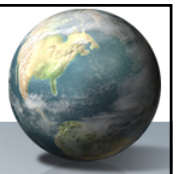
WAN Technologies and Internet Security

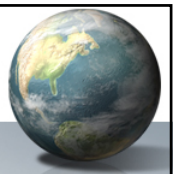
Akharin Khunkitti
KMITL

หัวข้อ



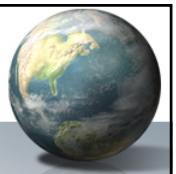
- Introduction
- WAN Technologies
- Remote Access Service (RAS)
- Virtual Private Network (VPN)
- Introduction to Internet Security
- Cryptography (Encryption and Decryption)
- Firewall and Firewall Types (Packet Filtering and Proxy)
- Network Address Translation (NAT)
- Intrusion Detection System (IDS)
- Summary

บทนำ



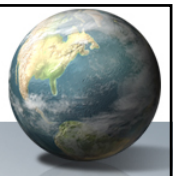
- ระบบเครือข่ายเป็นการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่างๆ เข้าด้วยกัน
  - การเชื่อมต่อเป็นโครงสร้างเครือข่ายจะมีรูปแบบต่างๆ กัน
- ในระบบเครือข่ายมีความหลากหลายในการให้บริการ สำหรับการสื่อสาร
  - จึงจำเป็นที่จะต้องทราบลักษณะของบริการต่างๆ ที่มีในระบบเครือข่ายโทรคมนาคม

การเชื่อมต่อระบบเครือข่าย

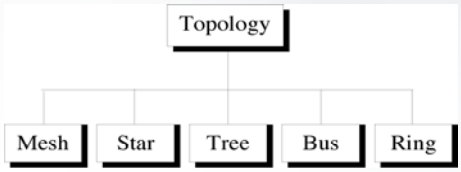


- ระบบเครือข่ายทุกชนิดจะต้องเชื่อมต่อเข้าด้วยกัน
  - รูปแบบหรือวิธีการเชื่อมต่อจะเป็นตัวกำหนดวิธีการทำงานของอุปกรณ์นั้นๆ
- การเชื่อมต่อแบบจุด-ต่อ-จุด (Point-to-Point Connection)
  - เชื่อมต่อโดยตรง
    - ระหว่างเทอร์มินอลกับเครื่องเมนเฟรม
    - ระหว่างเครื่องเมนเฟรมกับเทอร์มินอลบางเครื่องที่อยู่ไกลมาก
    - ระหว่างเครื่องคอมพิวเตอร์กับเครื่องคอมพิวเตอร์
- การเชื่อมต่อแบบหลายจุด (Multipoint Connection)
  - เชื่อมต่อหลายเครื่องเข้ากับสายสื่อสารเพียงเส้นเดียวหรือช่องทางสื่อสารเพียงช่องเดียว

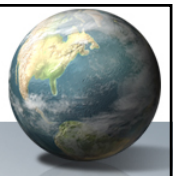
รูปแบบโครงสร้างระบบเครือข่าย



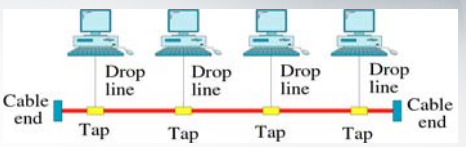
- รูปแบบโครงสร้าง (Topology) หมายถึง รูปแบบการวางตำแหน่งของอุปกรณ์ทั้งหมดในระบบเครือข่าย
- รูปแบบพื้นฐาน
  - แบบบัส (Bus)
  - แบบวงแหวน (Ring)
  - แบบดาว (Star)
  - แบบเมช (Mesh)
- รูปแบบประยุกต์
  - แบบต้นไม้ (Tree) หรือ
  - แบบลำดับชั้น (Hierarchical)
  - แบบผสม (Hybrid)

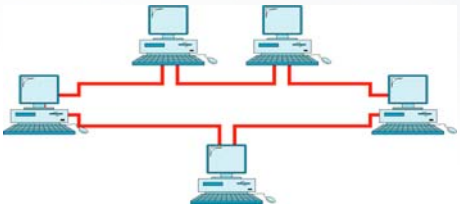


รูปแบบโครงสร้างระบบเครือข่าย



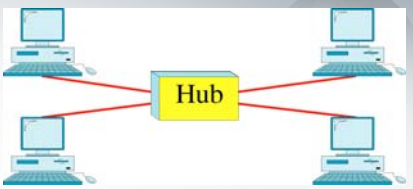
- รูปแบบโครงสร้างแบบบัส (Bus Topology)
  - ใช้สายสื่อสารเพียงเส้นเดียวหรือช่องทางสื่อสารช่องเดียว
  - เชื่อมต่อเครื่อง/อุปกรณ์ทุกเครื่องเข้าด้วยกันโดยตรง
- รูปแบบโครงสร้างแบบวงแหวน (Ring Topology)
  - เชื่อมต่อแบบจุด-ต่อ-จุดไปยังเครื่อง/อุปกรณ์ข้างเคียง ต่อๆกันไป
  - เชื่อมต่อเครื่อง/อุปกรณ์ลำดับสุดท้ายเข้ากับลำดับแรก => ทำให้เกิดครบเป็นวงแหวน
  - มีเส้นทางสำรองสำหรับการสื่อสาร

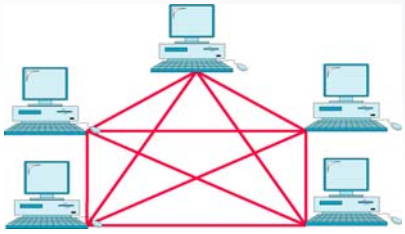




รูปแบบโครงสร้างระบบเครือข่าย

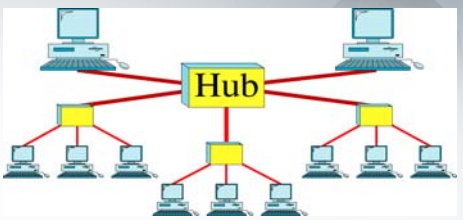
- รูปแบบโครงสร้างแบบดาว (Star Topology)
  - มีศูนย์กลางการเชื่อมต่อ เรียกว่า ฮับ (Hub)
  - เครื่อง/อุปกรณ์ทั้งหมดเชื่อมต่อแบบจุด-ต่อ-จุด มาที่ศูนย์กลาง (Hub)
  - ควบคุมได้ง่าย ที่ศูนย์กลาง
  - ถ้าศูนย์กลางหยุดทำงาน ระบบเครือข่ายจะใช้งานไม่ได้ทั้งระบบ
- รูปแบบโครงสร้างแบบเมช (Mesh Topology)
  - เชื่อมต่อทุกเครื่อง/อุปกรณ์เข้าด้วยกันทั้งหมด
  - ระบบมีความเชื่อถือได้สูง
  - ใช้จำนวนการเชื่อมต่อมาก

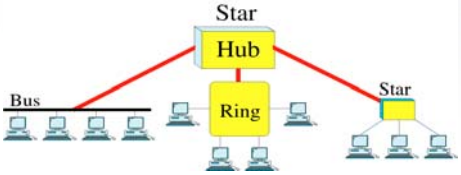




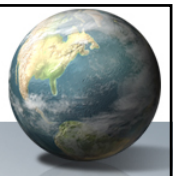
รูปแบบโครงสร้างระบบเครือข่าย

- รูปแบบโครงสร้างแบบต้นไม้ (Tree Topology) หรือแบบลำดับชั้น (Hierarchical Topology)
  - แบ่งการเชื่อมต่อเป็นโครงสร้างหรือลำดับชั้น
  - แบบต้นไม้ (Tree) เป็นการนำเอาแบบดาวมาเชื่อมต่อกับเป็นโครงสร้างลำดับชั้น
  - แบ่งกลุ่มการเชื่อมต่อ
  - มีความซับซ้อน
- รูปแบบโครงสร้างแบบผสม (Hybrid Topology)
  - ผสมการเชื่อมต่อหลายรูปแบบเข้าด้วยกัน
  - ขยายตัวได้ดี
  - มีความซับซ้อนมาก



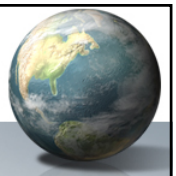


WAN Technologies



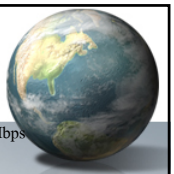
- WAN Technologies
  - Circuit Switching
    - Switched Circuits
      - Public Switch Telephone Network (PSTN) or Plain Old Telephone System (POTS)
      - Integrated Services Digital Network (ISDN)
        - » Narrowband
        - » Broadband
    - Dedicated Circuits or Leased Circuit or Leased Line
      - Analog
      - Digital
        - » T/E Carrier
        - » Synchronous Optical Network/Synchronous Digital Hierarchy (SONet/SDH)
        - » Digital Subscriber Line (xDSL)
  - Packet Switching
    - X.25
    - Frame Relay
    - Asynchronous Transfer Mode (ATM)
    - Ethernet

วงจรสวิทช์

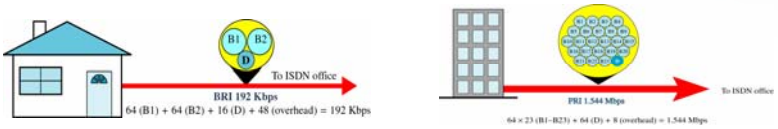


- ระบบเครือข่ายโทรศัพท์สาธารณะแบบสวิทช์ (Public Switched Telephone Network: PSTN) –
  - เป็นระบบแบบเก่าที่ใช้วิธีการส่งสัญญาณแบบอนาลอก
  - เป็นวงจรสื่อสารแบบที่ถูกนำมาใช้งานมาเป็นเวลานานมาก
  - แบ่งกลุ่มการเชื่อมต่อเข้ากับชุมสายในระดับต่างๆ เป็นโครงสร้างการเชื่อมต่อแบบลำดับชั้น
- ระบบเครือข่ายไอเอสดีเอ็น (Integrated Services Digital Network: ISDN) – ใช้วิธีการส่งสัญญาณแบบดิจิตอล
  - เป็นระบบเครือข่ายเพื่อสื่อสารข้อมูลอเนกประสงค์ – สามารถส่งสัญญาณเสียง ภาพวีดิทัศน์ และข้อมูลดิจิตอลได้พร้อมกัน
  - แบ่งออกเป็น 2 ประเภท
    - แนโรว์แบนด์ไอเอสดีเอ็น (Narrowband ISDN)
    - บรอดแบนด์ไอเอสดีเอ็น (Broadband ISDN)

Narrowband ISDN

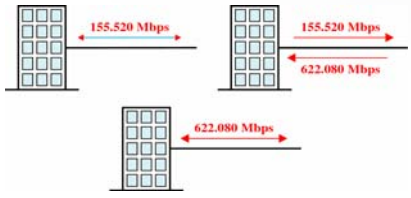


- ระบบแอสดีเอ็นยุคแรกเป็นแบบ Narrowband ISDN สามารถส่งข้อมูลด้วยความเร็วไม่เกิน 1.5 หรือ 2.0 Mbps
- ประกอบด้วยช่องสื่อสาร 2 ประเภท
  - ช่องสัญญาณบี (B Channel) ใช้สำหรับส่งข้อมูลของผู้ใช้ แต่ละช่องมีความเร็ว 64 Kbps
  - ช่องสัญญาณดี (D Channel) ใช้สำหรับส่งสัญญาณควบคุมการทำงานของการสื่อสาร มีความเร็ว 16 Kbps หรือ 64 Kbps (ขึ้นอยู่กับชนิดของการเชื่อมต่อ)
- N-ISDN มีการเชื่อมต่อ 2 แบบ
  - แบบบีอาร์ไอ (Basic Rate Interface: BRI) – ใช้สำหรับการเชื่อมต่อผู้ใช้ตามบ้านหรือการใช้งานทั่วไป เข้ากับระบบเครือข่าย มีช่องสัญญาณแบบ 2B+D
    - มี B-Channel จำนวน 2 ช่อง (ช่องละ 64 Kbps) และ D-Channel ที่มีความเร็ว 16 Kbps จำนวน 1 ช่อง
  - แบบพีอาร์ไอ (Primary Rate Interface: PRI) – ใช้สำหรับการเชื่อมต่อที่มีการใช้ช่องสัญญาณจำนวนมาก เช่นองค์กรต่างๆ มีช่องสัญญาณ (D-Channel มีความเร็ว 64 Kbps)
    - ในอเมริกาเป็น แบบ 23B+D
      - มี B-Channel จำนวน 23 ช่อง (ช่องละ 64 Kbps) และ D-Channel ที่มีความเร็ว 64 Kbps จำนวน 1 ช่อง
    - ในยุโรปเป็น แบบ 30B+D
      - มี B-Channel จำนวน 30 ช่อง (ช่องละ 64 Kbps) และ D-Channel ที่มีความเร็ว 64 Kbps จำนวน 1 ช่อง



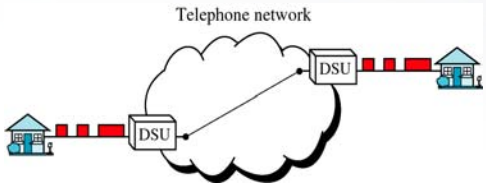
Broadband ISDN

- ระบบไอเอสดีเอ็นแบบใหม่เรียกว่า บรอดแบนด์ไอเอสดีเอ็น (Broadband ISDN: B-ISDN)
  - มีความเร็วในการส่งข้อมูลมากกว่าแบบเดิม คือตั้งแต่ 25 Mbps ขึ้นไป ถึงมากกว่า Gbps
  - มีความละเอียดในการเลือกใช้ความเร็วในการรับส่งข้อมูลมากขึ้น เป็น Kbps
    - (N-ISDN เลือกความเร็วเป็นจำนวนเท่าของ 64 Kbps)
  - ความเร็วในการรับและส่งข้อมูลมาจำเป็นต้องเท่ากัน (Asymmetric)



สายวงจรเฉพาะ

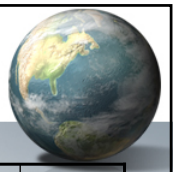
- สายวงจรเฉพาะ (Dedicated Line) หรือสายวงจรเช่า (Leased Line) คือสายโทรศัพท์ที่เชื่อมต่อระหว่างจุดสองจุดที่ผู้ใช้ต้องการและสงวนสายโทรศัพท์ในเส้นทางนั้นไว้ไม่ให้ผู้อื่นใช้
  - ผู้ที่เช่าจึงสามารถส่งข้อมูลผ่านวงจรนั้นได้ตลอดเวลาที่ต้องการ
  - โดยปกติสายวงจรเช่าจะถูกเลือกมาจากสายที่มีคุณภาพ จึงมีโอกาสเกิดข้อผิดพลาดในการส่งข้อมูลน้อยและสามารถใช้ความเร็วในการสื่อสารได้สูง
  - สายวงจรเฉพาะมีหลายประเภท
    - สายวงจรวอยซ์เกรด
    - สายวงจรไวด์แบนด์อนาลอก
    - สายวงจรชั้นที/อี
    - สายวงจรดีเอสแอล
    - โซเน็ต/เอสดีเอช



สายวงจรเฉพาะ

- สายวงจรวอยซ์เกรด (Voice-Grade Circuits) – สำหรับการสื่อสารเสียงสนทนาเท่านั้น มีความกว้างช่องสัญญาณ 4,000 Hz มีคุณภาพเพียงพอสำหรับการสื่อสารเสียงเท่านั้น
- สายวงจรไวด์แบนด์อนาลอก (Wideband Analog Circuits) – ช่องสื่อสารที่มีความกว้างมากบนสายโทรศัพท์ โดยการใช้สายหลายเส้นร่วมกัน ใช้หลักการของ Multiplexing

สายวงจรเฉพาะ

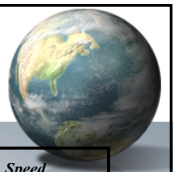


- สายวงจรชั้นที/อี (T/E-Carrier Circuits) เป็นสายวงจรเฉพาะที่ส่งสัญญาณดิจิตอลหลายช่องในสายวงจรเดียว โดยใช้หลักการ TDM
- ระบบดีเอส (Digital Signal: DS) เป็นระบบสัญญาณดิจิตอลที่มีโครงสร้างลำดับชั้น
- Fractional T-1/E-1 เป็นการแบ่งสายสัญญาณดิจิตอลเป็นส่วนย่อย (ไม่ใช้เต็มทุกช่องสัญญาณ) เช่น ต้องการใช้ความเร็ว 128, 256, 384, 512 หรือ 768 Kbps บนสาย T-1/E-1

T-Carrier	*DS Name*	*Rate*	*Voice Channels*
	DS-0	64 kbps	1
T-1	DS-1	1.544 Mbps	24
T-2	DS-2	6.312 Mbps	96
T-3	DS-3	33.375 Mbps	672
T-4	DS-4	274.176 Mbps	4032

Line	*Rate (Mbps)*	*Voice Channels*
E-1	2.048	30
E-2	8.448	120
E-3	34.368	480
E-4	139.264	1920

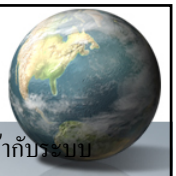
สายวงจรเฉพาะ



- โซเน็ต/เอสดีเอช (Synchronous Optical Network: SONET)/(Synchronous Digital Hierarchy: SDH) เป็นวงจรสื่อสารที่ใช้สายใยแก้วนำแสง
  - SONET ใช้ในอเมริกา
  - SDH ใช้ในยุโรปและเป็นมาตรฐานที่กำหนดโดย ITU-T
  - ใช้หลักการแบ่งช่องสัญญาณ (Multiplexing) แบบ TDM (Time Division Multiplexing)

SONET	*SDH*	*Speed*
OC-1		51.84 Mbps
OC-3	STM-1	155.52 Mbps
OC-9	STM-3	466.56 Mbps
OC-12	STM-4	622.08 Mbps
OC-18	STM-6	933.12 Mbps
OC-24	STM-8	1.244 Gbps
OC-36	STM-12	1.866 Gbps
OC-48	STM-16	2.488 Gbps
OC-192		9.952 Gbps
OC-768		39.813 Gbps

สายวงจรเฉพาะ



- สายวงจรดีเอสแอล (Digital Subscriber Line: DSL) เป็นสายวงจรการเชื่อมต่อเข้ากับระบบเครือข่ายบรอดแบนด์ไอเอสดีเอ็น
  - เชื่อมต่อผู้ใช้ตามบ้านหรือองค์กรขนาดเล็ก
  - นำเทคโนโลยีการผสมสัญญาณด้วยมักซ์และเทคนิคการบีบอัดข้อมูลเข้ามาช่วยเพิ่มประสิทธิภาพการทำงาน
  - ผู้ใช้ต้องมีสายวงจรเช่าที่มีการเชื่อมต่อตลอดเวลา
  - ใช้อุปกรณ์ที่ทำหน้าที่แยกสัญญาณ เช่น โมเด็มแบบพิเศษ เรียกว่าสปริทเทอร์ (Splitter) ติดตั้งไว้ที่ปลายสายสื่อสารทั้งสองด้าน

สายวงจรเฉพาะ

- วงจรดีเอสแอลแบ่งเป็นหลายชนิด
  - เอดีเอสแอล (Asymmetric Digital Subscriber Line: ADSL) ใช้สายโทรศัพท์ธรรมดาร่วมกับโมเด็มเอดีเอสแอล
    - ความเร็วในการส่งข้อมูลจากผู้ใช้ไปยังศูนย์ให้บริการ หรืออัพสตรีม (Upstream) จะไม่เท่ากับความเร็วที่ศูนย์ให้บริการส่งข้อมูลกลับมายังผู้ใช้ หรือดาวน์สตรีม (Downstream)
    - มีความเร็วดาวน์สตรีม 64 Kbps ถึง 9 Mbps และความเร็วอัพสตรีม 16 ถึง 640 Kbps ขึ้นอยู่กับคุณภาพของสายสื่อสารที่ใช้
  - เอชดีเอสแอล (High Bit-Rate/Data-Rate Digital Subscriber Line: HDSL) ใช้สาย T-1 ที่เป็นสายคู่ตีเกลียว (Twisted Pair)
    - มีความเร็วสองด้านเท่ากัน 1.5 หรือ 2.0 Mbps
  - ไอดีเอสแอล (ISDN Digital Subscriber Line: IDSL) พัฒนาโดยบริษัทลูเซนท์เทคโนโลยี (Lucent Technology) ใช้สายคู่ตีเกลียวส่งด้วยหลักการ ISDN ที่มีความเร็ว 144 Kbps
  - อาร์เอดีเอสแอล (Rate Adaptive Digital Subscriber Line: RADSL) โมเด็มสามารถปรับความเร็วในการส่งข้อมูลให้เหมาะสมกับระยะทาง และสภาพแวดล้อมของสายที่ใช้งานให้มีคุณภาพในระดับเดิม
    - มีความเร็วดาวน์สตรีม 40 Kbps ถึง 7 Mbps และความเร็วอัพสตรีมได้ไม่เกิน 768 Kbps
  - วีดีเอสแอล (Very High-Rate Digital Subscriber Line: VDSL) สามารถส่งข้อมูลได้ความเร็วสูงมาก แต่ผู้ใช้จะอยู่ห่างจากชุมสายได้ไม่เกิน 1,000 ฟุต
    - ใช้สายใยแก้วนำแสงจะมีความเร็วดาวน์สตรีม 12.96 Mbps ถึง 52 Mbps และความเร็วอัพสตรีมได้ไม่เกิน 3 Mbps

สายวงจรเฉพาะ

- สายวงจรดีเอสแอล (Digital Subscriber Line: DSL)

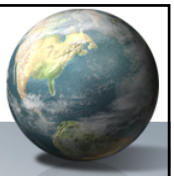
Name	*Meaning*	*Data Range*	*Mode*	*Application*
V.22, 32, 42	Voice band modem	1.2 Kbps to 28.8 Kbps	Duplex	Data Communications
DSL	Digital Subscriber Line	160 Kbps	Duplex	ISDN services Voice and data communications
HDSL	High data rate Digital Subscriber Line	1.544 Mbps 2.048 Mbps	Duplex Duplex	T1/E1 service Feeder plant, WAN, LAN access, server access
SDSL	Single line Digital Subscriber Line	1.544 Mbps 2.048 Mbps	Duplex Duplex	Same as HDSL, plus premises access for symmetric services
ADSL	Asymmetric Digital Subscriber Line	1.5 to 9 Mbps 16 to 640 Kbps	Down Up	Internet access, video-on-demand, simplex video, remote LAN access, interactive multimedia
VDSL, BDSL, or VADSL	Very High date rate Digital Subscriber Line	1.3 to 52 Mbps 1.5 to 2.3 Mbps	Down Up	Same as ADSL plus HDTV

ระบบเครือข่ายแบบแพ็กเกตสวิทช์

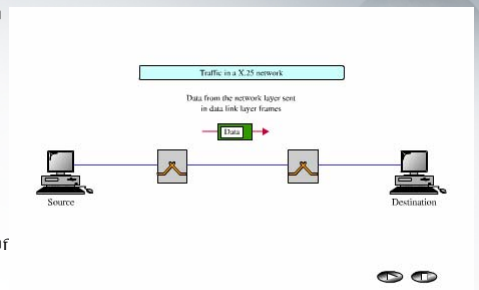
- ปัจจุบัน ระบบเครือข่ายแบบแพ็กเกตสวิทช์เป็นระบบเครือข่ายที่มีประสิทธิภาพดีที่สุดสำหรับการส่งข้อมูลดิจิตอล
- เทคโนโลยีที่นำมาใช้งานร่วมกับเครือข่ายแพ็กเกตสวิทช์ => บริการฟาสต์แพ็กเกต
  - X.25
  - เฟรมรีเลย์
  - เอทีเอ็ม

บริการฟาสต์แพ็กเกต

X.25



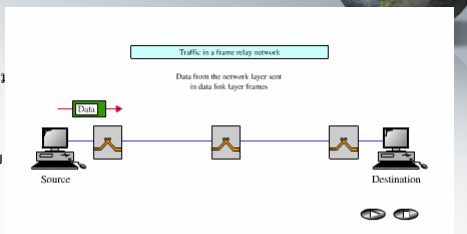
- X.25 เป็นระบบเครือข่ายแบบแพ็กเกตสวิทช์แบบแรก
- ใช้สำหรับการสื่อสารระหว่างโฮสต์กับเทอร์มินอล
- เป็นการเชื่อมต่อแบบจุด-ต่อ-จุด
- ใช้หลักการ “จัดเก็บแล้วส่งต่อ (Store-and-Forward)”
- ความเร็วของการเชื่อมต่อไม่จำเป็นต้องเท่ากัน
- ระบบมีการรับประกันความแน่นอนของข้อมูล (Data Integrity)
- มีข้อเสียในเรื่องความล่าช้า (Delay) ของข้อมูลที่ส่งออกไป
  - เนื่องจากมีการตรวจสอบความถูกต้องทุกช่วงของการเชื่อมต่อ



บริการฟาสต์แพ็กเกต

เฟรมรีเลย์

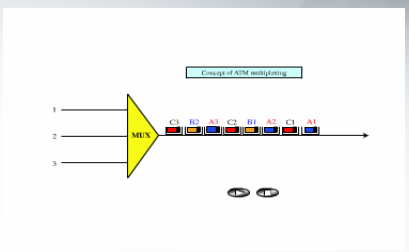
- เฟรมรีเลย์ (Frame Relay) พัฒนาต่อมาจาก X.25 เพื่อให้มีความเร็วสูงขึ้นและมีราคาถูกลง โดยไม่มีการรับประกันความถูกต้องของข้อมูล
- ใช้การส่งแพ็กเกตหรือเรียกว่า เฟรม (Frame) ให้เร็วที่สุด
- ไม่มีการตรวจสอบความถูกต้องของข้อมูลที่ส่ง ให้เป็นความรับผิดชอบของชั้นสื่อสารที่สูงขึ้นไปของอุปกรณ์ปลายทาง
  - เนื่องจากอุปกรณ์และเทคโนโลยีเครือข่ายมีความผิดพลาดน้อยและมีความเชื่อถือได้สูง

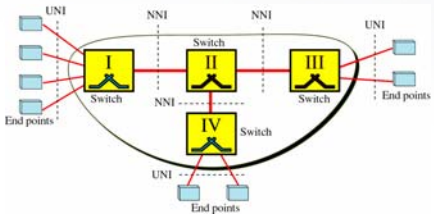


- กำหนดความเร็วในการส่งข้อมูลด้วย อัตราซีไออาร์ (Committed Information Rate: CIR) ซึ่ง
  - เป็นอัตราการส่งข้อมูลเฉลี่ย ที่ให้ผู้ใช้ส่งข้อมูลได้ตามที่ตกลงไว้
  - ถ้าส่งข้อมูลเกิน ระบบเครือข่ายมีสิทธิที่จะจัดการส่งเฟรมส่วนที่เกินให้ หรือลบเฟรมส่วนเกินนั้นทิ้งไปก็ได้
- นอกจากนี้ระบบเครือข่ายก็มีกลไกการแจ้งเตือนเมื่อระบบเครือข่ายเกิดความคับคั่ง เพื่อให้โปรแกรมผู้ใช้ทราบสถานะของระบบเครือข่าย และสามารถเพิ่มหรือลดจำนวนเฟรมที่ส่งออกมาได้ แทนที่ระบบจัดการลบบางเฟรมทิ้งไป เรียกว่า
  - Forward Explicit Congestion Notification (FECN)
  - Backward Explicit Congestion Notification (BECN)

บริการฟาสต์แพ็กเกต เอทีเอ็ม (ATM)

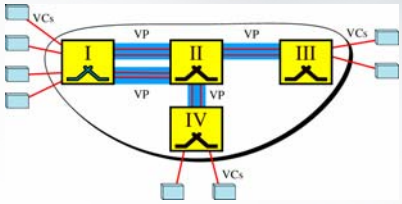
- ระบบเครือข่ายเอทีเอ็ม (Asynchronous Transfer Mode: ATM) – เป็นระบบแพ็กเกตสวิทช์ที่มีความสามารถในการส่งข้อมูลสูงมาก
  - แพ็กเกตในระบบเครือข่ายเอทีเอ็ม จะมีขนาดความยาว 53 ไบท์เท่ากันทุกแพ็กเกต เรียกว่า เซลล์ (Cell)
  - ระบบเครือข่ายเอทีเอ็มจึงเรียกอีกชื่อหนึ่งว่า เซลล์รีเลย์ (Cell Relay)
  - ใช้หลักการสื่อสารโดยใช้วงจรเสมือน
  - ระบบเครือข่ายเอทีเอ็มสามารถส่งข้อมูลได้หลายชนิดทั้ง ภาพวิดิทัศน์ เสียงและข้อมูลอิเล็กทรอนิกส์ทุกชนิดโดยมีการรับประกันการสื่อสารข้อมูลให้
  - มีความเร็วในการส่งข้อมูลตั้งแต่ 1.5 Mbps ขึ้นไปจนถึง 622.1 Mbps และมีการพัฒนาให้มีความเร็วสูงขึ้นในระดับหลาย Gbps
  - ระบบเครือข่ายเอทีเอ็มจะไม่มีการตรวจสอบความถูกต้องของข้อมูลที่ส่ง ให้เป็นความรับผิดชอบของชั้นสื่อสารที่สูงขึ้นไปของอุปกรณ์ปลายทาง เช่นเดียวกับเฟรมรีเลย์
  - เซลล์จะถูกส่งผ่านสวิทช์ ซึ่งจะตรวจดูข้อมูลเส้นทางวงจรเสมือนในเซลล์ แล้วส่งเซลล์ออกไป





บริการฟาสต์แพ็กเกต เอทีเอ็ม (ATM)

- ระบบเครือข่ายเอทีเอ็มทำงานแบบมีการเชื่อมต่อ (Connection-Oriented) คือจะต้องกำหนดเส้นทางวงจรเสมือนขึ้นมาก่อนการส่งข้อมูล และเส้นทางนี้จะถูกใช้งานไปจนกว่าการสื่อสารครั้งนั้นจะสิ้นสุด
  - Virtual Connection = Virtual Path + Virtual Channel
  - เซลล์ทุกเซลล์เดินทางไปยังจุดหมายทางเส้นทางเดียวกันและเรียงกันตามลำดับ
- การกำหนดเส้นทางวงจรเสมือน
  - แบบพีวีซี (Permanent Virtual Circuit: PVC) – ทำการกำหนดเส้นทางล่วงหน้า โดยก่อนการส่งข้อมูลไม่ต้องทำการสร้างวงจรเสมือนก่อนทุกครั้ง
  - แบบเอสวีซี (Switched Virtual Circuit: SVC) - กำหนดเส้นทางเดินข้อมูลเมื่อมีความต้องการ โดยจะต้องมีการสร้างวงจรเสมือนก่อนการส่งทุกครั้งและเมื่อใช้งานเสร็จก็จะต้องทำการยกเลิกวงจรเสมือนนั้นด้วย เส้นทางที่ถูกสร้างแต่ละครั้งอาจไม่ใช้เส้นทางเดิมก่อนหน้านี้ก็ได้

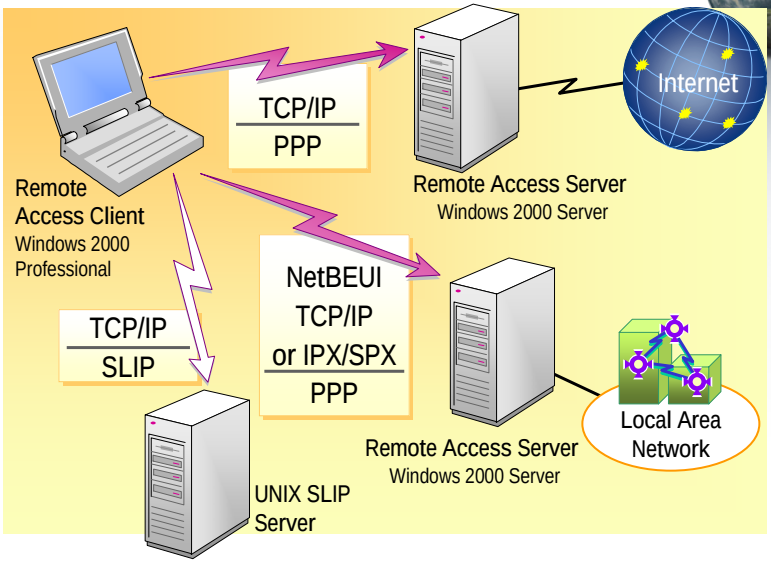


- มีการกำหนดระดับความสำคัญหรือระดับการให้บริการ เรียกว่า คุณภาพของบริการ (Quality of Services: QoS)
  - เช่นการส่งข้อมูลที่เป็นเสียงสนทนา (Voice) จะกำหนดระดับของการให้บริการ (QoS) สูงกว่าการส่งข้อมูลประเภทจดหมายอิเล็กทรอนิกส์
  - เนื่องจากข้อมูลเสียงจำเป็นจะต้องถูกส่งในทันที มิฉะนั้นทางผู้ฟังจะได้ยินเสียงขาดหายเป็นช่วงๆ ในขณะที่การส่งจดหมายอิเล็กทรอนิกส์อาจจะรอสักเล็กน้อย ก็ไม่ทำให้เกิดผลเสียหายใดๆ
    - เช่นอาจรอประมาณ 5 ถึง 20 วินาที ซึ่งการรอจดหมายอิเล็กทรอนิกส์สัก 20 วินาทีจะไม่มีผลต่อผู้ใช้ แตกต่างจากการรอเสียงสนทนา 20 วินาที ซึ่งหมายถึงเสียงขาดช่วงไป 20 วินาที

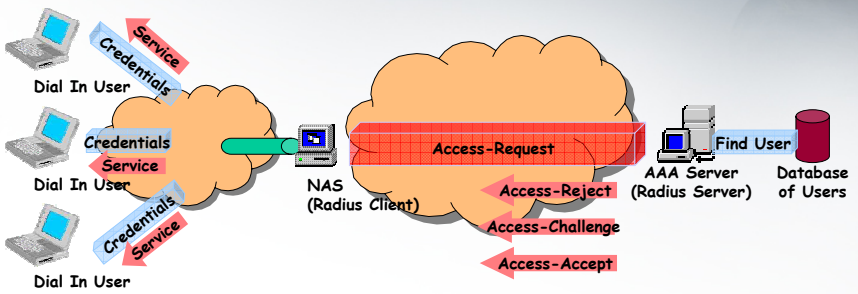
Remote Access Services (RAS)

- RAS เป็นการให้บริการการใช้งานระบบเครือข่ายจากระยะไกล
- ประกอบด้วย
  - Remote Access Client เป็นผู้ใช้บริการจากระยะไกล
  - Remote Access Server (RAS) หรือ Network Access Server (NAS) ทำหน้าที่ให้บริการการเชื่อมต่อจากผู้ใช้ระยะไกล
    - จะต้องมีการจัดเตรียมช่องทาง (Port) ให้ผู้ใช้ติดต่อเข้ามาใช้บริการ เช่น โทรศัพท์, ISDN
    - มีการเชื่อมต่อเข้ากับระบบเครือข่าย เพื่อให้ผู้ใช้ ใช้บริการเครือข่ายนั้นๆ ได้
  - Authentication, Authorization, Accounting (AAA) Server ทำหน้าที่ตรวจสอบผู้ใช้ที่เข้ามาใช้บริการ และกำหนดสิทธิการใช้บริการ ตลอดจนบันทึกการใช้งาน
  - Remote Access Protocol เป็นโพรโตคอลที่ผู้ใช้ใช้งานจากระยะไกลเข้ามายังเครือข่าย
  - AAA Protocol เป็นโพรโตคอลที่ใช้ติดต่อสื่อสารในการทำงานระหว่าง RAS กับ AAA Server
    - ที่นิยมใช้งานคือ RADIUS Protocol (Remote Authentication Dial In User Service)

การเชื่อมต่อ Remote Access

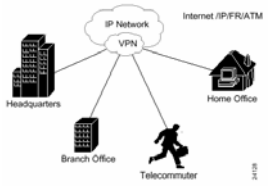


หลักการทำงานของ RAS ร่วมกับ AAA Server



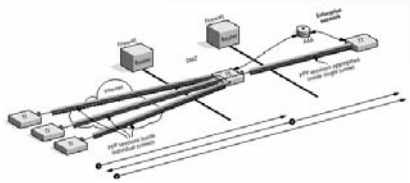
ระบบเครือข่ายวีพีเอ็น

- ระบบเครือข่ายวีพีเอ็น (Virtual Private Network: VPN)
  - เป็นระบบเครือข่ายส่วนตัว (Private Network) ที่ลดค่าใช้จ่ายในการสร้างระบบเครือข่าย
    - ด้วยการเชื่อมต่อเข้ากับระบบเครือข่ายสาธารณะ (Public Network)
    - แต่ยังคงมีความปลอดภัยในการใช้งานเสมือนเป็นระบบเครือข่ายส่วนตัว
  - โดยปกติจะเป็นการเชื่อมต่อระบบเครือข่ายเฉพาะบริเวณของหน่วยงานต่างๆ ในองค์กรหนึ่งที่ตั้งอยู่ในสถานที่ต่างกัน ผ่านระบบเครือข่ายวงกว้างซึ่งเป็นระบบเครือข่ายสาธารณะ
    - ประกอบกันเป็นระบบเครือข่ายเสมือนขององค์กร (Enterprise Network)
  - ข้อมูลจากโหนดอื่นในระบบเครือข่ายสาธารณะจะไม่สามารถส่งเข้ามาในโหนดใดๆขององค์กรได้



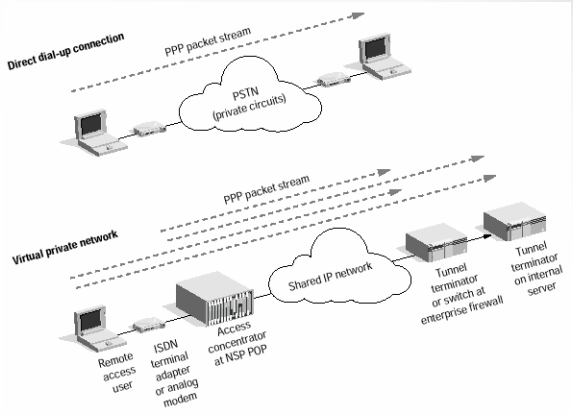
ระบบเครือข่ายวีพีเอ็น

- ระบบเครือข่ายวีพีเอ็นใช้เทคนิคในการสร้างช่องทางการสื่อสารแบบ “อุโมงค์ (Tunneling)”
- ช่องทาง”อุโมงค์”ที่สร้างขึ้น จะเป็นการเชื่อมต่อในลักษณะจุดต่อจุด (Point-to-Point)
  - โดยเชื่อมต่อผ่านระบบเครือข่ายสาธารณะหรือเครือข่ายที่ใช้งานร่วมกับผู้อื่น
- ทำให้เป็นการเชื่อมต่อระบบเครือข่ายผ่านเครือข่ายที่มีอยู่ได้

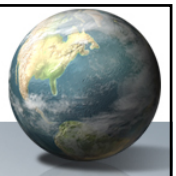


การทำงานของ VPN

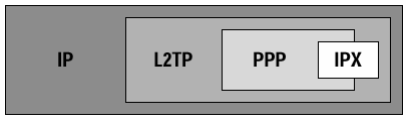
- Based on familiar networking technology and protocols



การทำงานของ VPN

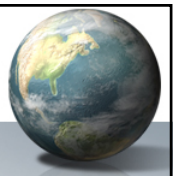


- Layer 2 Tunneling
- VPN tunnels are created by
  - Encapsulating network protocols (IP, IPX, AppleTalk, etc.) inside the PPP
  - Then encapsulating the entire inside a tunneling protocol, e.g. IP, ATM, FrameRelay

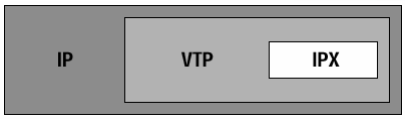


IP/UDP	L2F	PPP (Data)
Carrier Protocol	Encapsulating Protocol	Passenger Protocol

การทำงานของ VPN



- Layer 3 Tunneling
- Network protocols are encapsulated directly into a tunneling protocol

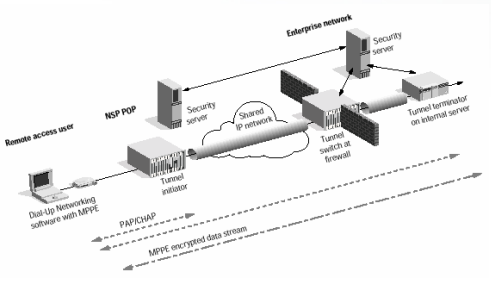


VPN Protocols

- Microsoft's Point-to-Point Tunneling Protocol (PPTP), bundled with MS-Windows
- Layer 2 Tunneling Protocol (L2TP)
  - Merging PPTP and Layer 2 Forwarding (L2F)
- 3Com's Virtual Tunneling Protocol (VTP)
  - Layer 3 Tunneling Protocol

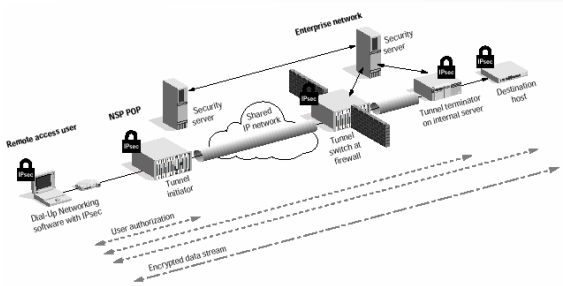
VPN Security (1)

- Microsoft Point-to-Point Encryption (MPPE)
  - Data encryption with MS-Dial up networking
  - 40-bit or 128-bit versions
  - Encrypt PPP packets before go into PPTP tunnel
  - Use MS-CHAP for user authentication



VPN Security (2)

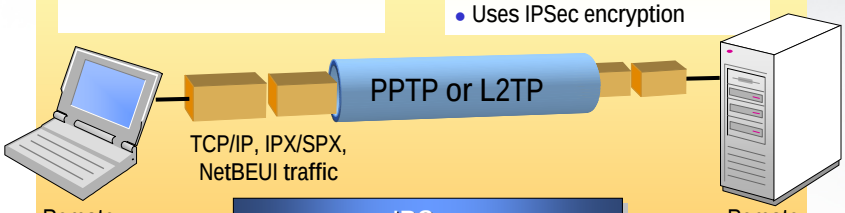
- Secured IP (IPSec)
  - IETF Standard for VPN security
  - Use with L2TP
  - User authentication, privacy, and data integrity



VPN Protocols ที่นิยมใช้งาน

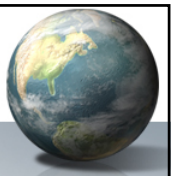
PPTP
- Internetwork must be IP-based
- Header compression
- No tunnel authentication
- Uses MPPE encryption

L2TP
- Internetwork can be IP, frame relay, X.25, or ATM-based
- Header compression
- Tunnel authentication
- Uses IPSec encryption

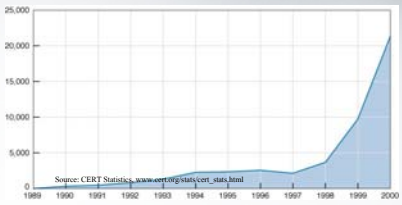


IPSec
- Ensures data security in IP-based communications
- Can be used by both PPTP and L2TP

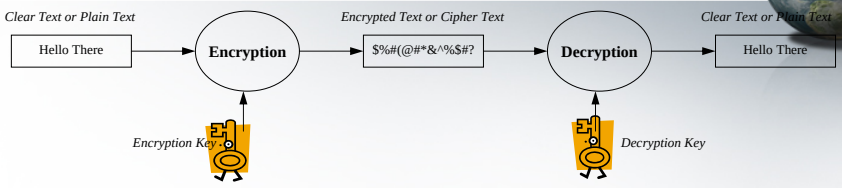
Introduction to Internet Security



- ระบบเครือข่ายอินเทอร์เน็ตและเครือข่ายไร้สายเป็นวิธีการสื่อสารหลักที่ได้รับความนิยมในการใช้งานมาก
  - ทำให้ต้องมีการรักษาความปลอดภัยให้ดีพอ
- สถิติของการเกิดเหตุการณ์ที่เกี่ยวข้องด้านความปลอดภัยที่เกิดขึ้นในระบบอินเทอร์เน็ตเพิ่มมากขึ้นทุกปี
- เหตุการณ์ส่วนใหญ่เป็นการบุกรุกเข้าไปในระบบที่ไม่ได้รับอนุญาตให้ใช้งานได้
- ระบบรักษาความปลอดภัยแบ่งออกเป็นหลายระดับ เรียกว่า ระดับการรักษาความปลอดภัย (Security Levels)
  - ระดับอาจจะมีการแบ่งได้หลายแบบ ขึ้นอยู่กับองค์กรนั้นๆ เช่น
  - อาจแบ่งตามระดับผู้ที่เกี่ยวข้องในระบบ
    - ผู้จัดการระบบเครือข่าย (Network Administrator) ได้รับอนุญาตให้ใช้งานได้ทุกส่วนของระบบเครือข่าย
    - ผู้ใช้ (Users) ได้รับอนุญาตให้ใช้งานได้จำกัด

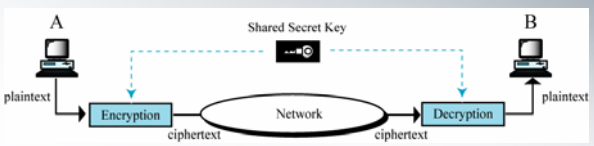


การเข้าและถอดรหัสข้อมูล (Cryptography)



- วิธีการทำให้ข้อมูลปลอดภัยที่ดีวิธีหนึ่งคือ การเข้ารหัสข้อมูล (Encryption) หมายถึงการเปลี่ยนข้อมูลจากรูปแบบปกติไปเป็นรูปแบบอื่นที่ไม่สามารถเข้าใจความหมายได้ สำหรับผู้ที่ไม่ทราบวิธีการแก้ไขหรือถอดรหัส (Decryption)
- ข้อมูลที่อยู่ในรูปแบบปกติที่สามารถเข้าใจความหายได้ เรียกว่า ข้อมูลธรรมดาหรือข้อมูลปกติ (Clear Text or Plain Text)
- ข้อมูลที่ผ่านการเข้ารหัสแล้วอยู่ในรูปแบบที่ไม่สามารถเข้าใจความหมายได้ เรียกว่า ข้อมูลที่เข้ารหัส (Encrypted Text or Cipher Text)
- การเข้ารหัส (Encryption) หมายถึงกรรมวิธีแปลงข้อมูลปกติให้เป็นข้อมูลที่เข้ารหัส
- การถอดรหัส (Decryption) หมายถึงกรรมวิธีแปลงข้อมูลที่เข้ารหัส ให้กลับมาเป็นข้อมูลปกติเดิม (ข้อมูลเดียวกับก่อนเข้ารหัส)
- การเข้ารหัส และการถอดรหัสจะเป็นคู่กัน เสมอ
- การเข้ารหัส และการถอดรหัสจะมีการใช้ข้อมูลพิเศษชุดหนึ่ง เรียกว่า กุญแจ (Key) ประกอบในการเข้าและถอดรหัสข้อมูล
  - กุญแจที่ใช้ในการเข้ารหัส เรียกว่า กุญแจเข้ารหัส (Encryption Key)
  - กุญแจที่ใช้ในการถอดรหัส เรียกว่า กุญแจถอดรหัส (Decryption Key)
- ผู้ที่ได้ข้อมูลที่เข้ารหัสไป ถ้าไม่รู้วิธีการถอดรหัสและกุญแจถอดรหัส ก็ไม่สามารถแปลงข้อมูลกลับเป็นข้อมูลปกติได้

การเข้ารหัสข้อมูล
การเข้ารหัสโดยใช้กุญแจแบบสมมาตร



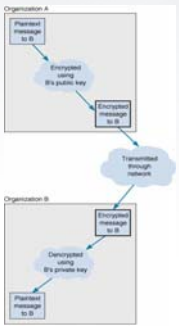
- การเข้ารหัสโดยใช้กุญแจแบบสมมาตร หรือการเข้ารหัสแบบคีย์สมมาตร (Symmetric Key Encryption) จะใช้กุญแจเพียงตัวเดียว นั่นคือกุญแจเข้ารหัสและถอดรหัสเป็นตัวเดียวกัน ทำให้ต้องเก็บกุญแจนั้นไว้เป็นความลับ บางครั้งจึงเรียกว่า Shared Secrete Key Encryption

ตัวอย่างวิธีการเข้ารหัสโดยใช้กุญแจแบบสมมาตร

- DES (Data Encryption Standard) – กุญแจมีขนาด 56 บิต ทำการเข้ารหัสข้อมูลครั้งละ 64 บิต
- Tripple DES: 3DES – กุญแจมีความยาว 112 บิต ทำให้มีความปลอดภัยเพิ่มขึ้น
- Blowfish – กุญแจมีความยาว 32 ถึง 448 บิต ไม่ได้จดทะเบียนลิขสิทธิ์ ทำให้นำมาใช้ได้อิสระ
- IDEA (International Data Encryption Algorithm) – กุญแจมีความยาว 128 บิต เป็นของ บ. Ascom-Tech อนุญาตให้ใช้ได้ฟรีสำหรับงานที่ไม่เกี่ยวข้องทางธุรกิจ เช่นสถาบันการศึกษา

การเข้ารหัสข้อมูล
การเข้ารหัสโดยใช้กุญแจแบบอสมมาตร

- การเข้ารหัสโดยใช้กุญแจแบบอสมมาตร (Asymmetric Key Encryption) เป็นการเข้าและถอดรหัสโดยใช้กุญแจสองตัว คือกุญแจเข้ารหัสและกุญแจถอดรหัสที่ไม่เหมือนกัน
  - โดยกุญแจเข้ารหัสจะทำการเผยแพร่หรือแจกจ่ายให้แก่ผู้อื่นที่ต้องการติดต่อเข้ามา ในลักษณะเผยแพร่สู่สาธารณะ เรียกว่า กุญแจสาธารณะ (Public Key)
  - ส่วนกุญแจถอดรหัสจะเก็บไว้เป็นความลับส่วนตัว เฉพาะผู้ถอดรหัสข้อมูล เรียกว่า กุญแจส่วนตัว (Private Key)
  - บางทีจึงเรียกว่าการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public Key Encryption)
- ถ้าใช้วิธีนี้ มักจัดตั้งระบบพีเคไอ (Public Key Infrastructure: PKI) ขึ้นมาช่วยในการแจกจ่ายกุญแจสาธารณะ



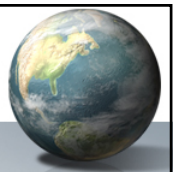
ตัวอย่างวิธีการเข้ารหัสโดยใช้กุญแจแบบอสมมาตร

- RSA – พัฒนาโดย Ron Rivest, Adi Shamir และ Leonard Adleman เป็นวิธีที่นิยมใช้มากที่สุด กำหนดความยาวของกุญแจรหัสได้ ส่วนมากใช้ความยาวกุญแจ 1024 บิต

รูปแบบการบุกรุกระบบคอมพิวเตอร์

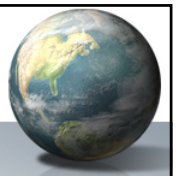
- ผู้ดูแลระบบเครือข่ายและผู้ใช้จะต้องป้องกันไม่ให้ผู้อื่นบุกรุกเข้ามาในเครื่องคอมพิวเตอร์หรือระบบเครือข่ายของตนเอง
- การบุกรุกโดยซอฟต์แวร์มีหลายประเภท
  - ไวรัสคอมพิวเตอร์ (Computer Virus)
    - เป็นโปรแกรมคอมพิวเตอร์ที่ออกแบบมาให้ทำอันตรายต่อระบบคอมพิวเตอร์หรือระบบเครือข่าย และ
    - มีความสามารถในการแพร่กระจายไปยังเครื่องคอมพิวเตอร์อื่นๆ โดยใช้พาหะหรือสื่อต่างๆ ของระบบคอมพิวเตอร์ เช่น แผ่นดิสก์ ไฟล์ข้อมูล จดหมายอิเล็กทรอนิกส์
  - หนอนคอมพิวเตอร์ (Computer Worm)
    - เป็นโปรแกรมคอมพิวเตอร์ที่ออกแบบมาให้ทำงานทั้งในด้านดีและไม่ดี และ
    - มีความสามารถในการแพร่กระจายไปยังเครื่องคอมพิวเตอร์อื่นๆ ด้วยตัวเอง โดยไม่จำเป็นต้องใช้พาหะหรือสื่อต่างๆ (ยกเว้นการสื่อสารผ่านระบบเครือข่ายคอมพิวเตอร์)
      - ส่วนใหญ่จะใช้ช่องโหว่ของระบบคอมพิวเตอร์ เพื่อทำการแพร่กระจายเข้าไปทำงาน
    - ตัวอย่างได้แก่ Internet Worm ซึ่งแพร่กระจายด้วยการสร้างสำเนาตัวเองไปยังเครื่องต่างๆ ในระบบอินเทอร์เน็ต แล้วเข้าไปจองทรัพยากรของเครื่องคอมพิวเตอร์นั้น จนไม่สามารถใช้งานได้ และการแพร่กระจายสามารถทำได้อย่างรวดเร็ว ในลักษณะเท่าทวีคูณ จนไม่สามารถควบคุมได้ ทำให้ระบบอินเทอร์เน็ตส่วนใหญ่ใช้งานไม่ได้ชั่วระยะเวลาหนึ่ง
  - ม้าโทรจัน (Trojan Horse) – เป็นโปรแกรมคอมพิวเตอร์ที่มีสองวัตถุประสงค์
    - วัตถุประสงค์หน้าฉากเป็นโปรแกรมที่ดูดีมีประโยชน์ หรือซ่อนการทำงานไว้
    - วัตถุประสงค์หลังฉากจะเป็นวัตถุประสงค์ที่ไม่ดี เช่นพยายามขโมยข้อมูลต่างๆ หรือบุกรุกระบบคอมพิวเตอร์ต่างๆ

รูปแบบการบุกรุกระบบคอมพิวเตอร์



- การป้องกันการบุกรุกโดยซอฟต์แวร์สามารถทำได้โดยใช้โปรแกรมป้องกันไวรัส หรือโปรแกรมต่อต้านไวรัส (Anti-Virus Program)
  - แต่เนื่องจากมีการบุกรุกโดยซอฟต์แวร์ใหม่ออกมาอยู่ตลอดเวลา ทำให้ต้องทำการปรับปรุงข้อมูลเกี่ยวกับการบุกรุกอยู่เสมอ ซึ่งสามารถทำได้โดยการ Update Virus Pattern เพื่อทำให้โปรแกรมป้องกันไวรัสรู้จักวิธีการทำงานการบุกรุกแบบใหม่ๆ และสามารถป้องกันการบุกรุกได้
- รูปแบบการบุกรุกอีกวิธีหนึ่ง ได้แก่ การทำให้เกิดการปฏิเสธการให้บริการ หรือ ดีโอเอส (Denial of Service: DoS) เป็นวิธีการทำให้บริการในระบบไม่สามารถให้บริการแก่ผู้ใช้บริการปกติได้ ซึ่งสามารถทำได้หลายแบบ เช่น
  - การเพิ่มปริมาณงานที่ดูเหมือนงานปกติจากผู้ใช้ทั่วไป แต่มีปริมาณสูงมากให้แก่เครื่องให้บริการอย่างต่อเนื่อง จนกระทั่งเครื่องให้บริการนั้น หรือการให้บริการนั้นไม่สามารถให้บริการแก่ผู้ใช้จริงๆ ได้

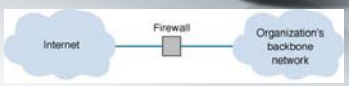
การป้องกันการบุกรุกระบบคอมพิวเตอร์

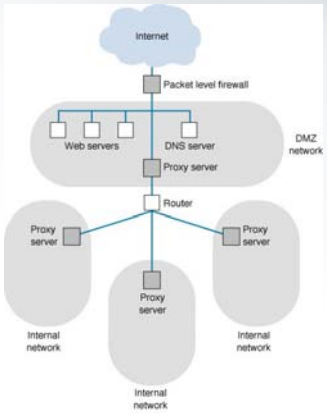


- การป้องกันการบุกรุกสามารถทำได้หลายระดับ และหลายวิธี เช่น
  - โปรแกรมไฟร์วอลล์
  - ระบบตรวจจับการบุกรุก

ไฟร์วอลล์

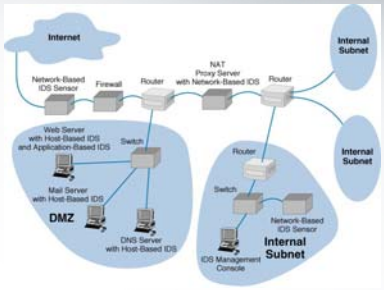
- ไฟร์วอลล์ (Firewall) เป็นอุปกรณ์หรือซอฟต์แวร์ที่ทำหน้าที่ในการตรวจสอบข้อมูลที่ผ่านเข้าออกระบบที่กำหนด แล้วทำการอนุญาตหรือไม่อนุญาตให้ข้อมูลนั้นผ่านเข้าออก นอกจากนี้อาจจะทำการเปลี่ยนแปลงข้อมูลนั้นด้วย
  - อาจมีการติดตั้งที่เครื่องคอมพิวเตอร์หรือในระหว่างระบบเครือข่าย
  - เปรียบเสมือนเจ้าหน้าที่รักษาความปลอดภัยหรือยามขององค์กร
- ไฟร์วอลล์แบ่งเป็น
  - ไฟร์วอลล์ระดับแพ็กเกต (Packet-Level Firewall) – จะตรวจข้อมูลในทุกแพ็กเกต เพื่อตรวจสอบว่าเป็นไปตามที่กำหนดไว้หรือไม่ แล้วทำการอนุญาตหรือไม่อนุญาตให้ผ่านเข้าออก
  - ไฟร์วอลล์ระดับโปรแกรมประยุกต์ (Application-Level Firewall) – ทำหน้าที่เป็นตัวกลางการเชื่อมต่อระหว่างเครือข่าย การทำงานจะซับซ้อนและปลอดภัยมากกว่า
    - หากทำงานแทนเครื่องที่ต้องการติดต่อด้วย เรียกว่า พร็อกซี่ (Proxy Server)
    - คช. เว็บพร็อกซี่จะทำหน้าที่ไปร้องขอข้อมูลจากเว็บไซต์แทนผู้ใช้ แล้วส่งข้อมูลที่ได้รับไปให้ผู้ใช้ ซึ่งอาจจะมีการเก็บข้อมูลที่ได้รับไว้ เพื่อให้การร้องขอได้ข้อมูลเร็วขึ้นและช่วยลดปริมาณข้อมูลที่สื่อสารได้ หรืออาจทำการปฏิเสธไม่ให้ผู้ใช้เข้าไปดูหรือรับข้อมูลจากเว็บไซต์บางแห่งได้





ระบบตรวจจับการบุกรุก

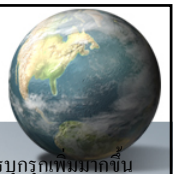
- ระบบการตรวจจับการบุกรุก (Intrusion Detection System: IDS) เป็นระบบที่ทำหน้าที่ตรวจสอบสิ่งต่างๆ ที่เกิดขึ้นในระบบ แล้วพิจารณาว่าเป็นการบุกรุกหรือไม่
- แบ่งเป็น
  - Network-based IDS เป็นการตรวจสอบโดยตรวจจับข้อมูลแพ็กเกตในระบบเครือข่าย
  - Host-based IDS เป็นการตรวจสอบกิจกรรมต่างๆ ที่เกิดขึ้นในเครื่องคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งข้อมูลที่เข้าสู่เครื่อง
  - Application-based IDS เป็นรูปแบบเฉพาะแบบหนึ่งของ Host-Based โดยทำการตรวจสอบการทำงานและข้อมูลของโปรแกรมประยุกต์



สรุป

- เทคโนโลยี WAN
  - ระบบเครือข่ายโทรศัพท์ => สื่อสารเสียงสนทนา
  - ระบบ ISDN เป็นระบบเครือข่ายข้อมูลดิจิตอล แบ่งเป็น
    - Narrowband ISDN ความเร็วไม่เกิน 1.5/2.0 Mbps ใช้หลักการ Circuit Switching มีการเชื่อมต่อ 2 แบบ
      - BRI มีช่องสัญญาณเป็นแบบ 2B+D
      - PRI มีช่องสัญญาณเป็นแบบ 23B+D หรือ 30B+D
    - Broadband ISDN ความเร็วสูง 25 Mbps ถึงมากกว่า 1,000 Mbps
  - สายวงจรเฉพาะ (Dedicated/Leased Line) เป็นวงจรเชื่อมต่อระหว่างจุดสองจุดที่ผู้ใช้ต้องการและสงวนเส้นทางนั้นไว้ไม่ให้ผู้อื่นใช้
  - สายวงจรชั้น T/E เป็นการสื่อสารโทรศัพท์ดิจิตอลหลายช่องสัญญาณ โดยใช้ TDM => T1/E1, T2/E2, T3/E3, T4/E4
  - ระบบ SONET/SDH เป็นระบบเครือข่ายสื่อสารบนใยแก้วนำแสงมีความเร็วสูงมาก ใช้หลักการ TDM
  - ระบบ DSL เป็นการเชื่อมต่อผู้ใช้ตามบ้านหรือสำนักงานขนาดเล็ก ความเร็วสูง มีหลายชนิด
    - Asymmetric DSL, High bit-rate/data-rate DSL, ISDN DSL, Rate Adaptive DSL, Very high-rate DSL
  - ระบบเครือข่ายแพ็กเกตสวิทช์ แบ่งเป็น
    - X.25 เป็นเครือข่ายแบบแรก มีความเร็วต่ำ ใช้ติดต่อสื่อสารระหว่างโฮสต์กับเทอร์มินอลในระยะไกล
    - Frame Relay เป็นเครือข่ายที่พัฒนาต่อมาให้มีความเร็วสูงขึ้น ส่งข้อมูลเป็นเฟรม
    - ATM เป็นเครือข่ายที่พัฒนาให้มีความเร็วสูงขึ้นอีก และมีการรับประกันการสื่อสารข้อมูลได้ ส่งข้อมูลเป็นเซลล์
- การให้บริการ RAS ทำให้ผู้ใช้สามารถใช้งานเครือข่ายได้จากระยะไกล
- ระบบเครือข่าย VPN เป็นเครือข่ายเฉพาะส่วนบุคคล ที่เชื่อมต่อเข้ากับระบบเครือข่ายสาธารณะ

สรุป



- ความปลอดภัยในระบบเครือข่ายมีความสำคัญมาก เนื่องจากมีเหตุการณ์ด้านความปลอดภัย เช่นการบุกรุกเพิ่มมากขึ้นเรื่อยๆ
- พื้นฐานของความปลอดภัยจะใช้การเข้า-ถอดรหัสข้อมูลเป็นหลัก
- การเข้ารหัสข้อมูลคือการแปลงข้อมูลปกติให้อยู่ในรูปแบบที่ไม่ทราบความหมายข้อมูล
- สามารถทำได้โดยใช้กุญแจสำหรับการเข้ารหัสและถอดรหัสข้อมูล
- การเข้ารหัสโดยการใช้กุญแจแบบสมมาตรจะมีกุญแจรหัสเพียงชุดเดียว ใช้ทั้งในการเข้ารหัสและถอดรหัส => ดังนั้นจึงต้องเก็บรักษากุญแจไว้เป็นความลับ
- การเข้ารหัสโดยการใช้กุญแจแบบอสมมาตรจะใช้กุญแจสองตัว ในการเข้าและถอดรหัส โดยจะมีกุญแจตัวหนึ่งเผยแพร่ทั่วไป เพื่อให้ผู้อื่นใช้ เรียกว่า กุญแจสาธารณะ (Public Key) และมีกุญแจอีกตัวหนึ่งที่ต้องเก็บเป็นความลับ เรียกว่ากุญแจส่วนตัว (Private Key)
- ระบบคอมพิวเตอร์อาจถูกบุกรุกโดยไวรัสคอมพิวเตอร์ ซึ่งเป็นโปรแกรมที่สามารถแพร่กระจายได้โดยใช้พาหะ
- ส่วนหนอนคอมพิวเตอร์จะเป็นโปรแกรมที่สามารถแพร่กระจายได้ด้วยตัวเอง
- การป้องกันการบุกรุกสามารถทำได้โดยใช้โปรแกรมป้องกันไวรัส หรือใช้ไฟร์วอลล์ เพื่อควบคุมการสื่อสารของระบบที่กำหนด โดยการอนุญาตหรือไม่อนุญาตให้มีการสื่อสารกัน โดยอาจนำเอาระบบตรวจจับการบุกรุกมาช่วยตรวจสอบเหตุการณ์ต่างๆ ในระบบร่วมด้วยก็ได้
- ไฟร์วอลล์แบ่งเป็นไฟร์วอลล์ระดับแพ็กเกต ทำหน้าที่ตรวจสอบข้อมูลแต่ละแพ็กเกตของระบบเครือข่าย และไฟร์วอลล์ระดับโปรแกรมประยุกต์ ทำหน้าที่ตรวจสอบการใช้งานระบบให้เป็นไปตามที่กำหนดไว้

END

Questions and Comments