CPE 426 Computer Networks

Chapter 12:
PART IV in Textbook
Text Chapter 30: NW Security
Text Chapter 31: NW Management

TOPICS

- Chapter 30 (Only Selected Topics)
  - Criminal Exploits and Attack
  - Security Policy
  - Security Technologies
  - Hashing and MAC
  - Access Control
  - Encryption
  - Authentication and Digital Signature
  - Key Authorities and Digital Certificates
  - Firewall
  - Intrusion Detection System
  - Deep Packet Inspection
  - VPN
  - Securities Technologies
- Chapter 31 NW Management
  - Intranet Management
  - FCAPS
  - NW Management Tools
  - SNMP
  - MIB

Ch.30; Major Internet Security Problems

- **Phishing**
  - เป็นการปลอมตัวเป็น Site ที่รู้จักกันดี เช่น Web ของธนาคาร เพื่อหลอกให้ผู้ใช้เข้าไปป้อนข้อมูล และทำการโขมยข้อมูลไป
- **Misrepresentation**
  - เป็นการเสนอสินค้าหรือบริการที่เกินความเป็นจริง หรือสินค้าที่มีมาตรฐานต่ำหรือสินค้าปลอม
- **Scams**
  - เป็นการหลอกลวงในรูปแบบต่างๆ เพื่อที่จะให้ผู้ใช้ที่ไม่รู้ เข้าไปลงทุน หรือกระทำความผิด
- **Denial of Service (DOS)**
  - เป็นการกีดกัน Internet บาง Site เพื่อไม่ให้ผู้ใช้เข้าไปใช้งานได้หรือใช้ได้อย่างสะดวก
- **Loss of Control**
  - เป็นการที่ผู้บุกรุกได้เข้าไปควบคุมระบบคอมพิวเตอร์ และใช้ระบบนั้นในการกระทำความผิด
- **Loss of Data**
  - เป็นการโขมยข้อมูลที่สำคัญหรือเป็นความลับขององค์กรอกไปภายนอก

Ch.30; Major Internet Security Problems

Problem	Description
Phishing	Masquerading as a well-known site such as a bank to obtain a user's personal information, typically an account number and access code
Misrepresentation	Making false or exaggerated claims about goods or services, or delivering fake or inferior products
Scams	Various forms of trickery intended to deceive naive users into investing money or abetting a crime
Denial of Service	Intentionally blocking a particular Internet site to prevent or hinder business activities and commerce
Loss of Control	An intruder gains control of a computer system and uses the system to perpetrate a crime
Loss of Data	Loss of intellectual property or other valuable proprietary business information

Ch.30; Techniques Used in Security Attacks

- **Wiretapping**
  - เป็นการดักและทำการ Copy Packet ข้อมูล ที่วิ่งอยู่ใน Network
  - จุดประสงค์ของ Wire Tapping เพื่อนำมาใช้ใน Replay Attack
  - สามารถทำได้ง่ายในกรณีของ Wireless LAN
- **Replay**
  - เป็นการส่ง Packet ที่ดักจับได้ก่อนหน้านี้ ซึ่งมีข้อมูลของ Password จากการ Login ครั้งก่อน นำไปใช้ในการ Login เข้าระบบ
- **Buffer Overflow**
  - เป็นการส่งข้อมูลจำนวนมากๆไปยังผู้รับ เพื่อที่จะให้ข้อมูลได้ถูกเก็บในพื้นที่นอกเหนือจาก Buffer เนื่องจากเกิด Buffer Overflow
- **Address Spoofing**
  - ทำการปลอม Source IP Address เพื่อหลอกให้มีการ Process Packet
  - IP และ MAC Address สามารถฟังได้จาก ARP Broadcast
  - อาจจะใช้วิธีการ Broadcast ARP ปลอม เพื่อให้ส่งข้อมูลให้ตนเอง
  - อาจจะปลอม Routing Protocol เพื่อส่งข้อมูลให้ตนเอง
  - หรือส่ง DNS Message ปลอม
- **Name Spoofing**
  - ใช้ชื่อที่เป็นที่รู้จักแต่เขียนให้ผิดเพียน หรือทำการเปลี่ยนแปลงข้อมูลใน Name Server เพื่อให้มีการเข้าใจผิด และส่ง IP ผิด

Ch.30; Techniques Used in Security Attacks

- **DoS and DDoS**
  - โจมตีโดยการป้อน Packet จำนวนมากๆ เพื่อไม่ให้ Site สามารถทำงานอย่างอื่นได้
  - DDOS จะ Attack ประสานกันโดยใช้หลายเครื่อง
- **SYN Flood**
  - ส่ง Random TCP SYN Segment เพื่อให้ผู้รับไม่มี TCP Connection เหลืออยู่
- **Key Breaking**
  - เป็นการคาดเดา Key หรือ Password แบบอัตโนมัติ เพื่อที่จะสามารถเข้าถึงระบบได้
- **Port Scanning**
  - พยายามที่จะเชื่อมต่อ โดยใช้ Protocol Port แบบต่างๆเพื่อที่จะหาจุดอ่อน
- **Packet Interception**
  - เป็นการดักจับ Packet ระหว่างทาง จากนั้นแทนที่ด้วย Packet ที่ต้องการ หรือเพื่อทำ Man-in-the-Middle Attack

Ch.30; Techniques Used in Security Attacks

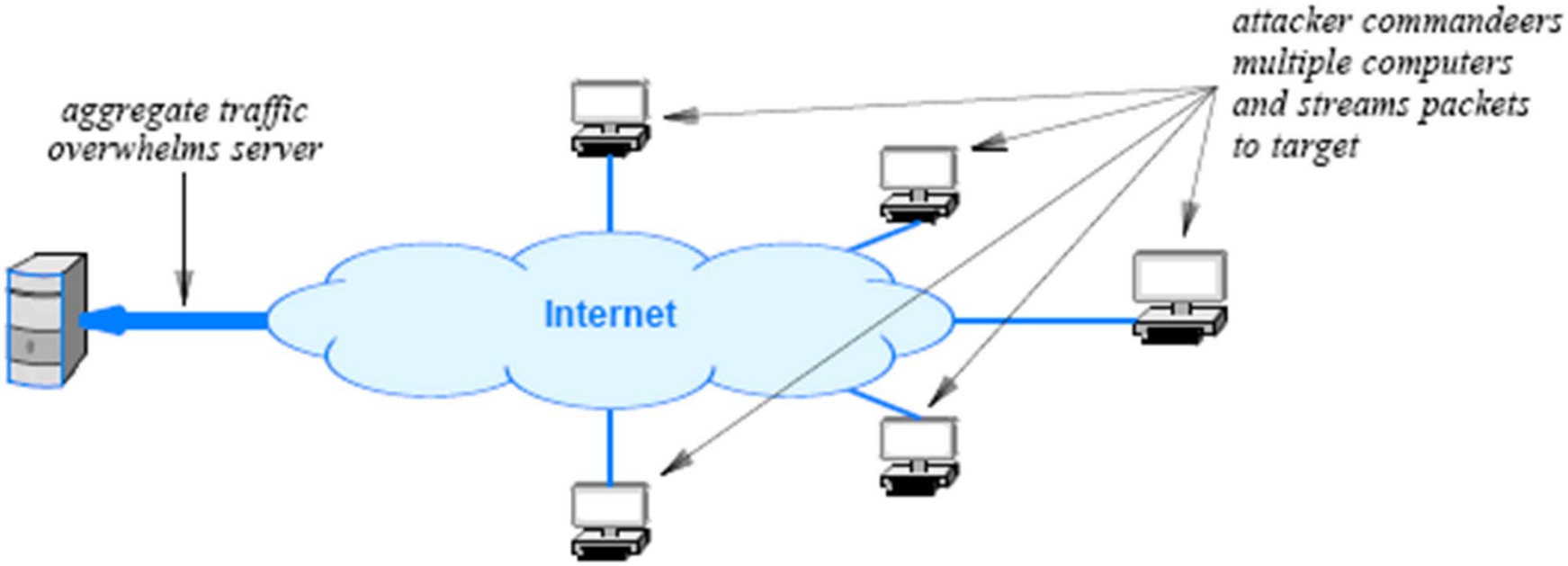


Figure 30.3 Illustration of a Distributed Denial of Service attack.

Ch.30; Techniques Used in Security Attacks

Figure 30.4 A man-in-the middle configuration and the attacks it permits.

Man-in-the middle Attack เป็นการ Intercept Packet จากนั้นส่ง Packet ที่ตัวเองต้องการออกไป อาจจะหลอกว่าเป็น Server ที่ Client ต้องการเชื่อมต่อ หรืออาจจะหลอกว่าเป็น Client เพื่อเชื่อมต่อกับ Server

Ch.30; Techniques Used in Security Attacks

Technique	Description
Wiretapping	Making a copy of packets as they traverse a network to obtain information
Replay	Sending packets captured from a previous session (e.g., a password packet from a previous login)
Buffer overflow	Sending more data than a receiver expects in order to store values in variables beyond the buffer
Address Spoofing	Faking the IP source address in a packet to trick a receiver into processing the packet
Name Spoofing	Using a misspelling of a well-known name or poisoning a name server with an incorrect binding
DoS and DDoS	Flooding a site with packets to prevent the site from successfully conducting normal business
SYN flood	Sending a stream of random TCP SYN segments to exhaust a receiver's set of TCP connections
Key Breaking	Automatically guessing a decryption key or a password to gain unauthorized access to data
Port Scanning	Attempting to connect to each possible protocol port on a host to find a vulnerability
Packet interception	Removing a packet from the Internet which allows substitution and man-in-the middle attacks

Security Policy

- **การกำหนด Security Policy ปกติจะสลับซับซ้อน**
  - เพราะจะต้องเกี่ยวข้องกับพฤติกรมของมนุษย์ และอุปกรณ์คอมพิวเตอร์และNetwork
  - องค์กรจะต้องตัดสินใจว่าต้องการ Security ในระดับใด และส่วนใหนของระบบเป็นส่วนที่สำคัญที่สุด และรองลงมา
  - อาจจะต้องมีการทำ Risk Analysis เพื่อหาอัตราส่วนระหว่างความสูญเสียและการลงทุน
- **ปกติการกำหนด Policy จะพิจารณาจาก**
  - Data Integrity: การป้องกันการเปลี่ยนแปลงข้อมูล
  - Data Availability: การป้องกันเพื่อให้ข้อมูลสามารถนำมาใช้งานได้
  - Data Confidentiality: การป้องกันความลับของข้อมูล
  - Privacy: การปกป้องผู้ส่ง หรือเจ้าของข้อมูล

Security Technologies

Technique	Purpose
Hashing	Data integrity
Encryption	Privacy
Digital Signatures	Message authentication
Digital Certificates	Sender authentication
Firewalls	Site integrity
Intrusion Detection Systems	Site integrity
Deep Packet Inspection & Content Scanning	Site integrity
Virtual Private Networks (VPNs)	Data privacy

Access Control and Password

- **เป็นการควบคุมผู้ใช้ หรือ Application Program ในการเข้าถึงข้อมูลและ Resource**
  - อาจจะอยู่ในรูป Password
  - หรืออาจจะใช้ Access Control List (ACL)
- **ในการขยายการทำ Access Control ผ่าน Network จะยุ่งยากกว่าระบบที่เป็น Standalone**
  - Wiretapping, Replay, Phishing, Spoofing etc.

AAA Protocol

- **เป็น Computer Security Protocol สำหรับ Authentication ผู้ใช้งานใน Network ที่จะกระทำ 3 อย่าง**
  - Authentication
    - คือขบวนการที่จะตรวจสอบเอกลักษณ์ของผู้ใช้ ว่าเป็นผู้ที่อ้างถึงนั้นจริงๆ เช่นการใช้ Password, Keycard, Biometrics
  - Authorization
    - เป็นการกำหนดสิทธิ์ให้กับแต่ละบุคคล ว่าจะสามารถทำอะไรได้บ้าง
  - Accounting
    - คือการบันทึกการใช้งานของแต่ละบุคคล

Hash and Message Authentication Code

- **Hash เป็นการสร้างตัวแทนของเอกสาร**
  - ได้จากการคำนวณค่า Hash ซึ่งจะมีจำนวน Bit ที่คงที่จากเอกสารที่มีความยาวไม่แน่นอน
  - Algorithm จะเป็น One-Way Function และมีการ Collision ต่ำ
  - สามารถใช้เป็นตัวตรวจสอบว่าเอกสารมีการแก้ไขหรือไม่
- **MAC ได้จากการนำ Data มารวมกับ Key และทำการสร้าง Hash**
  - จุดประสงค์เหมือนกับ Hash คือเพื่อจะใช้ตรวจสอบว่าเอกสารมีการแก้ไขหรือไม่
  - แต่ในการนี้ คนที่จะตรวจสอบได้จะต้องมี Key
- **HASH และ MAC ใช้ในการทำ Message Authentication**
  - MD5, SHA-1,

Encryption

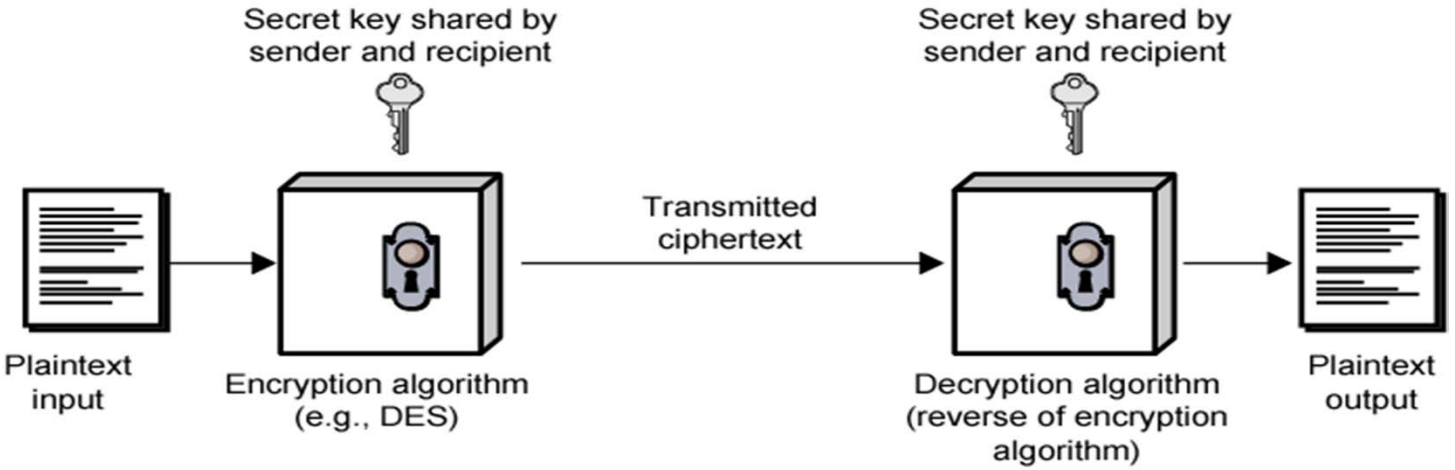
- ปกติ **Authentication** เป็นการพิสูจน์ตัวตน ใช้ป้องกันเรื่อง **Integrity**
- ในการป้องกันเรื่อง **Confidentiality** จะต้องใช้วิธีการ **Encryption**
- **Encryption** คือขบวนการเปลี่ยนแปลงเอกสารให้อยู่ในรูปที่ไม่สามารถอ่านได้
  - จะใช้ Encryption Algorithm และ Encryption Key
  - ขบวนการจะต้อง Inverse ได้
    - คือทำ Decryption ได้ โดยมี Decryption Algorithm ร่วมกับ Decryption Key

Encryption Terminology

- **Plaintext, M**
  - หมายถึงเอกสารที่ยังไม่ได้ถูกเข้ารหัส
- **Cyphertext, C**
  - เอกสารที่ถูกเข้ารหัสแล้ว
- **Encryption Key, K_1**
  - Bit String ที่ใช้สำหรับการเข้ารหัส
- **Decryption Key, K_2**
  - Bit String ที่ใช้สำหรับถอดรหัส
- **$C = encrypt(K_1, M)$**
- **$M = decrypt(K_2, C)$**
- **$M = decrypt(K_2, encrypt(K_1, M))$**

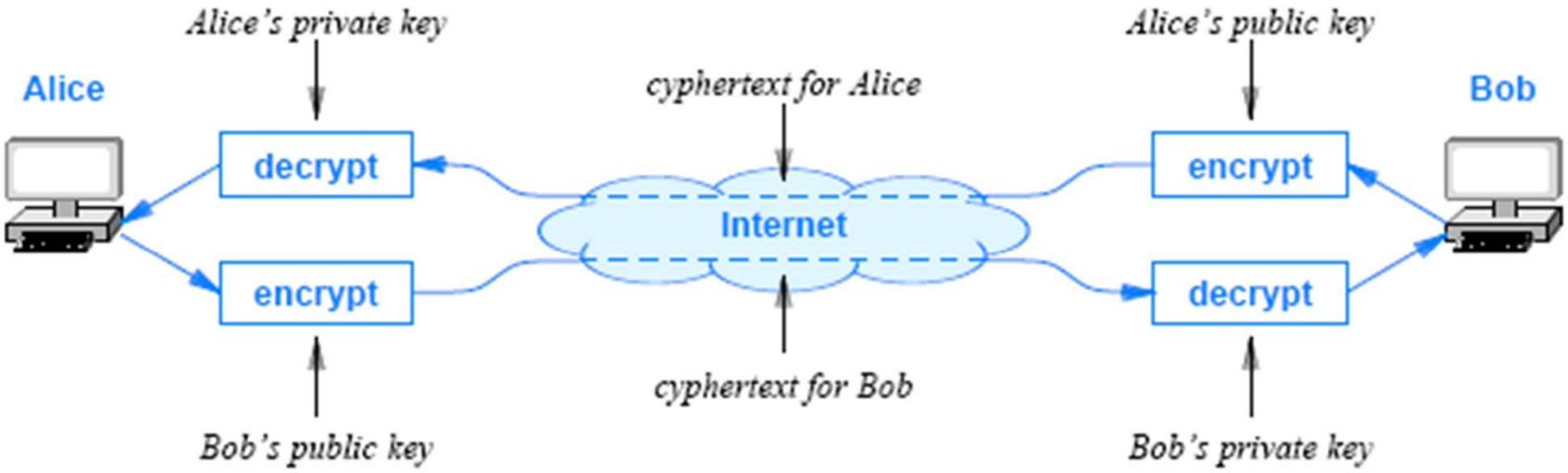
Private Key Encryption

- **Symmetric Cryptography**
- **Conventional Cryptography**
- **เป็นหนึ่งในสองเทคโนโลยีที่ใช้ในการเข้ารหัส**
- **กรณีนี้ Key ที่ใช้เข้ารหัสและถอดรหัสจะเป็นตัวเดียวกัน**
  - ผู้ส่งและผู้รับจะต้อง Share Key ร่วมกัน
  - DES, 3DES, AES



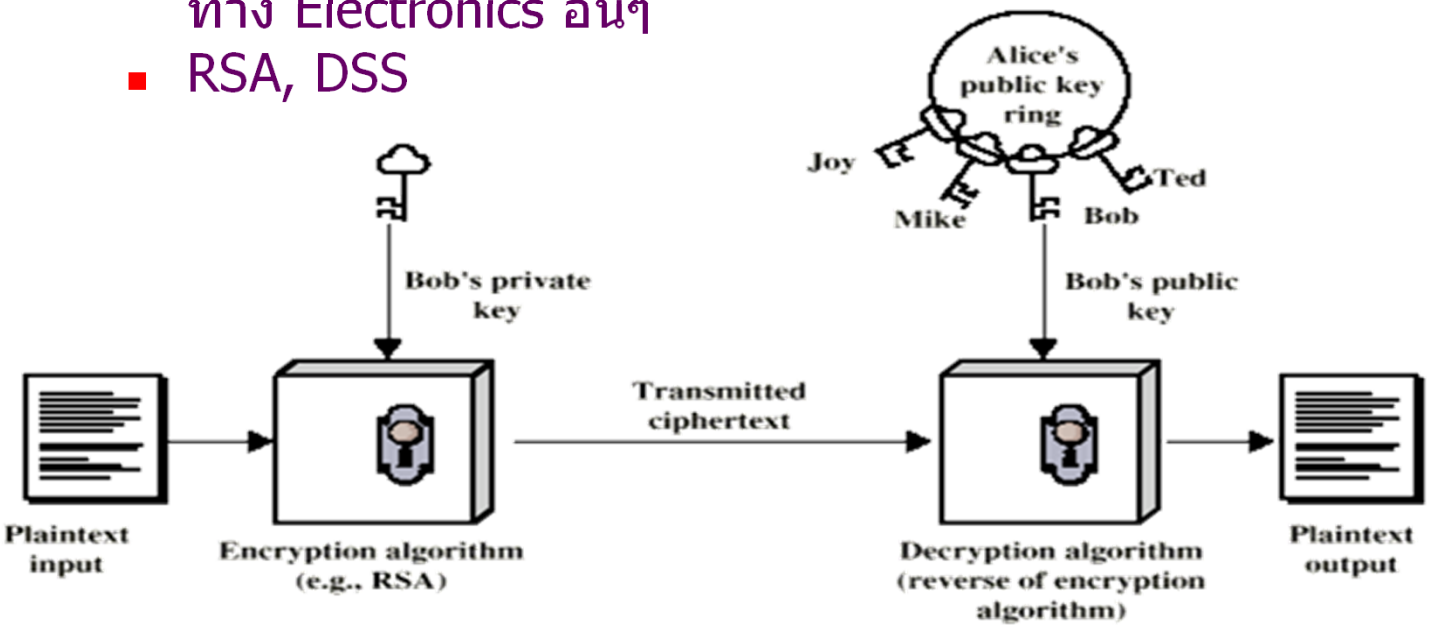
Public Key Encryption

- **Asymmetric Key Cryptography**
- **Key ที่ใช้เข้ารหัสเรียก Public Key สามารถแจกจ่ายได้**
- **Key ที่ใช้ถอดรหัส ต้องเป็นความลับ เรียก Private Key**
  - RSA, Diffie-Hellman, ECC
- **สามารถดัดแปลงมาใช้ทำ Digital Signature ได้**



Authentication With Digital Signature

- **ถ้าเรากลับ โดยเข้ารหัสด้วย Private Key แทนที่จะเป็น Public Key**
  - ดังนั้นจะมีเพียงเจ้าของ Key เท่านั้นที่สามารถสร้างเอกสารที่เป็น Ciphertext นี้ได้
  - เหมือนกับเป็นการเซ็นต์เอกสาร เพราะ Ciphertext ที่ได้เฉพาะเจาะจงว่าเป็นของผู้ใด
  - เรียกว่าเป็นการทำ Digital Signature
  - สามารถนำมาใช้ในการทำ Authentication รวมถึงการทำธุรกรรมทาง Electronics อื่นๆ
  - RSA, DSS



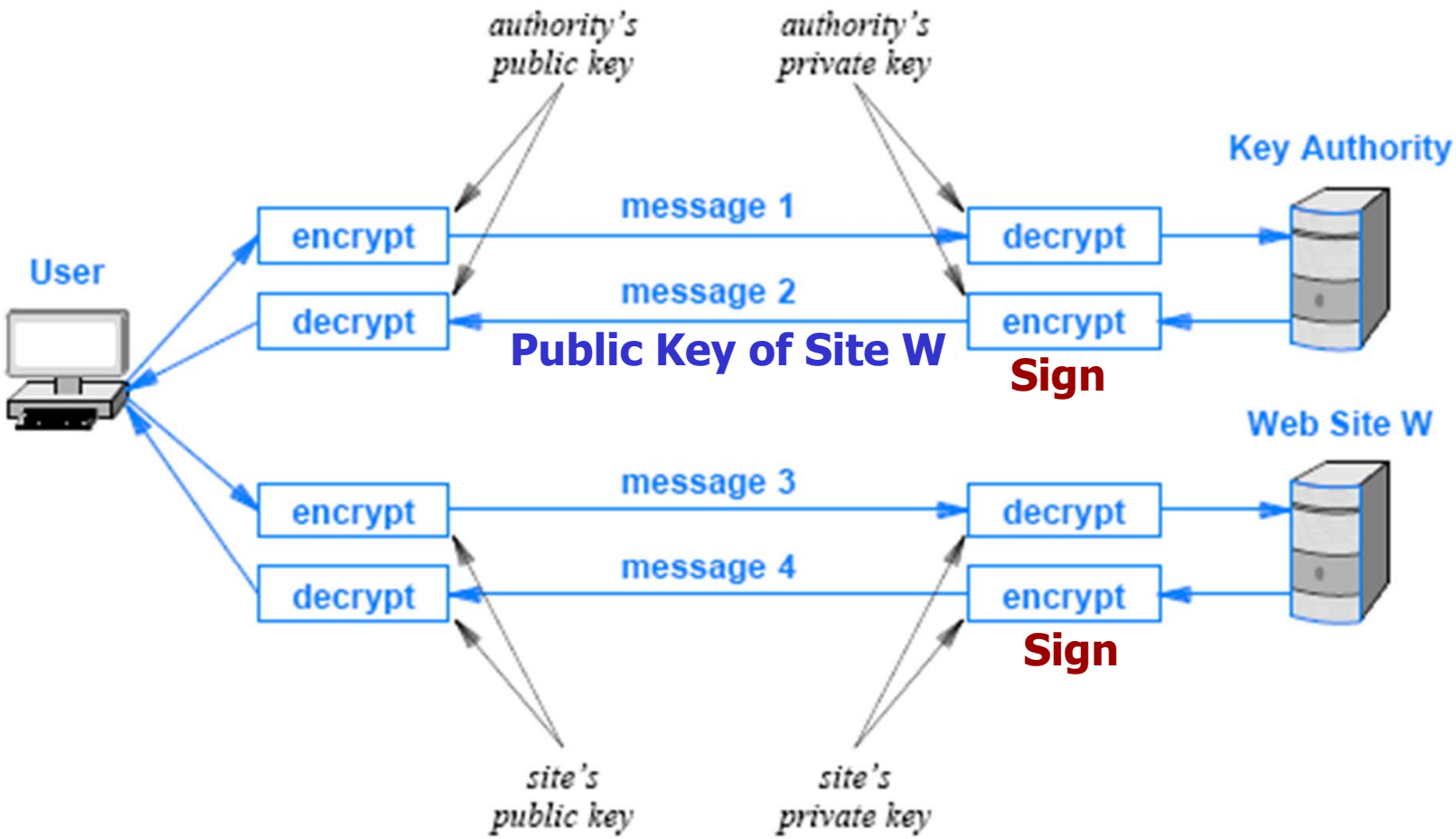
Key Authorities and Digital Certificates

- **ปัญหาของ Public Key คือการสร้างเอกสารส่งให้ใคร เราจะต้องได้ Public Key ของคนๆนั้น**
  - Public Key ไม่จำเป็นต้องเป็นความลับ สามารถส่งผ่านช่องทางการสื่อสารปกติ หรือประกาศออกมาได้
  - ปัญหาคือเรื่องของการ Authentication Public Key
    - เราจะรู้ได้อย่างไรว่า Public Key ที่ได้รับมานั้นเป็นของคนนั้นจริงๆ
    - Alice ต้องการส่งข้อมูลให้ Bob แบบปลอดภัย ต้องการ Public Key ของ Bob ซึ่ง Bob จะต้องส่งมาให้ แม้ว่าการส่งสามารถทำผ่านช่องทางปกติได้ และ Public Key ไม่ต้องเป็นความลับ แต่สามารถปลอมได้
      - ถ้าผู้ไม่หวังดี ส่ง Public Key ของตัวเองมา และหลอกว่าเป็น Public Key ของ Bob
      - เมื่อเราเข้ารหัสด้วย Key ปลอมนั้นส่งให้ Bob ตัว Bob ไม่สามารถนำ Private Key ของตัวเองมาถอดรหัสได้
      - ที่ร้ายกว่านั้นคือ ถ้าผู้ไม่หวังดีนั้น แอบดักฟังและ Copy (Wiretapped) เอกสาร เขาสามารถใช้ Private Key ที่เป็นคู่ของ Key ปลอม มาถอดรหัสและดูเอกสารได้
      - นี่คือ Man-in-the-middle attack
- **ปัญหานี้เราเรียก 'Key Distribution Problem'**
  - เราต้องการการ Authentication ของ Public Key

Key Authorities and Digital Certificates

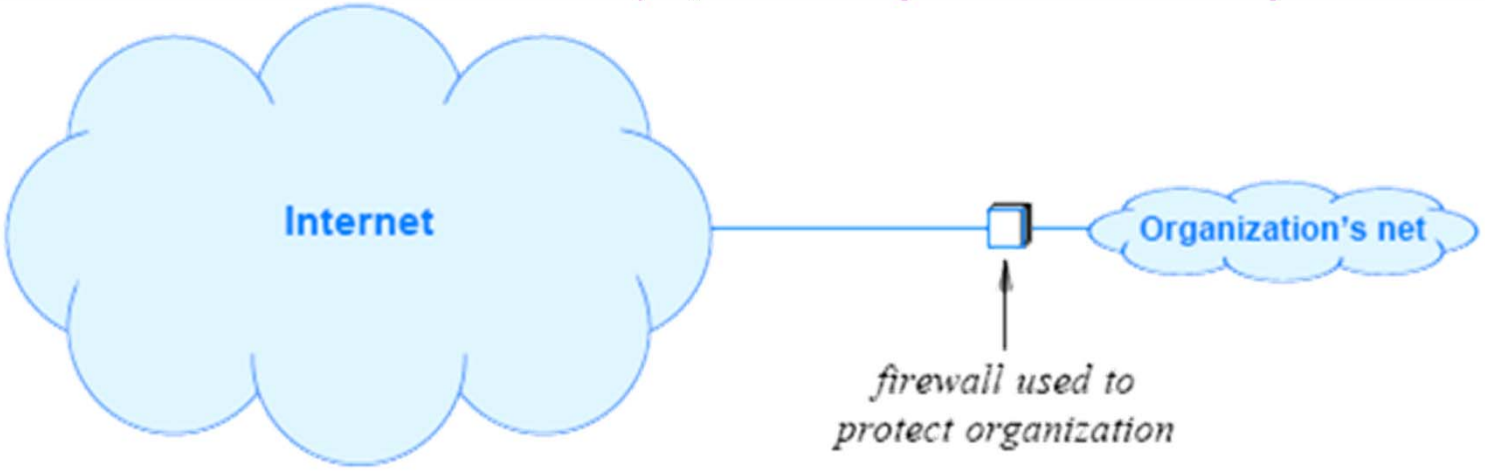
- **เราสามารถตั้ง Server กลาง ทำหน้าที่แจกจ่าย Key แบบอัตโนมัติ (และมีระบบรักษาความปลอดภัย)**
  - เรียก Key Distribution Center หรือ Key Authority
  - ทุกคนจะนำ Public Key ของตนเองไปฝากไว้
  - เมื่อต้องการส่งเอกสารให้ใคร ให้ขอ Public Key ของคนนั้นผ่าน Server นี้
- **ข้อเสียของ Key Authority คือ Server จะ Down ไม่ได้**
- **อีกวิธีหนึ่งคือออกเป็น Digital Certificate**
  - เป็นการนำ Public Key ของตนเอง ทำการรับรองโดยใช้ Digital Signature จาก Certification Authority
  - Certificate ไม่สามารถปลอมได้ สามารถตรวจสอบได้
  - User จะเก็บ Certificate ของตัวเองไว้ ถ้ามีใครต้องการส่งเอกสารให้ตน User จะทำการส่ง Certificate ให้กับคนนั้น
  - ดังนั้นการสื่อสารไม่ต้องใช้ Key Authority ที่ต้อง Online

Key Authorities and Digital Certificates



Firewalls

- เทคโนโลยีที่กล่าวข้างต้นใช้ในการปกป้องข้อมูลเป็นหลัก
- ในการปกป้อง Computer และ Network จาก Traffic ที่ไม่ต้องการ เราต้องใช้อีกเทคโนโลยีหนึ่ง คือ '**Firewall**'
- จุดประสงค์ของ Firewall คือเป็นตัวกั้น Traffic ที่ไม่ต้องการ ให้ผ่าน Network
  - ปกติจะวางกั้นระหว่างตำแหน่ง Network ขององค์กร และเส้นทางที่จะต่อออก Internet ทุกๆทางออก(ถ้ามีมากกว่าหนึ่ง)



Firewall

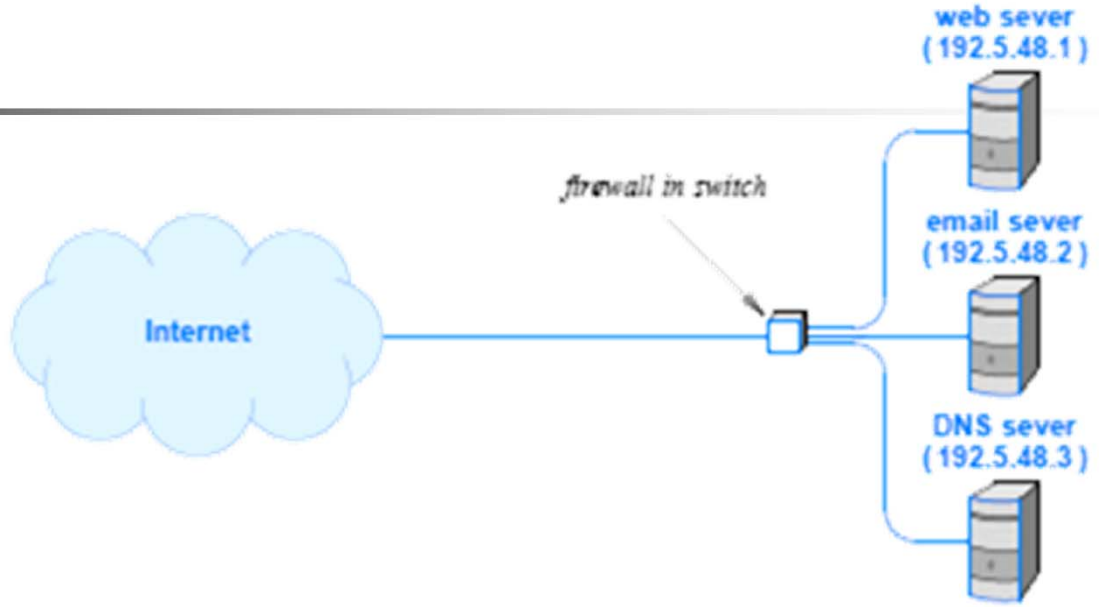
- **หลักในการควบคุม Traffic โดย Firewall**
  - ทุก Traffic ที่จะเข้ามาใน Network ขององค์กร ต้องผ่าน Firewall
  - ทุกๆ Traffic ที่จะออกจากองค์กร ต้องผ่าน Firewall
  - ที่ Firewall จะมีการกำหนด Security Policy ที่จะ Drop ทุกๆ Packet ที่ไม่เป็นไปตามข้อกำหนด
  - ตัว Firewall เองจะต้องคงทนต่อการ Attack
- **จุดที่วาง Firewall จะเป็นตัวกำหนด Secure Perimeter (ขอบเขต)**

ชนิดของ Firewall

- **Packet Filtering Router/Gateway**
  - ทำการกรอง Packet โดยดูจาก MAC Address, IP Address, Port Number, Protocol หรือข้อมูลในส่วน Header แต่จะไม่ดูภายใน Packet และไม่มีการบันทึกหรือจดจำ = Stateless
- **Application Level Gateway**
  - ปกติจะลงพวก Proxy Application ทำหน้าที่เป็นตัวแทนในการเชื่อมต่อกับ Application ภายนอก จะยอมให้เชื่อมต่อกับ Application ที่มี Proxy อยู่เท่านั้น ปกติสามารถทำเป็น Stateful สามารถตรวจสอบภายใน Packet และมี Function ของ Packet Filter อยู่ด้วย
- **Circuit Level Gateway**
  - เป็นตัว Relay สำหรับการทำ Connection ภายนอก ปกติจะทำงานร่วมกับ Proxy Gateway

Firewall Implementation with a Packet Filter

- สมมุติเรายอมให้เฉพาะ Traffic จาก Public Server เท่านั้นที่จะเข้า-ออก



Dir	Frame Type	IP Src	IP Dest	IP Type	Src Port	Dst Port
in	0800	*	192.5.48.1	TCP	*	80
in	0800	*	192.5.48.2	TCP	*	25
in	0800	*	192.5.48.3	TCP	*	53
in	0800	*	192.5.48.3	UDP	*	53
out	0800	192.5.48.1	*	TCP	80	*
out	0800	192.5.48.2	*	TCP	25	*
out	0800	192.5.48.3	*	TCP	53	*
out	0800	192.5.48.3	*	UDP	53	*

Intrusion Detection System

- IDS หรือ Intrusion Detection System จะตรวจสอบ Packet ทุกตัวที่เข้ามาใน Site และจะแจ้งแก่ผู้ดูแลระบบถ้ามี Packet ที่ไม่เป็นไปตามที่กำหนด
- เป็นการทำงานเสริมจาก Firewall แต่จะตรวจจับภายใน Network
- ปกติ IDS จะถูก Configure ให้ตรวจจับ Pattern เฉพาะของการ Attack เช่นการทำ Port Scanning
- บางครั้งจะทำงานร่วมกับ Firewall โดยแจ้งให้ Firewall ทำการ Block บาง Packet เช่นการทำ SYN Flood
- IDS จะเป็น Stateful มีการจดจำสถานะของการ Connection

Content Scanning and Deep Packet Inspection

- **ปกติ Firewall จะกัน Virus ไม่ได้ เพราะไม่สามารถตรวจสอบภายใน Packet**
  - เช่นการส่ง Virus ผ่าน E-mail Attachment
- **เราต้องการการทำ Content Analysis**
  - File Scanning ทำโดย Security Software บน PC
    - File Scanner จะนำ File ที่ได้รับ และทำการตรวจหา Pattern ที่น่าจะมีปัญหา เช่น String ของ Byte ที่เรียก 'Finger Print' อย่างไรก็ตาม เป็นไปได้ที่อาจจะเกิด 'False Positive' หรือ 'False Negative'
  - Deep Packet Inspection(DPI)
    - จะเป็นการตรวจสอบภายใน Packet แทนที่จะตรวจสอบ File ซึ่งในการนี้มันสามารถตรวจสอบ Packet ที่วิ่งเข้า-ออก ทั้งส่วน Header และ ภายใน Payload ด้วยเหตุนี้มันจะทำงานได้ค่อนข้างช้าเทียบกับ Firewall และไม่เหมาะกับ High-Speed Network

Virtual Private Network (VPN)

- **เป็น Technology ที่สำคัญที่สุดอันหนึ่งในการสร้าง Secure Access กับ Remote Site ผ่าน Internet**
  - สมัยก่อนจะใช้ Leased Circuit (Private Network) ในการเชื่อมต่อ ซึ่งจะมี Security สูง
  - ปัจจุบัน การต่อผ่าน Internet ราคาจะถูกกว่ามาก แต่มีปัญหาเรื่อง Security เพราะ Internet เป็น Public Network
  - วิธีแก้ คือการทำ Encryption ในข้อมูลที่ส่ง
    - อาจจะทำที่ Router ที่ทำหน้าที่เป็น Firewall ด้วย
    - อาจจะทำที่ Host
  - นี่คือ Technology ของ Virtual Private Network หรือ VPN คือทำ Internet ที่มีราคาถูกให้มีคุณภาพในแง่ Security เหมือน Private Network ที่ราคาแพง

Virtual Private Network (VPN)

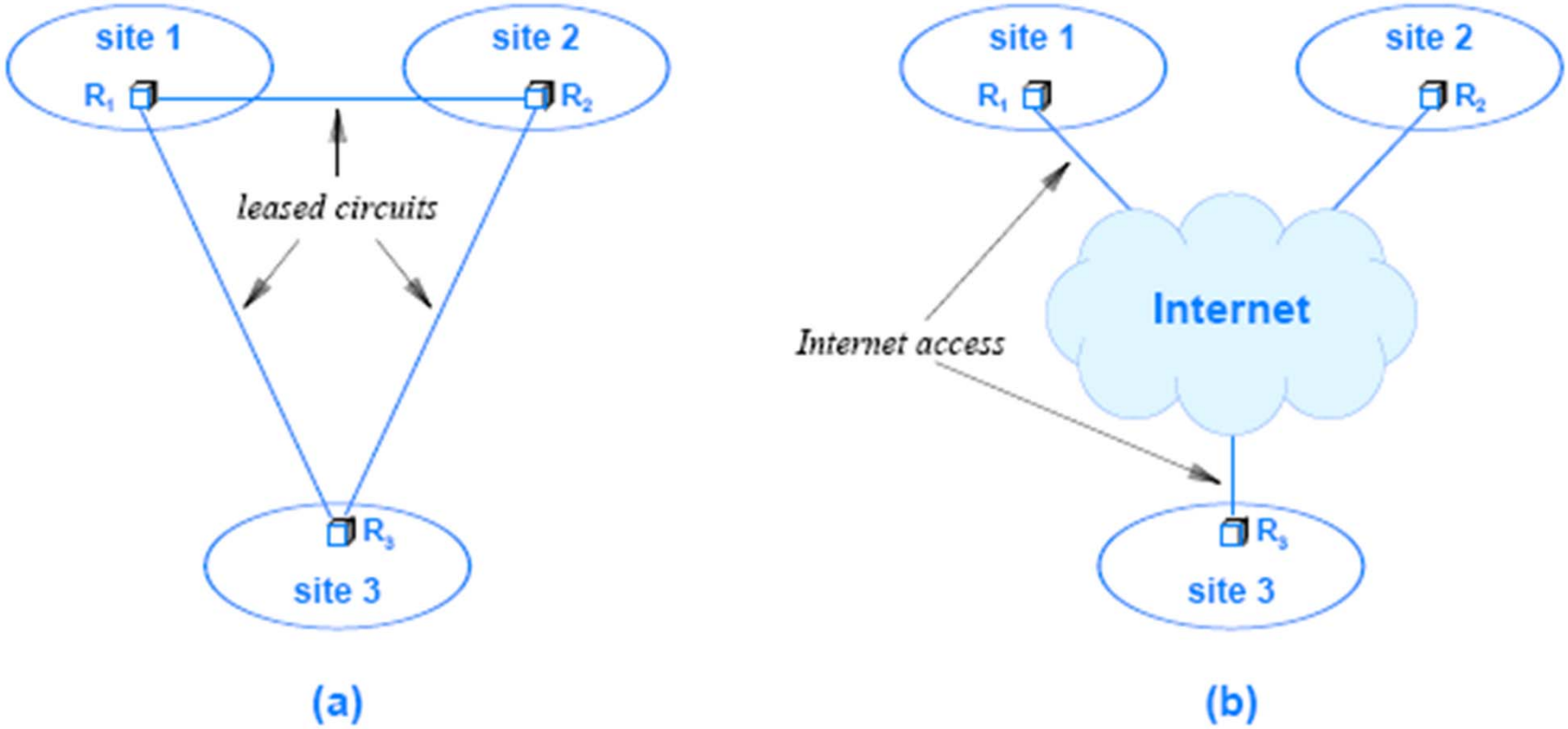


Figure 30.10 Sites connected by (a) leased circuits and (b) the Internet.

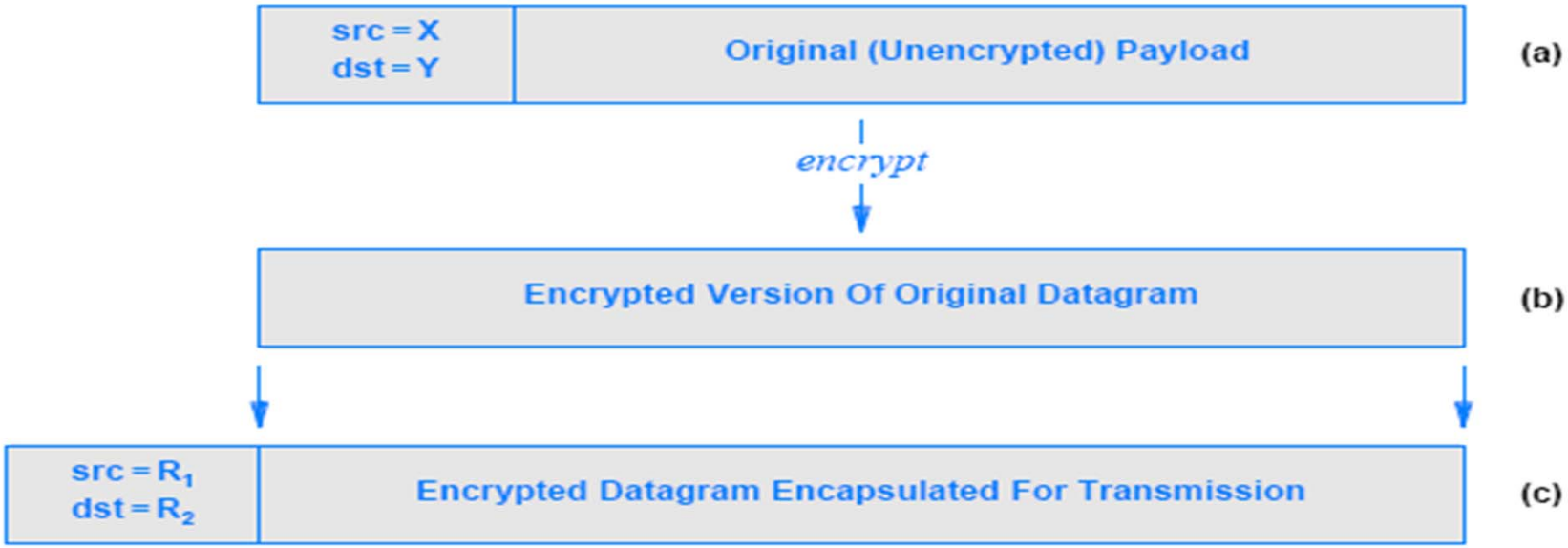
The Use of VPN Technology for Telecommuting

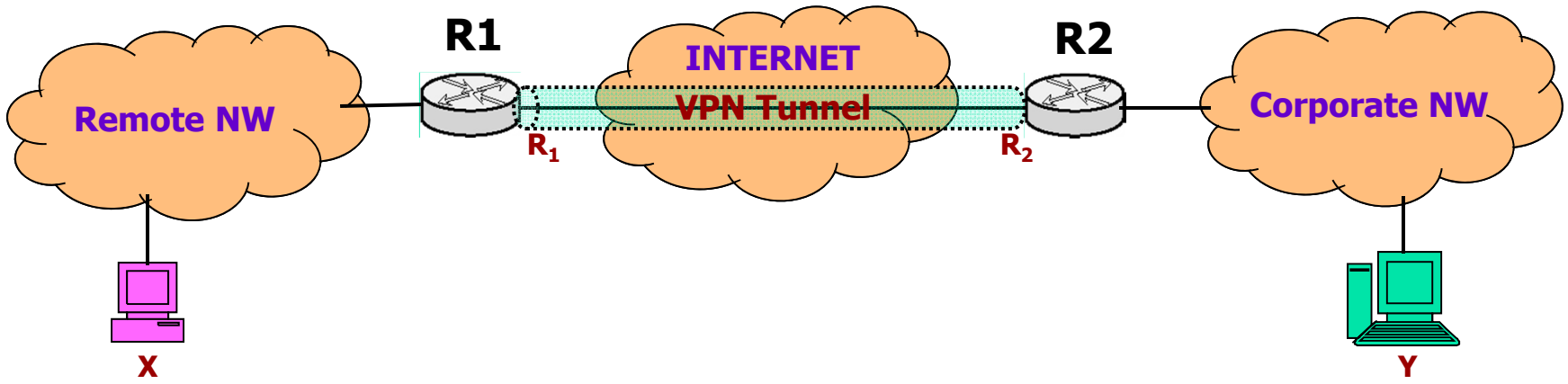
- **VPN มีการใช้งานสองรูปแบบ**
  - Stand-Alone Device
    - โดยการใช้อุปกรณ์ที่เรียก VPN Router ต่อกับ Internet โดยอุปกรณ์นี้จะสร้างช่องการสื่อสารที่ปลอดภัยกับ VPN Server ขององค์กร โดยจะส่ง Encrypt Packet และจะ Decrypt Packet ที่ได้รับ ผู้ใช้เมื่อต่อผ่าน Internet จะเสมือนว่าตัวเองได้ต่อตรงเข้ากับ LAN ขององค์กร โดยมีการจ่าย IP ผ่าน DHCP ขององค์กร
  - VPN Software
    - โดยการ Run VPN Software ที่ Host ของผู้ใช้ที่ต้องการเชื่อมต่อกับ Network ขององค์กรผ่าน Internet โดยที่ VPN Software จะดักจับ Packet ที่เข้าและออกจาก Host นั้น เพื่อทำการ Decryption และ Encryption ตามลำดับ

Packet Encryption vs. Tunneling

- **การทำ Encryption ของ VPN มีทางเลือกหลักสามทาง**
  - Payload Encryption
    - เฉพาะส่วน Payload ของ Datagram จะถูก Encrypt ดังนั้นผู้ดักฟังสามารถจะรู้ Address และ Port Number ของ Datagram ได้ เหมาะกับกรณีที่ส่วน Header ของ Datagram ไม่มีความสำคัญที่ต้องปกป้อง
  - IP-in-IP Tunneling
    - ในกรณีนี้ ทั้ง Datagram จะถูก Encrypt จากนั้น Packet ที่ถูก Encrypt แล้วจะถูกนำไปใส่ใน Datagram อันใหม่ ปกติ IP Address ใหม่ที่ใช้คือ IP ของ Router ที่ทำ Encryption ต้นทางและ Decryption ปลายทาง ผลลัพธ์คือทั้ง Datagram จะถูกปกป้อง แต่ Datagram ใหม่จะยาวมากกว่าเดิม

Packet Encryption vs. Tunneling





Packet Encryption vs. Tunneling

- **การทำ Encryption ของ VPN มีทางเลือกหลักสามทาง**
  - Payload Encryption
  - IP-in-IP Tunneling
  - IP-in-TCP Tunneling
    - จะใช้การบรรจุ IP Packet ที่ถูก Encrypt ลงใน TCP Segment จากนั้นจึงบรรจุ TCP ลงใน IP อีกทีหนึ่ง ข้อดีคือสามารถอาศัย TCP ในการส่งข้อมูลแบบเชื่อถือได้ ข้อเสียคือ ถ้า Packet ใดใน Connection นั้นสูญหาย ข้อมูลที่ได้รับต่อจากนั้นจะไม่สามารถส่งจากชั้น TCP ขึ้นไป Decrypt ที่ IP ชั้นบนได้

VPN Tunneling Performance

- **การใช้ VPN จะทำให้ Performance ของระบบลดลง ดังนี้**
  - Latency
    - การใช้ VPN ในการเชื่อมต่อกับ Site อื่น จะต้องผ่านท่อ VPN ไปยังองค์กร แล้วจึงต่อไปยัง Site นั้นได้ ทำให้เกิด Delay เพิ่มขึ้น
  - Throughput
    - แม้ว่าการเชื่อมผ่าน VPN จะเสมือนต่อกับ LAN ขององค์กร แต่ข้อมูลต้องวิ่งผ่าน Internet ทำให้ Throughput ต่ำกว่าการใช้งานของ LAN ปกติ
  - Overhead and Fragmentation
    - การทำ Tunnel จะเพิ่ม Overhead ในการส่ง Datagram และเป็นไปได้เมื่อทำแล้วทำให้ความยาวของ Packet สูงกว่าค่า MTU ซึ่งจะส่งผลให้เกิดการทำ Fragmentation

Security Technologies ที่สำคัญ

- **PGP (Pretty Good Privacy)**
  - เป็นระบบการเข้ารหัสข้อมูล ใช้สำหรับ Application เข้ารหัสข้อมูลก่อนที่จะส่งออกไป
- **SSH (Secure Shell)**
  - เป็น Application Layer Protocol สำหรับทำ Remote login เข้ามา ซึ่งจะมีการเข้ารหัสข้อมูลระหว่างการส่ง ผิดกับ 'Telnet' ที่จะส่งเป็น Plaintext
- **SSL (Secure Socket Layer)**
  - พัฒนาโดย Netscape Communication ใช้ทำ Authentication และปกป้องข้อมูล โดยจะเป็น Layer อยู่ระหว่าง Application และ Socket API (Transport Layer) ใช้สำหรับการสื่อสารผ่าน Web ในการทำ Financial Transaction
- **TLS (Transport Layer Security)**
  - เป็นมาตรฐานของ IETF เพื่อเป็นมาตรฐานแทน SSL โดยออกแบบจากพื้นฐายของ SSL v.3 ทั้ง SSL และ TLS สามารถนำมาใช้ร่วมกับ HTTPS

Security Technologies ที่สำคัญ

- **HTTPS (HTTP Security)**
  - เป็นเทคโนโลยีที่รวม HTTP และ SSL หรือ TLS เข้าด้วยกันกับการทำ Certificate เพื่อให้การสื่อสารผ่าน Web ได้อย่างปลอดภัย HTTPS จะใช้ TCP Port 443 แทนที่จะเป็น 80
- **IPsec (IP Security)**
  - เป็นเทคโนโลยีในการทำ Security กับ IP Datagram โดยสามารถเลือกทำ Authentication หรือ Confidentiality (Encryption)
- **RADIUS (Remote Authentication Dial-In User Service)**
  - เป็น Protocol ใช้สำหรับการทำ Authentication, Authorization และ Accounting (AAA) นิยมใช้ใน Dialup และ VPN สำหรับ Remote User
- **WEP (Wired Equivalent Privacy)**
  - เป็นส่วนหนึ่งของ Wi-Fi WLAN Standard ปัจจุบันถูกแทนที่ด้วย WPA (Wi-Fi Protection Access) เนื่องจากมีจุดอ่อน

Chapter 31: Network Management (SNMP)

- **NW Manager หรือ NW Administrator เป็นผู้ทำหน้าที่**
  - Planning
  - Installing
  - Operating
  - Monitoring
  - Controlling
- **NW Manager จะตรวจดู/แก้ไข ทั้ง HW และ SW เพื่อทำให้ NW ทำงานได้อย่างมีประสิทธิภาพ**

Chapter 31: 31.3 NW Management Standard Model

- **Industry Standard Model**
- **FCAPS**
  - Fault Detection and Correction
  - Configuration and Operation
  - Accounting and Billing
  - Performance Assessment and Optimization
  - Security Assurance and Protection

Chapter 31: 31.4 Network Elements

- หมายถึงอุปกรณ์ ระบบ หรือกลไก ที่สามารถจัดการได้ รวมถึง Service ต่างๆ ของ Network ด้วย

Manageable Network Elements	
Layer 2 Switch	IP router
VLAN Switch	Firewall
Wireless Access Point	Digital Circuit (CSU/DSU)
Head-End DSL Modem	DSLAM
DHCP Server	DNS Server
Web Server	Load Balancer

Chapter 31: 31.5 Network Management Tools

- **Physical Layer Testing**
  - One-Touch, DSP 4000, Cable Tester, RF Signal Meter
- **Reachability and Connectivity**
  - Ping
- **Packet Analysis**
  - Packet Analyzer (Protocol Analyzer) เช่น Ethereal, Wireshark, Sniffer
- **Network Discovery**
  - ใช้ในการสร้าง NW Map
- **Device Interrogation Tool**
  - ใช้ในการส่งคำสั่งไปยังอุปกรณ์ต้องการ

Chapter 31: 31.5 Network Management Tools

- **Event Monitoring**
  - เป็นตัวแสดงการทำงานของอุปกรณ์แต่ละตัวผ่านทางจอภาพ จะมีการส่ง Alert บนจอเมื่อมีสิ่งผิดปกติเกิดขึ้น
- **Performance Monitoring**
  - เป็นตัวตรวจจับและบันทึกประสิทธิภาพการทำงานของ NW
- **Flow Analysis**
  - เช่น NetFlow Analyzer แสดง Traffic ในแต่ละ Link และแต่ละ Application ที่วิ่งอยู่ใน NW

Chapter 31: 31.5 Network Management Tools

- **Routing and Traffic Engineering และ General Configuration Tools**
  - Routing จะควบคุมเส้นทางการไหลของข้อมูล และ ทำ Configuration Routing Protocol
  - Traffic Engineering จะตรวจจับและทำ Configuration ของเส้นทางของข้อมูลเพื่อให้เป็นไปตาม QoS ที่ต้องการ
  - General Configuration Tool ใช้สำหรับการทำ Configuration ทั่วไป

Chapter 31: 31.5 Network Management Tools

- **Security Enforcement**
  - ใช้เพื่อบังคับให้การทำงานของ NW เป็นไปตาม Security Policy
- **Network Planning**
  - จะเป็นตัวที่สลับซับซ้อนมากที่สุด ใช้สำหรับการวางแผนในการทำงานของ NW เช่นใช้ทำ NW Optimization สำหรับ NW Architecture หรือ Traffic Engineering

Chapter 31: 31.6 NW Management Application

- **ปกติเป็น Application Layer จะทำงานในลักษณะ Client-Server**
  - ส่วน Client จะทำงานบน PC เรียก Manager
  - ส่วน Server จะทำงานในอุปกรณ์ NW เรียก Agent
- **Manager จะร้องขอข้อมูลจาก Agent ที่อยู่บนอุปกรณ์ต่างๆ เพื่อมาเก็บไว้ในฐานข้อมูลและทำการวิเคราะห์**
  - การร้องขอและส่งข้อมูลจะกระทำผ่าน NW Management Protocol (Application Layer Protocol)

Chapt 31: 31.7 Simple Network Management Protocol (SNMP)

- เป็นมาตรฐานที่ใช้ใน Internet
  - ปัจจุบันคือ SNMPv3
- กำหนด Format ของข้อมูลที่ส่งระหว่าง Manager และ Agent
  - ข้อมูลที่ส่ง จะใช้รหัสแบบ ASN.1
    - Abstract Syntax Notation 1

Decimal Integer	Hexadecimal Equivalent	Length Byte	Bytes Of Value (in hex)
27	1B	01	1B
792	318	02	03 18
24,567	5FF7	02	5F F7
190,345	2E789	03	02 E7 89

Chapter 31: 31.8 SNMP's Fetch-Store Paradigm

- **SNMP มี Primitive Command เพียงไม่กี่ตัว**
- **ใช้ Fetch-Store Paradigm**
  - Fetch ใช้ในการดึงค่ามาจากตัวอุปกรณ์
  - Store ใช้ในการตั้งค่าให้กับอุปกรณ์
  - Operation จะกระทำกับ Object โดยกำหนด Object Name

Chapter 31: 31.9 SNMP MIB and Object Names

- **แต่ละ Object ที่จะสื่อสารผ่าน SNMP จะต้องมีชื่อเฉพาะเป็นของตนเอง**
  - ทั้ง Manager และ Agent จะต้องใช้ชื่อเดียวกันสำหรับ Object เดียวกัน
- **Set ของทุกๆ Object ที่ใช้ใน SNMP รู้จักกันในนาม MIB**
  - Management Information Base
- **มาตรฐาน MIB จะแยกออกจากมาตรฐานของ SNMP**
  - MIB ของอุปกรณ์แต่ละชนิด จะมีมาตรฐานแตกต่างกันออกไป

Chapter 31: 31.9 SNMP MIB and Object Names

- **Object ใน MIB จะถูกกำหนดโดยใช้ชื่อตามแบบของ ASN.1**
  - แต่ละ Object จะกำหนดด้วย Prefix ที่จะแน่ใจว่าชื่อจะไม่ซ้ำกัน
  - เช่น ชื่อ Object ที่ใช้นับจำนวนของ Datagram ที่อุปกรณ์ได้รับจะเป็น
    - Iso.org.dod.internet.mgmt.mib.ip.ipInReceives
- **แต่เมื่อชื่อ Object ถูกส่งไปใน Message ของ SNMP มันจะถูกแทนที่ด้วย Integer เช่นตัวอย่างข้างบนจะเป็น**
    - 1.3.6.1.2.1.4.3

Chapter 31: 31.10 ชนิดของ MIB Variables

- **SNMP ไม่ได้กำหนด Set ของ MIB ดังนั้น MIB สามารถออกแบบและกำหนดเป็นมาตรฐานได้อย่างอิสระ**
  - MIB ที่เป็นมาตรฐานเช่น UDP, TCP, IP, ARP และส่วนของ Ethernet
  - MIB สำหรับอุปกรณ์เช่น Switch, Router, Modem, Printer
  - เมื่อมี Protocol ใหม่เกิดขึ้น สามารถกำหนด MIB เพิ่มเติม โดยไม่ต้องแก้ไขส่วน SNMP
  - ผู้ผลิตอุปกรณ์สามารถเพิ่มเติมส่วน MIB Extension สำหรับอุปกรณ์ของตนเอง
- **RMON เป็น MIB Extension ที่สำคัญ สำหรับ Manage ใน Layer 2(LAN)**

Chapter 31: 31.11 MIB Variable สำหรับ Array

- นอกเหนือจาก **MIB Variable** ที่กำหนดเป็นค่า **Integer** แล้ว ยังมี **MIB** ที่กำหนดเป็น **Array** หรือ ตาราง
  - เช่น MIB สำหรับ Routing Table (Forwarding Table)
- อย่างไรก็ตาม ใน **ASN.1** ไม่มีการกำหนด **Index** ของ **Array** เราจะต้องรู้ตำแหน่งของ **Object** ในตาราง และกำหนด **Index** เอง ต่อจาก **Object Name** เช่น **IP Forwarding Table**
  - Standard MIB prefix.ip.ipRoutingTable
  - ถ้าเราต้องการเฉพาะบาง Field เราจะใช้
  - Standard MIB prefix.ip.ipRoutingTable.ipRouteEntry.<field>.IPdestaddr

End of Chapter 30-31 (Week 16)

- HW 10 Download: Last Homework
- Due Monday May 2 Before 12.00 Noon
  - เฉลยจะประกาศวันพุธ
- Course Ends: No Class Next Week
- Final Exam: Friday 13 May 13.30-16.00

Final Exam Preparations

- **Final Exam**
  - เน้นที่หลัง Midterm ก่อน MT จะออกเรื่อง IP และ IP Address
  - No Calculator
  - คะแนนเก็บ Final 50% (6 ข้อ 60 คะแนน)
    - การบ้าน 10 ครั้ง 15%
    - Midterm Exam 35%
  - เกณฑ์ผ่านคือคะแนนรวมต้องได้ 40%

Final Exam Preparations

- **Final Exam List**
- 1. IP Address and Subnetting
- 2. TCP/UDP
- 3. Routing General, Least Cost Algorithm
- 4. IP Routing, RIP, OSPF, BGP, Multicast
- 5. QoS and IP Telephony
- 6. NW Security และ NW Management
- เทอม 1/59 เปิด 1 Sec (จันทร์)