



บทที่ 5 : Network Security

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Agenda

➤ Web Security

➤ HTTPS

➤ SSL/TLS

➤ Remote Login Security

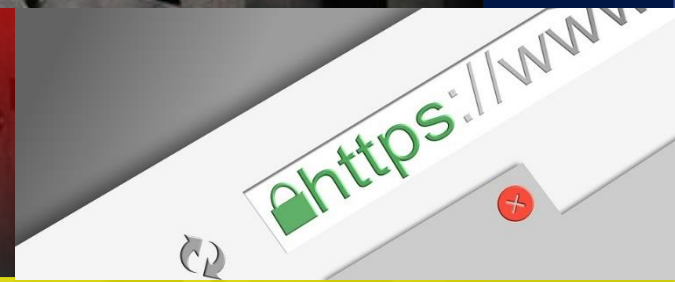
➤ SSH

➤ Network Security

➤ VPN



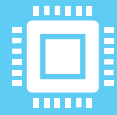
Web Security : HTTPS



- ▶ 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 เป็นโปรโตคอลที่ใช้บริการ
เข้ารหัสและพิสูจน์ตัวตนระหว่างเว็บเซิร์ฟเวอร์กับไคลเอนต์



เริ่มต้นจะมีการตกลงกันก่อนว่าจะใช้อัลกอริทึมและคีย์ใดใน
การเข้ารหัสและการพิสูจน์ตัวตน



จากนั้นเริ่มสื่อสารโดยข้อมูลที่รับส่งมีการเข้ารหัสด้วยเซสชัน
คีย์



เว็บเซิร์ฟเวอร์และเว็บเบราว์เซอร์ส่วนใหญ่จะรองรับโปรโตคอล
นี้อยู่แล้ว

Web Security : SSL/TLS

TLS ได้มีการพัฒนาต่อมาจาก SSL ซึ่งได้ขยายการรองรับ

Digital Signature



TLS



การทำงานของ SSL เทียบกับ HTTP ปกติ

วิธีการส่งข้อมูลแบบปกติ



วิธีการส่งข้อมูลด้วย SSL



Remote Login & File Transfer Security

- ➔ การใช้งานรีโมทล็อกอินจำเป็นต้องมีการเข้ารหัสข้อมูล เพื่อป้องกันการแอบดูข้อมูลที่สื่อสารกัน
- ➔ โพรโตคอลที่ใช้ในการรีโมทล็อกอินทั่วไปคือ TELNET ซึ่งได้มีการพัฒนาเป็นโปรโตคอล SSH เพื่อเข้ารหัสระหว่างการสื่อสาร
- ➔ โพรโตคอลที่ใช้ในการดาวน์โหลด-อัปโหลดไฟล์ คือ FTP ปกติจะไม่มีมีการเข้ารหัส จึงได้พัฒนาโปรโตคอล SFTP ขึ้นมาเพื่อเข้ารหัสข้อมูล

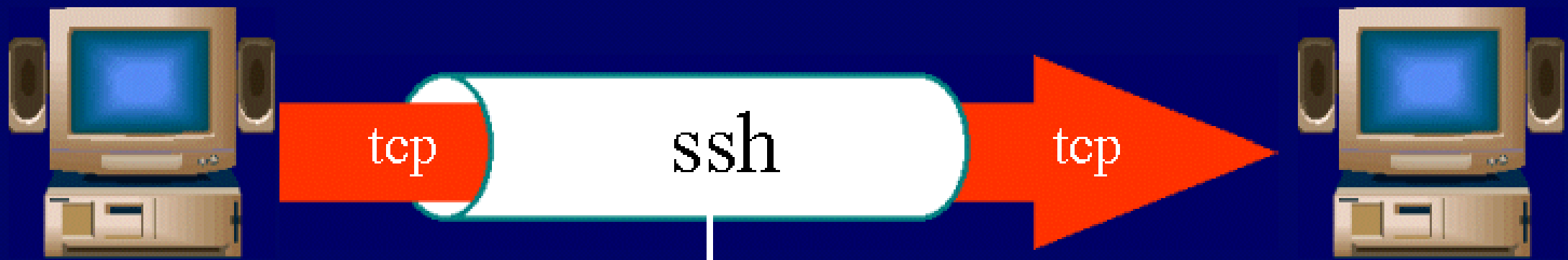
Remote Login & File Transfer Security: SSH

- ▶ 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

MS or UNIX
client

UNIX
server



X

network is "shielded" by ssh



sniffer

โปรแกรม Putty บน Linux

```
169.254.255.1 - PuTTY
login as: root
root@169.254.255.1's password:

BusyBox v1.1.3 (2006.11.21-19:49+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

_ _ _ _ _
|_| |_| |_|
|_| |_| |_|
|_| |_| |_|

Fonera Firmware (Version 0.7.1 rev 1) -----
*
* Based on OpenWrt - http://openwrt.org
* Powered by FON - http://www.fon.com
-----
root@OpenWrt:~# █
```


โปรแกรม OpenSSH



Network Security

- ▶ โพรโตคอลที่กล่าวมาข้างต้นทั้งหมดเป็นการเข้ารหัสข้อมูลในเลเยอร์ที่เหนือกว่าชั้นเน็ตเวิร์ค ส่วนใหญ่จะเป็นแอปพลิเคชันที่พัฒนาขึ้นเป็นพิเศษ
- ▶ การรักษาความปลอดภัยในระดับที่ต่ำลงมา เช่นในระดับเน็ตเวิร์ค จะต้องใช้โปรโตคอลที่ทำงานในระดับเน็ตเวิร์ค เช่น VPN ส่วนโปรโตคอลย่อยที่นิยมคือ IPsec



Network Security : VPN

- เครือข่ายส่วนบุคคลเสมือน หรือ VPN (Virtual Private Network) หมายถึงระบบเครือข่ายส่วนบุคคลที่สร้างโดยแชร์ลิงก์ (เช่น อินเทอร์เน็ต)
- ช่วยให้ผู้ใช้สามารถแชร์ข้อมูลผ่านเครือข่ายสาธารณะโดยมีการเข้ารหัสไว้ ทำให้ดูเหมือนว่าเป็นการสื่อสารกันภายในเครือข่ายส่วนบุคคล
- ข้อดีคือทำให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถเชื่อมต่อเข้ามายังเครือข่ายขององค์กรได้อย่างปลอดภัย



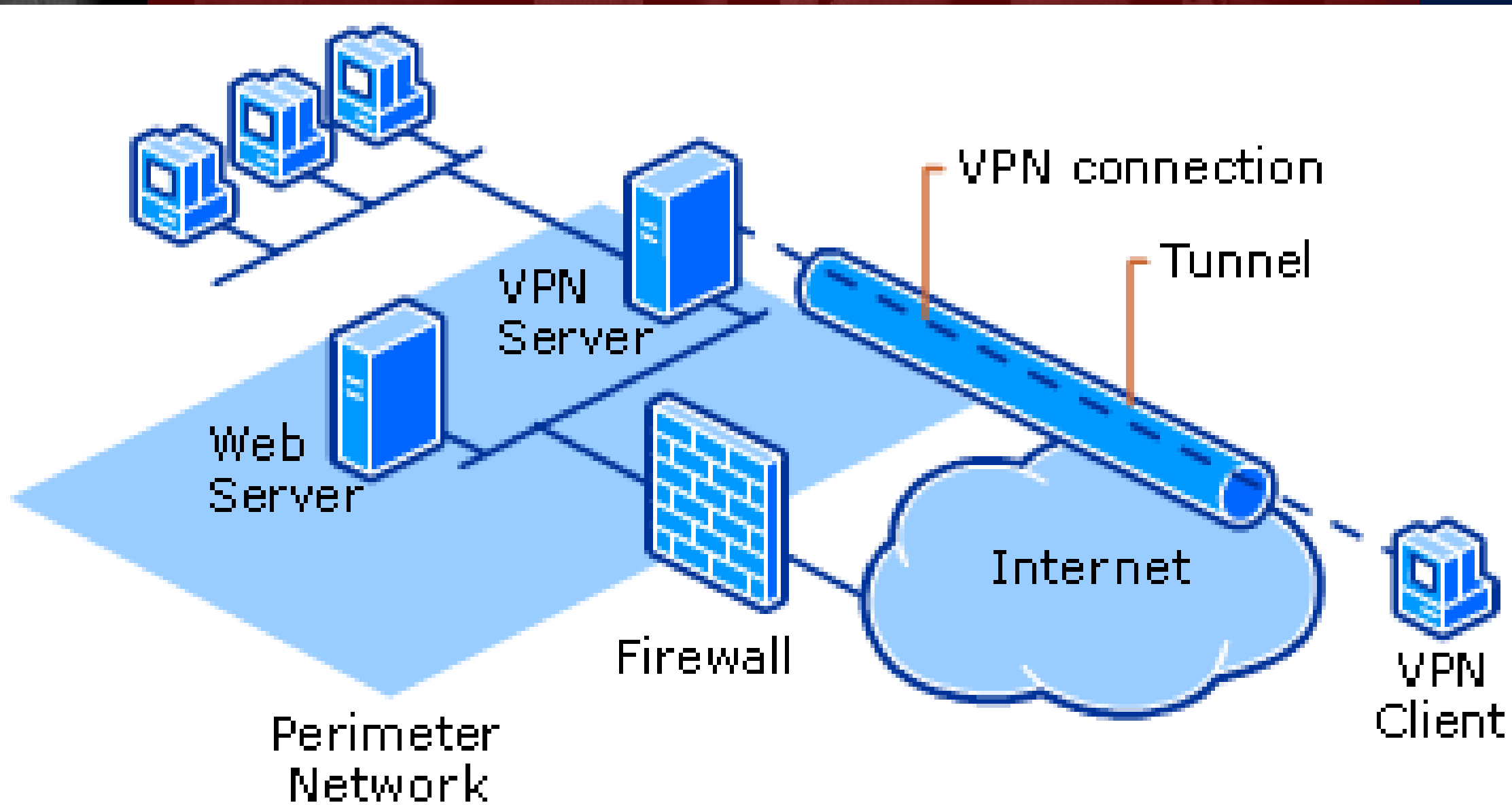
Network Security : VPN

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 ในการแลกเปลี่ยนเซสชันคีย์ผ่านเครือข่ายสาธารณะ
- ▶ AES-GCM : สำหรับการเข้ารหัสข้อมูลและยืนยันตัวตน
- ▶ SHA2-256: ใช้ในการตรวจสอบความคงสภาพ
- ▶ Digital Certificate : สำหรับตรวจสอบเจ้าของพับลิคคีย์

การใช้งาน VPN ของมหาวิทยาลัยแม่โจ้ เพื่อสืบค้นข้อมูลจากภายนอกเครือข่ายมหาวิทยาลัย



The screenshot shows the website for the Central Library of Maejo University. The header features the university's logo and name in Thai and English. A navigation bar includes links for Home, E-books, Journals, Video on Demand, and Direct Staff. The main content area is titled 'การสืบค้นข้อมูลนอกเครือข่ายมหาวิทยาลัย' (Accessing information outside the university network). The text explains that faculty and students can use VPN technology to access external resources. It lists various databases like ThaiLIS (TDC) and provides login instructions for different user groups. At the bottom, it provides contact information and the website URL.

หน้าแรก + สืบค้นทรัพยากร + ข้อมูลองค์กร VIDEO ON DEMAND Select Language

สำนักหอสมุด มหาวิทยาลัยแม่โจ้ CENTRAL LIBRARY MAEJO UNIVERSITY

สายตรงผู้อำนวยการ -
+

การสืบค้นข้อมูลนอกเครือข่ายมหาวิทยาลัย

อาจารย์ บุคลากร นักศึกษา มหาวิทยาลัยแม่โจ้ สามารถสืบค้นข้อมูลจากภายนอกเครือข่ายมหาวิทยาลัยได้โดยใช้เทคโนโลยีระบบเครือข่ายเสมือนส่วนตัว หรือ Virtual Private Network (VPN) โดยสามารถสืบค้น และดาวน์โหลดข้อมูล จากฐานข้อมูลออนไลน์ ฐานข้อมูลหนังสือ/วารสารอิเล็กทรอนิกส์ ฐานข้อมูลวิทยานิพนธ์/วิจัย ฐานข้อมูลเอกสารอิเล็กทรอนิกส์โครงการ ThaiLIS (TDC) หรือการใช้งานระบบอื่นๆ ที่จำเป็นต้องใช้ IP Address ของมหาวิทยาลัยแม่โจ้

รายละเอียดเพิ่มเติม
คลิกที่นี่

- สำหรับอาจารย์และบุคลากร
username และ password เดียวกันกับการเข้าใช้งานระบบหนังสือเวียนอิเล็กทรอนิกส์
- สำหรับนักศึกษา
username และ password เดียวกันกับการเข้าใช้งานอินเทอร์เน็ตของมหาวิทยาลัย
- กรณีไม่มี username และ password สามารถติดต่อลงทะเบียนได้ที่
ศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยแม่โจ้ โทร. 0 5387 8505 เบอร์ภายใน 4040 www.it.mju.ac.th

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