บทที่ 1 : การรักษาความปลอดภัยข้อมูล Part2

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Agenda

- องค์ประกอบของความปลอดภัยของข้อมูล
- ภัยคุกคาม (Threat)

องค์ประกอบของความปลอดภัยของข้อมูล

- ความลับ (Confidentiality)
- ความถูกต้องสมบูรณ์ (Integrity)
- ความพร้อมใช้งาน (Availability)

CIA

ความลับ (Confidentiality)

- หมายถึง การอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงข้อมูลได้เท่านั้น
- กลไกที่ใช้รักษาความลับคือ ***1) การเข้ารหัสข้อมูล*** (Cryptography หรือ Encryption)
  - หากบุคคลอื่นสามารถถอดรหัสได้ แสดงว่าความลับถูกทำลาย (Compromised) หรือถูกเปิดเผย (Exposure)
- ***2) กลไกควบคุมการเข้าถึง*** (Access Control) จะพิสูจน์ทราบว่าผู้ที่เข้ามาใช้งานระบบ ได้รับอนุญาตหรือไม่ เช่น ระบบ Authentication

"ถ้าไม่รู้ว่าข้อมูลนั้นมีอยู่ ก็จะไม่มีความพยายามขโมยข้อมูลนั้น"

(การปกปิดการมีอยู่ของข้อมูลเป็นสิ่งสำคัญ)

ความถูกต้องสมบูรณ์ (Integrity)

- หมายถึง ความเชื่อถือได้ของข้อมูลหรือแหล่งที่มา หรือการป้องกันไม่ให้ข้อมูล**ถูกเปลี่ยนแปลง**ไปจากเดิม
  - ความถูกต้องของ**เนื้อหา**ข้อมูล
  - ความถูกต้องของ**แหล่งที่มา**ของข้อมูล
- กลไกในการรักษาความคงสภาพของข้อมูลมี 2 ส่วน
  - การป้องกัน (Prevention)
  - การตรวจสอบ (Detection)


Data Without Integrity is Just Numbers

ความถูกต้องสมบูรณ์ (Integrity) [2]

- การป้องกัน (Prevention)
  - ป้องกันการเปลี่ยนแปลงที่เกิดจากผู้ที่ไม่ได้รับอนุญาต
  - ผู้ที่ได้รับอนุญาตพยายามแก้ไขข้อมูลนอกเหนือจากสิทธิ์ที่มี
- การตรวจสอบ (Detection) ตรวจสอบว่าข้อมูลยังคงมีความน่าเชื่อถืออยู่หรือไม่ เช่น การใช้ Hash Function


abc
1
HASH FUNCTION
2
7f0579bc2d
3

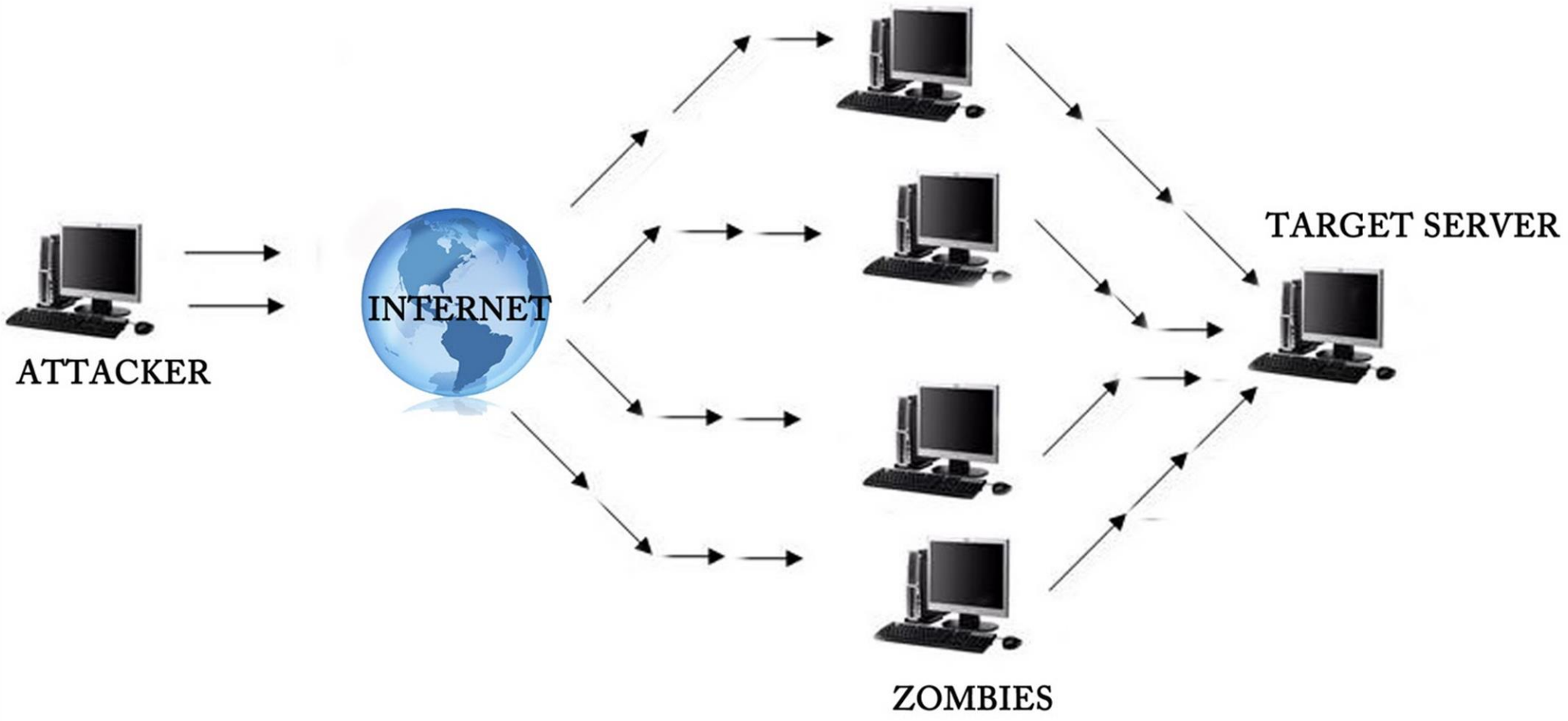
ความพร้อมใช้งาน (Availability)

- ความสามารถในการใช้ข้อมูลหรือทรัพยากรเมื่อต้องการ

“ระบบที่ไม่พร้อมใช้งาน แย่พอ ๆ กับการที่ไม่มีระบบ”

- ระบบปกติจะถูกออกแบบให้เหมาะสมกับสภาพแวดล้อมของการใช้งาน
- *กลไกการรักษาความพร้อมใช้งานจะทำงานในกรณีที่ระบบทำงานไม่ได้ในสภาพปกติที่ออกแบบไว้ เช่น การมี* **ระบบสำรอง**
- การโจมตีเพื่อทำลายความพร้อมใช้งานเรียกว่า **การโจมตีแบบปฏิเสธการให้บริการ (Denial of Service : DOS)**

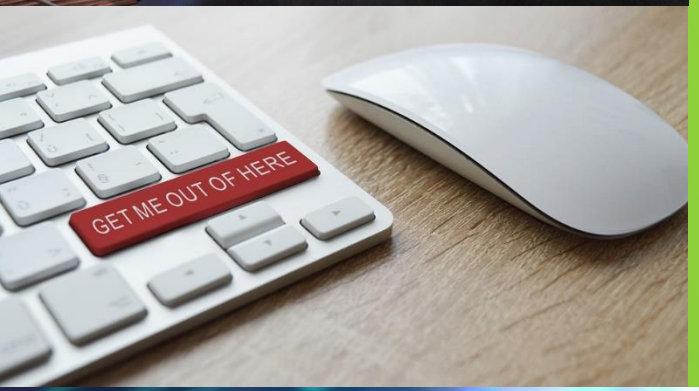
DOS ATTACK



ภัยคุกคาม (Threat)

- หมายถึง สิ่งที่อาจจะก่อให้เกิดความเสียหายต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน
- การกระทำที่อาจก่อให้เกิดความเสียหายเรียกว่า “การโจมตี” (Attack) เรียกผู้ที่กระทำเหตุการณ์ดังกล่าวว่า “ผู้โจมตี” (Attacker) หรือ “แฮคเกอร์” (Hacker) หรือ “แคร็คเกอร์” (Cracker) และเรียกเครื่องที่ถูกโจมตีว่า “เหยื่อ” (Victim)

ประเภทของภัยคุกคาม

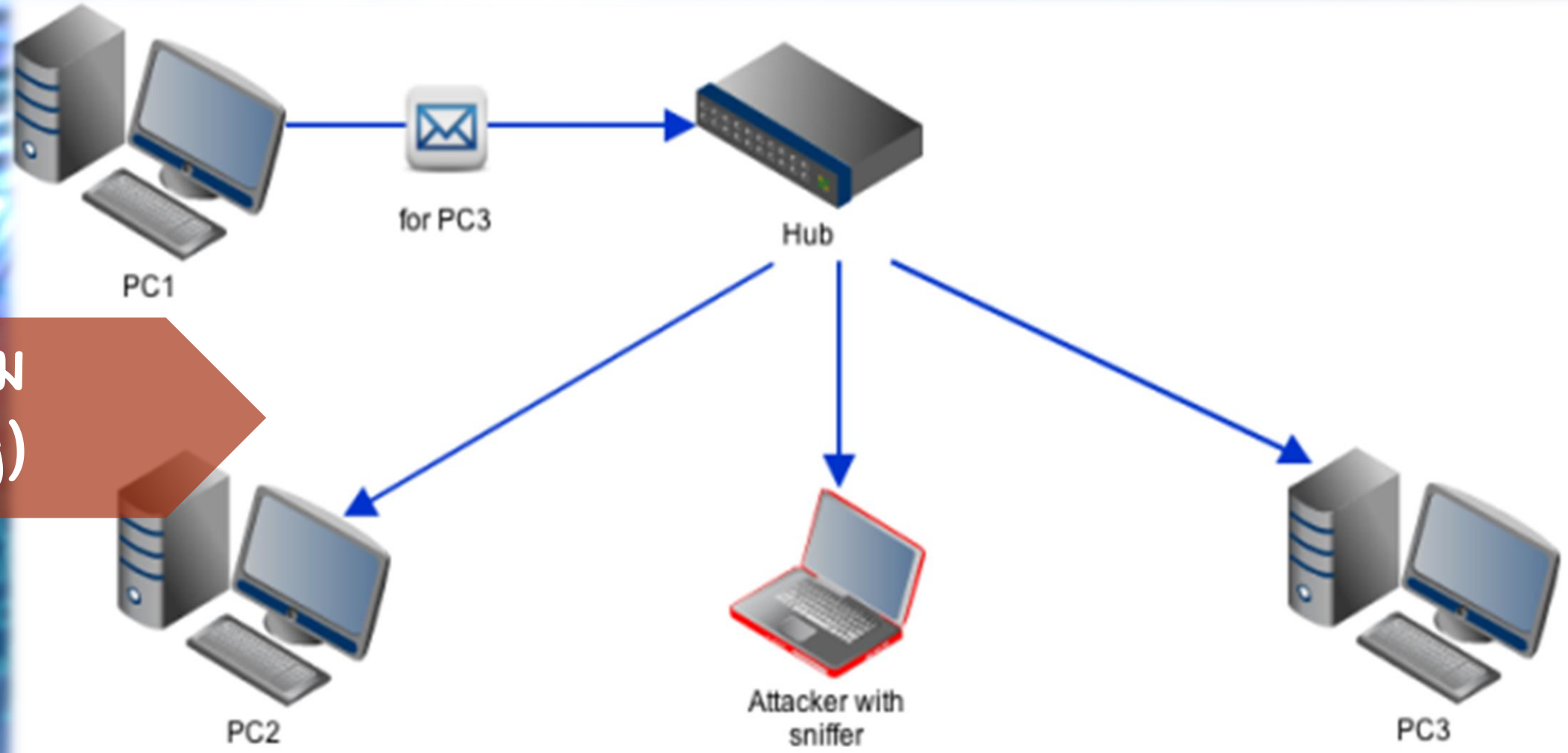


- **การเปิดเผย** (Disclosure, Exposure) : การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต เป็นการโจมตีด้านความลับ
- **การแก้ไข** (Modification) : การแก้ไขข้อมูลโดยไม่ได้รับอนุญาต เป็นการโจมตีด้านความถูกต้อง
- **การปฏิเสธการให้บริการ** (Denial of Service) : เป็นการขัดขวางทำให้ไม่สามารถเข้าถึงข้อมูลได้ เป็นการโจมตีด้านความพร้อมใช้งาน

ภัยคุกคาม (Threat) : การสอดแนม (Snooping)

- การสอดแนม (Snooping หรือ Sniffing หรือ Eavesdropping) หมายถึงการดักเพื่อแอบดูข้อมูล จัดอยู่ในภัยคุกคามประเภท**การเปิดเผย** (Disclosure)
- เป็น**การโจมตีแบบ Passive** คือไม่มีการเปลี่ยนแปลงหรือแก้ไขข้อมูล
- *ป้องกันได้โดยการเข้ารหัสข้อมูล (Encryption)*
- แอพพลิเคชันที่สามารถดักจับแพ็คเก็ตที่วิ่งบนเครือข่าย เรียกว่า **“Packet Sniffer”** เช่น โปรแกรม Wireshark

การสอดแนม (Snooping)

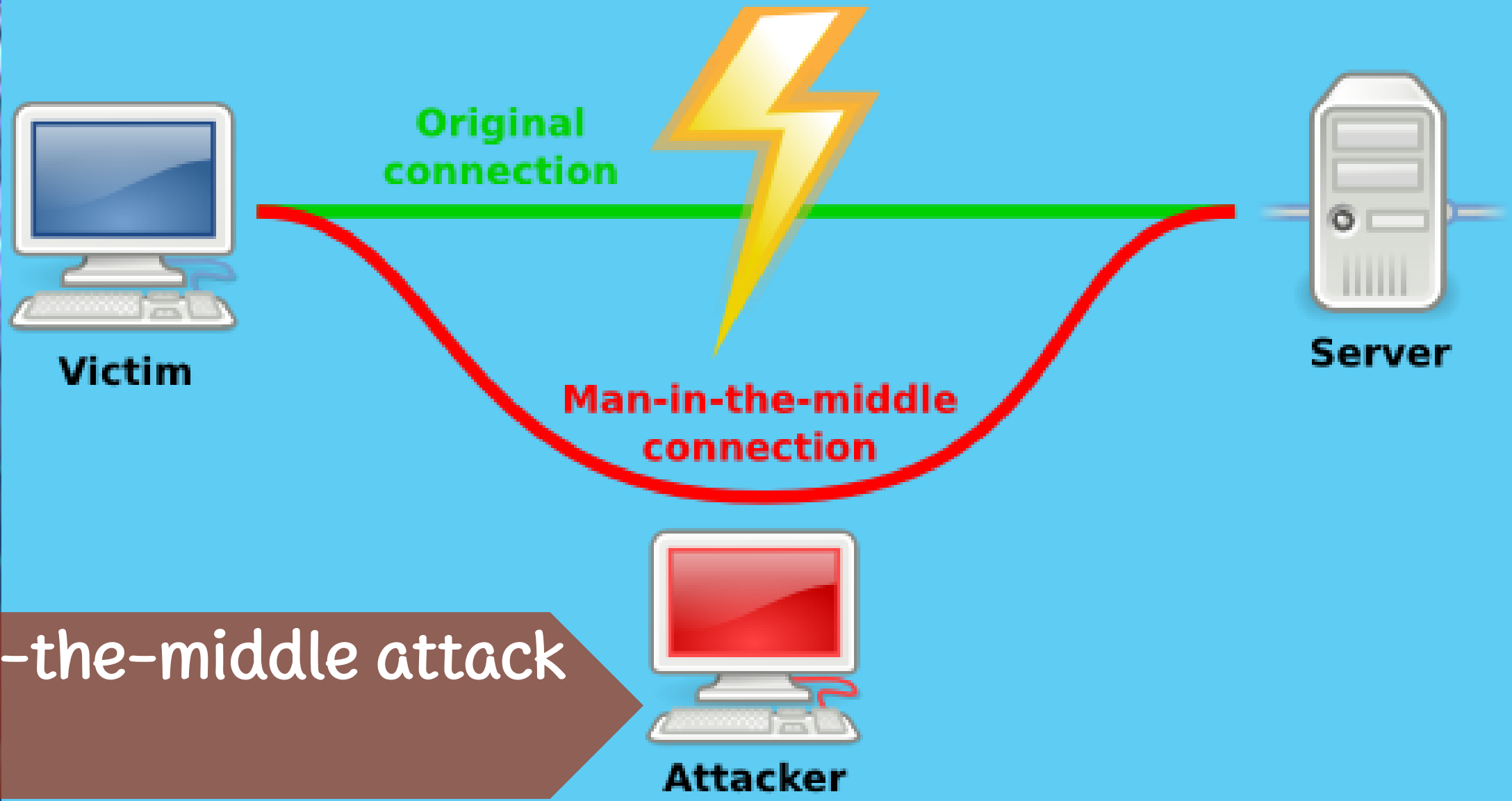


ภัยคุกคาม (Threat) : การเปลี่ยนแปลงข้อมูล (Modification)

- หมายถึงการแก้ไขข้อมูลโดยที่ไม่ได้รับอนุญาต เป็นภัยที่อยู่ใน 3 ประเภท
  - **การหลอกลวง** (Deception): ถ้าผู้รับได้ข้อมูลที่ผิดแล้วนำไปใช้
  - **การขัดขวาง** (Disruption): เปลี่ยนแปลงข้อมูลแล้วทำให้ระบบใช้การไม่ได้
  - **การควบคุมระบบ** (Usurpation): เปลี่ยนแปลงข้อมูลแล้วทำให้ระบบถูกควบคุม
- เป็นการโจมตีแบบ Active คือมีการเปลี่ยนแปลงข้อมูล

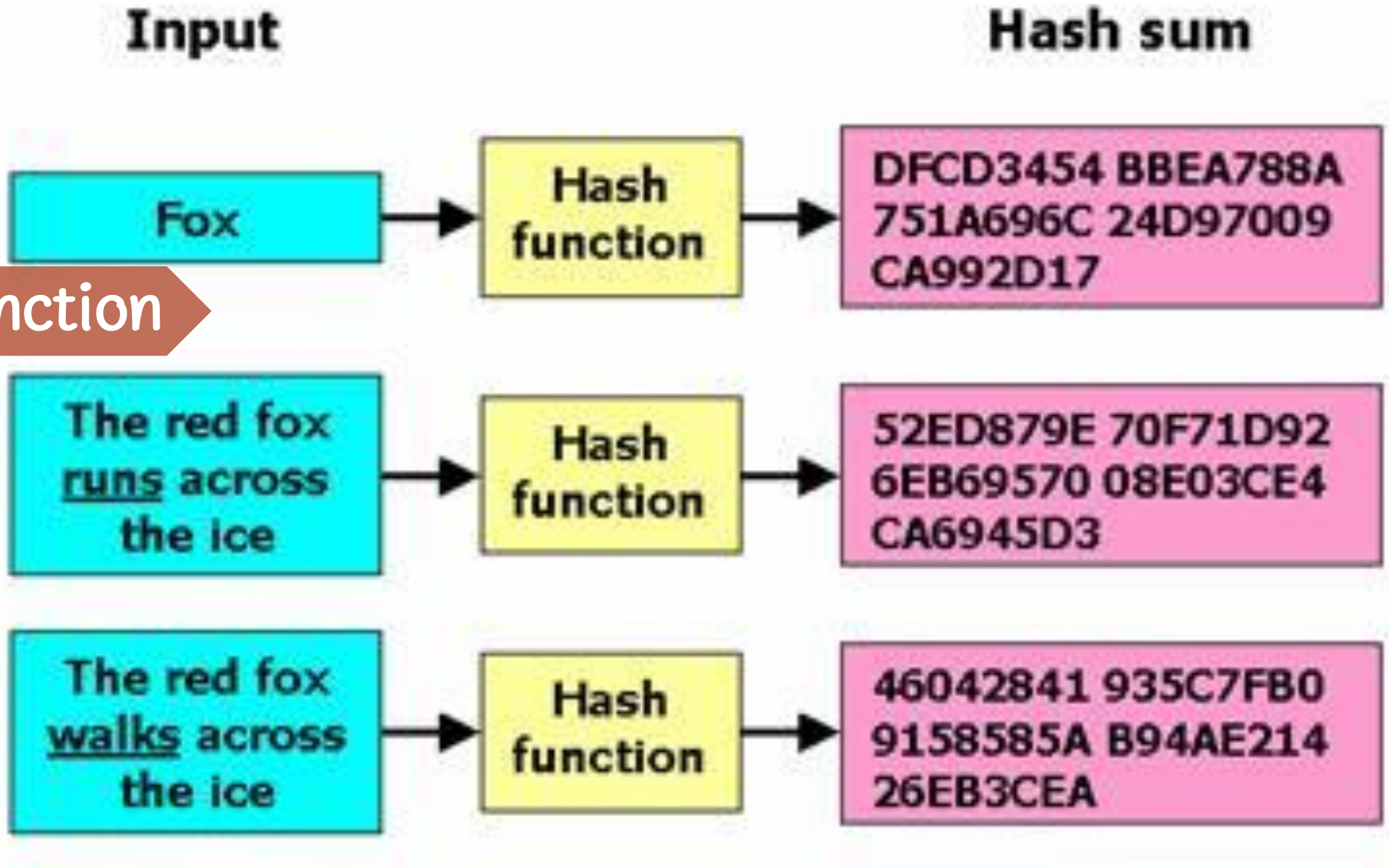
ภัยคุกคาม (Threat) : การเปลี่ยนแปลงข้อมูล (Modification) [2]

- เช่น การโจมตีผ่านคนกลาง (Man-in-the-middle : MITM) ผู้บุกรุกอ่านข้อมูลจากผู้ส่งแล้วแก้ไขก่อนจะส่งต่อไปให้ผู้รับ
- หรือผู้โจมตีพยายามฝังมัลแวร์ลงในไฟล์ติดตั้งโปรแกรม แล้วปล่อยให้เหยื่อทำการดาวน์โหลดไฟล์โปรแกรมไปติดตั้ง
- **ป้องกันโดยการพยายามรักษาความคงสภาพ (Integrity) เช่น การใช้ Hash Function**



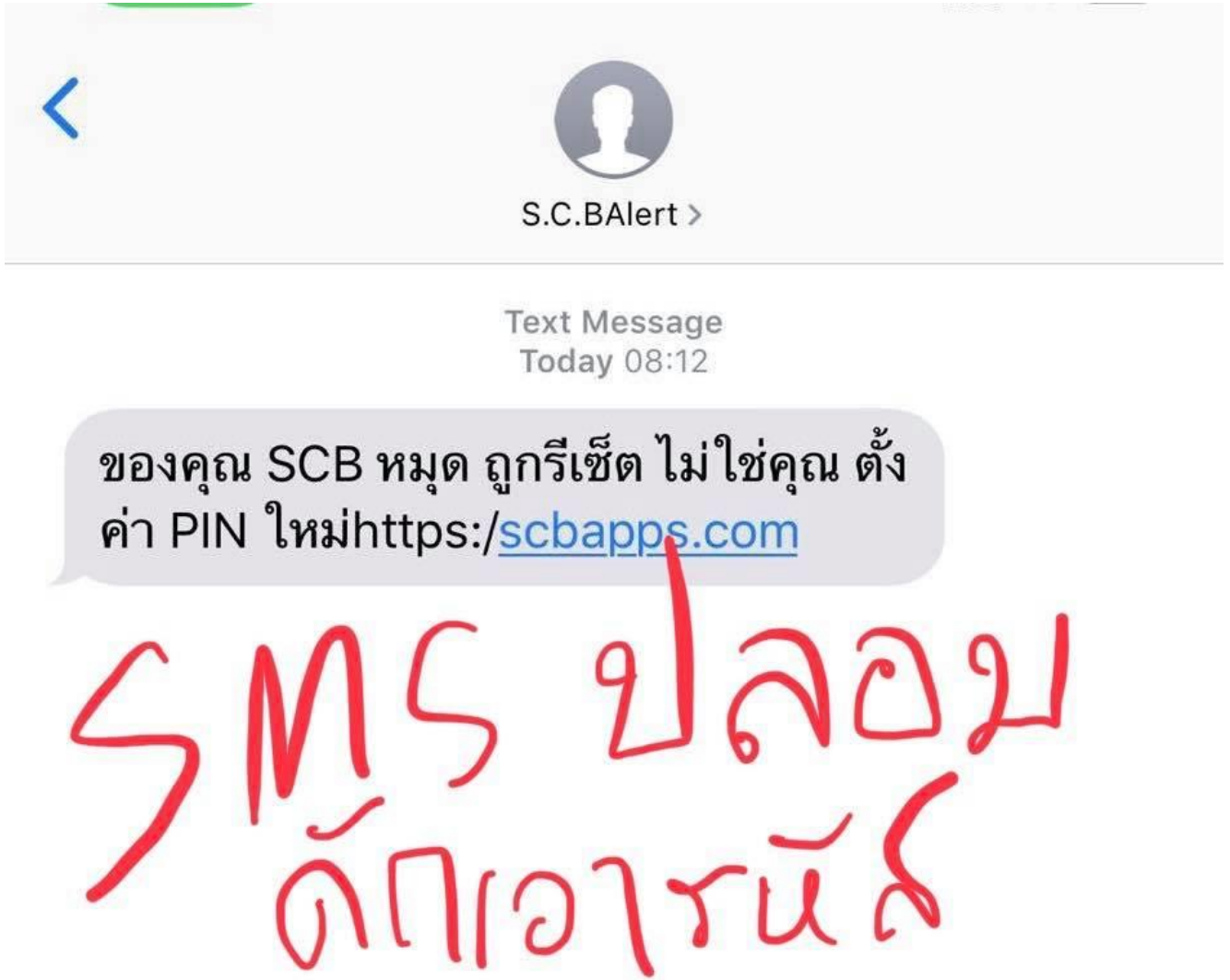
Man-in-the-middle attack : MITM

Hash Function



ภัยคุกคาม (Threat) : การปลอมตัว (Spoofing)

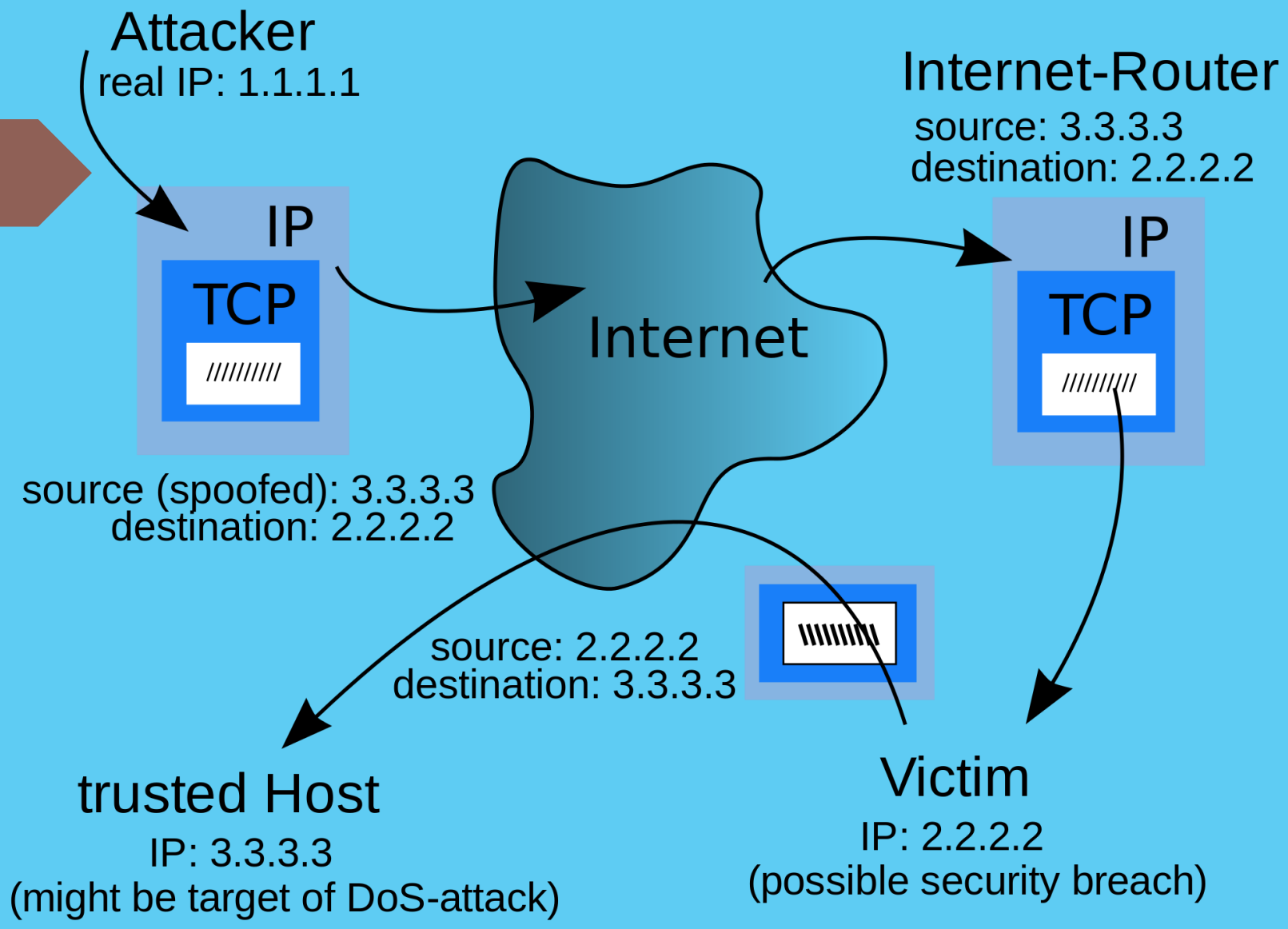
- หมายถึง การทำให้อีกฝ่ายหนึ่งเข้าใจว่าตัวเองเป็นบุคคลหนึ่ง จัดอยู่ในประเภทการหลอกลวง (Deception) และการควบคุมระบบ (Usurpation)
- เช่น ผู้ใช้ต้องการจะล็อกอินเข้าสู่ระบบปกติ แต่มีการหลอกให้ล็อกอินเข้าอีกระบบหนึ่งที่ผู้ใช้เข้าใจว่าเป็นระบบที่ต้องการจริงๆ
- ส่วนใหญ่จะเป็นการโจมตีแบบ Active
- ป้องกันโดยการใช้การพิสูจน์ทราบตัวตน (Authentication)


S.C.BAlert
Text Message
Today 08:12
ของคุณ SCB หมุด ถูกรีเซ็ต ไม่ใช่คุณ ตั้ง ค่า PIN ใหม่https:/scbapps.com
SMS ปลอม
ดักเอาธนัส

ภัยคุกคาม (Threat) : การปลอมตัว (Spoofing) [IP Spoofing]

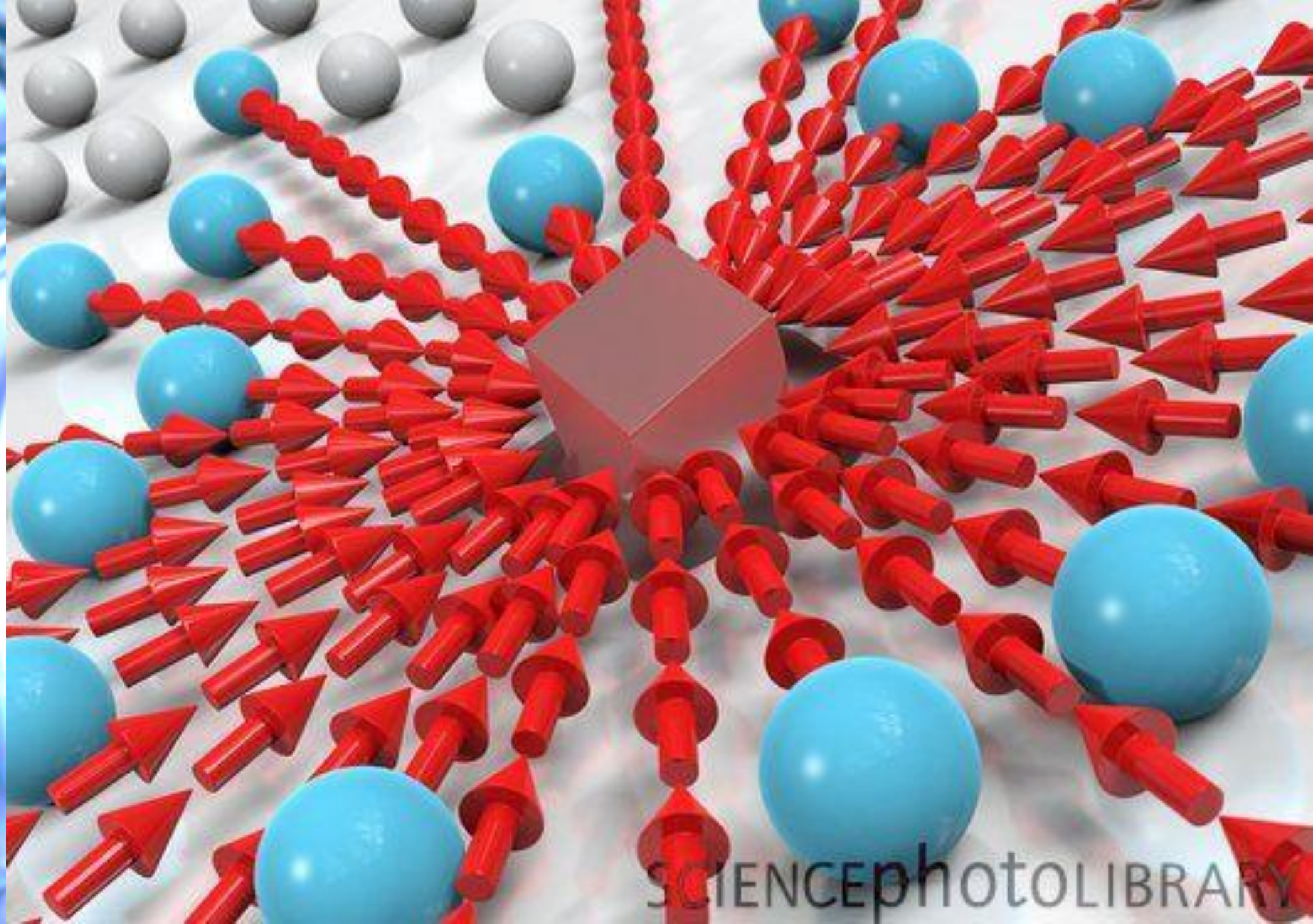
- หมายถึงการที่ผู้บุกรุกอยู่นอกเครือข่ายแล้วปลอมว่าเป็นคอมพิวเตอร์ที่เชื่อถือได้ (Trusted) โดยอาจจะใช้ไอพีแอดเดรสเหมือนกับที่ใช้ในเครือข่าย
- ผู้บุกรุกสามารถปรับเปลี่ยน Routing Table เพื่อให้ส่งข้อมูลไปยังเครื่องปลอมได้ ผู้บุกรุกอาจเป็นผู้ใช้ภายในที่ไม่มีสิทธิ์ก็ได้

IP Spoofing

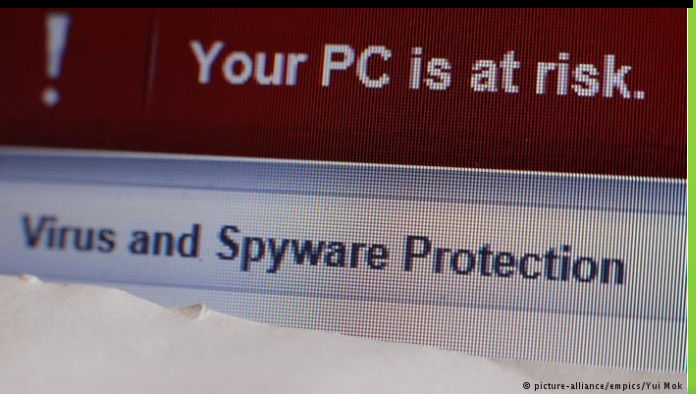

Attacker
real IP: 1.1.1.1
IP
TCP
source (spoofed): 3.3.3.3
destination: 2.2.2.2
Internet
Internet-Router
source: 3.3.3.3
destination: 2.2.2.2
IP
TCP
source: 2.2.2.2
destination: 3.3.3.3
trusted Host
IP: 3.3.3.3
(might be target of DoS-attack)
Victim
IP: 2.2.2.2
(possible security breach)

ภัยคุกคาม (Threat) : การปฏิเสธการให้บริการ (Denial of Service : DoS)

- หมายถึง การขัดขวางการให้บริการของเซิร์ฟเวอร์เป็นเวลานาน
- อาจเกิดขึ้นที่เซิร์ฟเวอร์ โดยขัดขวางไม่ให้เซิร์ฟเวอร์ใช้ทรัพยากรที่จำเป็นได้ หรือใช้ทรัพยากรของเซิร์ฟเวอร์จนหมด (Overload)
- ป้องกันได้โดยการรักษาความพร้อมใช้งาน (Availability) เช่น การสำรองข้อมูล การมีเซิร์ฟเวอร์สำรอง
- เรียกการโจมตีแบบกระจายมาจากหลายแหล่งว่า ***“Distributed Denial of Service (DDoS)”*** ซึ่งมีความรุนแรงมาก


SCIENCE PHOTO LIBRARY

ภัยคุกคาม (Threat) : ไวรัส เวิร์ม และโทรจัน (Virus, Worm , Trojan) [1]



- **มัลแวร์** (Malware) หรือ Malicious Code เป็นโปรแกรมประสงค์ร้ายที่ออกแบบมาเพื่อเจาะทำลายระบบ หรือสร้างความเสียหายกับระบบ
- **ไวรัส** (Virus) คือโปรแกรมที่เป็นอันตรายต่อคอมพิวเตอร์ โดยกระจายไปยังไฟล์อื่นๆที่อยู่ในเครื่องเดียวกัน ต้องอาศัยคนเปิดไฟล์ที่ติดไวรัสแล้วค่อยทำงาน

ภัยคุกคาม (Threat) : ไวรัส เวิร์ม และโทรจัน (Virus, Worm , Trojan) [2]

- **เวิร์ม** (Worm) คือ โปรแกรมที่เป็นอันตรายต่อคอมพิวเตอร์ โดยแพร่กระจายตัวเอง (Copy) ไปยังคอมพิวเตอร์เครื่องอื่นๆ**ที่อยู่ในเครือข่าย** และสามารถรันตัวเองเพื่อสร้างความเสียหายได้
- **โทรจัน** (Trojan) คือโปรแกรมที่ทำลายระบบคอมพิวเตอร์โดย**แฝงมากับโปรแกรมอื่นๆ** เมื่อติดตั้งโปรแกรมเสร็จแล้วโทรจันที่แฝงมาด้วยก็จะทำลายระบบคอมพิวเตอร์ หรือสร้างช่องทางให้โปรแกรมอื่นเข้ามาทำลายระบบ (Backdoor)

ป้องกันเบื้องต้นด้วยการใช้ Antivirus ที่มีการอัพเดตอยู่เสมอ