FUNDAMENTAL PRINCIPLES OF CYBERSECURITY

- Instructor : Surachet Suchaiya , PhD.

TOPICS

Fundamental Principles Of Cybersecurity

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
2. ภัยคุกคามและแนวโน้มภัยคุกคามด้านการรักษาความความมั่นคงปลอดภัยไซเบอร์
3. รูปแบบและเทคนิคการบุกรุกการรักษาความมั่นคงปลอดภัยไซเบอร์
4. การวิเคราะห์กระบวนการทำงานขององค์กรเพื่อปรับปรุงและแก้ไขปัญหาความมั่นคงปลอดภัย
5. เครื่องมือในการรักษาความมั่นคงปลอดภัยไซเบอร์
6. นโยบายการรักษาความมั่นคงปลอดภัยข้อมูล
7. การบริหารจัดการความต่อเนื่องทางธุรกิจ ด้านไซเบอร์
8. กฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

INSTRUCTOR EXPERIENCE

INSTRUCTOR EXPERIENCE

CYBER SECURITY CHAPTER 1
แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Introduction


Hospitals


Care Homes


Production


Retail


Buildings

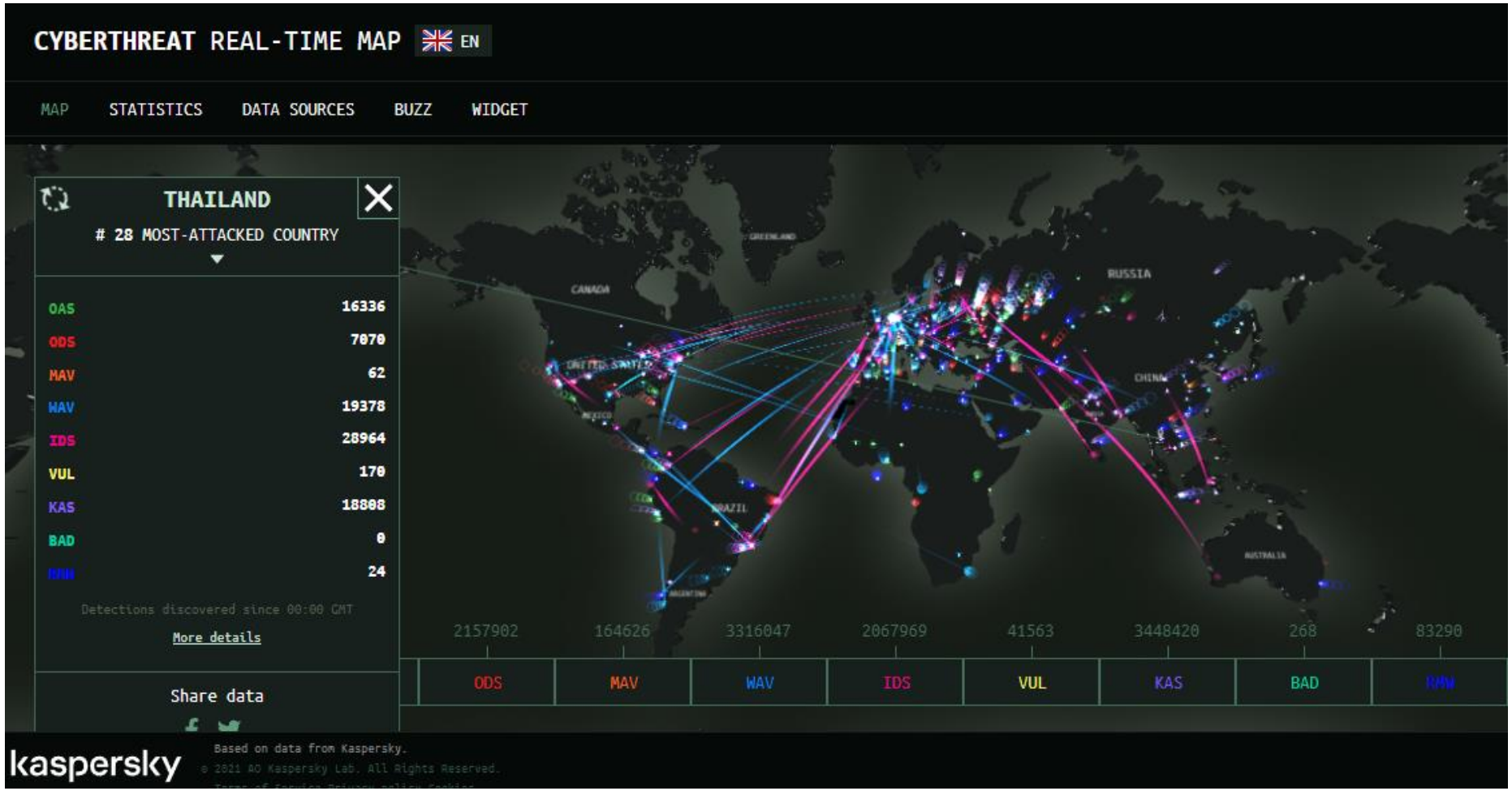

Warehouse


Office Buildings


Transportation

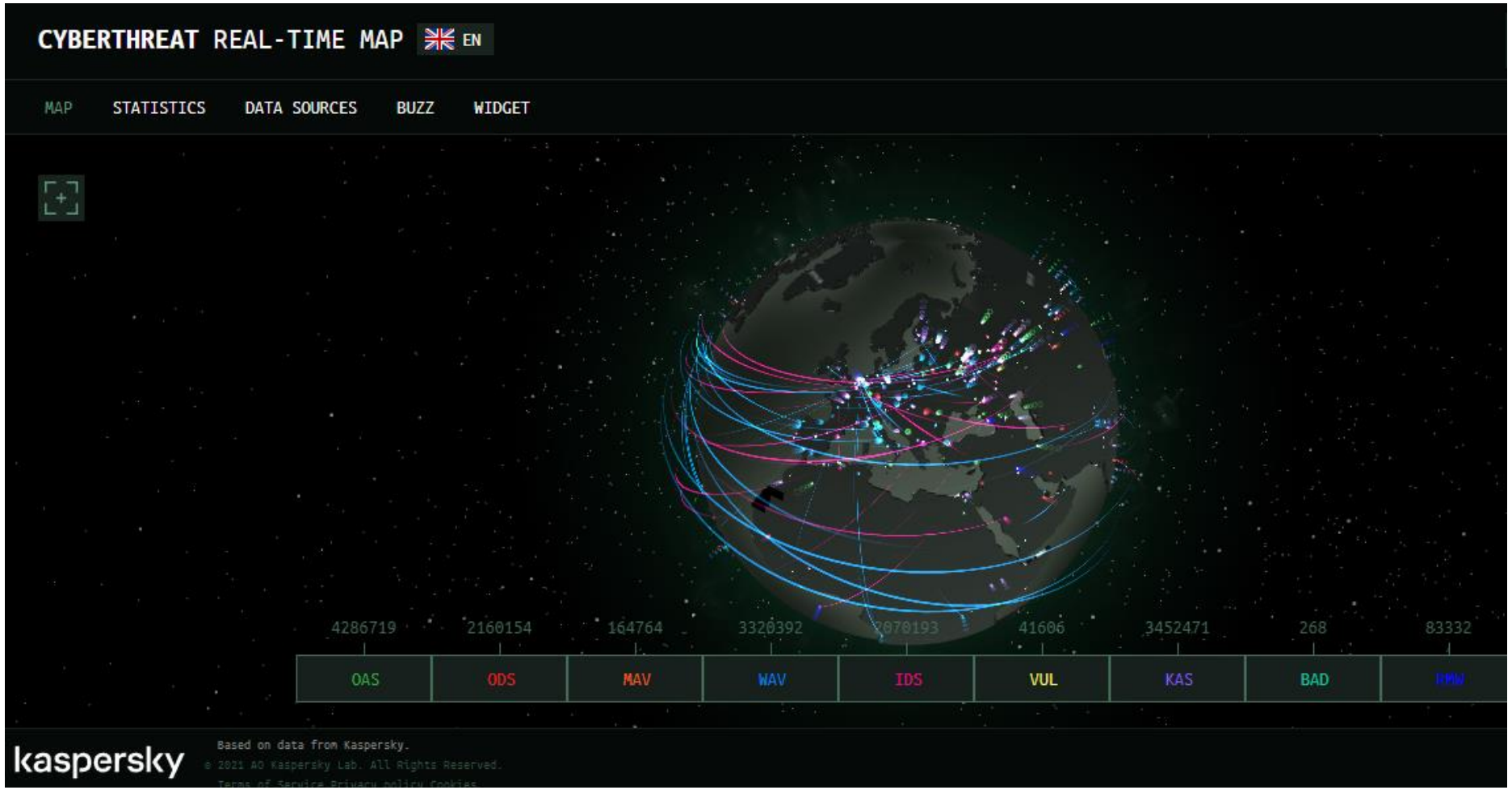
1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Introduction : Cyberthreat – Realtime MAP



1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

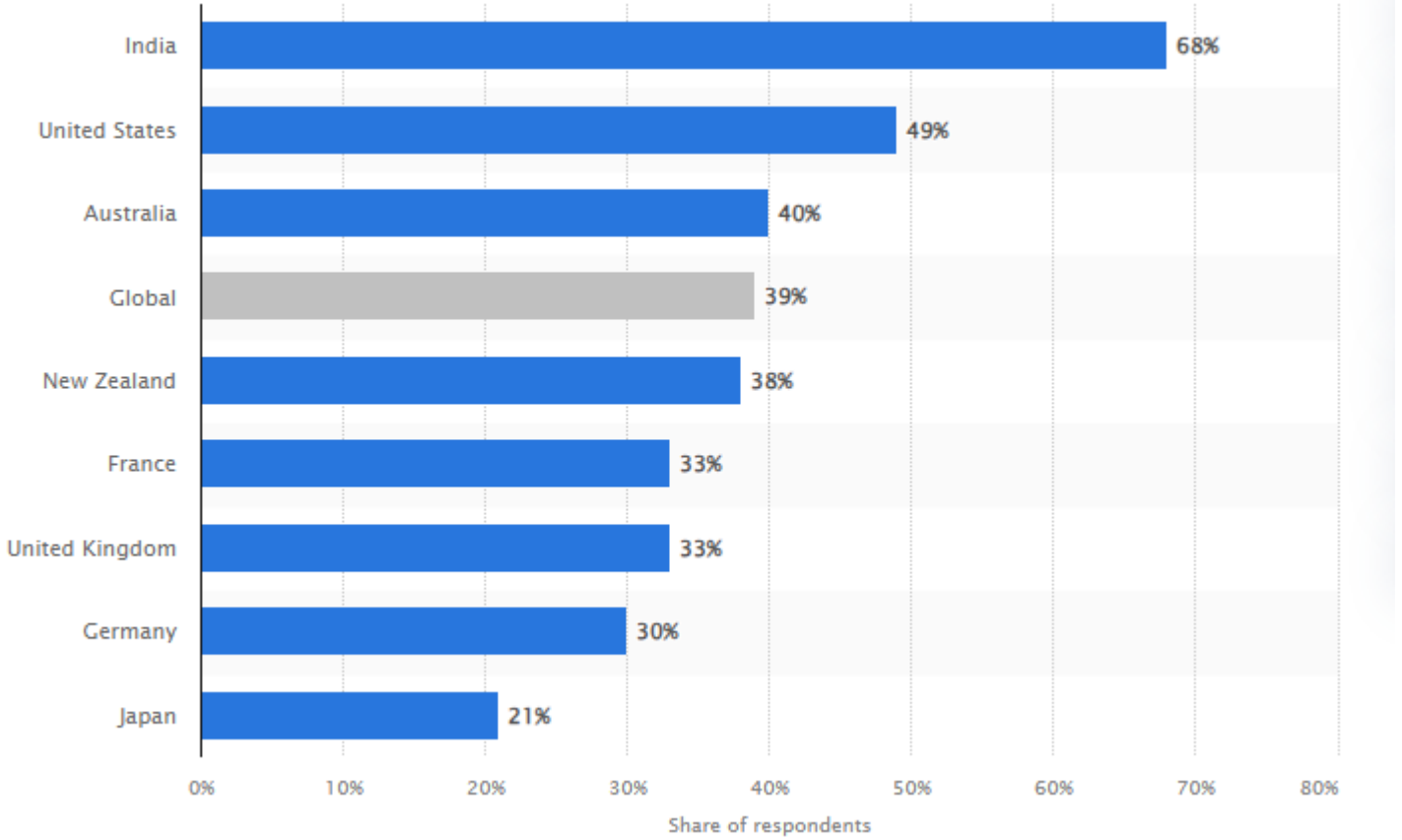
Introduction : Cyberthreat – Realtime MAP



1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวโน้มและอันตรายที่เกิดขึ้นจากภัยคุกคามทางโลกไซเบอร์

Percentage of internet users in selected countries who have ever experienced any cybercrime in 2022

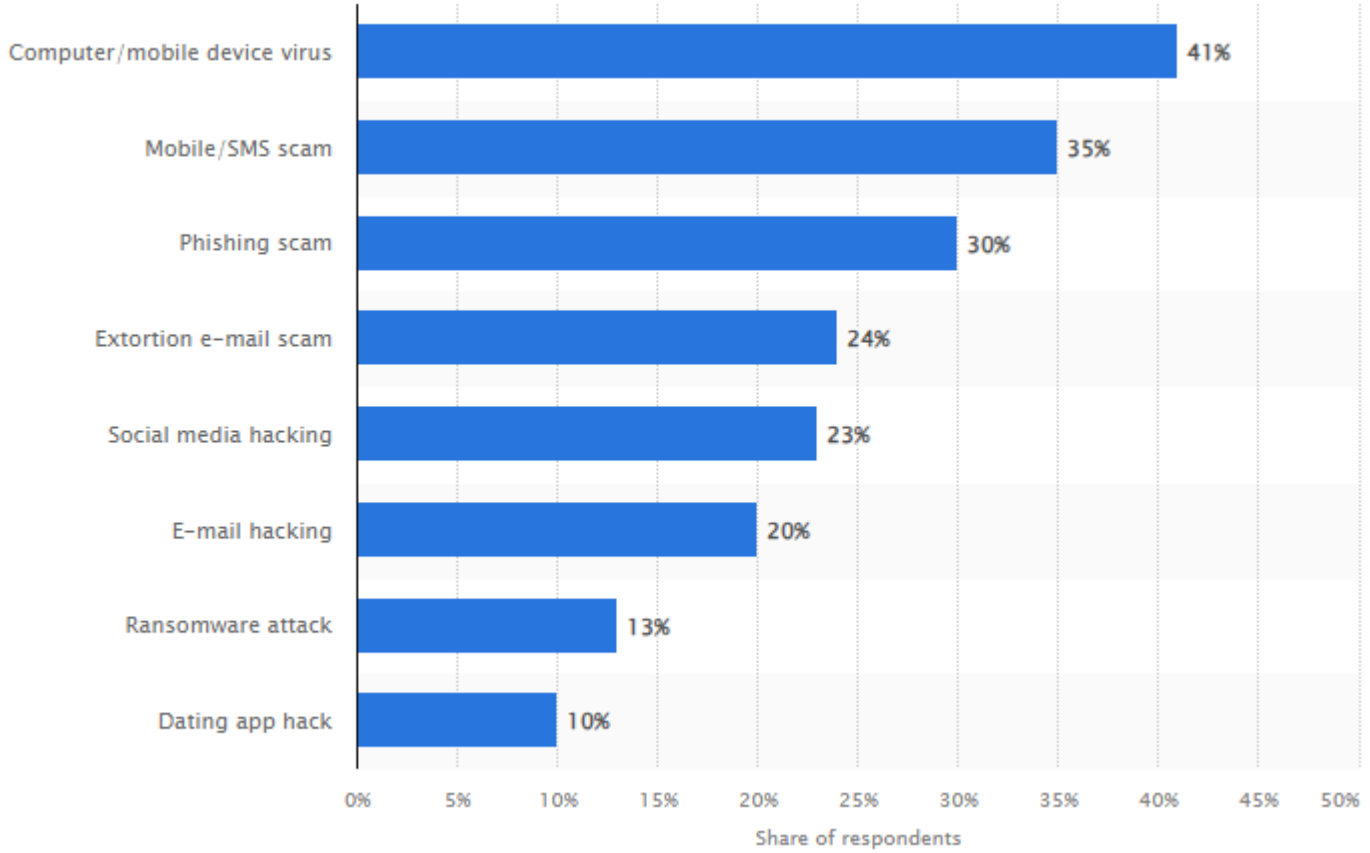


ข้อมูลจาก https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวโน้มและอันตรายที่เกิดขึ้นจากภัยคุกคามทางโลกไซเบอร์

Share of adults worldwide who have experienced cyber crime as of January 2023

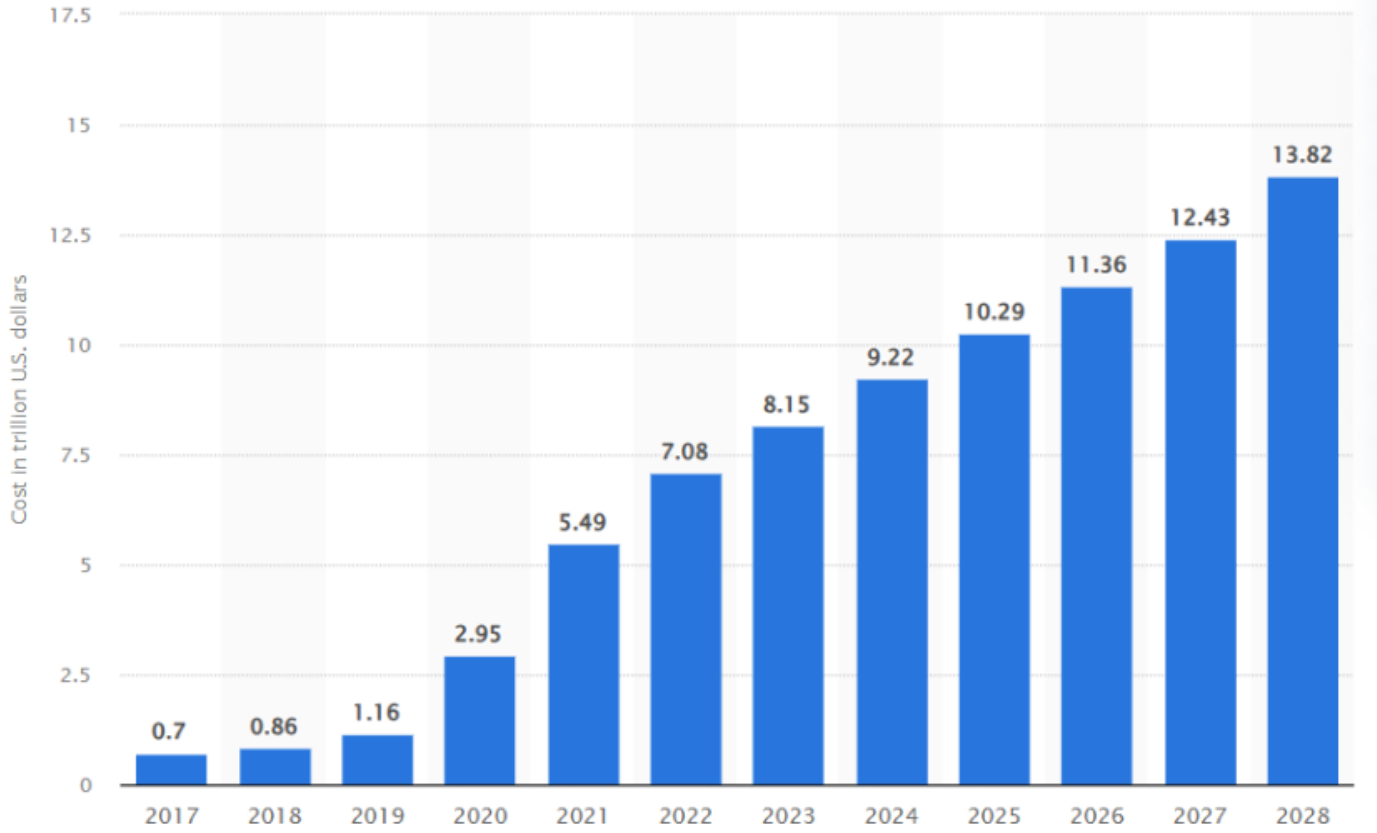


ข้อมูลจาก https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

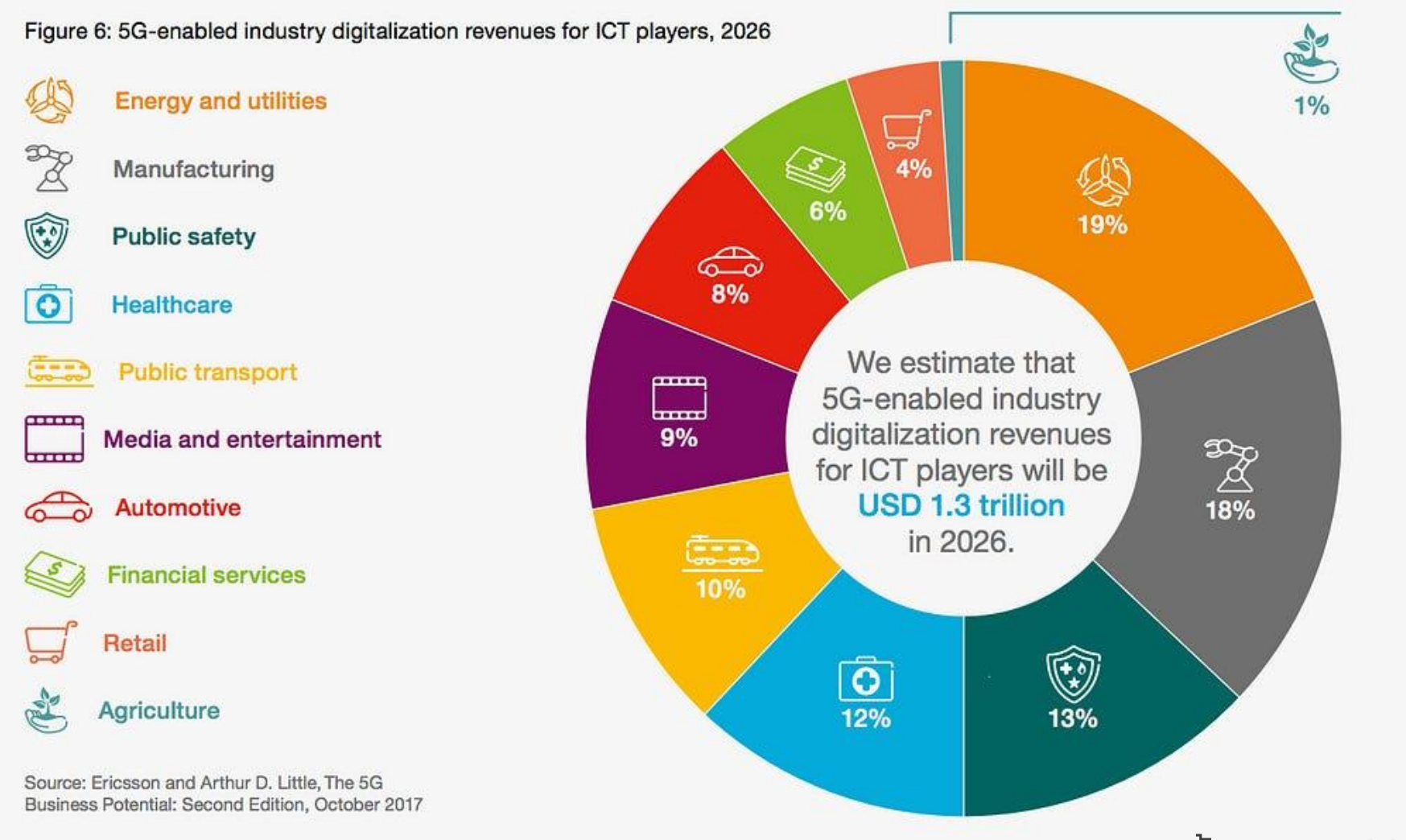
แนวโน้มและอันตรายที่เกิดขึ้นจากภัยคุกคามทางโลกไซเบอร์

Estimated cost of cybercrime worldwide 2017-2028(in trillion U.S. dollars)



ข้อมูลจาก https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

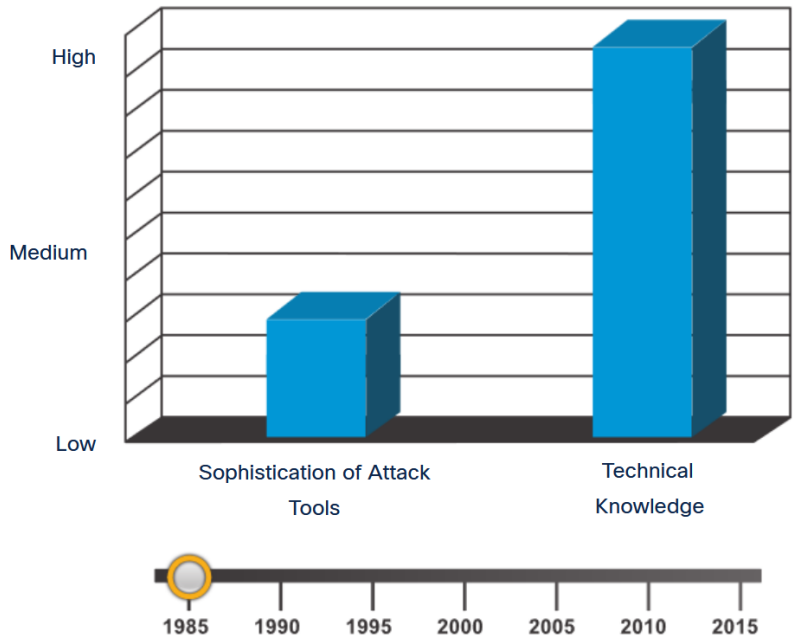
1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

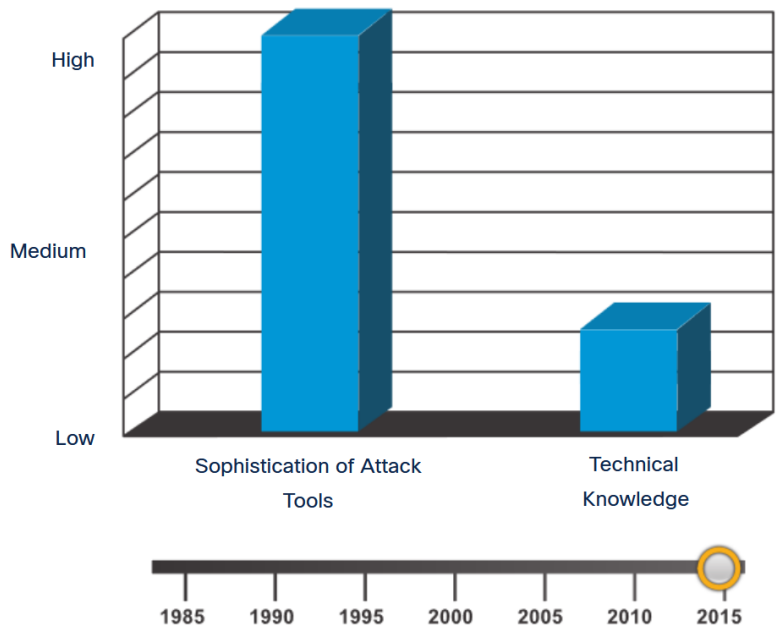


ข้อมูลจาก Medium

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Introduction : Attack Tools





1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

- ตัวอย่างต้นทุนการก่ออาชญากรรมทางไซเบอร์ ที่รวบรวมจากแหล่งข้อมูลต่างๆใน Internet

Source : Bromium Into The Web of Profit		
Tools ในการ Hack Adobe exploit	$30,000	1,07,100THB
Tools ในการ Hack iOS exploit	$250,000	8,937,500THB
Tools ในการสร้าง Malware เพื่อใช้โจมตี	$200	7,150THB
Tools ในการสร้าง Spywareเพื่อใช้แอบดูข้อมูล	$200	7,150THB
Tools ในการSMS Spoofing/month	$20	715THB
ค่าจ้าง Hacker	$200	7,150THB

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

- ตัวอย่างต้นทุนการก่ออาชญากรรมทางไซเบอร์ ที่รวบรวมจากแหล่งข้อมูลต่างๆใน Internet

Source : Secureworks State of Cybercrime Report 2021

ต้นทุนการเช่า anonymised servers/month เพื่อก่ออาชญากรรมทาง Cyber	$100	3,575THB

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

วิวัฒนาการของการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

วิวัฒนาการของการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

- ยุคที่ 1 : การรักษาความมั่นคงปลอดภัยทางกายภาพ (Physical Security)
- ยุคที่ 2 : การรักษาความมั่นคงปลอดภัยเครือข่าย (Network Security)
- ยุคที่ 3 : การรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security)
- ยุคที่ 4 : การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

วิวัฒนาการของการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

- ยุคที่ 1 : การรักษาความมั่นคงปลอดภัยทางกายภาพ (Physical Security)

การรักษาความมั่นคงปลอดภัยระบบสารสนเทศมุ่งเน้นไปที่การป้องกันการเข้าถึงข้อมูล และระบบสารสนเทศทางกายภาพเป็นหลัก เช่น การป้องกันอาคาร, สถานที่เก็บข้อมูล, ห้องServer เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง และ อุปกรณ์ระบบเครือข่าย

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

วิวัฒนาการของการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

- ยุคที่ 2 : การรักษาความมั่นคงปลอดภัยเครือข่าย (Network Security)

เมื่อระบบสารสนเทศเริ่มเชื่อมต่อกับเครือข่ายมากขึ้น การรักษาความมั่นคงปลอดภัยจึงเริ่มให้ความสำคัญกับการป้องกันภัยคุกคามทางเครือข่าย เช่น การโจมตีด้วยไวรัส การโจมตีด้วยมัลแวร์ และการเข้ารหัสข้อมูล

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

วิวัฒนาการของการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

- ยุคที่ 3 : การรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security)

การรักษาความมั่นคงปลอดภัยเริ่มให้ความสำคัญกับการป้องกันข้อมูลและทรัพย์สินทางปัญญา(Intellectual Property)มากขึ้น เช่น การป้องกันการโจรกรรมข้อมูล(Data Theft Protection) การละเมิดข้อมูล (Data Breach) และการใช้ข้อมูลในทางที่ผิด

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

วิวัฒนาการของการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

- ยุคที่ 4 : การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

โลกได้เข้าสู่ยุคดิจิทัล การรักษาความมั่นคงปลอดภัยจึงให้ความสำคัญกับการป้องกันภัยคุกคามทางไซเบอร์ที่หลากหลายมากขึ้น เช่น การโจมตีด้วยแรนซัมแวร์(Ransomware) การโจมตีด้วยฟิชชิง(Phishing) และการก่ออาชญากรรมไซเบอร์(Cybercrime)

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

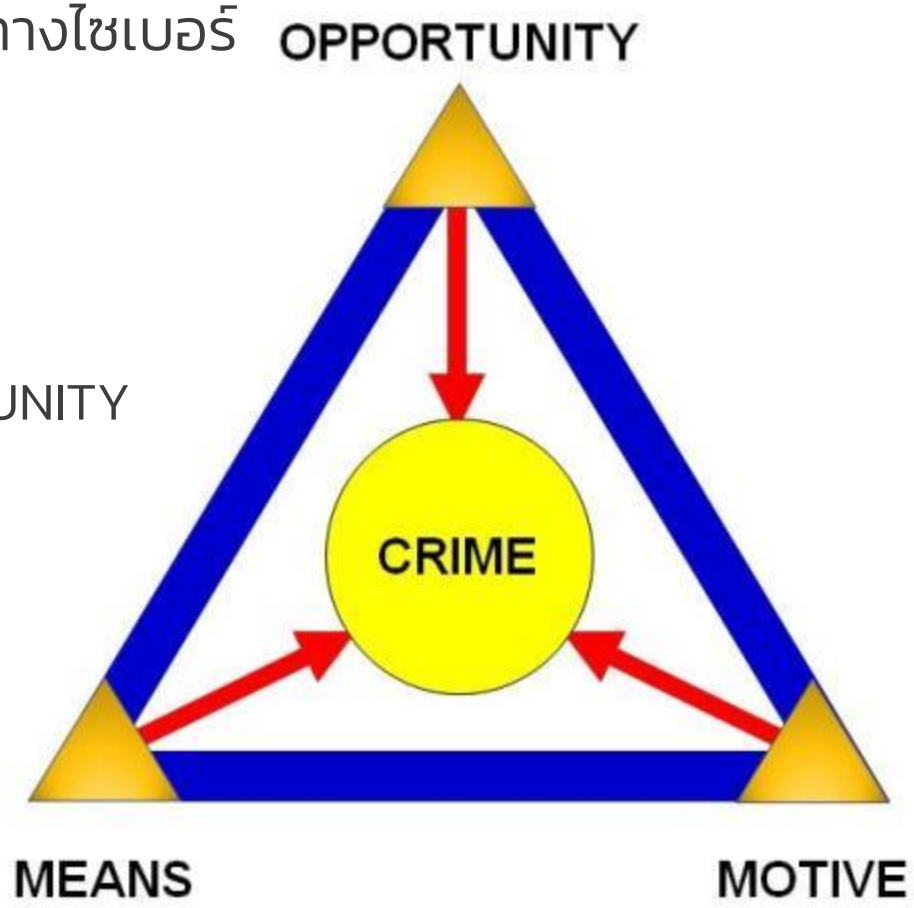
องค์ประกอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Introduction

- ปัจจัยที่ทำให้เกิดการก่ออาชญากรรมทางไซเบอร์

CRIME = MOTIVE + MEANS + OPPORTUNITY

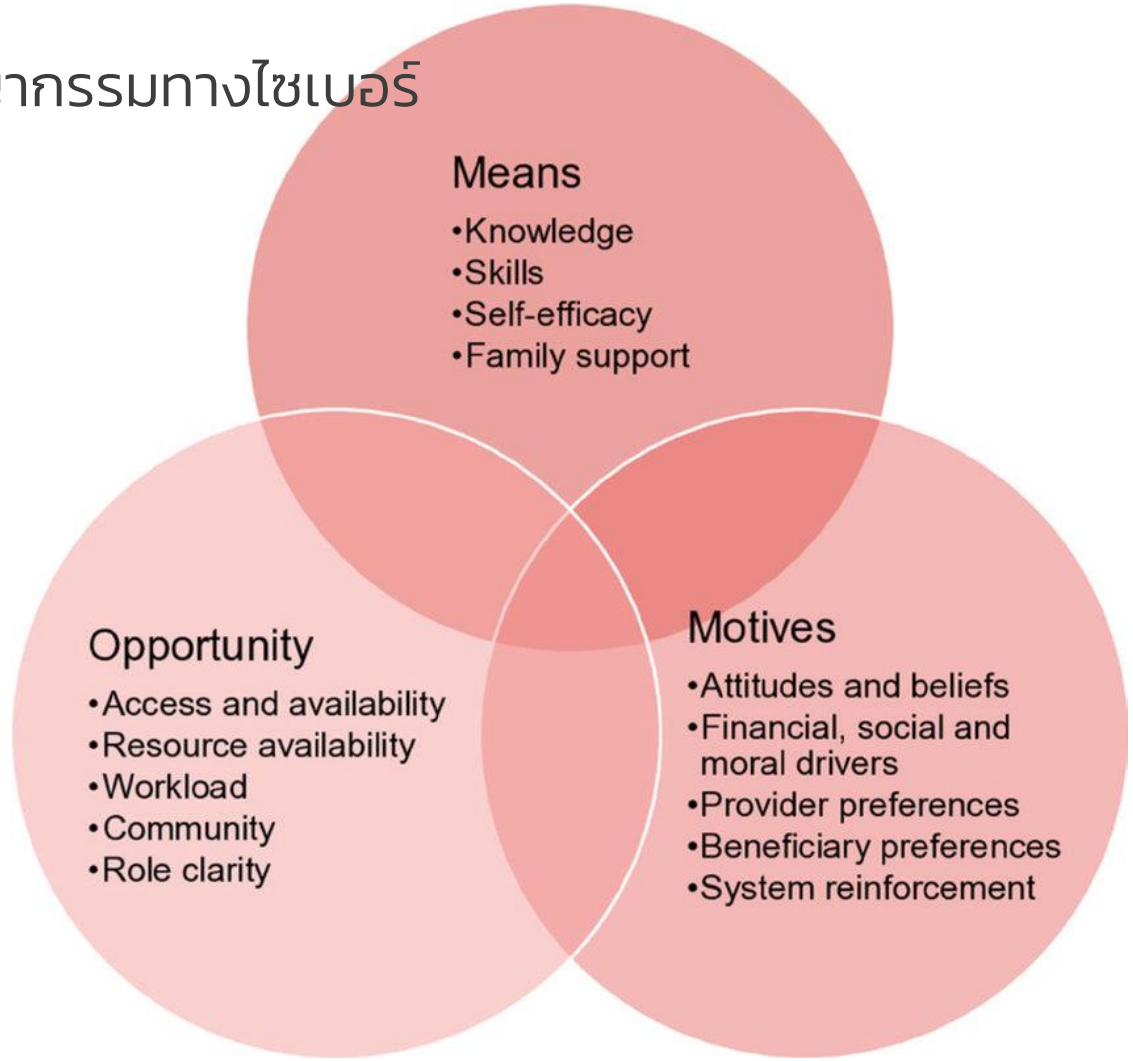


ภาพจาก www.lbna.ca

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Introduction

- ปัจจัยที่ทำให้เกิดการก่ออาชญากรรมทางไซเบอร์



ข้อมูลจาก Researchgate.net

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

องค์ประกอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

1. แนวคิดทฤษฎีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Fundamentals of information system security

The CIA Triad consists of three components of information security:

- **Confidentiality** – Only authorized individuals, entities, or processes can access sensitive information.
- **Integrity** – This refers to the protection of data from unauthorized alteration.
- **Availability** – Authorized users must have uninterrupted access to the network resources and data that they require.

ภาพจาก Cisco.com

CYBER SECURITY CHAPTER 2
รูปแบบและเทคนิคในการบุกรุกระบบสารสนเทศในชีวิตประจำวัน

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

รูปแบบและเทคนิคในการบุกรุกระบบสารสนเทศในชีวิตประจำวัน

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

รูปแบบและเทคนิคในการบุกรุกระบบสารสนเทศในชีวิตประจำวัน

Definition of term

- Event (เหตุการณ์ที่เกิดขึ้นตามปกติ)
- Incident (เหตุการณ์ที่อาจกลายเป็นภัยคุกคาม)
- Threat (ภัยคุกคาม)
- Intrusion (การบุกรุก)
- Vulnerability (ช่องโหว่)
- Breach (การละเมิด)
- Exploit (การเจาะระบบผ่านช่องโหว่)
- Zero Day (ช่องโหว่ที่ยังไม่ค้นพบ)
- IRT (Incident Response Team)

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

รูปแบบและเทคนิคในการบุกรุกระบบสารสนเทศในชีวิตประจำวัน

- IRT (Incident Response Team)

ทีมรับมือและตอบสนองการโจมตีทางไซเบอร์ เพื่อการลดความเสียหาย ฟื้นฟูการปฏิบัติงานตามปกติ แจ้งเตือน ให้คำแนะนำ การอบรม บริหารจัดการ และรวบรวมข้อมูลเพื่อการวิเคราะห์และปรับปรุง

บางองค์กร อาจมีชื่อเรียกที่ต่างกันไป เช่น

CSIRT (Computer Security Incident Response Team),

CIRT (Computer Incident Response Team),

SERT (Security Incident Response Team).

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

รูปแบบและเทคนิคในการบุกรุกระบบสารสนเทศในชีวิตประจำวัน

- Malware
- Phishing
- Ransomware
- Denial-of-Service (DoS) and
- Distributed Denial-of-Service (DDoS) attacks
- Man-in-the-Middle (MitM) attacks
- SQL Injection
- Social Engineering
- Insider Threats
- Advanced Persistent Threats (APTs)
- AI Deepfake Technology

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface)

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface)

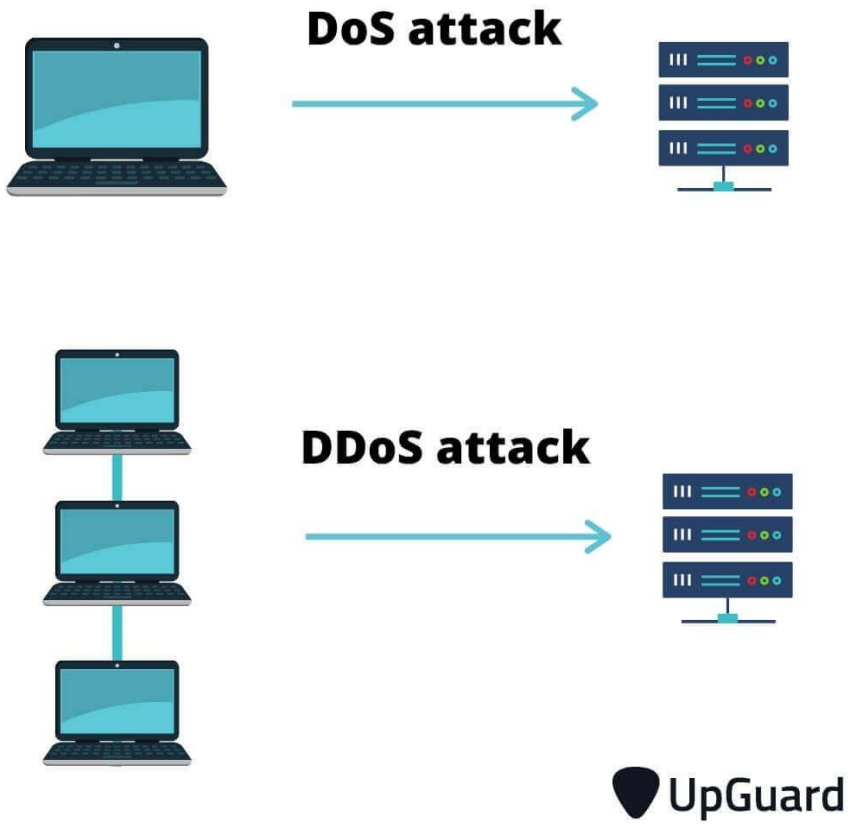
Attack Surface ในระบบไอที

- เครือข่าย (Networks)
- อุปกรณ์ (Devices)
- ซอฟต์แวร์ (Software)
- ผู้ใช้งานระบบ (People)

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Network

- Denial of Service หรือ DoS เป็นการปฏิเสธบริการ ใช้โจมตีเครือข่าย

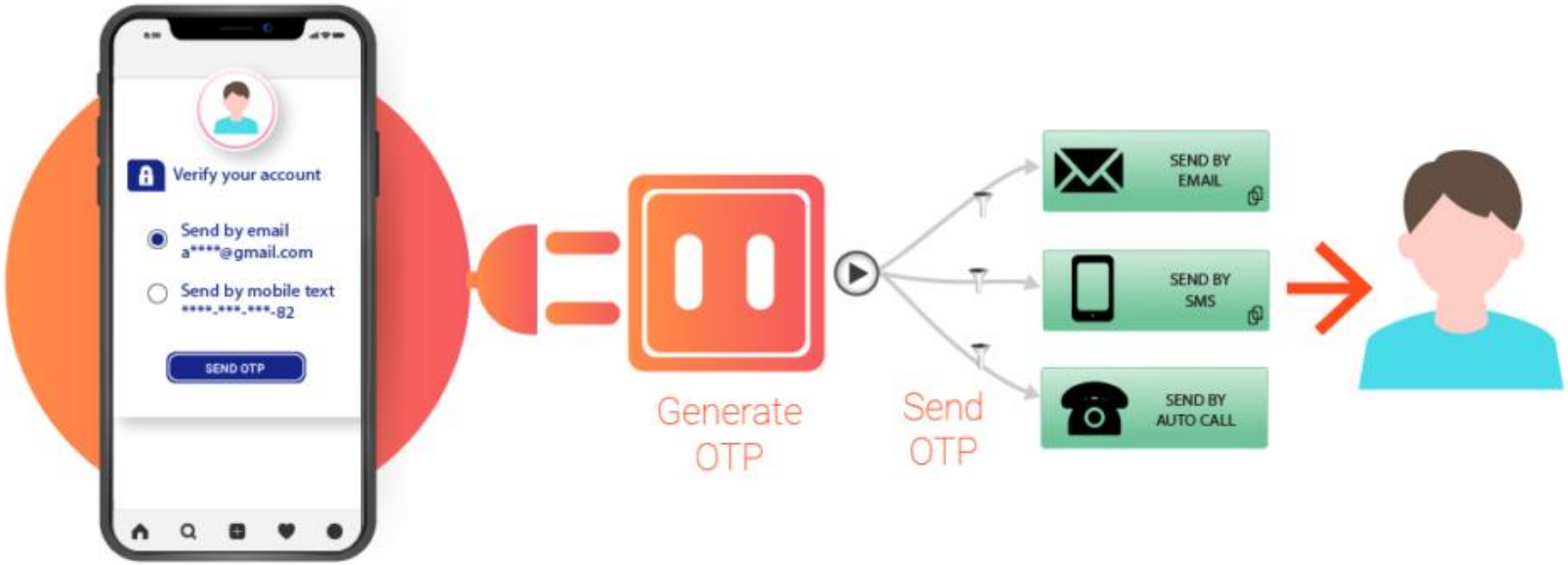


2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Network

แนวทางป้องกัน DoS

- ใช้ CAPTCHA หรือ One-Time Password (OTP) ร่วมในการรับข้อมูล
- ใช้อุปกรณ์ตรวจจับการใช้งานเครือข่ายที่ผิดปกติ

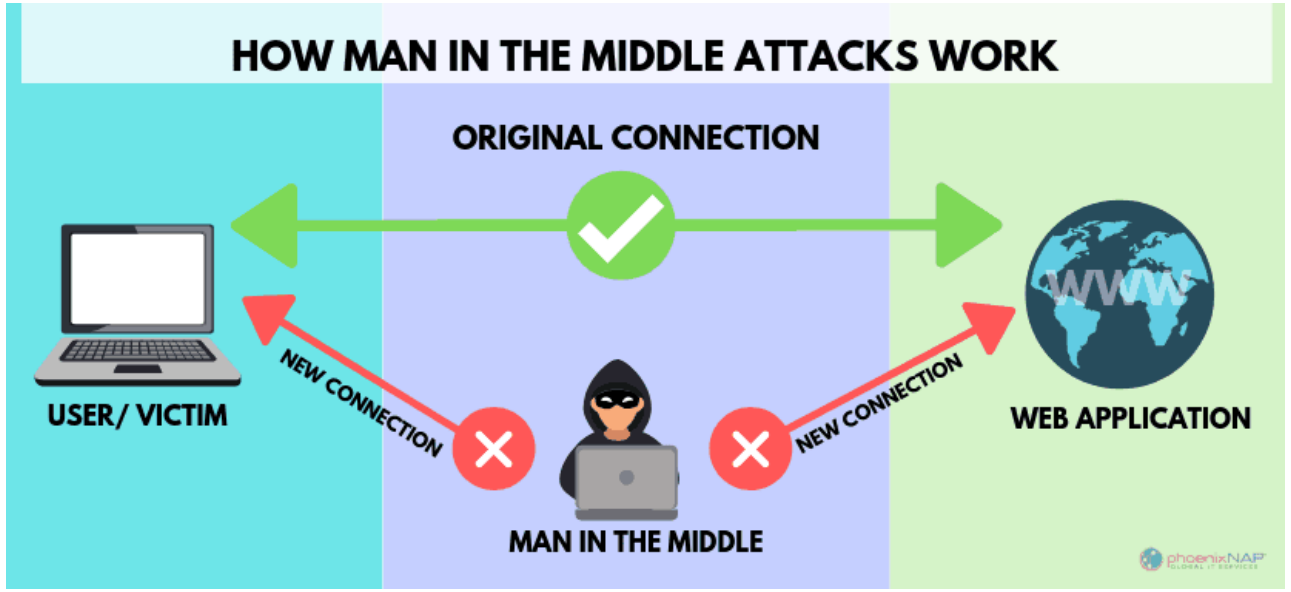


2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Network

การโจมตีเครือข่ายแบบ Man in the Middle

- Man in the Middle คือ การที่มีผู้ประสงค์ร้ายแทรกเข้ามาทำตัวเป็นตัวกลางระหว่างการติดต่อของผู้ส่งและผู้รับ โดยทั้งสองไม่ทราบ ทำให้ผู้ประสงค์ร้ายสามารถกำหนดการสื่อสารนั้นได้
- Man in the Middle ผ่าน WiFi โดยแทรกกลางระหว่าง ผู้ใช้งาน WiFi กับ Website



2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Network

แนวทางป้องกัน Man in the Middle

- ผู้ใช้ (User)
  - ป้องกันโปรแกรมแปลกปลอมเข้ามาในเครื่อง
  - พยายามใช้website ที่มีการเข้ารหัส ใช้ https แทนการใช้ http
  - มีการยืนยันตัวตนผู้ที่ติดต่อด้วยผ่านช่องทางอื่นไม่ใช้คอมพิวเตอร์ เช่น โทรสอบถามกัน
- ผู้ใช้ (Administrator / Supervisor)
  - ตั้งรหัส WiFi ที่ปลอดภัยเพื่อป้องกันผู้ไม่ประสงค์ดีลักลอบเข้ามาใช้ระบบ

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Devices

การพิสูจน์ตัวตน, ระบุตัวตน, และบัญชีผู้ใช้งาน (AAA : Authentications, Authorizations and Accounting)

- Confidentiality กำหนดว่าผู้ที่เข้าใช้งานข้อมูลได้จะต้องเป็นผู้ได้รับสิทธิเท่านั้น
  - ต้องมีการเก็บรายชื่อผู้มีสิทธิ และ สิทธิที่ได้
- การพิสูจน์ว่าคนๆหนึ่ง คือ ผู้ที่เขาอ้างจริง (Authentication) สามารถทำด้วยการยืนยันสามแบบคือ
  - Something you know สิ่งที่คุณรู้ (เช่น Password)
  - Something you have สิ่งที่คุณมี (Smartphone ของเรา)
  - Something you are สิ่งที่คุณเป็น (Biometrics)

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Devices

การพิสูจน์ตัวตน, ระบุตัวตน, และบัญชีผู้ใช้งาน (AAA : Authentications, Authorizations and Accounting)

ตัวอย่าง Password อันตรายที่คนส่วนใหญ่ใช้มากที่สุด

123456	**12345678**	**1234567890**
123456789	Abc123	123123
Qwerty	1234567	Iloveyou
Password	Password1	1234
11111111	12345	1q2w3e4r5t

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Devices

การพิสูจน์ตัวตน, ระบุตัวตน, และบัญชีผู้ใช้งาน (AAA : Authentications, Authorizations and Accounting)

การใช้ password ที่ไม่ควรทำ

- ตั้ง password สั้น ไม่ซับซ้อน
- ใช้ password เดียวในหลายระบบ

การจัดการ password ที่อ่อนแอ

- ระบบเก็บ password ที่ไม่เข้ารหัส ผู้อื่นสามารถเห็นได้

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Devices

การพิสูจน์ตัวตน, ระบุตัวตน, และบัญชีผู้ใช้งาน (AAA : Authentications, Authorizations and Accounting)

แนวทางป้องกัน Man in the Middle

- ผู้ใช้ (User)
  - เก็บ password ไว้เป็นความลับส่วนตัว
  - password ไม่เป็นคำ ไม่ใช้อักษาซ้ำ ยาวไม่ต่ำกว่า 8 ตัวอักษร
  - เปลี่ยน password ทุกเดือน
  - หลีกเลี่ยง password ซ้ำในหลายระบบ
- ผู้ใช้ (Administrator / Supervisor)
  - เก็บ password แบบมองไม่เห็น (password hashing)

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

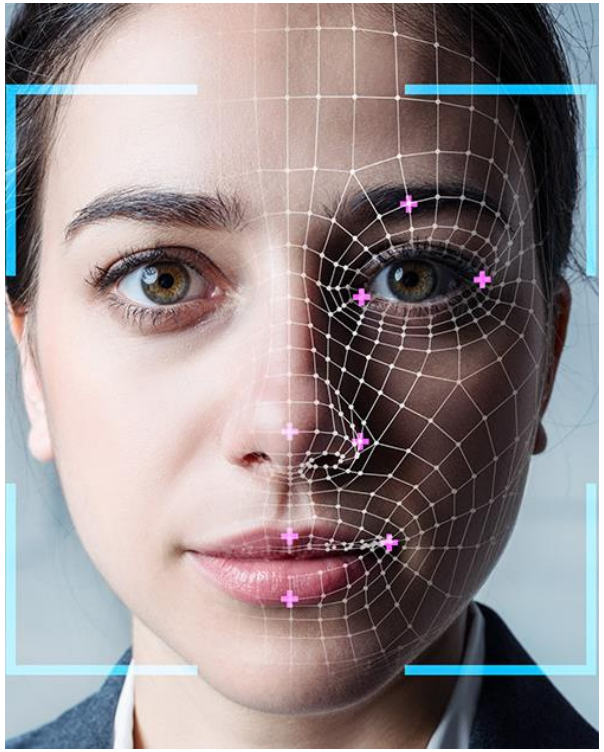
จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Devices

การพิสูจน์ตัวตน, ระบุตัวตน, และบัญชีผู้ใช้งาน (AAA : Authentications, Authorizations and Accounting)

การพิสูจน์ตัวตนด้วยชีวมิติ (Biometric Authentication)

Biometric เป็นเอกลักษณ์เฉพาะตัวบุคคล

- การยืนยันตัวตนด้วยลายนิ้วมือ finger scan
- การยืนยันตัวตนด้วยม่านตา retina scan
- การตรวจสอบใบหน้า face recognition
- การยืนยันตัวตนด้วยเสียง voice identification
- การยืนยันตัวตนด้วยเส้นเลือด vein recognition
- ...etc...



2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Devices

การพิสูจน์ตัวตน, ระบุตัวตน, และบัญชีผู้ใช้งาน (AAA : Authentications, Authorizations and Accounting)

การพิสูจน์ตัวตนด้วยชีวมิติ (Biometric Authentication)

ข้อดีของ Biometric

- ไม่สูญหาย <-> บัตร ATM
- ถูกขโมยไปใช้ไม่ได้ <-> password
- ไม่สามารถทำซ้ำได้ <-> กุญแจ
- ปฏิเสธการใช้งานไม่ได้ <-> mobile phone

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Devices

การพิสูจน์ตัวตน, ระบุตัวตน, และบัญชีผู้ใช้งาน (AAA : Authentications, Authorizations and Accounting)

การพิสูจน์ตัวตนด้วยชีวมิติ (Biometric Authentication)

ข้อจำกัดของ Biometric

- ความแม่นยำ Accuracy
  - False Rejection Rate (FRR) คือ อัตราที่ตัวตนถูกต้องแต่ระบบไม่อนุญาตให้ใช้งาน
  - False Acceptance Rate (FAR) คือ อัตราที่ตัวตนไม่ถูกแต่ระบบอนุญาตให้เข้าใช้งาน
- เวลาตอบสนอง Response Time
  - การตอบสนองช้า ทำให้ผู้ใช้งานไม่สะดวก
  - การตอบสนองเร็ว ทำให้ต้นทุนสูงหรือความปลอดภัยลดลง

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Devices

Malware

- **Malware (มัลแวร์)** หรือ Malicious Software หมายถึงโปรแกรมคอมพิวเตอร์ที่มีจุดประสงค์ร้ายต่อคอมพิวเตอร์และระบบเครือข่าย ตัวอย่างเช่น
  - Virus
  - Trojan Horse
  - Keylogger
  - ...etc...

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Devices

Malware –> Virus (ไวรัส)

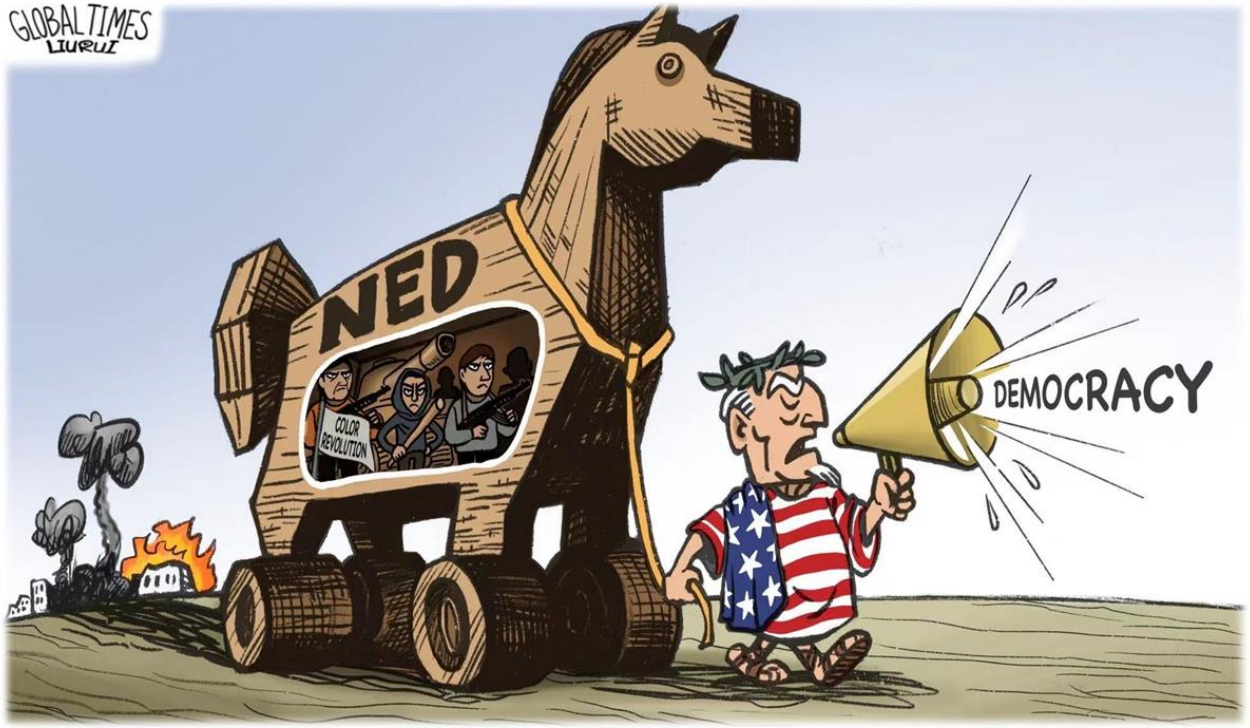
- **Virus (ไวรัส)** คือโปรแกรมที่ก่อกวนการใช้งานเครื่องคอมพิวเตอร์ หรือ ทำลายข้อมูล ส่วนใหญ่สามารถระบาดไปสู่คอมพิวเตอร์เครื่องอื่นได้ ผ่านระบบเครือข่าย หรือ removable media
- **อาการที่พบบ่อยในเครื่องที่ติด virus**
  - เครื่องช้า ค้าง หรือ หยุดทำงาน
  - ไฟล์เสีย เพิ่มขนาดเอง หรือ หายไป
  - มีตัวอักษรแสดงบนจอ หรือ มีเสียงจากลำโพง
  - ขนาดของหน่วยความจำลดลง
- **แนวทางป้องกัน**
  - ใช้ removable media กับคอมพิวเตอร์ที่เชื่อถือได้เท่านั้น
  - ติดตั้ง Antivirus หรือ โปรแกรมที่ดักจับและทำลายไวรัส

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Devices

Malware –> Trojan Horse

- **Trojan Horse** เป็น malware ที่แสดงต่อผู้ใช้เสมือนเป็นโปรแกรมทำงานปกติ แต่มีการทำงานเบื้องหลังที่ประสงค์ร้าย



2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Devices

Malware –> Keylogger(คีย์ล็อคเกอร์)

- Keylogger เป็นการเก็บบันทึกการกดปุ่ม Keyboard ของผู้ใช้ โดยไม่ให้ผู้ใช้ทราบ
- Keylogger มักมีจุดประสงค์เพื่อดักจับ username และ password
- การทำ Keylogger มีรูปแบบทั้ง hardware และ software

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Devices

Malware –> Hack Tools

- Logic bomb คือ มัลแวร์ที่ฝังตัวอยู่ และเริ่มทำร้ายระบบเมื่อถึงเวลาที่ตั้งไว้
- Botnet คือ มัลแวร์ที่ฝังตัวอยู่ รอรับคำสั่งจากผู้คุม
- Backdoor คือ มัลแวร์ที่ฝังตัวอยู่ คอยเปิดทางเข้าให้ผู้คุมภายนอกเข้ามาใช้ระบบ
- Rootkit คือ มัลแวร์ที่เข้าควบคุมเครื่องคอมพิวเตอร์

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Devices

Ransomware

- Ransomware หรือ โจรเรียกค่าไถ่ จะทำการเข้ารหัสไฟล์ในเครื่องคอมพิวเตอร์เพื่อไม่ให้ผู้ใช้เข้าใช้งานไฟล์ได้ หากผู้ใช้ต้องการใช้งานไฟล์นั้นจะต้องจ่ายเงินให้เจ้าของ ransomware โดยมากจากเป็น bitcoin
- แนวทางป้องกัน
  - สำรองข้อมูลเป็นประจำ
  - เก็บข้อมูลที่สำรองแต่ละครั้งไว้ในสื่อ
  - ที่ไม่สามารถเชื่อมต่อถึงกัน
  - แยกระบบกู้ข้อมูลออกจากระบบจริง

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

Secure Software Development

- การพัฒนาซอฟร์แวร์อย่างปลอดภัย
- การออกแบบระบบจะต้องคำนึงถึงความปลอดภัยในทุกขั้นตอน
- จำกัดสิทธิผู้ใช้ให้น้อยที่สุดเท่าที่จำเป็น (least privilege authorization)
- กำหนดมาตรฐานด้วยความปลอดภัยในการเขียนโปรแกรม (coding)
- เข้ารหัสข้อมูลที่สำคัญ
- มีการตรวจสอบความปลอดภัยระบบก่อนใช้งานจริง และเมื่อมีการแก้ไขซอฟต์แวร์

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

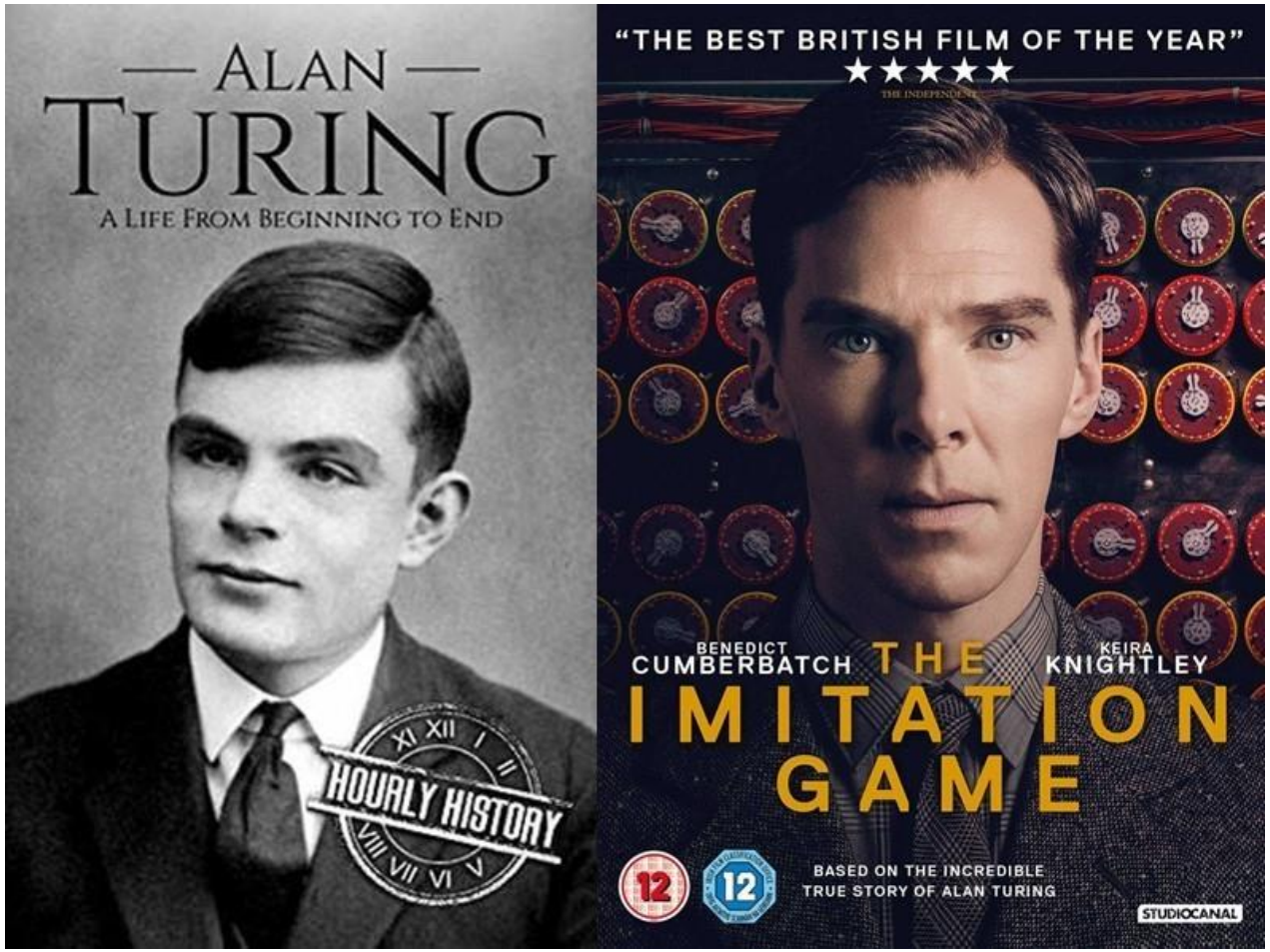
จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

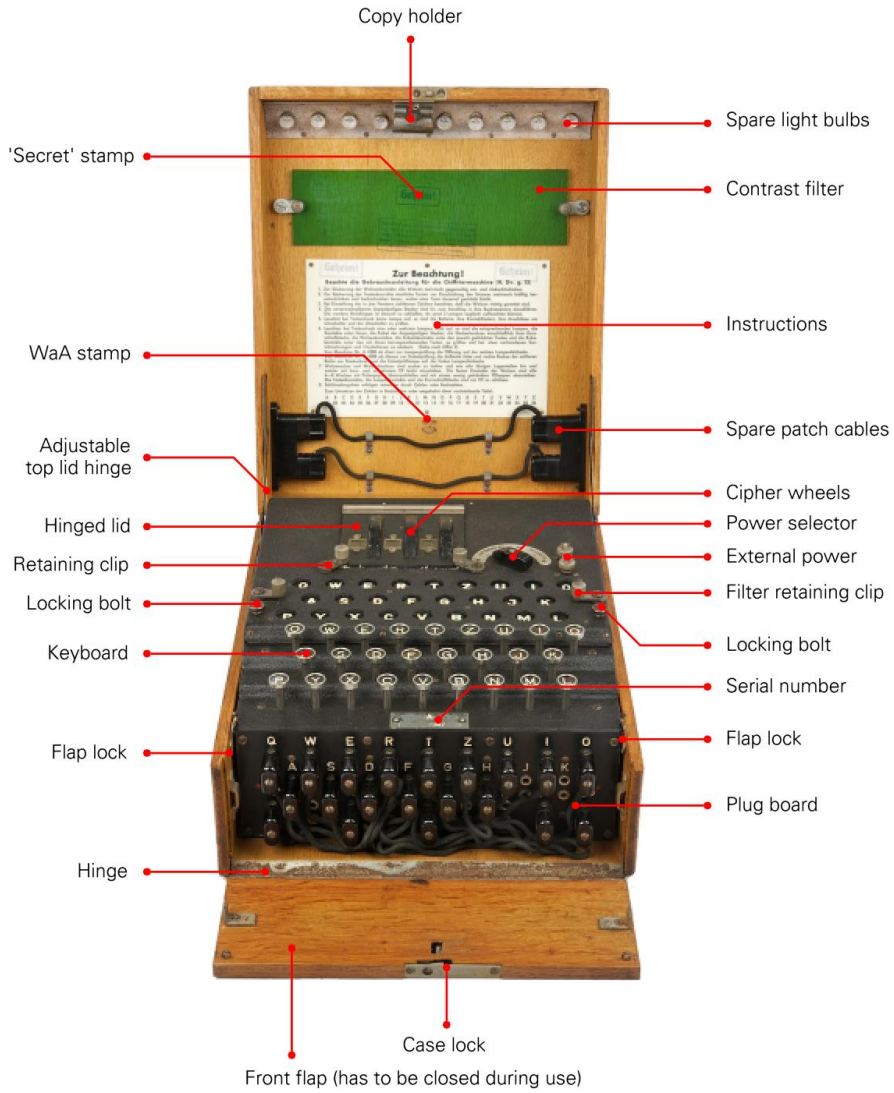
การเข้ารหัส

- วิทยาการเข้ารหัส (Cryptography) คือ กระบวนการทางคอมพิวเตอร์สำหรับทำให้การติดต่อสื่อสารระหว่าง 2 บุคคลเพื่อให้
  - ผู้ที่สามารถดูข้อมูลได้คือผู้ส่งและผู้รับเท่านั้น
  - ผู้ที่ส่งข้อมูลไม่สามารถปฏิเสธได้ว่าส่งข้อมูลนั้น
  - แยกระบบกู้ข้อมูลออกจากระบบจริง
- การเข้ารหัส (Encryption) คือ วิธีการเปลี่ยนแปลงข้อความเพื่อไม่ให้ผู้อื่นเข้าใจความหมายของข้อมูลนั้น

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software





2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

ตัวอย่างการเข้ารหัส

การเข้ารหัสแบบแทนที่

Plain text	A	B	C	D			W	X	Y	Z
Cipher text	z	y	x	w			d	c	b	a

Plain text : BAY ⇨ Cipher text :

การเข้ารหัสแบบ Ceasar

Plain text	A	B	C	D			W	X	Y	Z
Cipher text	Y	Z	A	B			U	V	W	X

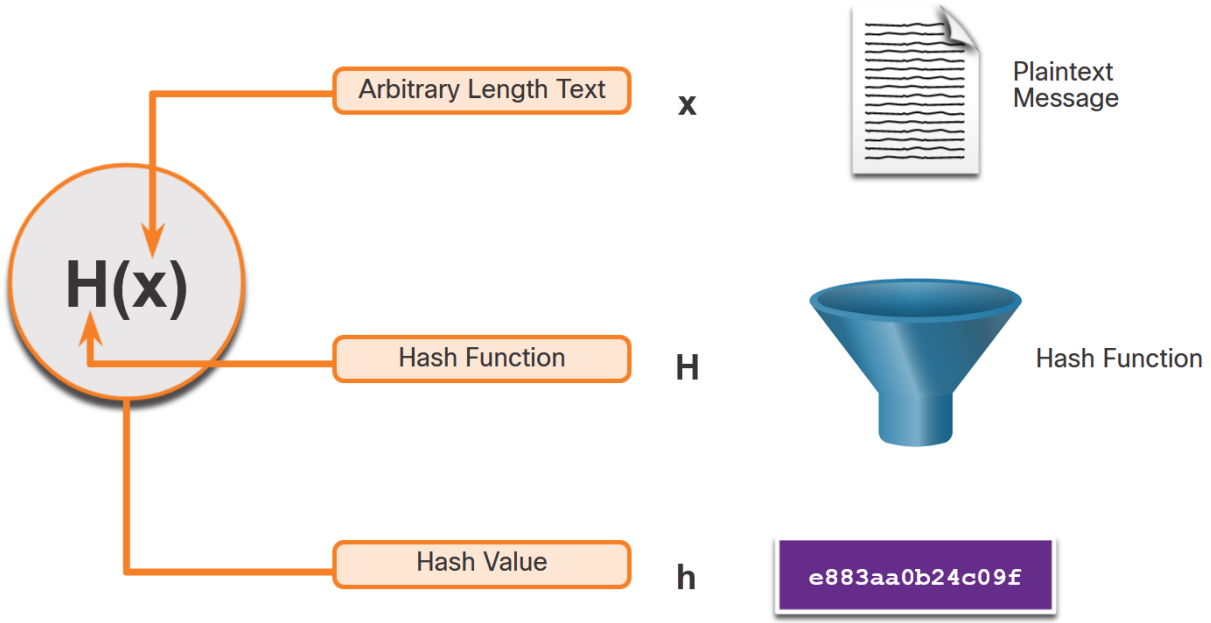
Plain text : BAY ⇨ Cipher text :

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

Cryptographic Hash Operation – Confidentiality

- Mathematically, the equation h= H(x) is used to explain how a hash algorithm operates. As shown in the figure, a hash function H takes an input x and returns a fixed-size string hash value h.



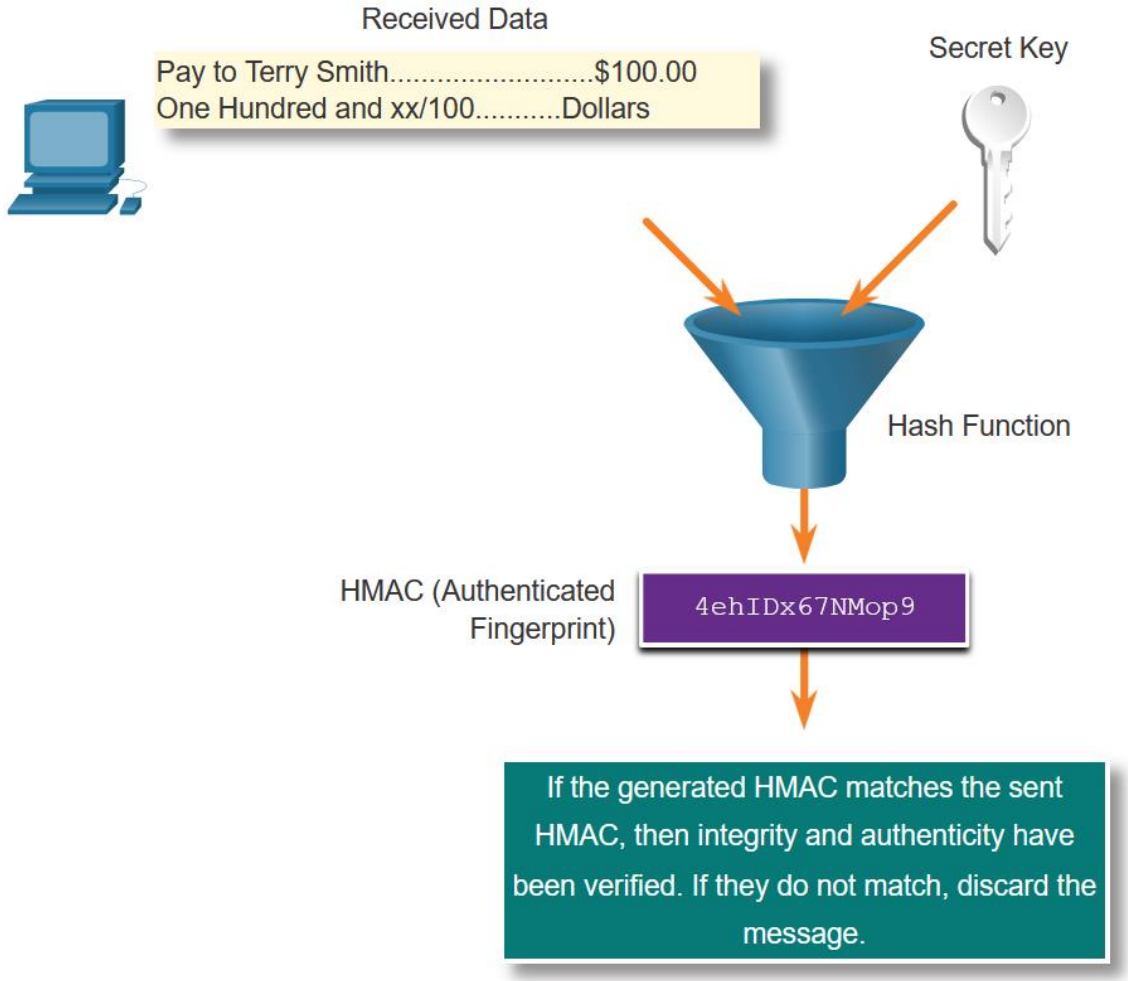
ภาพจาก Cisco.com

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

Origin Authentication – Confidentiality

- In the figure, the receiving device removes the digest from the message and uses the plaintext message with its secret key as input into the same hashing function. If the digest that is calculated by the receiving device is equal to the digest that was sent, the message has not been altered. Additionally, the origin of the message is authenticated because only the sender possesses a copy of the shared secret key. The HMAC function has ensured the authenticity of the message.



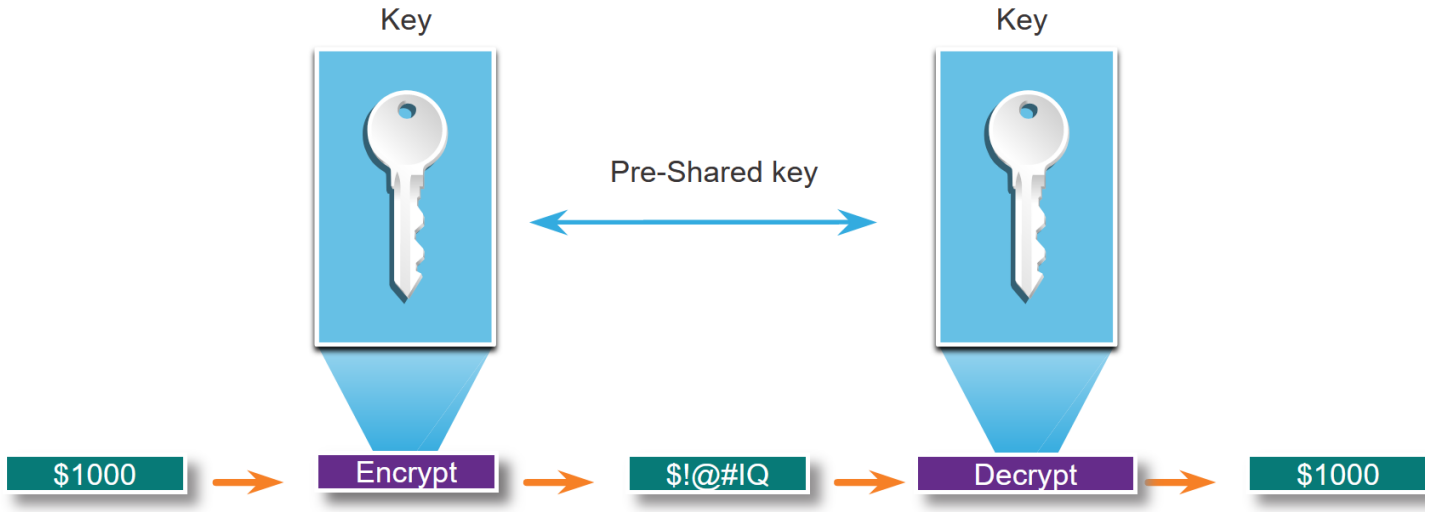
ภาพจาก Cisco.com

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

Symmetric Encryption – Confidentiality

- Symmetric algorithms use the same pre-shared key to encrypt and decrypt data. A pre-shared key, also called a secret key, is known by the sender and receiver before any encrypted communications can take place.



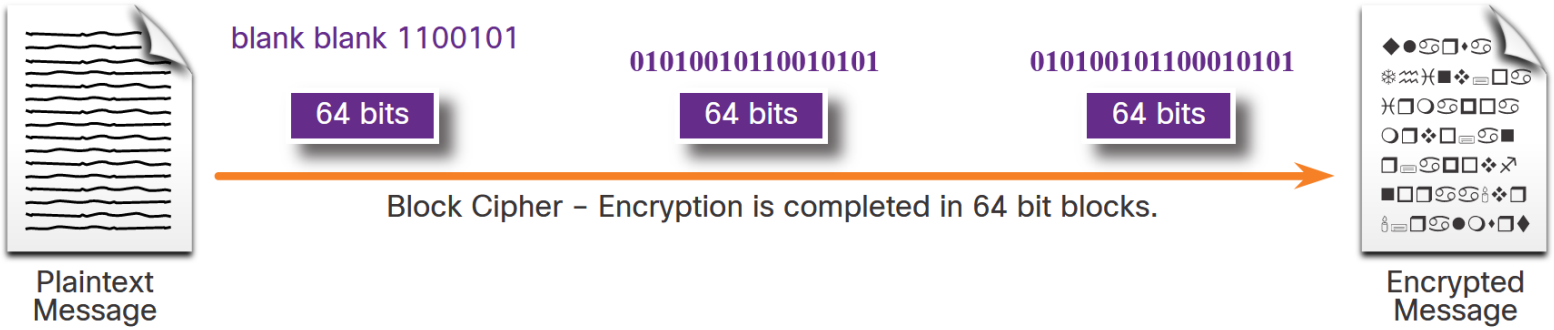
ภาพจาก Cisco.com

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

Symmetric Encryption – Confidentiality

- Block ciphers transform a fixed-length block of plaintext into a common block of ciphertext of 64 or 128 bits. Common block ciphers include DES with a 64-bit block size and AES with a 128-bit block size.



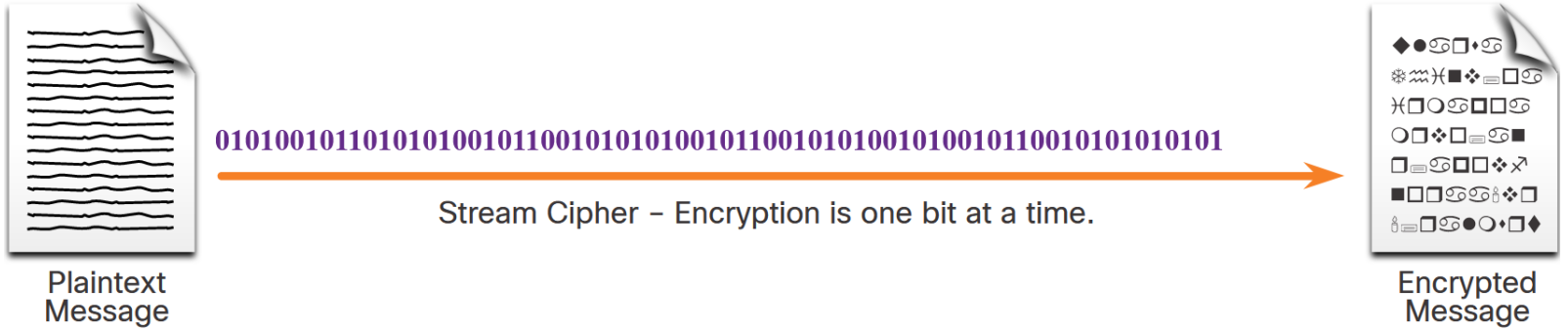
ภาพจาก Cisco.com

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

Symmetric Encryption – Confidentiality

- Stream ciphers encrypt plaintext one byte or one bit at a time. Stream ciphers are basically a block cipher with a block size of one byte or bit. Stream ciphers are typically faster than block ciphers because data is continuously encrypted.



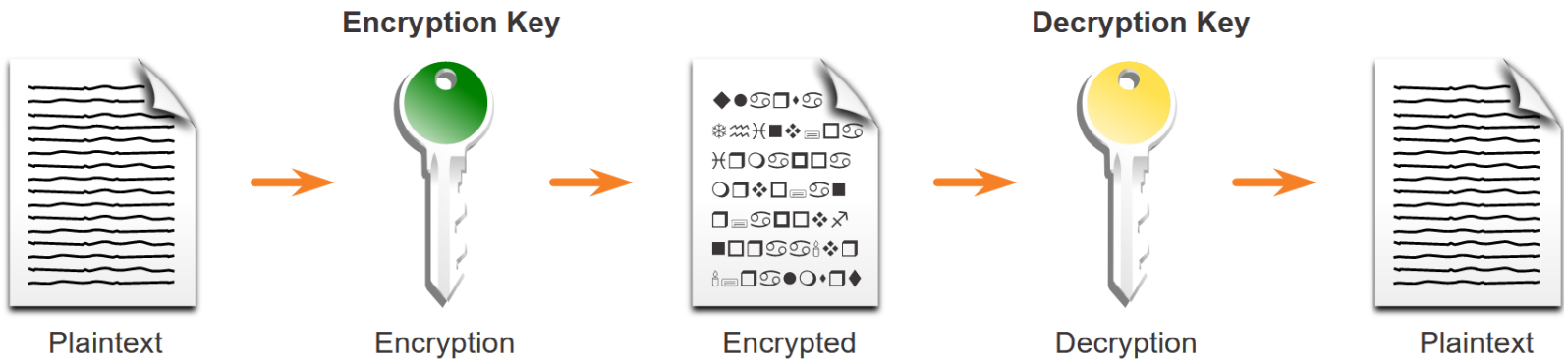
ภาพจาก Cisco.com

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

Asymmetric Encryption – Confidentiality

- Asymmetric algorithms, also called public-key algorithms, are designed so that the key that is used for encryption is different from the key that is used for decryption



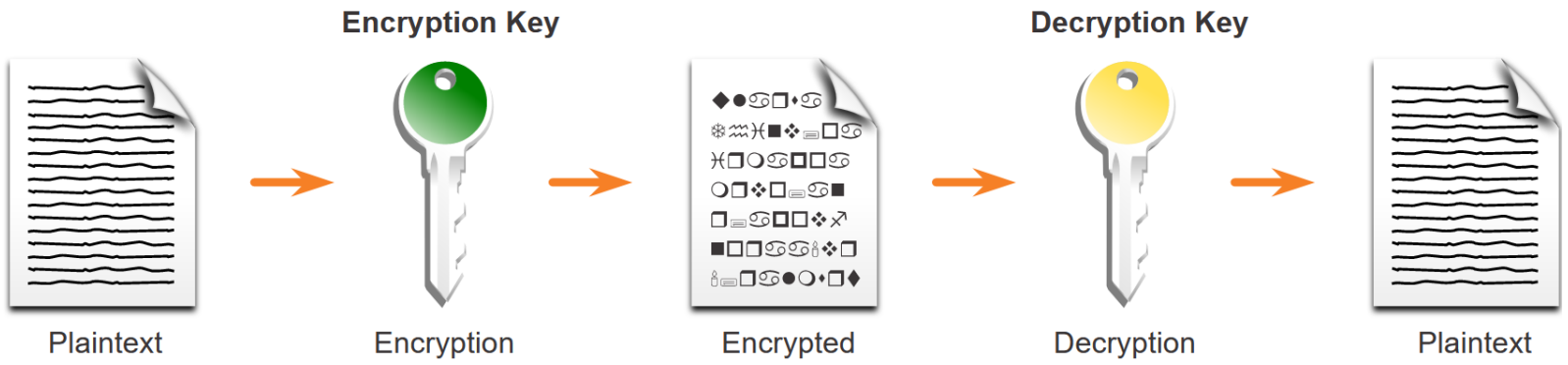
ภาพจาก Cisco.com

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

Asymmetric Encryption – Confidentiality

- **Internet Key Exchange (IKE)** – This is a fundamental component of IPsec VPNs.
- **Secure Socket Layer (SSL)** – This is now implemented as IETF standard Transport Layer Security (TLS).
- **Secure Shell (SSH)** – This protocol provides a secure remote access connection to network devices.
- **Pretty Good Privacy (PGP)** – This computer program provides cryptographic privacy and authentication. It is often used to increase the security of email communications.



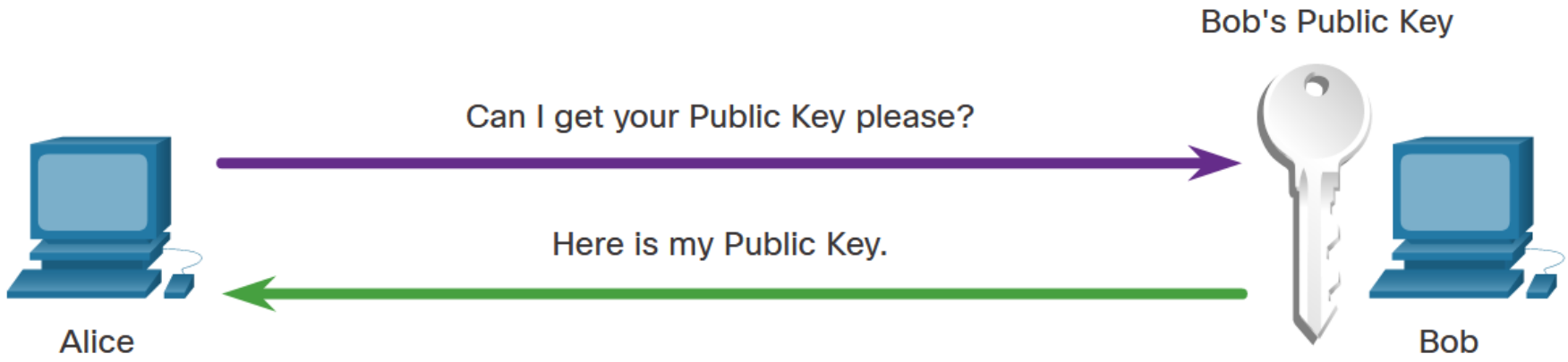
ภาพจาก Cisco.com

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

Asymmetric Encryption – Confidentiality

- Public Key (Encrypt) + Private Key (Decrypt) = Confidentiality



Public Key (Encrypt) + Private Key (Decrypt) = Confidentiality

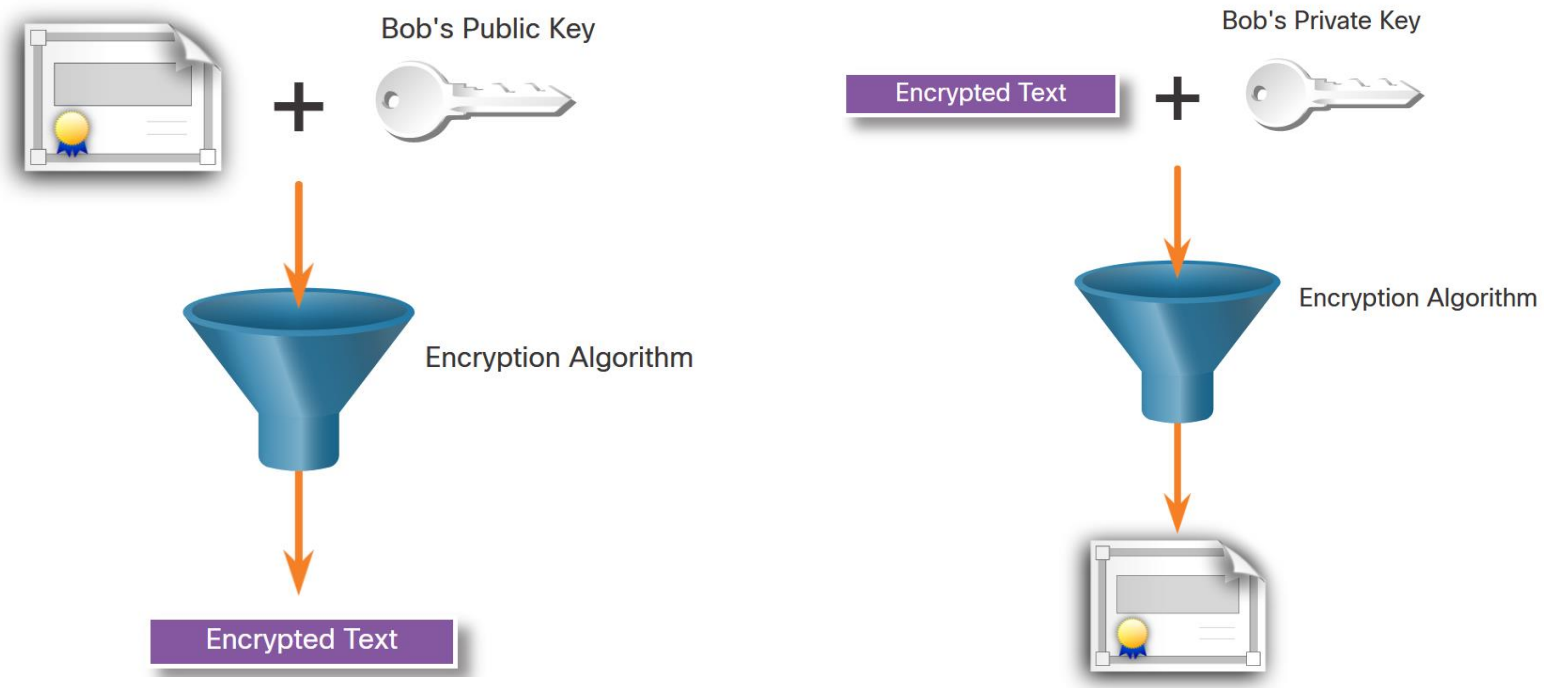
ภาพจาก Cisco.com

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

Asymmetric Encryption – Confidentiality

- Public Key (Encrypt) + Private Key (Decrypt) = Confidentiality



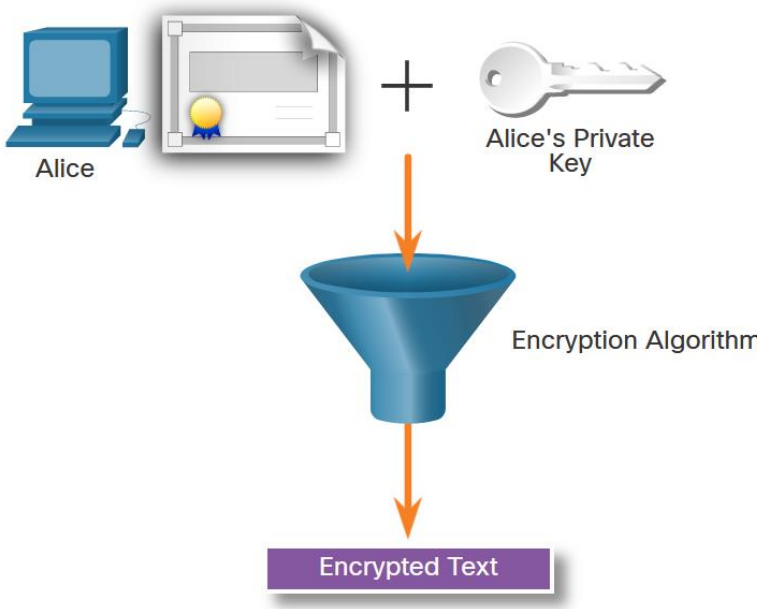
ภาพจาก Cisco.com

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

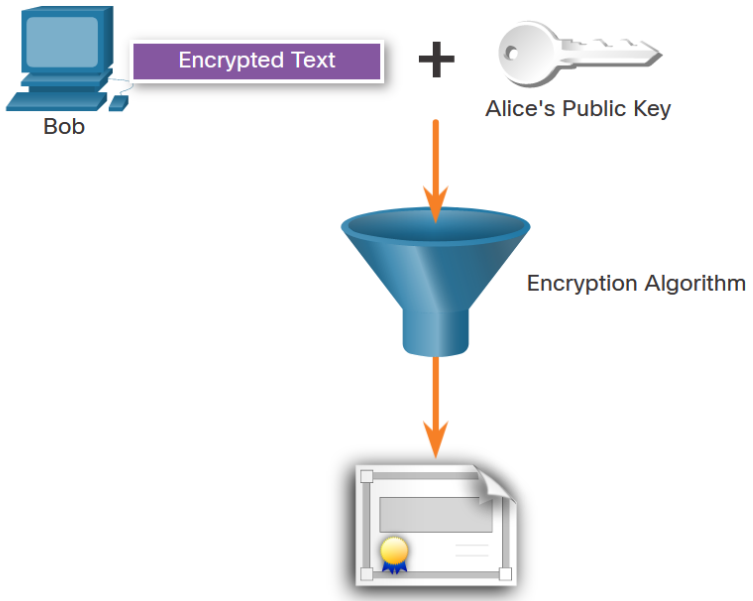
จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

Asymmetric Encryption – Authentication

- Public Key (Encrypt) + Private Key (Decrypt) = Authentication



Private Key (Encrypt) + Public Key (Decrypt) = Authentication

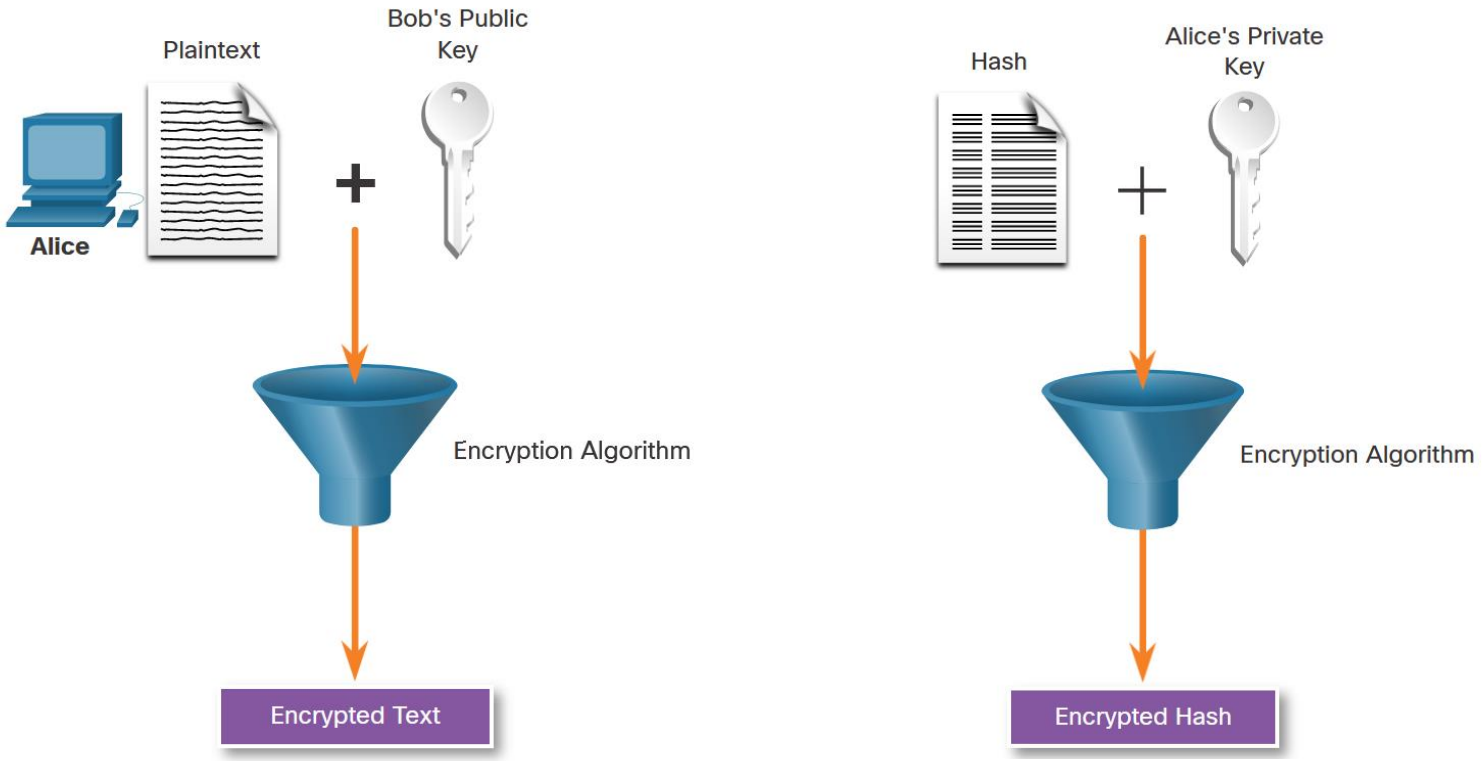


Bob uses the public key to successfully decrypt the message and authenticate that the message did, indeed, come from Alice.

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

Asymmetric Encryption – Integrity



ภาพจาก Cisco.com

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : Software

The Secret is in the Keys

The table lists some common cryptographic hashes, protocols, and algorithms.

Integrity	Authenticity	Confidentiality
MD5 (legacy)	HMAC-MD5 (legacy)	3DES (legacy)
SHA	HMAC-SHA-256	AES
	RSA and DSA	

ตารางจาก Cisco.com

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : People

People (ผู้ใช้งานระบบ)

- ไม่รอบครอบ
  - รักษาความลับของ password ไม่ดี
  - ใช้เครื่องคอมพิวเตอร์ที่ไม่ปลอดภัย
  - ให้ผู้อื่นเข้าถึงคอมพิวเตอร์ของตนเอง
  - Download ข้อมูลที่ไม่ปลอดภัย
- ถูกหลอกลวง
  - Phishing

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

จุดอ่อนที่จะเกิดความไม่ปลอดภัย (Attack Surface) : People

Phishing คือ การพยายามหลอกลวงเอาข้อมูลสำคัญจากผู้ใช้คอมพิวเตอร์ เช่น username , password , หมายเลขบัญชีธนาคาร เป็นต้น โดยใช้สื่อสารสนเทศ

- นอกเหนือจากการหลอกลวงเอาข้อมูลสำคัญแล้ว phishing ยังถูกใช้เป็นช่องทางเพื่อแอบติดตั้งมัลแวร์ลงในเครื่องของเหยื่อ
- ช่องทางที่พบการหลอกลวงบ่อย
  - SMS
  - E-Mail
  - Facebook
  - Line
  - ...etc...

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

กรณีศึกษา ภัยคุกคามด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

- Example 1 : 2010 ; Stuxnet การโจมตีทาง OT cyber attack. เป้าหมาย โรงงานนิวเคลียร์ Iran
- ใช้โดย highly sophisticated worm ยิง exploited multiple zero-day

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

- Example 1 : 2010 ; Stuxnet การโจมตีทาง OT cyber attack.

ผลกระทบ : เครื่องจักรในโรงงานนิวเคลียร์ ได้รับความเสียหาย ทำให้ความสามารถในการเสริมสมรรถนะยูเรเนียมช้าลง

จุดประสงค์การโจมตี

- ก่อวินาศกรรม และขัดขวางกระบวนการเสริมสมรรถนะยูเรเนียม

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

- Example 2 : 2015 and 2016 ; Ukraine Power Grid Attacks

การโจมตีทาง OT cyber attack. เป้าหมาย โครงข่ายไฟฟ้าของยูเครน ในช่วง Dec2015 และ Dec2016 โดยใช้ Malware ที่เรียกว่า BlackEnergy และ KillDisk

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

- Example 2 : 2015 and 2016 ; Ukraine Power Grid Attacks

ผลกระทบ : สร้างความเสียหายให้กับโครงข่ายไฟฟ้าของยูเครน ทำให้ไฟฟ้าดับเป็นวงกว้าง การให้บริการด้านพลังงานหยุดชะงัก ประชาชนได้รับความเดือดร้อน

จุดประสงค์การโจมตี

- ก่อกวนและทำให้ critical infrastructure ด้านพลังงานของ ยูเครนสั่นคลอน
- แสดงให้เห็นความสามารถในการแทรกซึม
- แสดงแสงยานุภาพด้าน Cyber Warfare

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

- Example 3 : Dec2017 ; Triton/Trisis

การโจมตีทาง OT cyber attack. เป้าหมาย โรงงานปิโตรเคมีใน Saudi Arabia โดยใช้ Malware ที่เรียกว่า Triton หรือ TRISIS (Triconex Safety Instrumented System)

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

- Example 3 : Dec2017 ; Triton/Trisis

ผลกระทบ : เกิดความเสี่ยงและไม่ปลอดภัยในการปฏิบัติงานของบุคลากรในโรงงานปิโตรเคมี

จุดประสงค์การโจมตี

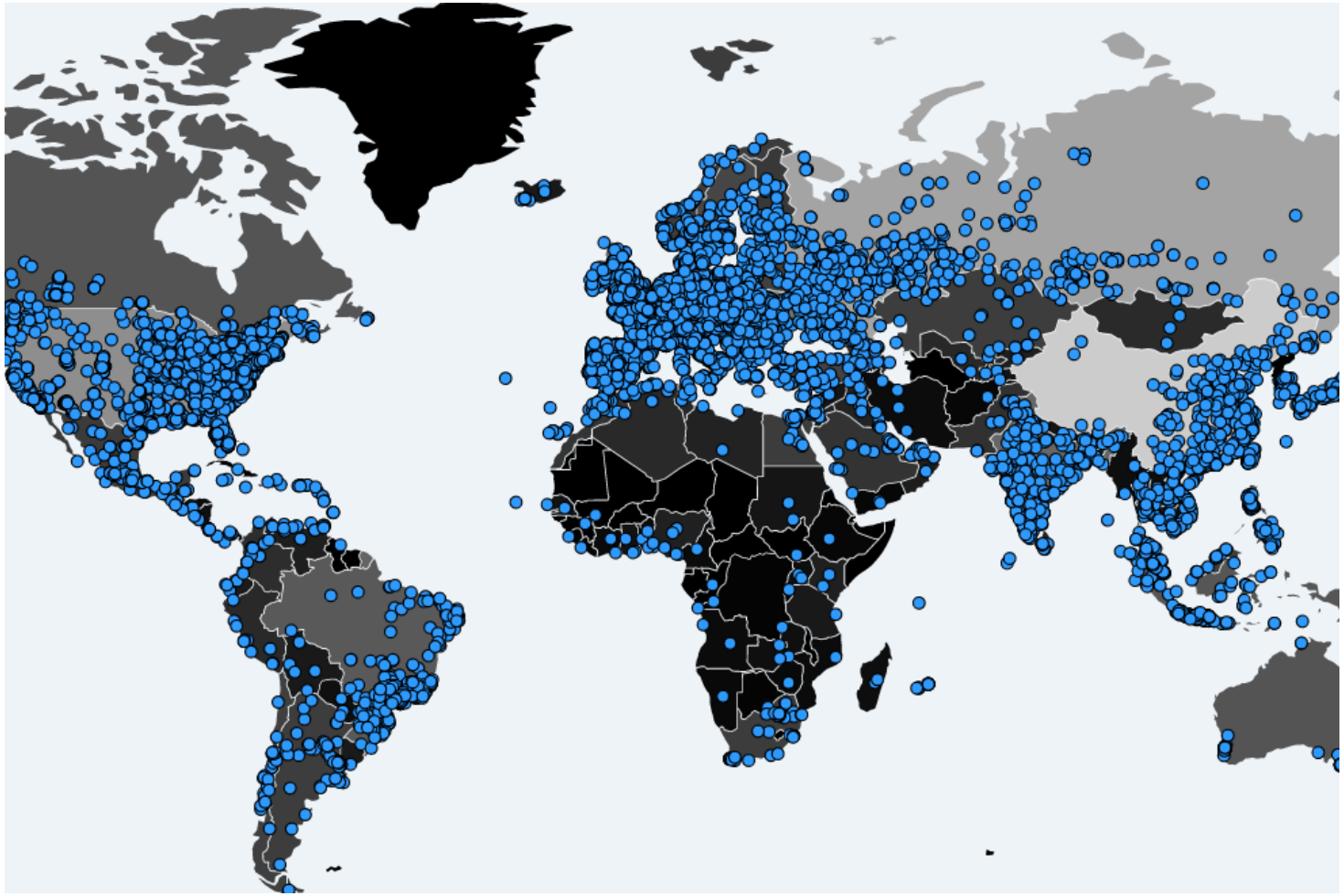
- ขัดขวางการดำเนินงานของภาคอุตสาหกรรม
- ให้เครื่องจักรและอุปกรณ์ทำงานผิดปกติ
- ทำให้เกิดความเสี่ยงกับบุคลากรและสิ่งอำนวยความสะดวกต่างๆ

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

- Example 4 : May-2017 ; Ransomware WannaCry

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

- Example 4 : May-2017 ; Ransomware WannaCry



2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

- Example 4 : May-2017 ; Ransomware WannaCry

ผลกระทบจาก Ransomware WannaCry

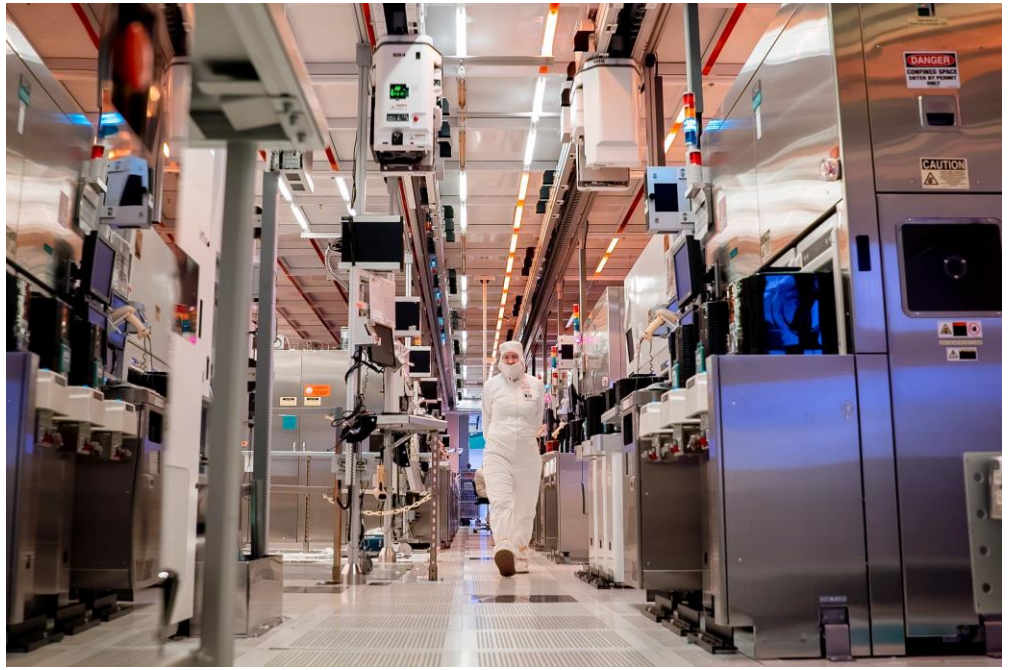
- National Health Service hospital in England and Scotland
- คอมพิวเตอร์ , เครื่อง MRI Scanner , ตู้เย็นแช่เลือด , เครื่องฉายภาพยนต์ เสียหาย ประมาณ 70,000 เครื่อง
- Nissan Motor Manufacturing UK (England)
- หยุดการผลิตชั่วคราว

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

- Example 4 : May-2017 ; Ransomware WannaCry

ผลกระทบจาก Ransomware WannaCry

- ปี2018 Taiwan semiconductor Manufacturing (TSMC) ปิดโรงงาน เนื่องจากได้รับผลกระทบจาก Ransomware WannaCry



2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

- Example 5 : 2017 ; NotPetya

การโจมตีทาง cyber attack. เป้าหมาย องค์กรต่างๆ ทั่วโลก โดยใช้ Ransomware เมื่ออยู่ในระบบ มันจะเขียนทับ Master Boot Record (MBR) และเข้ารหัสไฟล์สำคัญ ทำให้ระบบใช้งานไม่ได้

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

- Example 5 : 2017 ; NotPetya

ผลกระทบ : ระบบคอมพิวเตอร์หยุดชะงัก เนื่องจากถูกเข้ารหัสไฟล์สำคัญ ทำให้ระบบใช้งานไม่ได้ และแพร่กระจายอย่างรวดเร็ว

จุดประสงค์การโจมตี

- ต้องการความเสียหายในวงกว้างมากกว่า ต้องการเรียกค่าไถไฟล์
- ให้การทำงานของระบบเครือข่ายเป้าหมายหยุดชะงัก

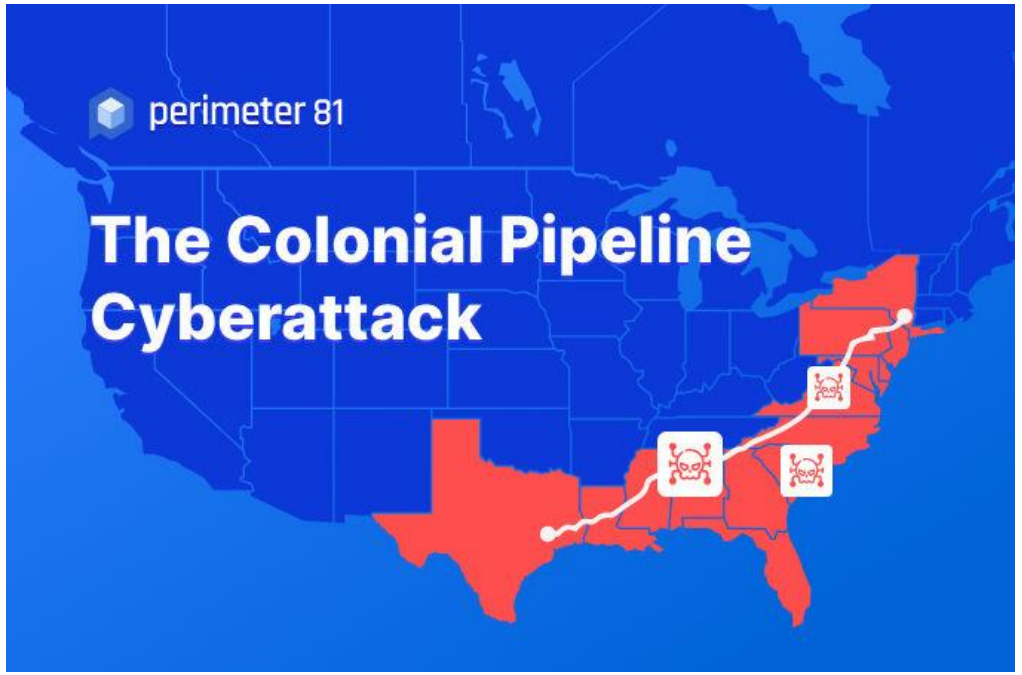
2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

- Example 6 : May2021 ;

  Colonial Pipeline Attack

การโจมตีทาง cyber attack.

เป้าหมาย ระบบท่อส่งเชื้อเพลิง Colonial Pipeline ซึ่งทำหน้าที่ส่งเชื้อเพลิงไปยังภาคตะวันออกของ USA โดย Ransomware Group ที่ชื่อ Dark Side เป็นให้บริการ ransomware-as-a-service (RaaS)



2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

- Example 6 : May2021 ; Colonial Pipeline Attack

ผลกระทบ : ท่อส่งต้องปิดดำเนินการเป็นเวลาหลายวัน นำไปสู่การขาดแคลนเชื้อเพลิงและราคาที่สูงขึ้น

จุดประสงค์การโจมตี

- เรียกค่าไถเงินจาก Colonial Pipeline แลกกับการกู้คืนข้อมูลที่ถูกเข้ารหัส

2. รูปแบบภัยคุกคามและเทคนิคการบุกรุกด้านไซเบอร์

สรุปเนื้อหาความรู้ที่ได้จากบทเรียนนี้

- ให้แต่ละกลุ่ม Discussing เนื้อหาบทที่ 1-2 ในมุมมองของตัวเอง และนำเสนอ(5นาที) ใน Class ก่อนเรียนครั้งถัดไป

Thank you for attention

www.MySurachet.com

Mobile : 085 636 2551

E-Mail : Surachet@catinfonet.com

Line : Scan to Add Friend