บทที่ 5 : Network Security

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Agenda

- Web Security
  - HTTPS
  - SSL/TLS
- Remote Login Security
  - SSH
- Network Security
  - VPN

Web Security : HTTPS

- HTTPS (HTTP over SSL) เป็นโปรโตคอลที่พัฒนาโดย Netscape
- ใช้เข้ารหัสข้อมูลที่รับส่งระหว่างเซิร์ฟเวอร์และบราวเซอร์
- ปกติ HTTPS จะใช้พอร์ต 443 แทนที่พอร์ต 80 (HTTP)
- เวอร์ชันแรกใช้การเข้ารหัสแบบ RC4-40 bits ต่อมานิยมใช้ RSA 2048 bits และ ECC 256 bits โดยระบุบน Digital Certificate

Web Security : SSL/TLS

SSL พัฒนาโดย Netscape เป็นโปรโตคอลที่ใช้บริการเข้ารหัสและพิสูจน์ตัวตนระหว่างเว็บเซิร์ฟเวอร์กับไคลเอนต์

เริ่มต้นจะมีการตกลงกันก่อนว่าจะใช้อัลกอริทึมและคีย์ใดในการเข้ารหัสและการพิสูจน์ตัวตน

จากนั้นเริ่มสื่อสารโดยข้อมูลที่รับส่งมีการเข้ารหัสด้วยเซสชั่นคีย์

เว็บเซิฟเวอร์และเว็บบราวเซอร์ส่วนใหญ่จะรองรับโปรโตคอลนี้อยู่แล้ว

Web Security : SSL/TLS

TLS ได้มีการพัฒนาต่อมาจาก SSL ซึ่งได้ขยายการรองรับ Digital Signature

การทำงานของ SSL เทียบกับ HTTP ปกติ

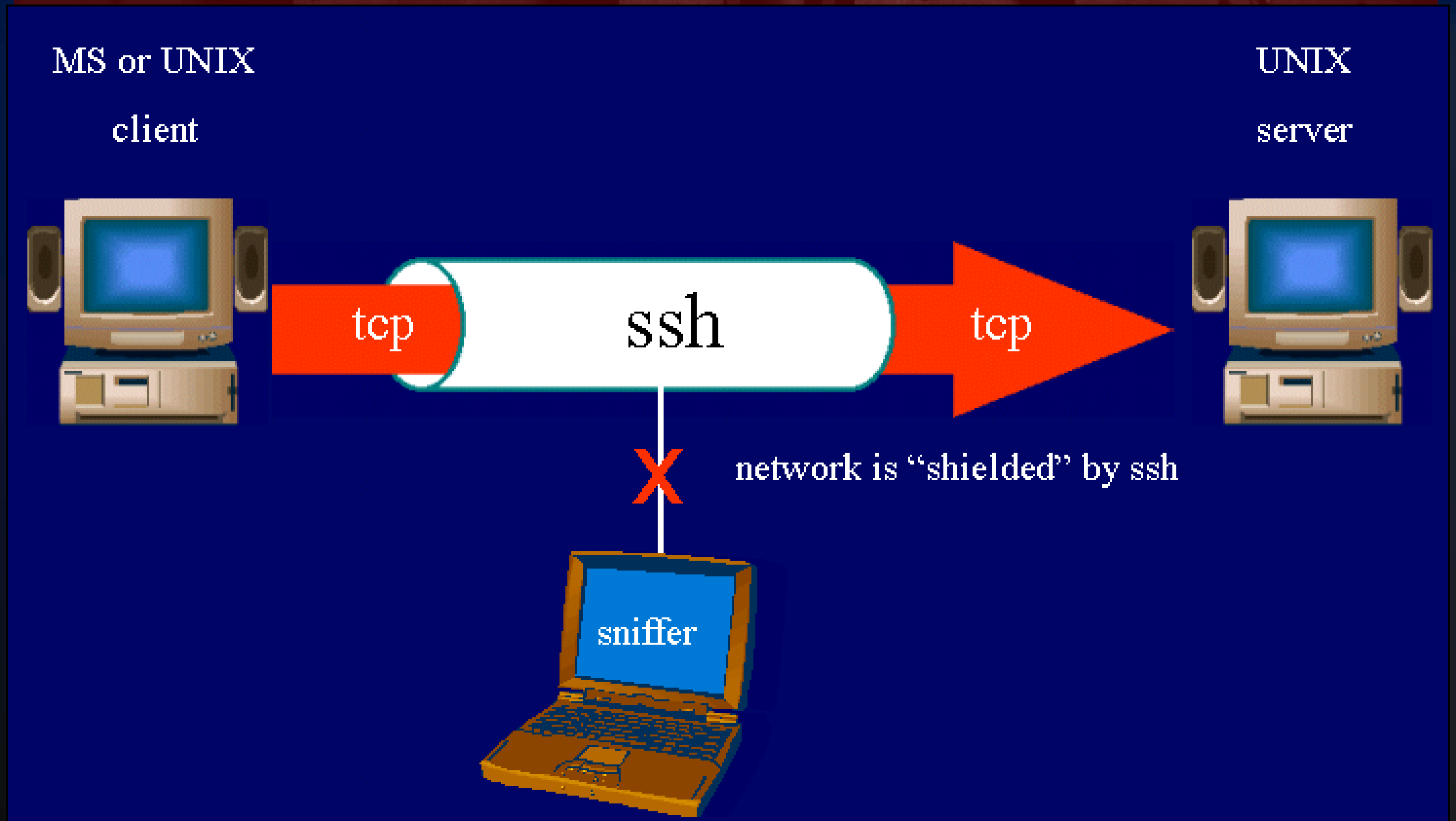
Remote Login & File Transfer Security

- การใช้งานรีโมทล็อกอินจำเป็นอย่างยิ่งที่จะต้องมีการเข้ารหัสข้อมูล เพื่อป้องกันการแอบดูข้อมูลที่สื่อสารกัน
- โปรโตคอลที่ใช้ในการรีโมทล็อกอินทั่วไปคือ TELNET ซึ่งได้มีการพัฒนาเป็น**โปรโตคอล SSH** เพื่อเข้ารหัสระหว่างการสื่อสาร
- โปรโตคอลที่ใช้ในการดาวน์โหลด-อัพโหลดไฟล์ คือ **FTP** ปกติจะไม่มีการเข้ารหัส จึงได้พัฒนาโปรโตคอล **SFTP** ขึ้นมาเพื่อเข้ารหัสข้อมูล

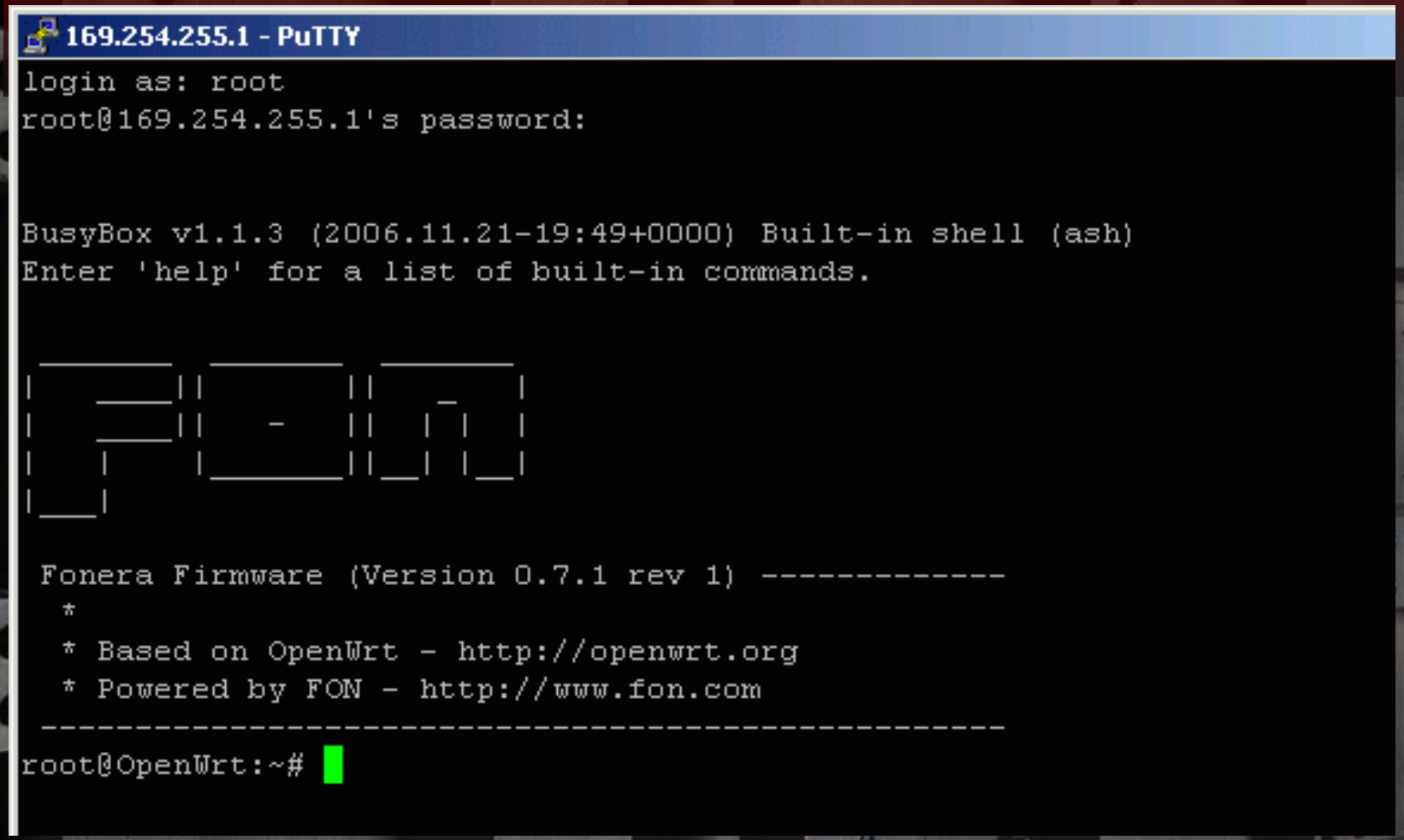
Remote Login & File Transfer Security: SSH

- SSH (Secure Shell) เป็นรูปแบบการรีโมทล็อกอินและ FTP ที่นิยมมากที่สุด ใช้สำหรับเข้ารหัสข้อมูลที่รับ-ส่งระหว่างไคลเอนต์และเซิร์ฟเวอร์
- ใช้พอร์ต 22 แทนพอร์ต 23 (TELNET) และ 21 (FTP)
- หลักการคือไคลเอนต์จะเชื่อมต่อไปยังเซิร์ฟเวอร์ เพื่อสร้าง Public Key สำหรับการเชื่อมต่อ ปัจจุบันนิยมใช้ RSA ร่วมกับ SHA-256 ในการเข้ารหัสข้อมูลและทำ Digital Signature
- โปรแกรม SSH ที่นิยม เช่น Putty, OpenTerm, OpenSSH

แบบจำลองการทำงานของ SSH



โปรแกรม Putty บน Linux



โปรแกรม OpenSSH

Network Security

- โปรโตคอลที่กล่าวมาข้างต้นทั้งหมดเป็นการเข้ารหัสข้อมูลในเลเยอร์ที่เหนือกว่าชั้นเน็ตเวิร์ค ส่วนใหญ่จะเป็นแอพพลิ-เคชันที่พัฒนาขึ้นเป็นพิเศษ
- การรักษาความปลอดภัยในระดับที่ต่ำลงมา เช่นในระดับเน็ตเวิร์ค จะต้องใช้โปรโตคอลที่ทำงานในระดับเน็ตเวิร์ค เช่น VPN ส่วนโปรโตคอลย่อยที่นิยมคือ IPsec

Network Security : VPN

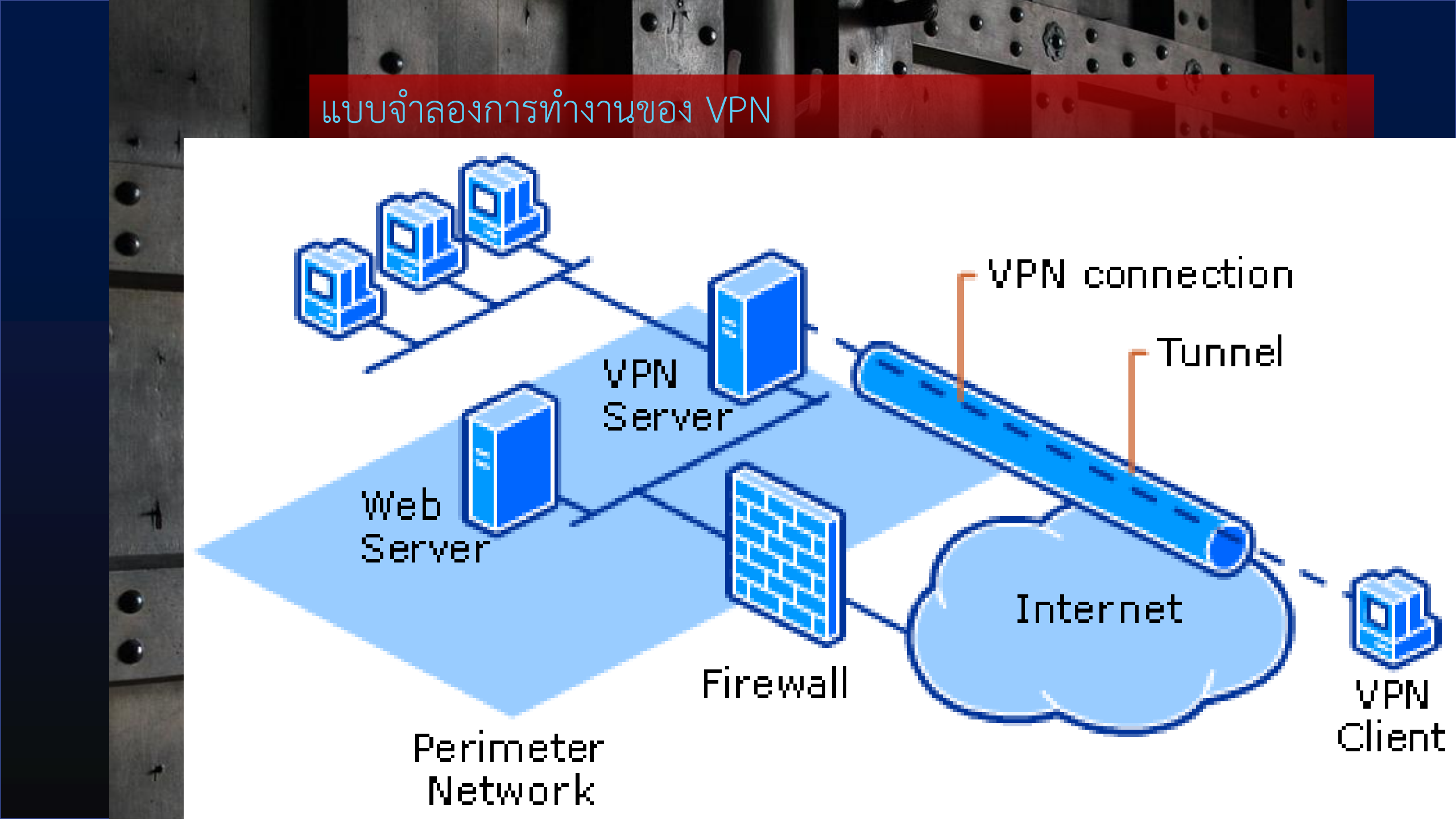
- เครือข่ายส่วนบุคคลเสมือน หรือ VPN (Virtual Private Network) หมายถึงระบบเครือข่ายส่วนบุคคลที่สร้างโดยแชร์ลิงก์ (เช่น อินเทอร์เน็ต)
- ช่วยให้ผู้ใช้สามารถแชร์ข้อมูลผ่านเครือข่ายสาธารณะ โดยมีการเข้ารหัสไว้ ทำให้ดูเสมือนว่าเป็นการสื่อสารกันภายในเครือข่ายส่วนบุคคล
- ข้อดีคือทำให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถเชื่อมต่อเข้ามายังเครือข่ายขององค์กรได้อย่างปลอดภัย

Network Security : VPN

VPN แบ่งเป็น 3 ประเภท ขึ้นอยู่กับลักษณะการใช้งาน

- **Access VPN** : ใช้เชื่อมต่อผู้ใช้ระยะไกล เช่น พนักงานที่ต้องเดินทางบ่อยๆ
- **Intranet VPN** : เชื่อมต่อกับเครือข่ายย่อยขององค์กร ผ่านเครือข่ายอินเทอร์เน็ต เช่น สาขาย่อยของบริษัท
- **Extranet VPN** : ใช้เชื่อมต่อระหว่างองค์กร

แบบจำลองการทำงานของ VPN



Network Security : VPN -> IPSec

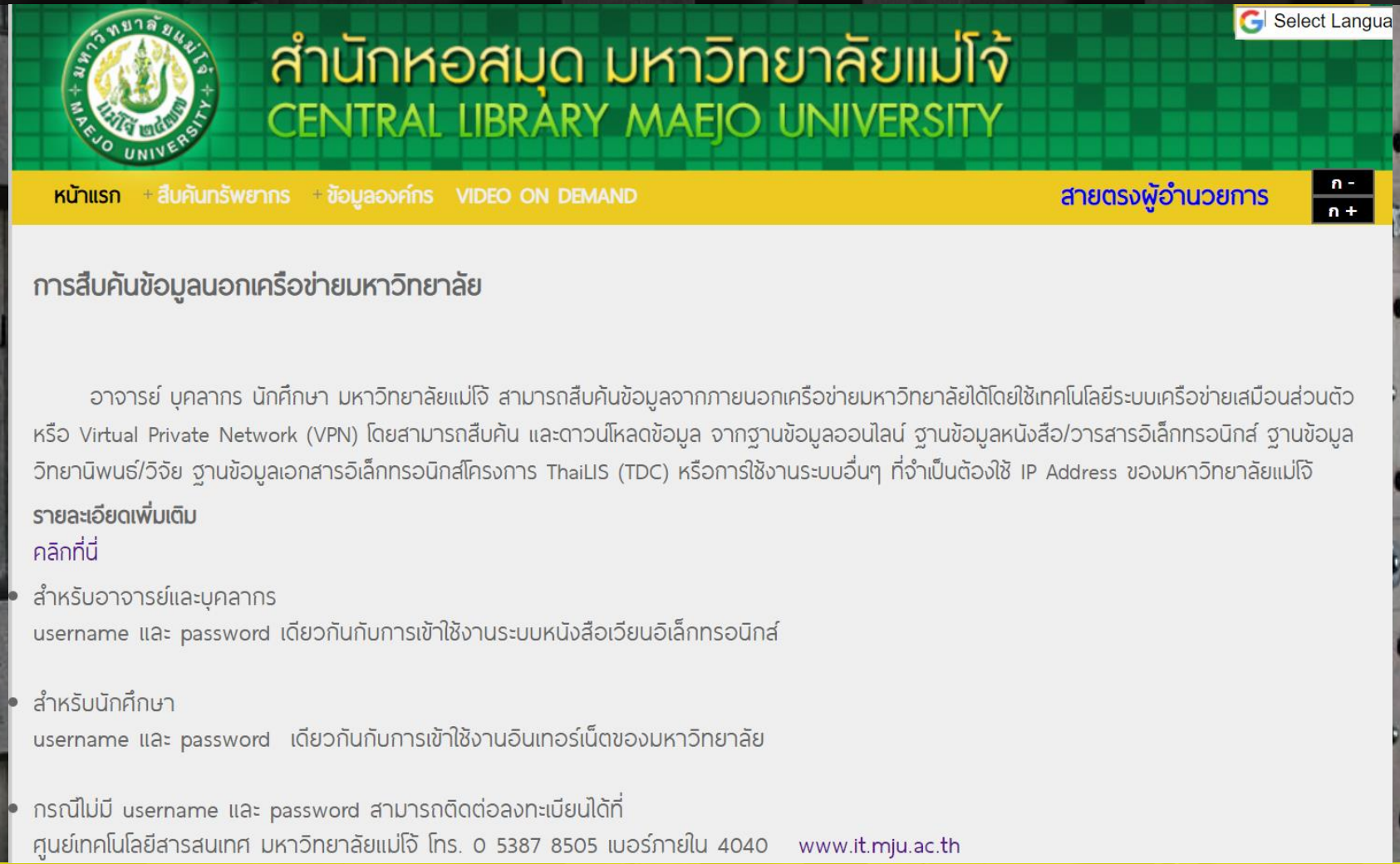
- เป็นโปรโตคอลที่รักษาความปลอดภัยข้อมูลในระดับเน็ตเวิร์คเลเยอร์
- ถือเป็นโปรโตคอลที่เหมาะสมสำหรับการสร้าง VPN
- ออกแบบมาสำหรับการเข้ารหัสข้อมูลแพ็กเก็ตของโปรโตคอล IP
- รับรองความลับของข้อมูล (Confidentiality), ความคงสภาพของข้อมูล (Integrity) และการพิสูจน์ตัวตน (Authentication)

Network Security : VPN -> IPSec [2]

อัลกอริทึมที่ IPSec ใช้เข้ารหัสข้อมูล คือ

- ใช้ Diffie-Hellman ในการแลกเปลี่ยนเซสชั่นคีย์ผ่านเครือข่ายสาธารณะ
- AES-GCM : สำหรับการเข้ารหัสข้อมูลและยืนยันตัวตน
- SHA2-256: ใช้ในการตรวจสอบความคงสภาพ
- Digital Certificate : สำหรับตรวจสอบเจ้าของพับลิกคีย์

การใช้งาน VPN ของมหาวิทยาลัยแม่โจ้ เพื่อสืบค้นข้อมูลจากภายนอกเครือข่ายมหาวิทยาลัย



https://library.mju.ac.th/content.php?page=data&id=102:VPN