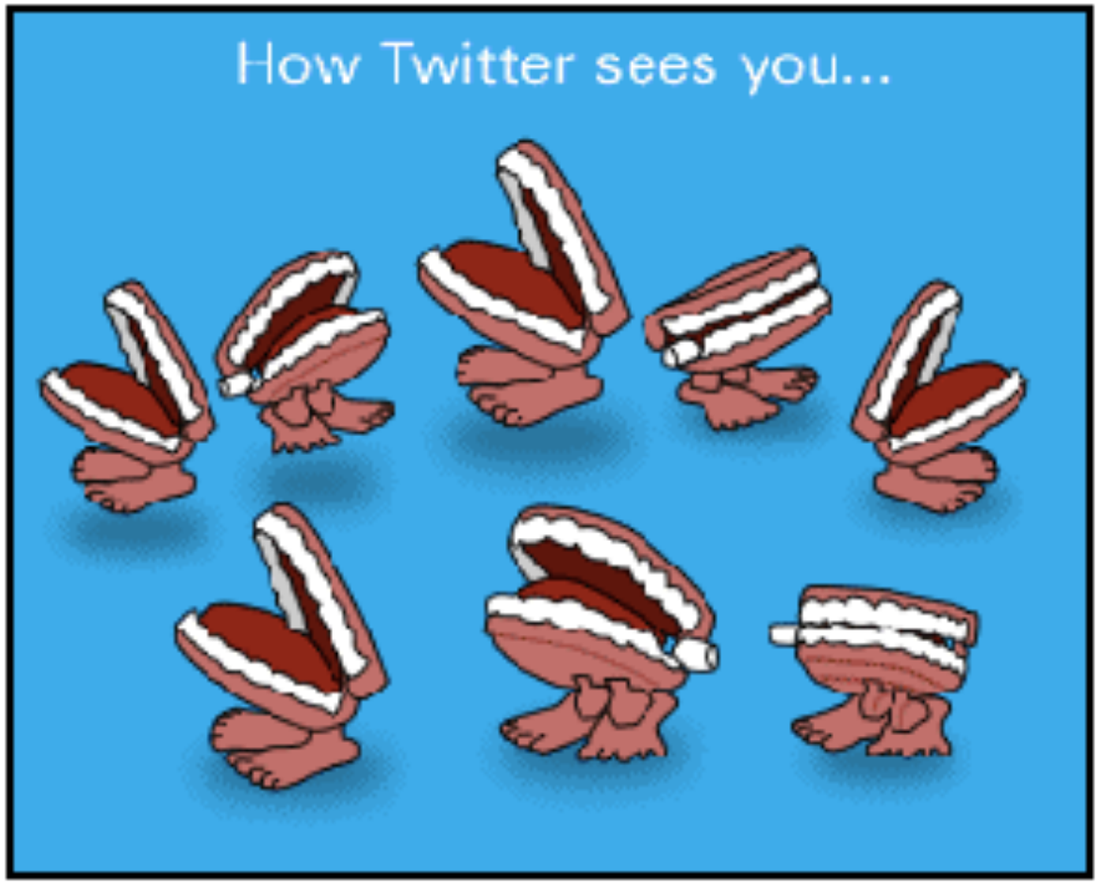
Total Line user in Thailand

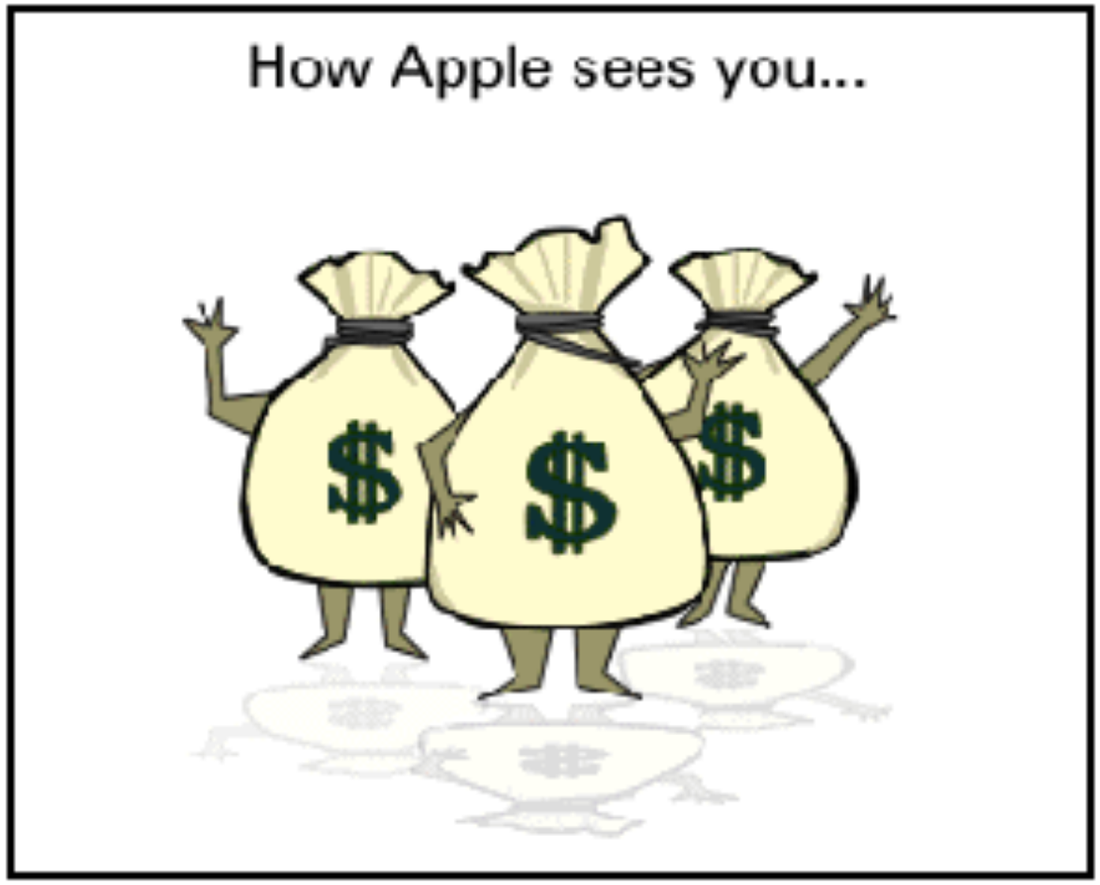
15 Million User

The Joy of Tech™

by Nitrozac & Snaggy







Account Compromised

- Attack the weak password
  - Guess, Bruce force, Dictionary, etc.
- Attack the forgotten password feature
  - Need your private information
  - Can you guess where can we find?
    - Will talk again in the Privacy Violation topic
- Attack other related account (such as Email)
- Social Engineering (Phishing or Vishing)

Information Warfare

- Discredit the opposite
- Rumors

Source pic :
http://danzarrella.com/
http://www.112victims.net/

Political problems in Thailand

FB and Thai Politics

facebook 3 Search

Red Democracy ประชาธิปไตยในทัศนะของคนเสื้อแดง

facebook 3 Search

กลุ่มคนต่อต้านม็อบเสื้อแดง - Anti-Red Shirt Join

Wall | Info | Discussions | Photos | Video | Events

Basic Info

Name: กลุ่มคนต่อต้านม็อบเสื้อแดง - Anti-Red Shirt

Category: Common Interest - Politics

Description: เราไม่ชอบการชุมนุมแบบอันธพาล จาบจ้วงสถาบันและองคมนตรี เที่ยวทุบทำลายเผาบ้านเผาเมือง
ปากว่าทำเพื่อประชาธิปไตย แต่ว่าแท้จริงแล้วทำเพื่อไอ้หน้าเหลี่ยม

ก่อตั้งเมื่อ วันพุธ ที่ ๑๗ กุมภาพันธ์ ๒๕๕๓ เวลา ๒:๐๖ นาฬิกา
(read more)

Privacy Type: Open: All content is public.

Recent News

Suggest to Friend

http://www.rajdur
index.php

http://www.matich

ถ้าเข้ามาเยี่ยมเฉยๆก็แล้วไปจ้ะ แต่ถ้าเข้ามาแสดงความบ้องตื๊นคุณจะเละคาบอร์ดเนี่ยแหละ ^^

Do you know them?

Violation of Privacy

- Private information
  - Birthday, Tel no., e-mail, and activities etc.
- Photo of specific person
- job title, resume, favorites
- Location
  - Geotagging, Places, 4square, etc.
- Video - Socialcam
- Relationship
  - Touchgraph

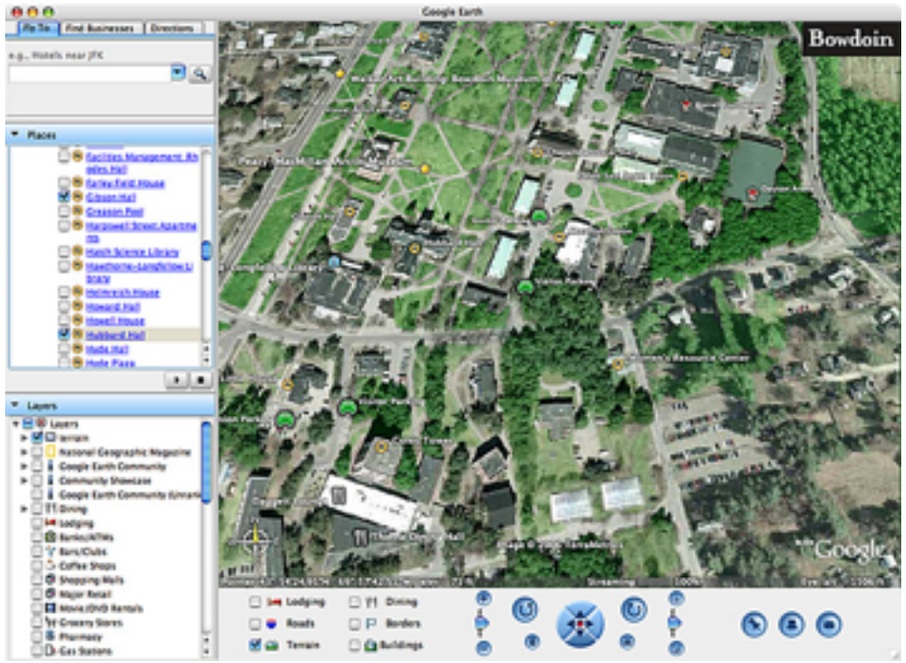
Cyber Stalking

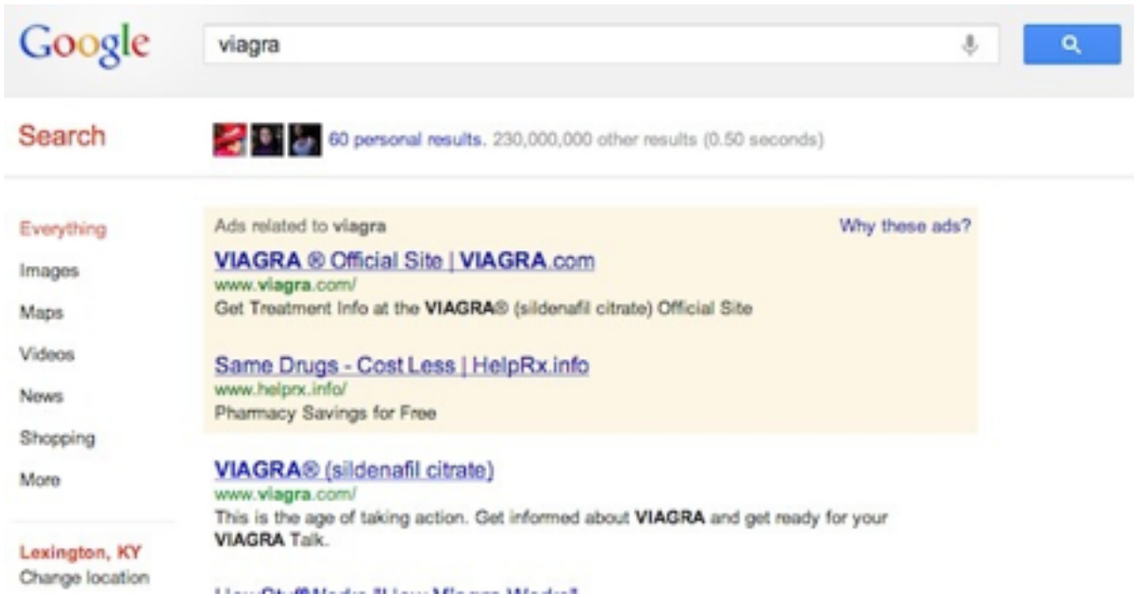
Mobile device + Camera + GPS + Social media = ?

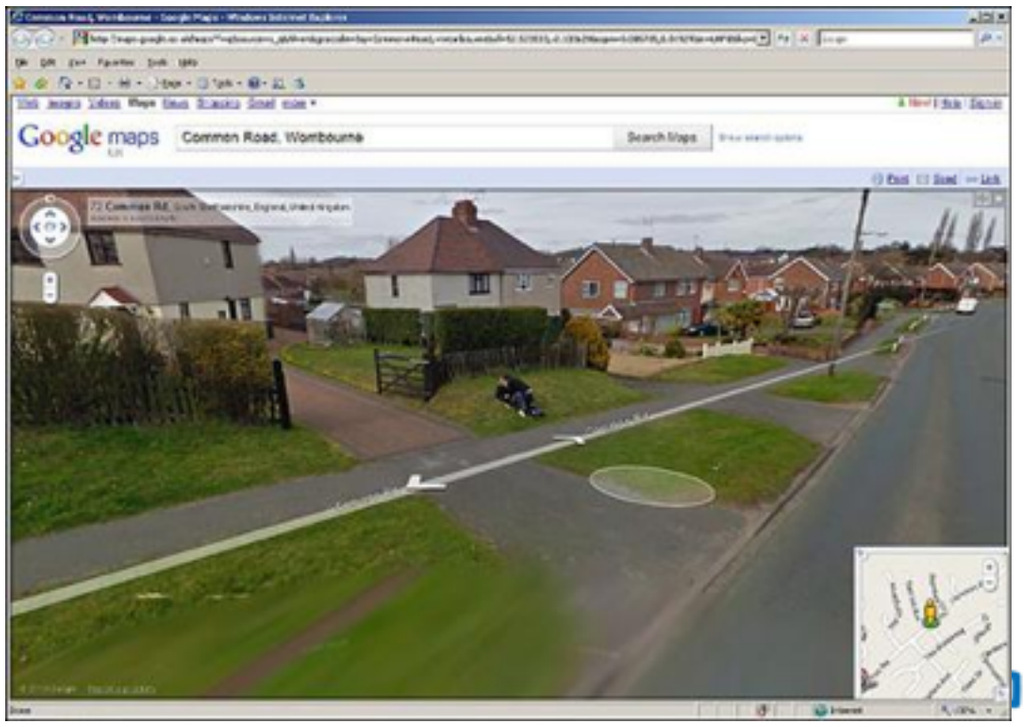
- EXIF (EXchange Information Format)
- Location service is “ON”
- Lead to the Cyber Stalking

```
GPS Altitude                    : 0 m Above Sea Level
GPS Latitude                    : 14 deg 4' 37.98" N
GPS Longitude                   : 100 deg 36' 7.20" E
GPS Position                    : 14 deg 4' 37.98" N, 100 deg 36' 7.20" E
```

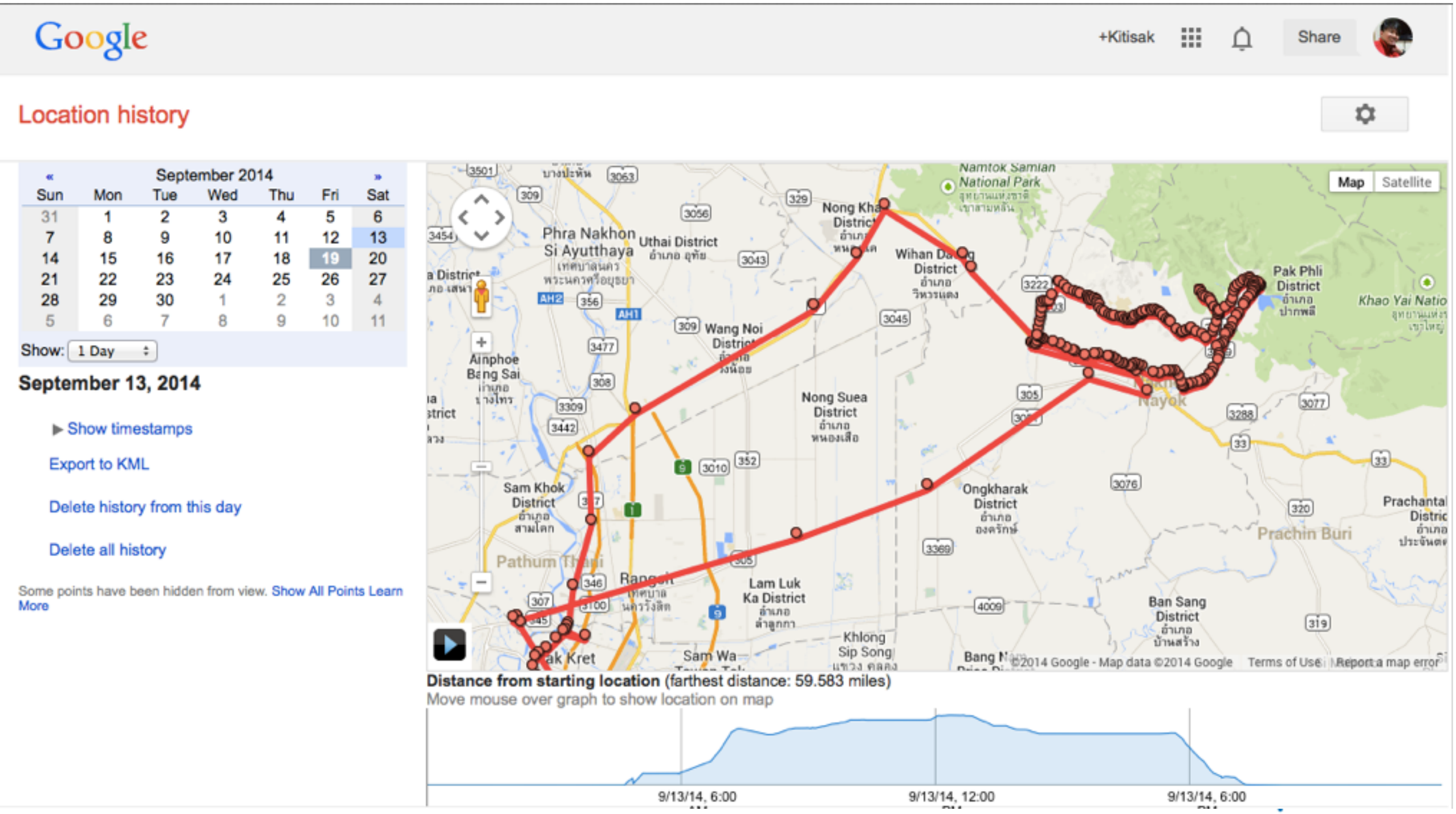
One Stop service - Google







Google map tracking



Tips

- Strong passwords
- Classify information to be stored on cloud
- Do not connect to untrusted wifi
- 2 Factors (steps) authentication
- Update patches and Anti-malware software

Strong Password

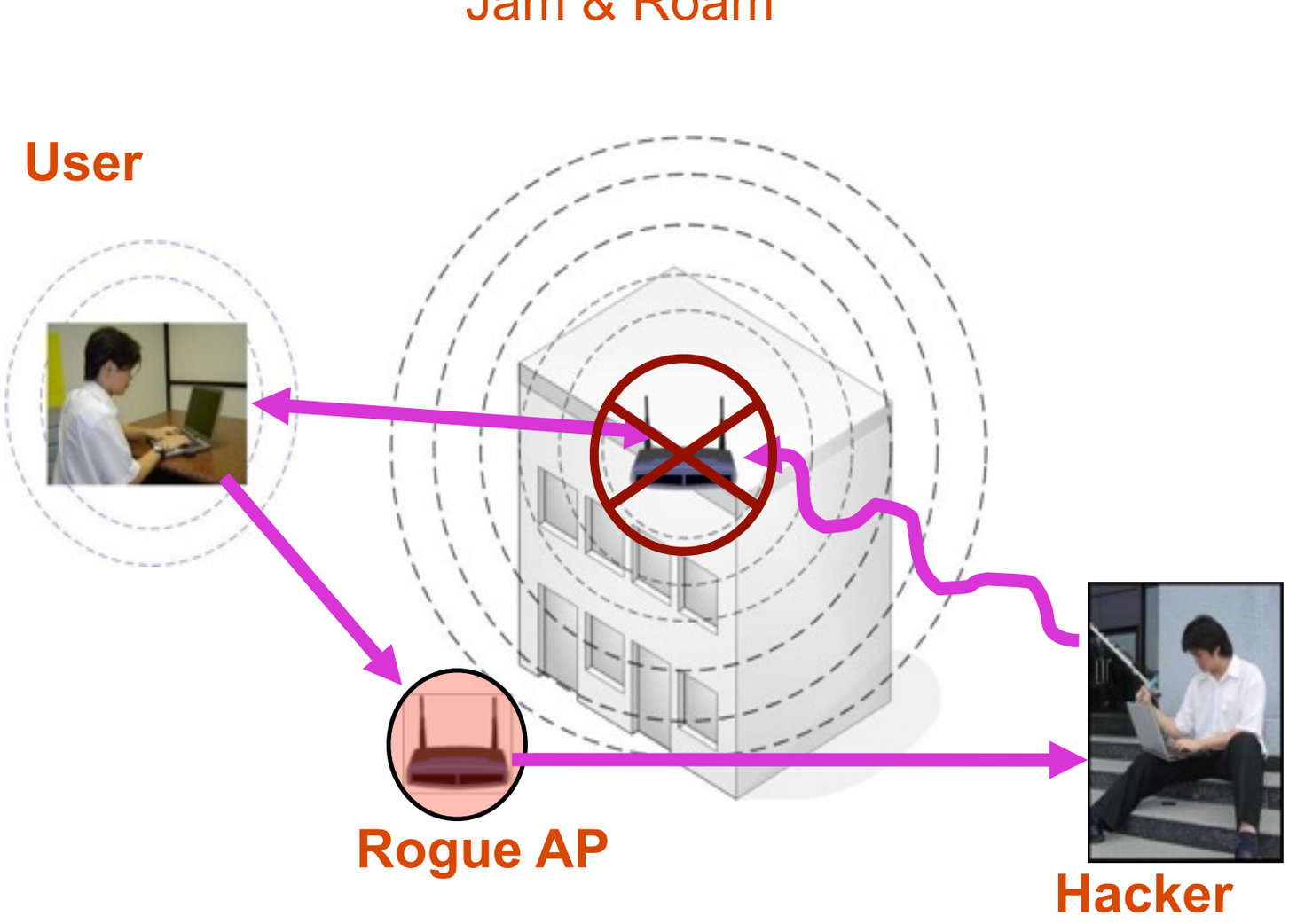
- Long and Complex
  - 8++ characters
  - Lower and Upper case, Number and Special characters
- Do not use specific name or word in dictionary
- Change frequently (every 3 months)
- Do not put your password on your screen

Which information can be stored on Cloud?

- General
  - Public information
- Confidential
  - Do not store on cloud
  - Encrypt before storing

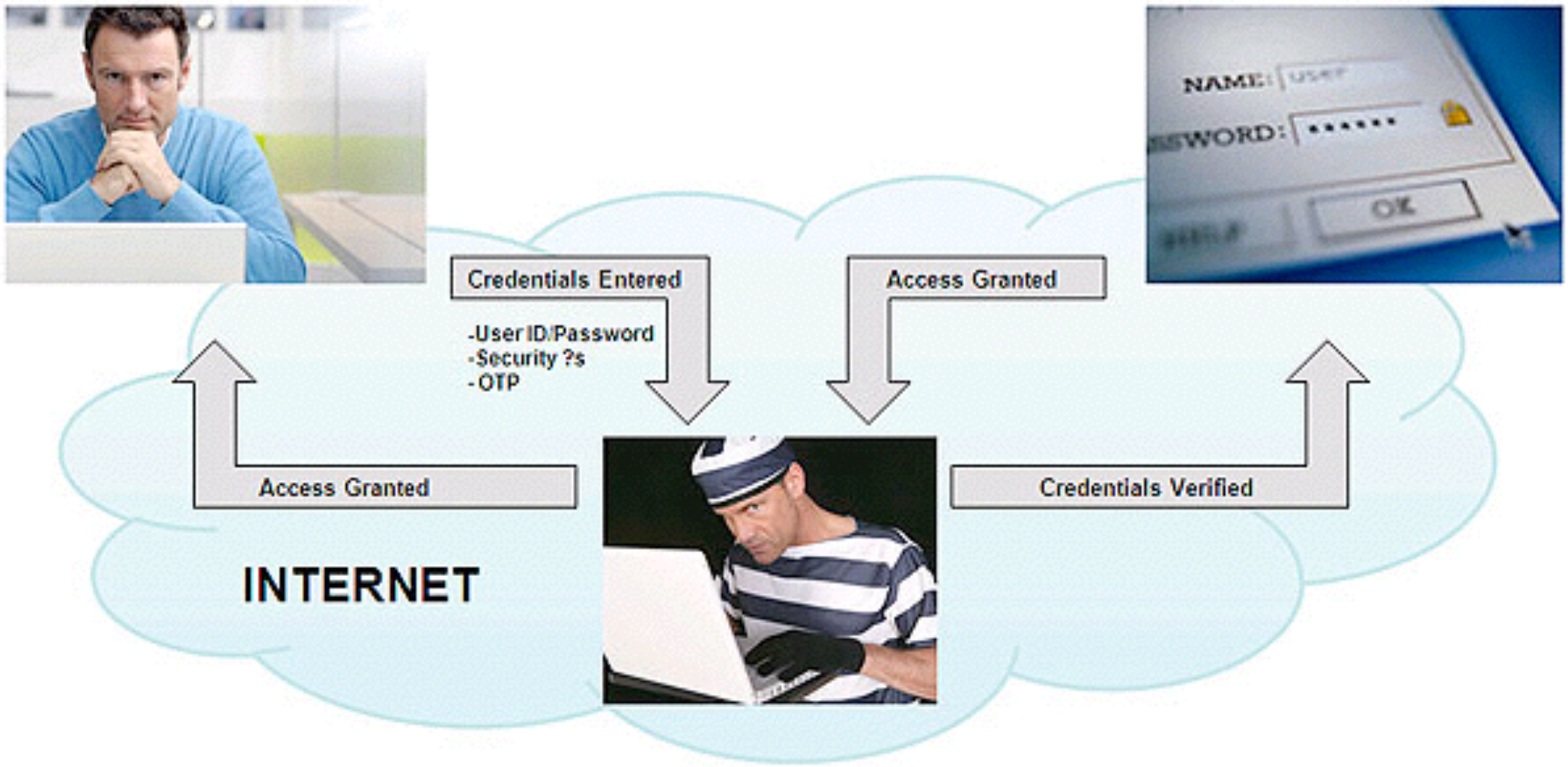
WLAN Security Threats

- User hijacking & Man-in-the-middle attack



- Inverse Wardriving
- Sniff & Modify
- Fake server and AP
- Https hack
- SSL Strip
- Faked Certification
- Password stealing
- “Phishing”

Man In The Middle attack

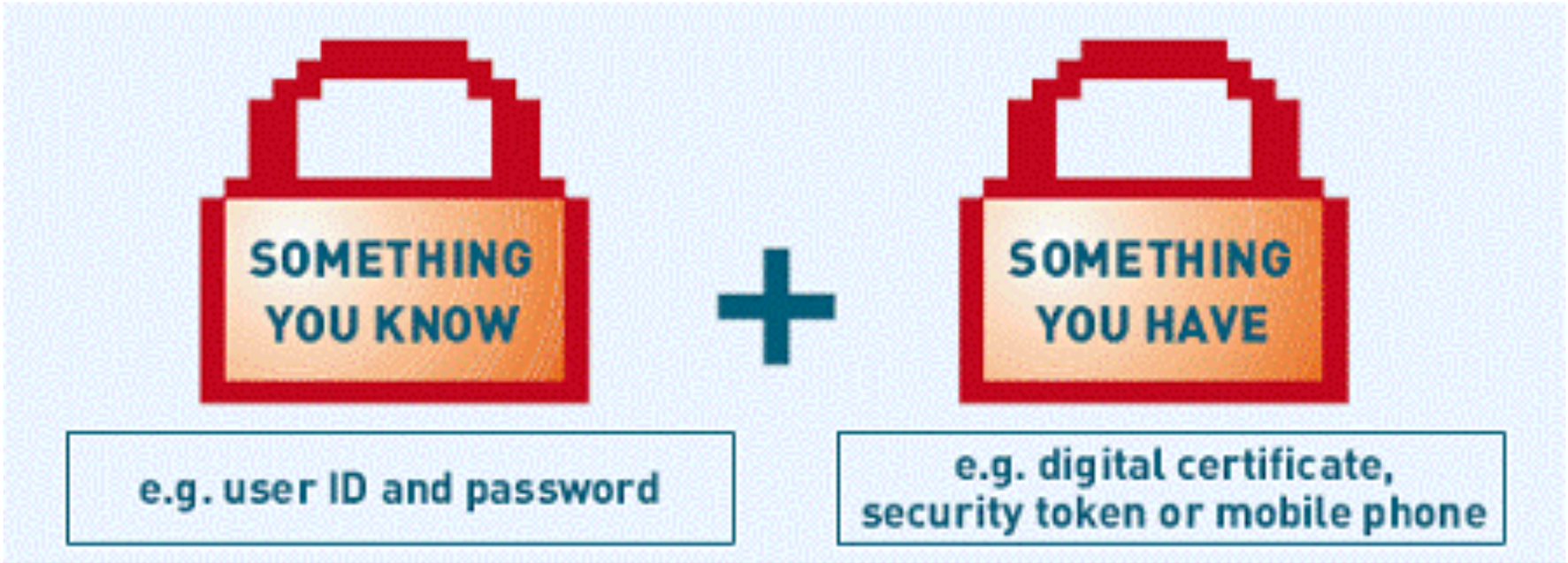


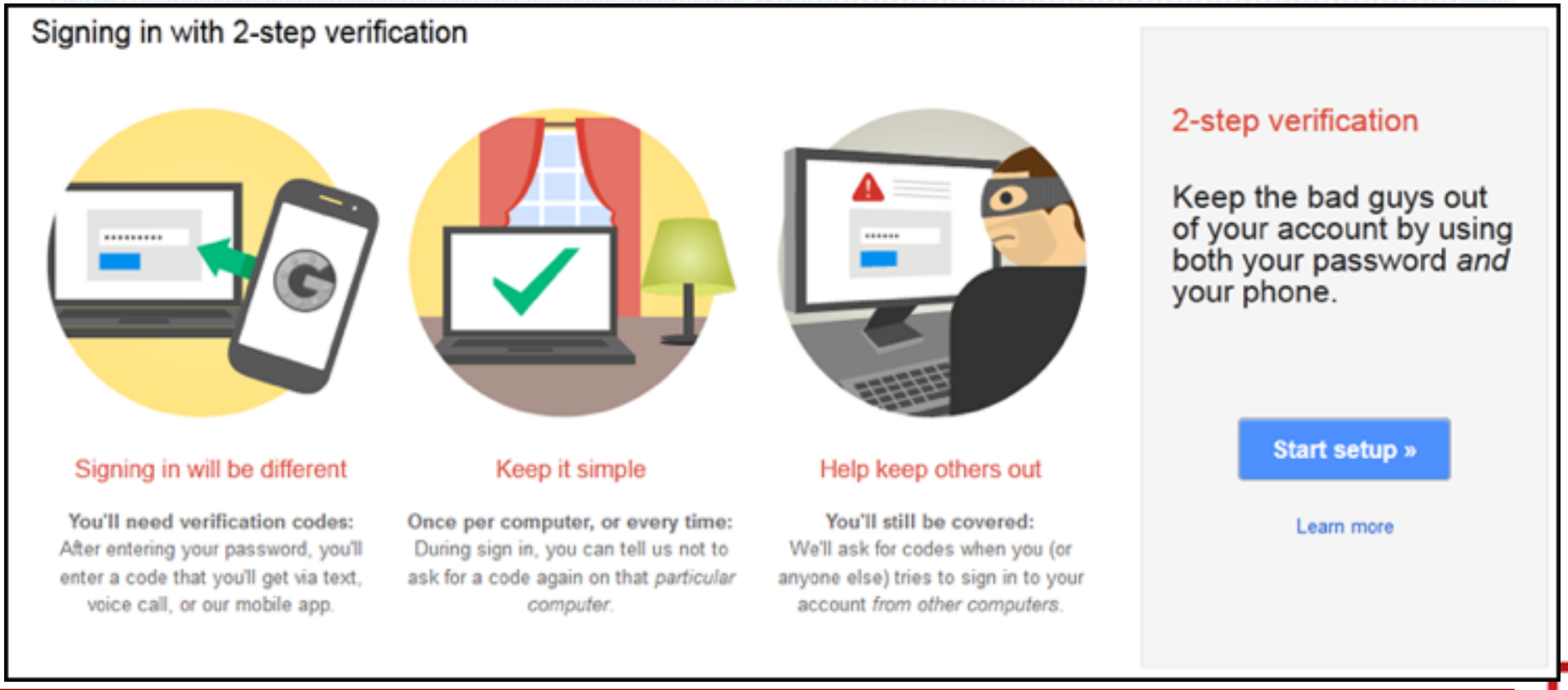
How to use WiFi securely?

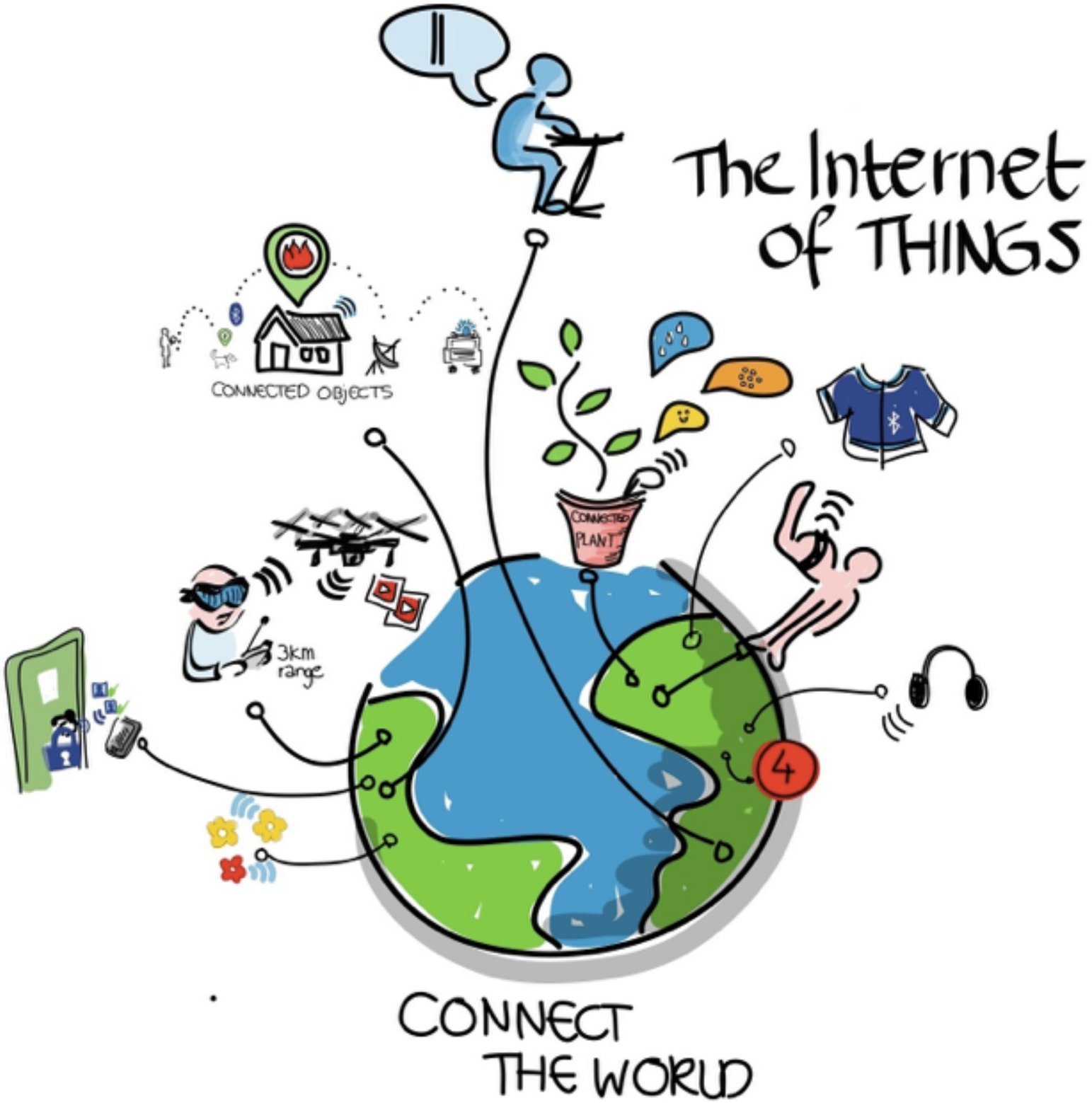
- Use only trusted WiFi network (access point)
- Look carefully at the access point name
- Remove the unused access point name from list
- Select to connect to only the encrypted connection (WPA2, WPA and WEP)
- Install “HTTPS Everywhere” extension for Chrome and Firefox
- Do not share files and folders
- Turn on personal firewall

  Details in Thai : http://foh9.blogspot.com/2012/09/blog-post.html

2-Factor/Step Authentication

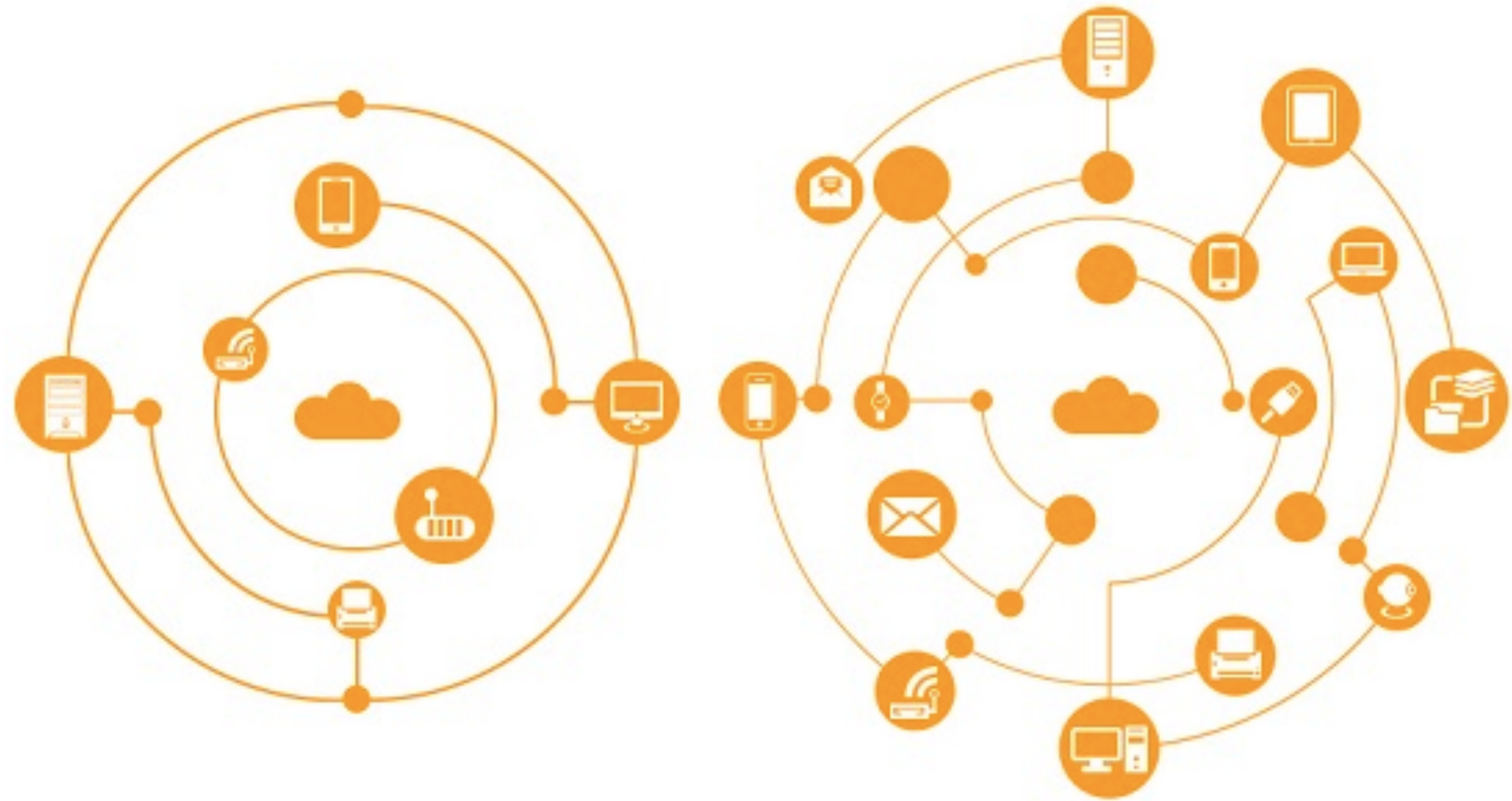






http://static.myce.com/images_posts/2015/11/Internet_of_Things.jpg

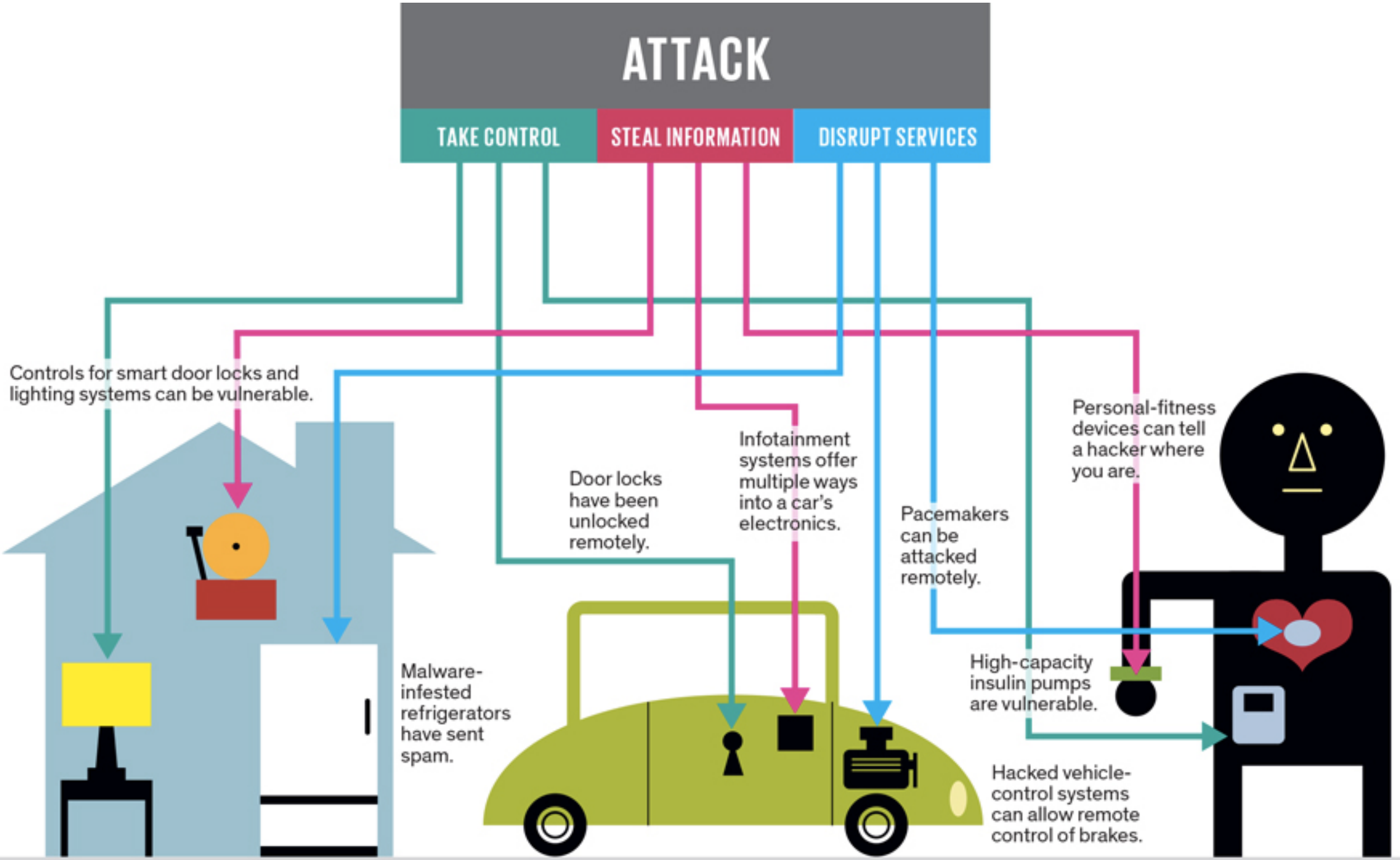
IoT era



Corporate networks then

Corporate networks now

http://blog.trendmicro.com/trendlabs-security-intelligence/organizational-challenges-in-the-internet-of-things/


ATTACK
TAKE CONTROL
STEAL INFORMATION
DISRUPT SERVICES
Controls for smart door locks and lighting systems can be vulnerable.
Door locks have been unlocked remotely.
Infotainment systems offer multiple ways into a car's electronics.
Personal-fitness devices can tell a hacker where you are.
Pacemakers can be attacked remotely.
Malware-infested refrigerators have sent spam.
High-capacity insulin pumps are vulnerable.
Hacked vehicle-control systems can allow remote control of brakes.


HISTORY
Dailymotion
LOVE FiLM.COM
YouTube VIDEOS
AccuWeather.com
gettyimages
rovi TV Listings
USA TODAY
BBC iPlayer
MUZU.TV THE MUSIC VIDEO SITE
Wii
PLAYSTATION 3

Wearable devices

DLNA

New generation

- PC liked
- Connect to the internet
- Many apps provided
- Not many people concern about security

What will we do, if ...

- Malware is infected on TV or Refrigerator
- TVs are hacked
- Spam are sent to show on our TV
- Game consoles break down because of malware or hacker
- We need to investigate TV or other non-PC devices for finding criminals

How to protect Malware?

- Antivirus
- Personal firewall
- Apply security patch
  - To OS and applications
- Stop file sharing
- Back up
- Monitor information
- Do not access to suspicious website
- Do not open suspicious e-mail

Contact me

Name : Kitisak Jirawannakool

Facebook : http://www.facebook.com/kitisak.note

Email : kitisak.jirawannakool@ega.or.th

jkitisak@gmail.com

Weblog : http://foh9.blogspot.com

Twitter : @kitisak

Thank You