บทที่ 1 : การรักษาความปลอดภัยข้อมูล Part3

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

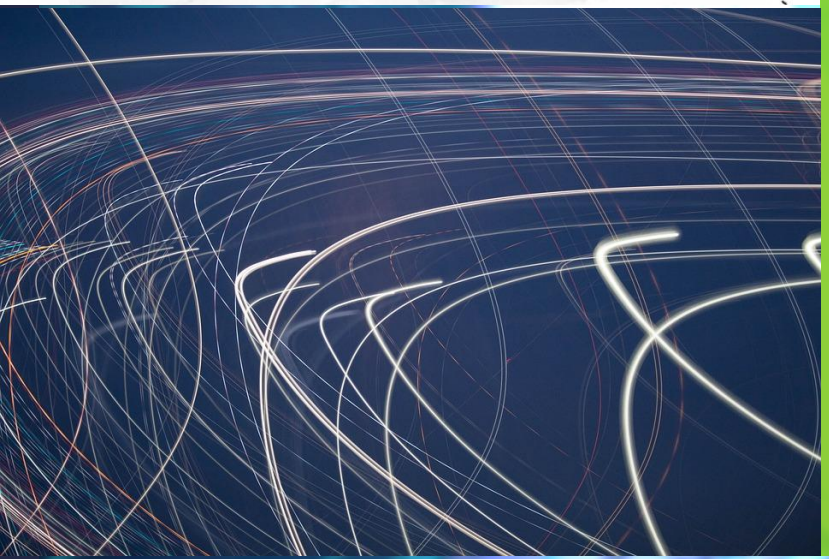
Agenda

- แนวโน้มการโจมตี
- เครื่องมือสำหรับการรักษาความปลอดภัย

แนวโน้มการโจมตี

- การโจมตีที่มีความรวดเร็ว
- การโจมตีที่มีความซับซ้อน
- การค้นหาจุดอ่อนได้อย่างรวดเร็ว
- การโจมตีเป็นแบบกระจาย

การโจมตีที่มีความรวดเร็ว



- ด้วยความสามารถของเครื่องมือสมัยใหม่ และความง่ายในการได้มาซึ่งเครื่องมือ ทำให้ผู้โจมตีสามารถสแกนหาเป้าหมายที่มีช่องโหว่และโจมตีด้วยความรวดเร็ว
- ปัจจุบันเครื่องมือสำหรับการโจมตี สามารถโจมตีได้เองโดยไม่ต้องอาศัยมนุษย์ในการควบคุม จึงทำให้ใช้ระยะเวลาในการโจมตีลดลงเรื่อยๆ

Powered by ThreatCloud Intelligence

THREATCLOUD

LIVE CYBER ATTACK THREAT MAP

Check Point SOFTWARE TECHNOLOGIES, INC.

5

ATTACKS TODAY

(since 12AM PST)

281,854

ATTACKS YESTERDAY

3,918,066

- TOP TARGET COUNTRIES
- TOP ATTACKING COUNTRIES

TIME	ATTACK	ATTACKING COUNTRY	TARGET COUNTRY
23:00:42	Phishing.dgocfm	France	Switzerland
23:00:42	Phishing.dgocfm	France	Switzerland
23:00:42	infecting website.lkbc	United Kingdom	United Kingdom
23:00:42	Malicious Binary.crwpzde	Russia	Ukraine
23:00:42	Generic.cmvq	Germany	Switzerland

Attackers

Targets

https://threatmap.checkpoint.com/ThreatPortal/livemap.html

การโจมตีที่มีความซับซ้อน

- รูปแบบการโจมตีในปัจจุบันมีความซับซ้อนเพิ่มมากขึ้นเรื่อยๆ บางเครื่องมือโจมตีมีความหลากหลายในตัวเอง ทำให้การโจมตีแต่ละครั้งแตกต่างกันไป ทำให้ตรวจจับยาก
- เช่น หันมาใช้โปรโตคอลที่ใช้เป็นงานปกติในการโจมตี ทำให้ยากที่จะแยกแยะความแตกต่างระหว่างการโจมตีและการใช้งานปกติ

พบมัลแวร์รูปแบบใหม่ นำเทคนิค AI มาใช้งาน ปรับตัวเองตลอดเพื่อให้ไม่ถูกตรวจจับง่ายๆ

By: mk on 3 July 2017 - 21:44 Tags: Malware Security Artificial Intelligence

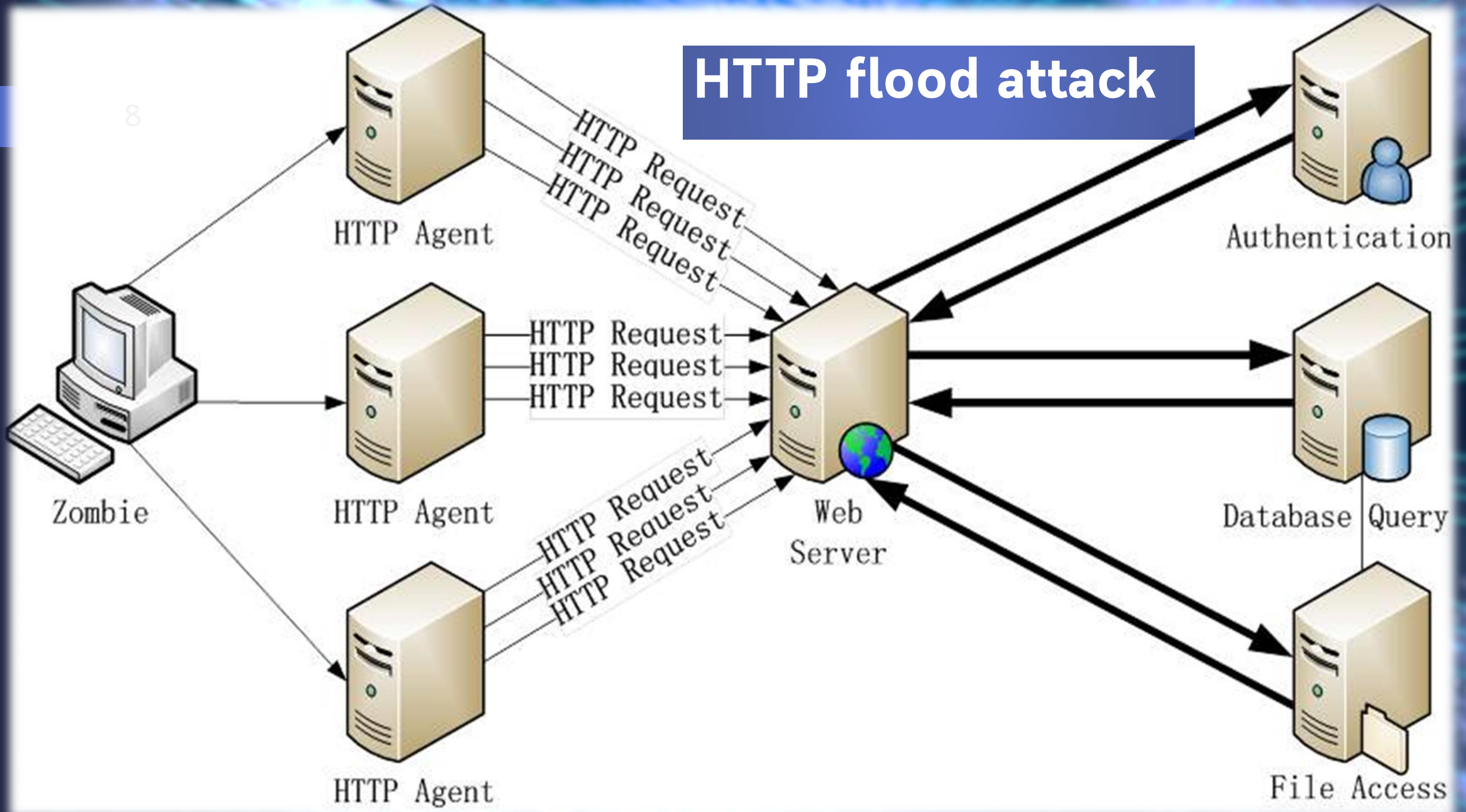
บริษัทความปลอดภัย Darktrace ระบุว่าเริ่มค้นพบมัลแวร์รูปแบบใหม่ๆ ที่นำเทคนิคด้าน AI มาใช้งาน เพื่อให้มัลแวร์สามารถเรียนรู้สภาพแวดล้อม และปลอมตัวได้เนียนกว่าเดิม

Nicole Eagan ซีอีโอของ Darktrace บอกว่ามัลแวร์กลุ่มนี้จะปรับพฤติกรรมไปเรื่อยๆ เพื่อให้อยู่ในระบบโดยไม่ถูกตรวจจับได้นานที่สุดเท่าที่จะทำได้ อย่างไรก็ตาม มัลแวร์กลุ่มนี้ยังไม่ได้มีศักยภาพด้าน AI เต็มขั้น แต่ก็เริ่มหยิบบางส่วนมาใช้งาน

อีกประเด็นที่น่าสนใจคือมัลแวร์เหล่านี้ถูกพบในประเทศกำลังพัฒนา มากกว่าประเทศพัฒนาแล้ว เนื่องจากบริษัทยักษ์ใหญ่ในประเทศพัฒนาแล้วมีระบบป้องกันทางไอทีที่เข้มแข็งกว่า ส่งผลให้แฮ็กเกอร์หันไปทดสอบมัลแวร์ของตัวเองในประเทศที่ไม่ได้สนใจความปลอดภัยไซเบอร์มากนัก ตัวอย่างที่โด่งดังคือ การแฮ็กธนาคารกลางของบังกลาเทศ ที่ในภายหลัง Symantec พบการโจมตีรูปแบบเดียวกัน ถูกใช้ในอีก 31 ประเทศ

ที่มา - The New York Times

HTTP flood attack



การค้นหาจุดอ่อนได้อย่างรวดเร็ว

- จำนวนของจุดอ่อนใหม่ที่ค้นพบ เพิ่มขึ้นเป็นสองเท่าในทุกๆปี จนทำให้ผู้พัฒนาซอฟต์แวร์ปิดช่องโหว่ไม่ทัน
- สิ่งที่น่ากลัวที่สุดคือ การโจมตีแบบ **Zero-day Attack** หมายถึง การโจมตีจุดอ่อนที่ยังไม่มีแพตช์จากเจ้าของผลิตภัณฑ์ออกมาอุดช่องโหว่

ช่องโหว่ใน Vault 7 ครอบคลุมทั้งระบบปฏิบัติการ iOS, Android, Windows, OSX, Linux, เราเตอร์ รวมไปถึงสมาร์ททีวีของซัมซุง ที่ถูกเปลี่ยนให้เป็นไมโครโฟนลับดักฟังข้อมูลได้ ทำงานในโหมด Fake-Off ที่เจ้าของเครื่องรู้สึกว่าปิดทีวีแล้ว แต่จริงๆ ทีวียังทำงานอยู่

ข้อมูลทั้งหมดดูได้จาก Vault 7 และจากการตรวจสอบเบื้องต้นโดยผู้เชี่ยวชาญที่ไม่มีส่วนเชื่อมโยงกับ WikiLeaks เชื่อว่าเอกสารเหล่านี้น่าจะเป็นของจริง

ที่มา - WikiLeaks, Wired

WikiLeaks แฉเอกสารลับ รวมช่องโหว่ที่ CIA ใช้แฮ็กคนอื่นเกือบ 9 พันรายการ

By: mk on 8 March 2017 - 09:52 Tags: CIA Hacking Wikileaks Security

เป็นที่รู้กันว่าหน่วยงานด้านข่าวกรองอย่าง NSA และ CIA มีเครื่องมือแฮ็กระบบของตัวเองใช้งานอยู่เงียบๆ เครื่องมือเหล่านี้ประกอบด้วยช่องโหว่ที่ยังไม่เปิดเผยต่อสาธารณะ (zero day) เพื่อใช้เจาะระบบ รวมถึงมัลแวร์ ไวรัส โทรจัน ที่ใช้เผยแพร่ต่อผ่านช่องโหว่เหล่านี้

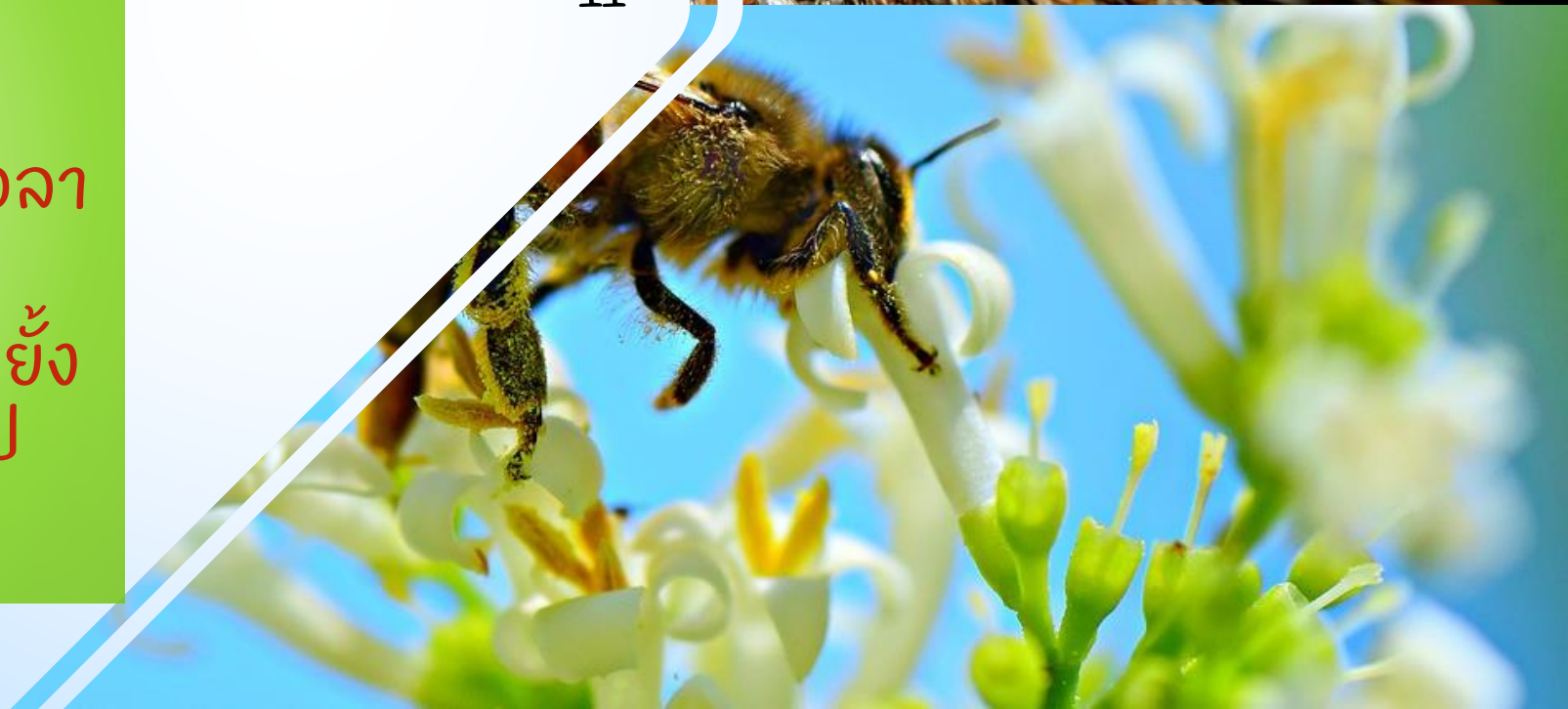
เครื่องมือการแฮ็กของ NSA ถูกนำมาแฉโดย Edward Snowden จนเป็นเหตุให้เขาต้องลี้ภัยไปนอกสหรัฐ ล่าสุดเว็บไซต์ WikiLeaks เผยแพร่ข้อมูลของเครื่องมือแบบเดียวกันในฝั่ง CIA บ้าง

WikiLeaks เรียกข้อมูลชุดนี้ว่า **Vault 7** ประกอบด้วยเอกสารและไฟล์ทั้งหมด 8,761 รายการ โดย WikiLeaks อ้างว่าเอกสารเหล่านี้ที่มีชื่อเรียกภายใน CIA ว่า Year Zero ถูกเก็บไว้ในเครือข่ายภายในของศูนย์ความปลอดภัยไซเบอร์ของ CIA ที่รัฐเวอร์จิเนีย แต่เมื่อไม่นานมานี้ CIA "เสียการควบคุม" เครื่องมือเหล่านี้ ส่งผลให้โลกรู้ว่า CIA มีขีดความสามารถในการแฮ็กระบบอย่างไรบ้าง

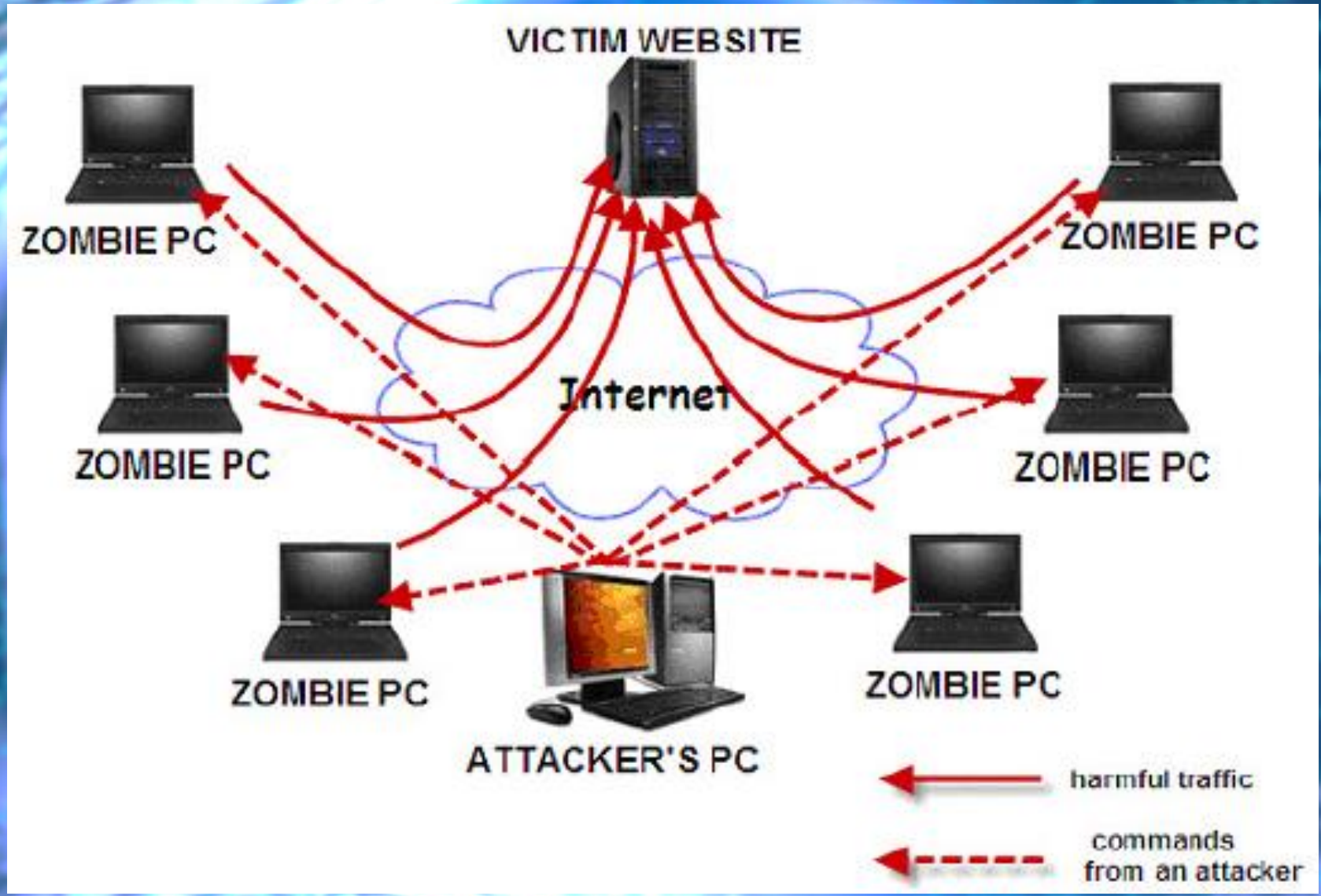
WikiLeaks ไม่ได้บอกว่าเครื่องมือเหล่านี้หลุดออกมาจาก CIA ได้อย่างไร แต่บอกว่ามันถูกเผยแพร่กันในหมู่แฮ็กเกอร์ที่ทำงานให้รัฐบาลสหรัฐมาสักระยะแล้ว ก่อนที่ข้อมูล "บางส่วน" ถูกส่งต่อมายัง WikiLeaks

การโจมตีแบบกระจาย (Distributed Attack)

- คือการที่ผู้โจมตีใช้คอมพิวเตอร์หลายพันหลายแสนเครื่องเพื่อโจมตีเป้าหมายเดียวกัน
- ผู้โจมตีทำการค้นหาเครื่องร่วมโจมตี ฝังโค้ดและตั้งเวลาโจมตีพร้อมกัน
- ยากต่อการป้องกันและยับยั้งเพราะแหล่งที่มามากเกินไปจนไม่สามารถบล็อกได้ทัน



Distributed Denial of Service Attack (DDoS)



Cloudflare รายงานช่องโหว่จากกล้องวงจรปิดจำนวนมากกำลังถูกใช้โจมตี DDoS

By: lew on 12 October 2016 - 14:05 Tags: CloudFlare Internet of Things Security Mirai

หลังแฮกเกอร์ปล่อยซอร์สโค้ดมัลแวร์ Mirai ตอนนี้ Cloudflare ก็ออกมารายงานว่ามีการโจมตีจากมัลแวร์ตัวนี้อย่างต่อเนื่อง

มัลแวร์ Mirai มีความร้ายแรงในการโจมตีหนักว่า botnet อื่นๆ เพราะมันส่งข้อมูล HTTP โดยตรง ไม่ใช่เพียง TCP SYN/ACK, NTP, หรือ DNS ตัวอย่างการโจมตีของ Cloudflare แสดงการส่ง HTTP GET ขนาดถึง 800KB เพื่อโจมตีเซิร์ฟเวอร์

ทาง Cloudflare ไล่ตามมัลแวร์เหล่านี้พบว่ามันมาจากเวียดนามเป็นส่วนใหญ่ เมื่อตรวจสอบบางเครื่องพบว่ามันเป็นระบบกล้องวงจรปิดที่เปิดเว็บเอาไว้

ปัญหาของความปลอดภัยสินค้า IoT เป็นปัญหาใหญ่ที่ดูผู้ผลิตจะไม่สนใจแก้ไขนัก วันนี้นักวิจัยรายงานช่องโหว่ 14 ช่องของระบบกล้องวงจรปิด Avtech ที่ตรวจพบว่าเข้าถึงจากอินเทอร์เน็ตได้กว่า 130,000 เครื่อง โดยนักวิจัยเผยแพร่รายงานหลังจากพยายามติดต่อ Avtech ไปแล้วถึงสองครั้งห่างกันหลายเดือน

ที่มา - Cloudflare, The Register

https://www.blognone.com/node/86270

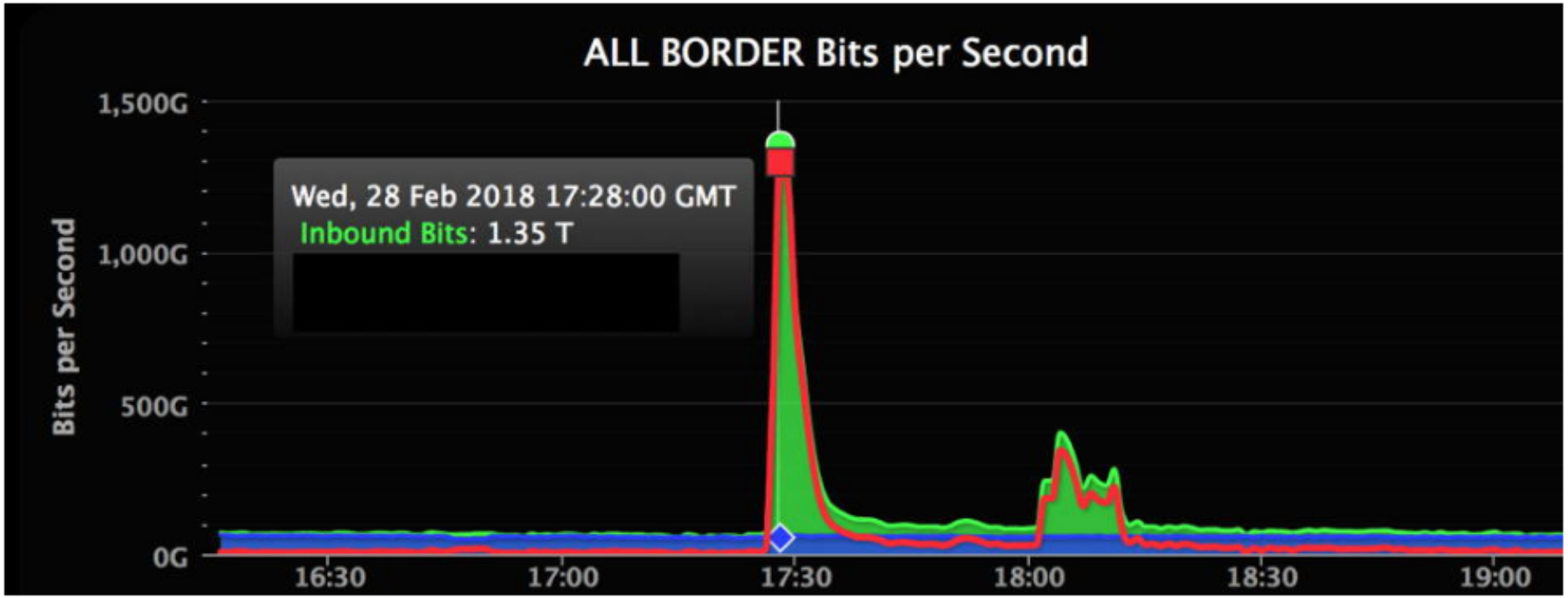
1. GitHub: 1.35 Tbps

https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

On Feb. 28, 2018, GitHub—a popular developer platform—was hit with a sudden onslaught of traffic that clocked in at 1.35 terabits per second. If that sounds like a lot, that's because it is—that amount of traffic is not only massive, it's record-breaking.

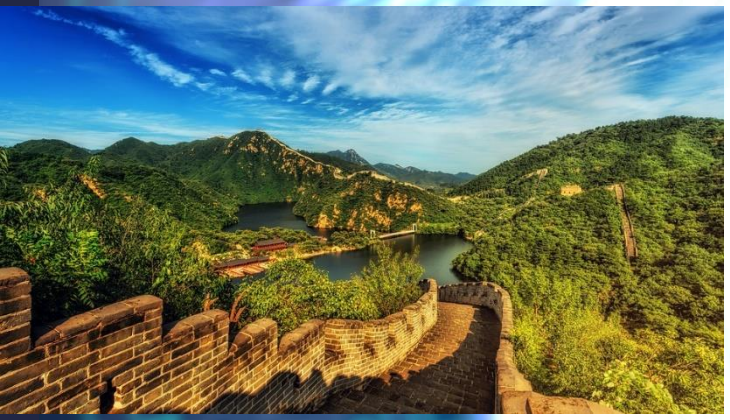
According to GitHub, the traffic was traced back to "over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints."

In this graph, you can see just how much of a difference there was between normal traffic levels and those of the attack:



GitHub DDoS Attack

เครื่องมือสำหรับการรักษาความปลอดภัยข้อมูล



- ไฟร์วอลล์ (Firewall)
- ระบบตรวจจับการบุกรุก (IDS)
- การเข้ารหัสข้อมูล (Data Encryption)
- ซอฟต์แวร์ป้องกันไวรัส (Anti-Virus Software)
- ระบบการรักษาความปลอดภัยทางกายภาพ

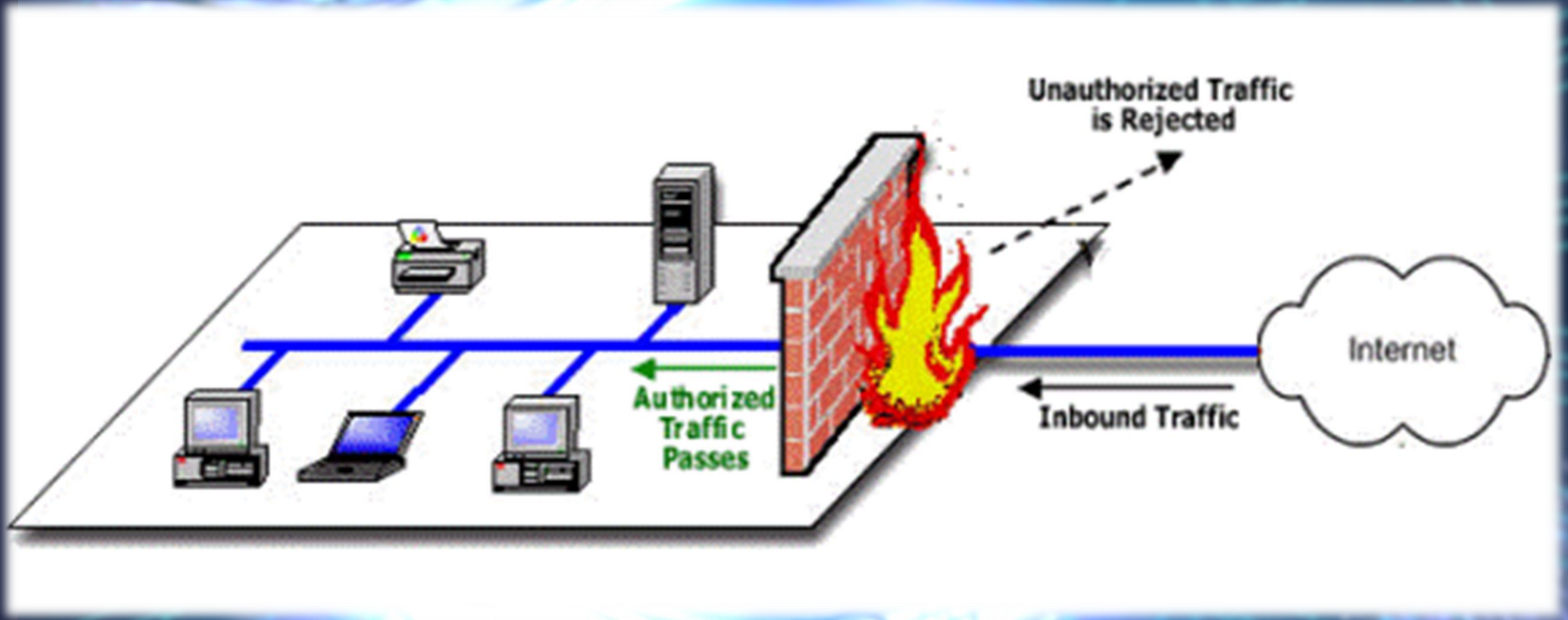
เครื่องมือสำหรับการรักษาความปลอดภัยข้อมูล

- เนื่องจากภัยมีรอบด้าน ดังนั้นจึงไม่สามารถใช้เครื่องมือประเภทใดประเภทหนึ่งเพื่อรักษาความปลอดภัยทั้งองค์กรได้
- จำเป็นต้องใช้ผลิตภัณฑ์หลายประเภททำงานร่วมกันเป็นระบบเพื่อป้องกันและรักษาความปลอดภัย

ไฟร์วอลล์ (Firewall)

- เป็นระบบควบคุมการเข้าออกของเครือข่าย **ใช้ปกป้องการโจมตีจากภายนอก**
- ปกติจะติดตั้งขวางกั้นระหว่างสองเครือข่าย **ตั้งอยู่ก่อนหรือหลังเราเตอร์**
- ไฟร์วอลล์ไม่สามารถป้องกันการโจมตีที่ใช้ช่องทางปกติที่เปิดไว้โดยไฟร์วอลล์ได้
- แพ็คเก็ตที่อนุญาตให้ผ่านหรือไม่ให้ผ่าน จะขึ้นอยู่กับนโยบายการรักษาความปลอดภัยขององค์กรเป็นหลัก

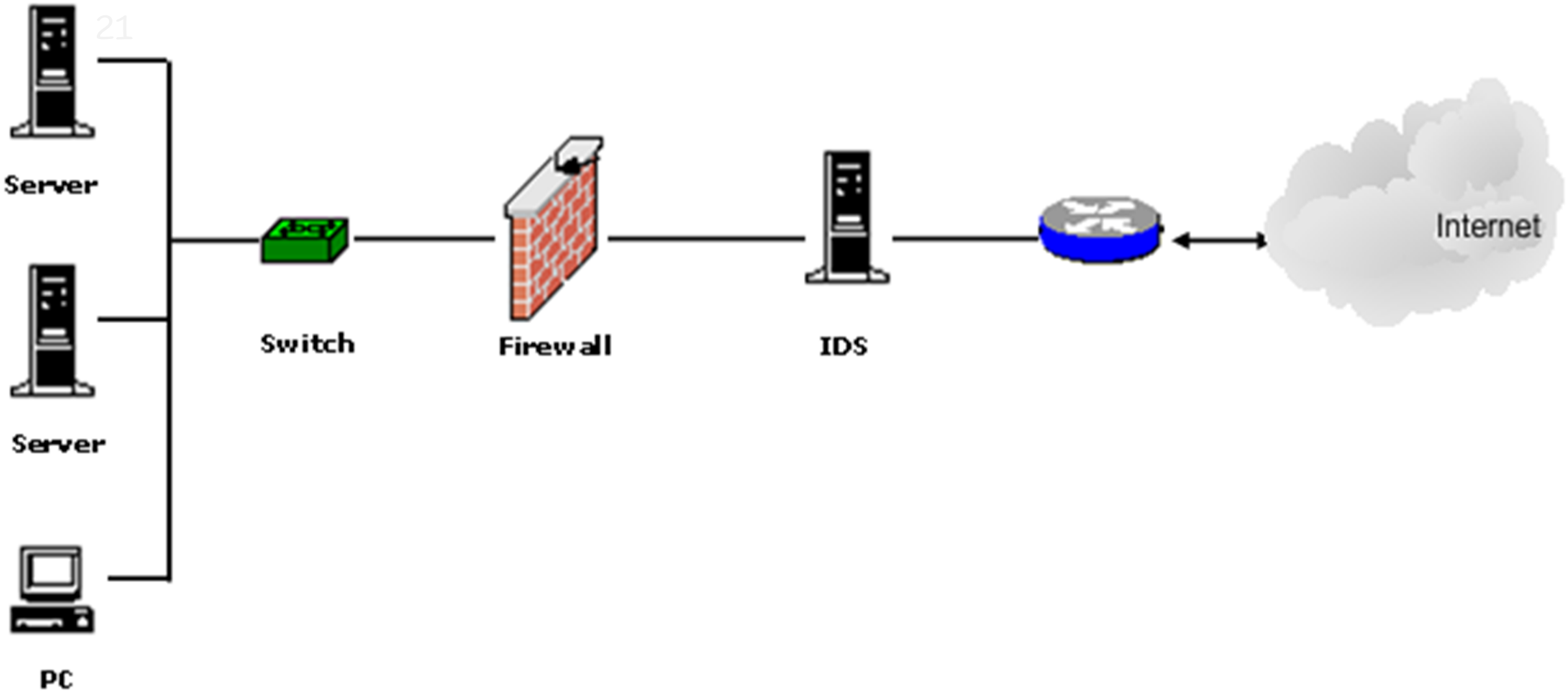

FORTINET
FortiGate 300D
FORTINET


Unauthorized Traffic
is Rejected
Internet
Authorized
Traffic
Passes
Inbound Traffic

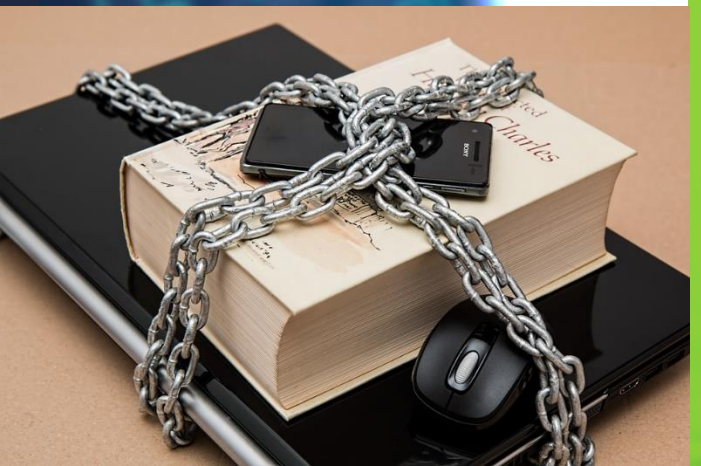
ระบบตรวจจับและป้องกันการบุกรุก (IDPS)

- IDPS (Intrusion Detection Prevention System) เป็นระบบที่ใช้เฝ้าระวัง **เตือนภัยเมื่อมีการบุกรุก และพยายามยับยั้งการบุกรุก** เมื่อมีสิ่งผิดปกติเกิดขึ้นในระบบ
- IDPS จำเป็นต้องมีการอัพเดตข้อมูลอยู่เสมอ เพราะช่องโหว่ใหม่เกิดขึ้นอยู่ตลอดเวลา
- IDPS ไม่สามารถตรวจจับผู้ใช้ที่ได้รับอนุญาต ที่พยายามเข้าถึงไฟล์หรือใช้โปรแกรมที่ไม่ได้รับอนุญาตได้

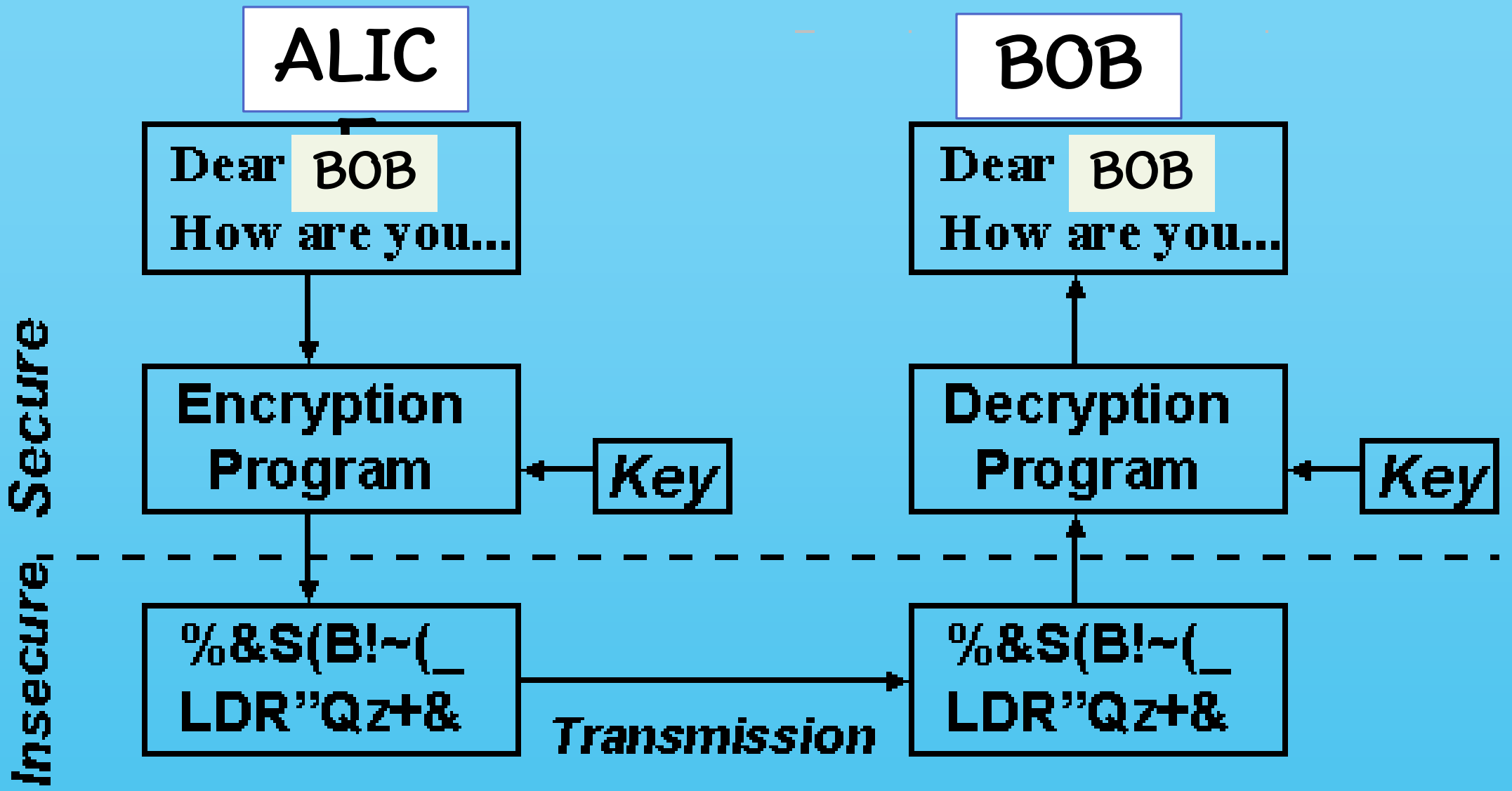
Intrusion Detection System



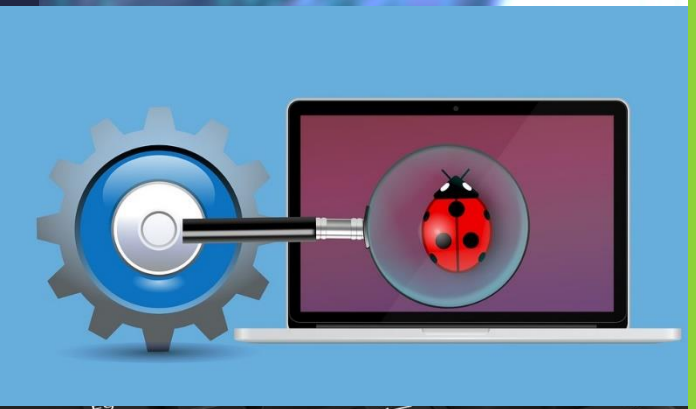
การเข้ารหัสข้อมูล (Data Encryption)



- เป็นกลไกป้องกันข้อมูลที่อยู่ระหว่างการสื่อสาร ถ้าเข้ารหัสดีพอ ข้อมูลจะถูกป้องกันไม่ให้อ่านได้จากผู้ไม่ประสงค์ดีได้
- ผู้ใช้ที่ส่ง-รับ จะต้องสามารถเข้า-ถอดรหัสข้อมูลนี้ได้ แต่ระบบการเข้า-ถอดรหัสจะไม่สามารถแยกแยะได้ระหว่างผู้ที่ได้รับอนุญาตหรือผู้บุกรุก
- ถ้าจะให้การเข้ารหัสได้ผล ต้องมีระบบป้องกันการขโมยคีย์ควบคู่ไปด้วย


ALIC
BOB
Dear BOB
How are you...
Dear BOB
How are you...
Encryption Program
Key
Decryption Program
Key
Secure
Insecure
%&S(B!~(_ LDR"Qz+&
Transmission
%&S(B!~(_ LDR"Qz+&

ซอฟต์แวร์ป้องกันไวรัส (Anti-Virus Software)



- ปัจจุบันภัยคุกคามที่มีผลกระทบต่อองค์กรมากที่สุดคือ มัลแวร์ ดังนั้นการป้องกันและกำจัดสิ่งเหล่านี้จึงเป็นสิ่งที่สำคัญที่สุด
- การติดตั้งและใช้งานโปรแกรมป้องกันไวรัสอย่างถูกต้อง สามารถลดความเสี่ยงต่อมัลแวร์ได้ แต่ไม่สามารถป้องกันมัลแวร์ได้ทุกชนิด
- ต้องมีการอัพเดตฐานข้อมูลไวรัสอยู่เสมอ รวมถึงต้องสแกนระบบเป็นประจำด้วย

ซอฟต์แวร์ป้องกันไวรัส (AntiVirus Software) [2]

- สิ่งที่ซอฟต์แวร์ป้องกันไวรัส**ไม่สามารถป้องกันได้คือ**
- ผู้บุกรุกจากที่อื่นที่เจาะระบบเข้ามาแล้วรันโปรแกรมประสงค์ร้าย
- ไม่สามารถป้องกันผู้ใช้ที่ได้รับอนุญาต แต่พยายามจะเข้าถึงไฟล์หรือระบบที่ไม่ได้รับอนุญาตได้

การรักษาความปลอดภัยทางกายภาพ

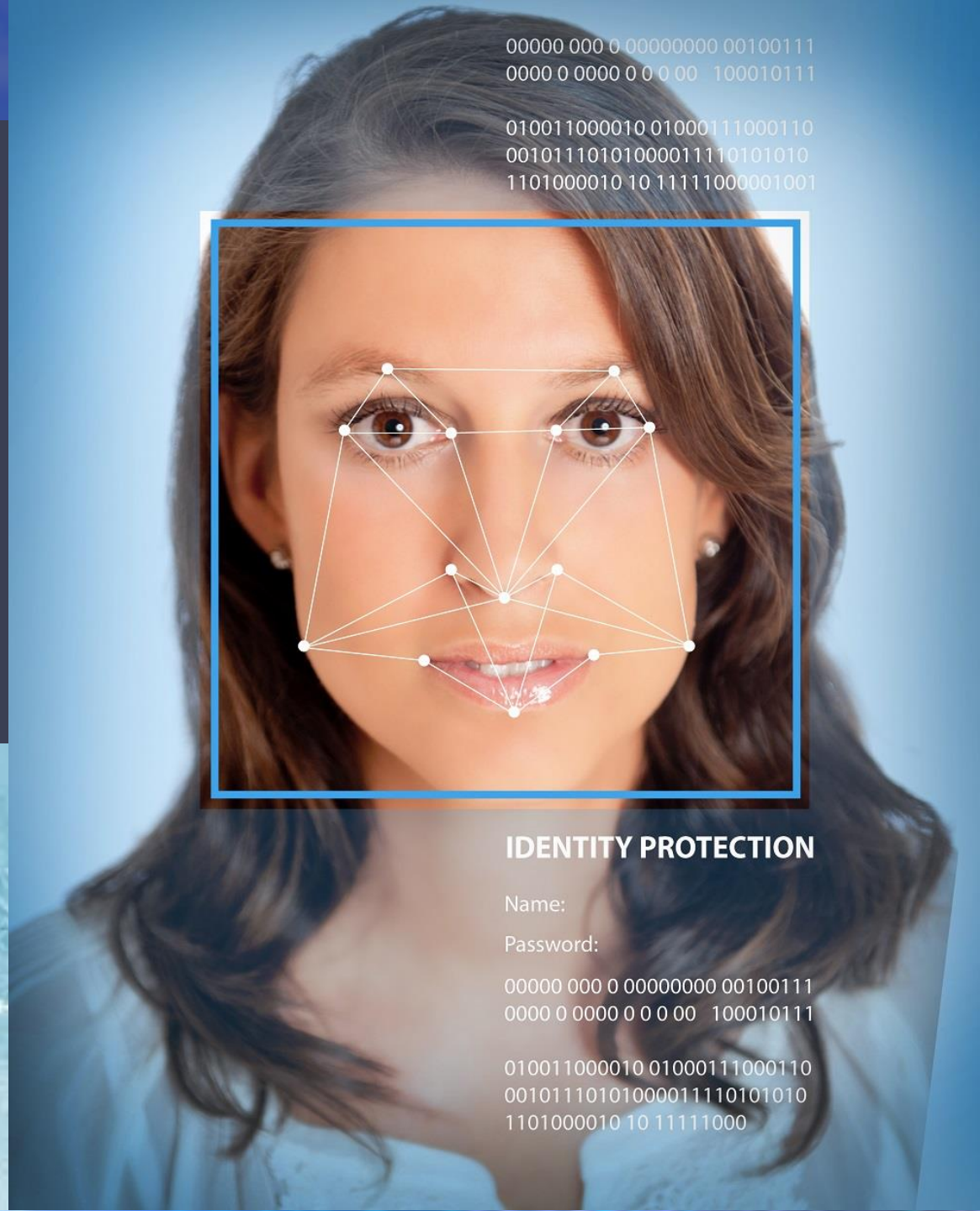
- การพิสูจน์ตัวตนสามารถทำได้โดยใช้การตรวจสอบคุณสมบัติ 3 อย่างของผู้ใช้ คือ
  - **สิ่งที่คุณรู้ (Something you know)**
  - **สิ่งที่คุณมี (Something you have)**
  - **สิ่งที่คุณเป็น (Something you are)**
- การใช้เพียง Password เป็นการตรวจสอบเฉพาะ “สิ่งที่คุณรู้” แต่อาจถูกเดาหรือถูกขโมยได้

การรักษาความปลอดภัยทางกายภาพ [2]

- **Smart Card** จัดอยู่ในประเภท *“สิ่งที่คุณมี”* สามารถป้องกันการเดารหัสผ่านได้ แต่หากสมาร์ทการ์ดถูกขโมยไป ระบบจะไม่สามารถป้องกันการโจมตีจากผู้บุกรุกคนนั้นได้
- **Biometrics** จัดอยู่ในประเภท *“สิ่งที่คุณเป็น”* สามารถป้องกันการเดารหัสผ่านหรือขโมยสมาร์ทการ์ดได้ ถือว่าเป็นระบบพิสูจน์ตัวตนที่ค่อนข้างแข็งแกร่ง ตัวอย่างเช่น การสแกนลายนิ้วมือ มือ ใบหน้า ม่านตา เป็นต้น

Biometrics


BIOMETRIC FINGERPRINT SCAN
LITTLE
RING
MIDDLE
INDEX
THUMB
INDEX
ANALYZING...
MIDDLE
ANALYZING...
RING
ANALYZING...
LITTLE
ANALYZING...
THUMB
ANALYZING...
STATUS: ANALYZING
%38
PATTERN ANALYSIS
DATABASE ACCESS


00000 000 0 00000000 00100111
0000 0 0000 0 0 0 00 100010111
010011000010 01000111000110
001011101010000111101010101
1101000010 10 11111000001001
IDENTITY PROTECTION
Name:
Password:
00000 000 0 00000000 00100111
0000 0 0000 0 0 0 00 100010111
010011000010 01000111000110
001011101010000111101010101
1101000010 10 11111000