INT307 - Security I

Topic

- IP Security
- Authentication Header (AH)
- Web Security
- SSL (Secure Socket Layer)
- TLS (Transport Layer Security)
- Server Security
- Virtualization
- The Inheritance of Permission
- Password Policies

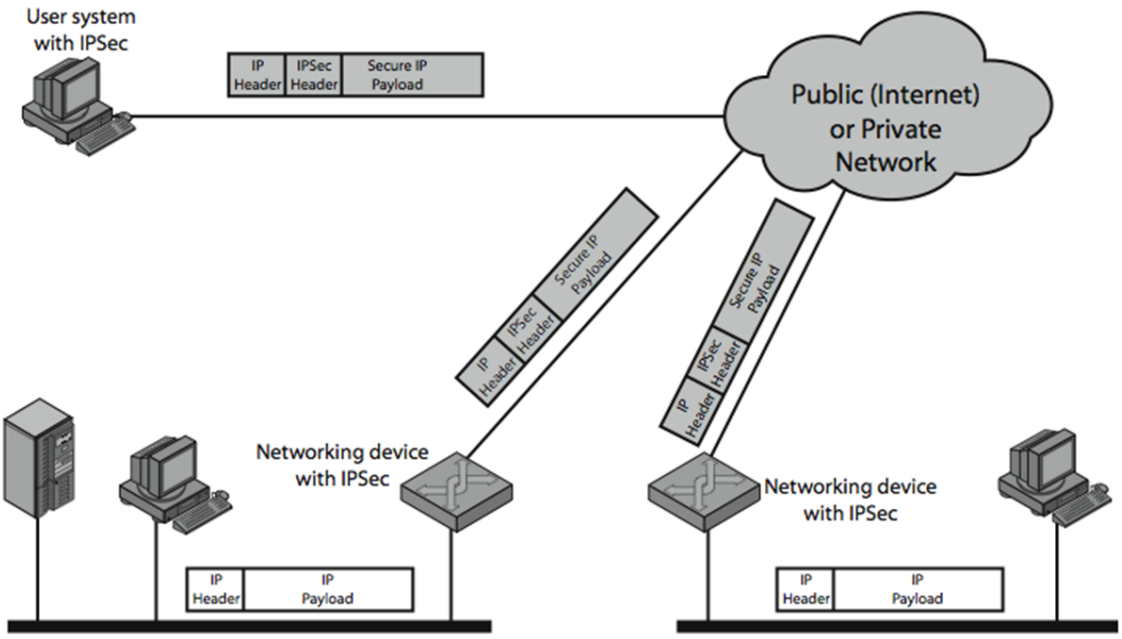
Note

IP Security (IP Sec)

What is ?

- คือเราก็รู้อยู่แล้วว่าปัจจุบันมีวิธีสร้างความปลอดภัยมากมาย เช่น S/MIME, PGP, Kerberos, SSL/HTTPS แต่ user ก็ยังไม่ไว้ใจระบบความปลอดภัยมากพอ เพราะก็ยังคงมีบาง app ที่เลือกที่จะไม่ใช้ระบบความปลอดภัยที่กล่าวมาข้างต้น จึงเกิดเป็นการรักษาความปลอดภัยในระดับ IP เรียกว่า IP Sec
- มี function 3 อย่างหลัก ๆ คือ
  - authentication → รับประกันว่าแพ็กเก็ตที่ได้รับนั้นถูกส่งโดยฝ่ายที่ระบุว่าเป็นแหล่งที่มาในส่วนหัวของแพ็กเก็ต และแพ็กเก็ตนั้นไม่ได้รับการเปลี่ยนแปลงระหว่างการส่ง
  - confidentiality → เข้ารหัสข้อความเพื่อป้องกันการดักฟังโดยบุคคลที่สาม
  - key management → การแลกเปลี่ยนคีย์ที่ปลอดภัย IPSec ให้ความสามารถในการรักษาความปลอดภัยการสื่อสารผ่าน LAN ผ่าน WAN ส่วนตัวและสาธารณะ และผ่านอินเทอร์เน็ต

- ใช้งานได้ทั้ง LAN WAN และทั้งใน สาธารณะ และส่วนตัว



Benefits

- สามารถใช้งานได้กับ Firewall/Router ได้เพื่อให้ได้ strong security ในขอบเขตของตัวเอง
- ใน Firewall/Router สามารถป้องกันการ Bypass ด้วย IP ได้
- เนื่องจากอยู่ใน transport layer ทำให้ transparent ต่อ Application และ End user (Application และ End user ไม่รับรู้หรือไม่จำเป็นต้องรับรู้ว่ามี feature นี้อยู่)
- สามารถเปิดใช้ได้ถึงระดับ User แต่ละรายได้เลย

Architecture

- ข้อกำหนดค่อนข้างซับซ้อน
- ข้อกำหนดถูกกำหนดตาม RFC จำนวนมาก เช่น RFC 2401/2402/2406/2408 หรือจัดกลุ่มตามหมวดหมู่
- เป็นข้อบังคับใน IPv6 และเป็น optional ใน IPv4
- มี Extension ใน Header เพิ่มคือ
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)

Services

- Access control
- Connectionless integrity → ตรวจสอบความถูกต้องของข้อมูลที่ส่งไปยังปลายทางว่าข้อมูลนั้นไม่ได้ถูกเปลี่ยนแปลงหรือทำลายระหว่างการส่ง

- Data origin authentication → ยืนยันว่าแหล่งที่มาของข้อมูลเป็นของจริงและเป็นที่รู้จัก
- Rejection of replayed packets → ป้องกันการโจมตีแบบ replay attack
  - a form of partial sequence integrity
- Confidentiality (encryption) → ทำให้ข้อมูลที่ส่งไปยังปลายทางไม่สามารถถูกอ่านได้โดยบุคคลที่ไม่ได้รับอนุญาต
- Limited traffic flow confidentiality → ซ่อนลักษณะการส่งข้อมูล เช่น ปริมาณข้อมูลหรือช่วงเวลาที่มีการส่ง

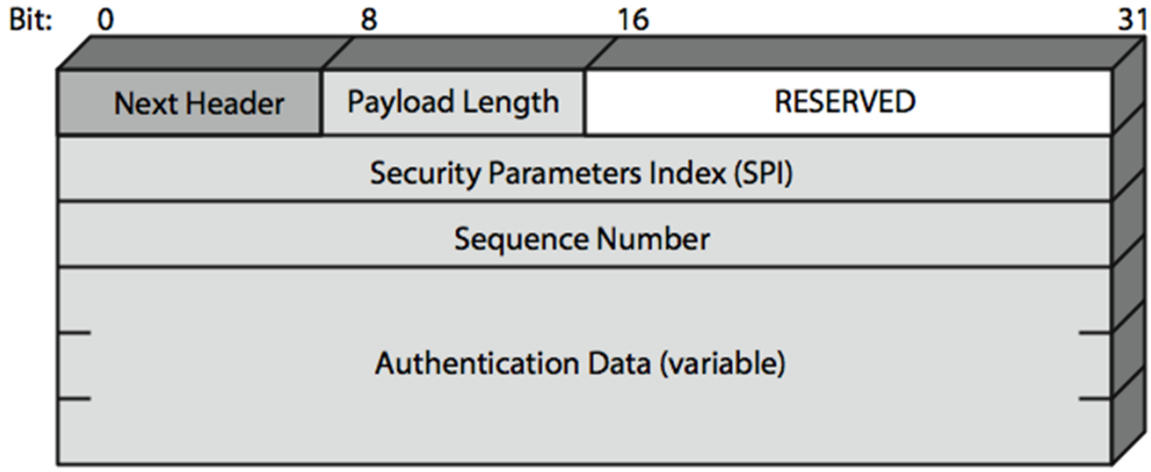
Security Associations (SA)

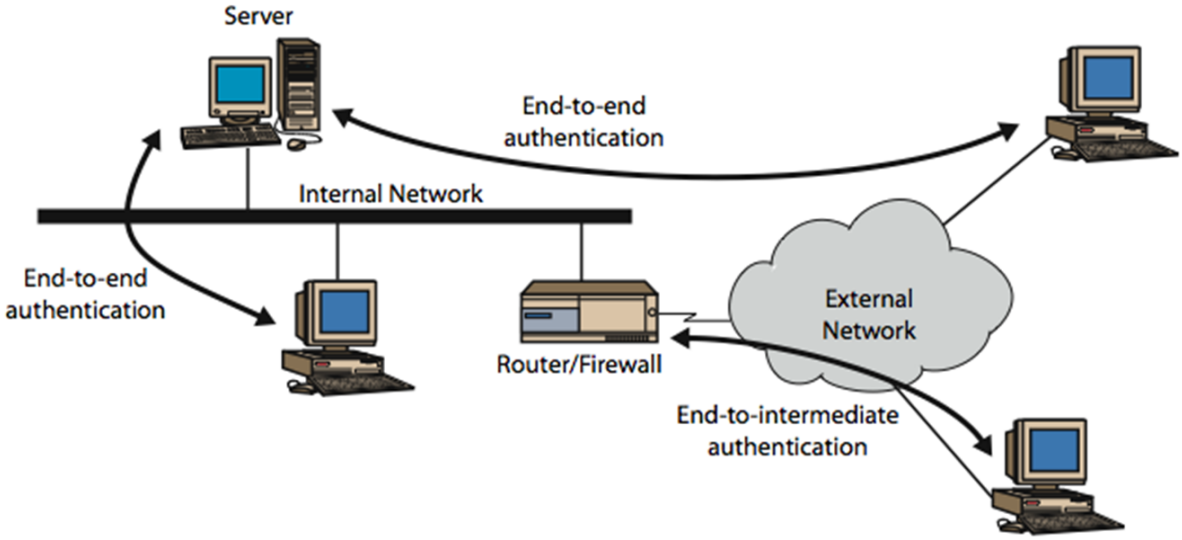
- เป็นแนวคิดสำคัญใน IPsec ที่ใช้ในการจัดการความปลอดภัยในการสื่อสาร , เป็น one-way relationship ระหว่างผู้ส่งและผู้รับ
- มี 3 parameters หลัก ๆ คือ
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier
- แต่ก็อาจจะมี parameters อื่น ๆ ด้วยเช่น seq no, AH & EH info, lifetime
- have a database of Security Associations → เก็บข้อมูลเกี่ยวกับพารามิเตอร์ต่าง ๆ ที่เกี่ยวข้องกับแต่ละ SA

Authentication Header (AH)

- ช่วยป้องกันในส่วนของ IP packets
- มี Sequence Number เพื่อตรวจจับการส่งข้อมูลซ้ำ
- ป้องกันการโจมตีด้วย Address Spoofing กับ Replay Attack ได้
- ใช้ MAC (Message Authentication Code) เพื่อ encoded มี algorithm ที่รองรับอยู่ตามนี้
  - **HMAC-MD5-96**: ใช้ HMAC (Hash-based Message Authentication Code) กับ MD5 ซึ่งให้ค่าแฮชขนาด 128 บิต
  - **HMAC-SHA-1-96**: ใช้ HMAC กับ SHA-1 ซึ่งให้ค่าแฮชขนาด 160 บิต

- ใช้ Shared Secret Key เพื่อสร้างและตวจสอบ MAC ที่ได้รับ

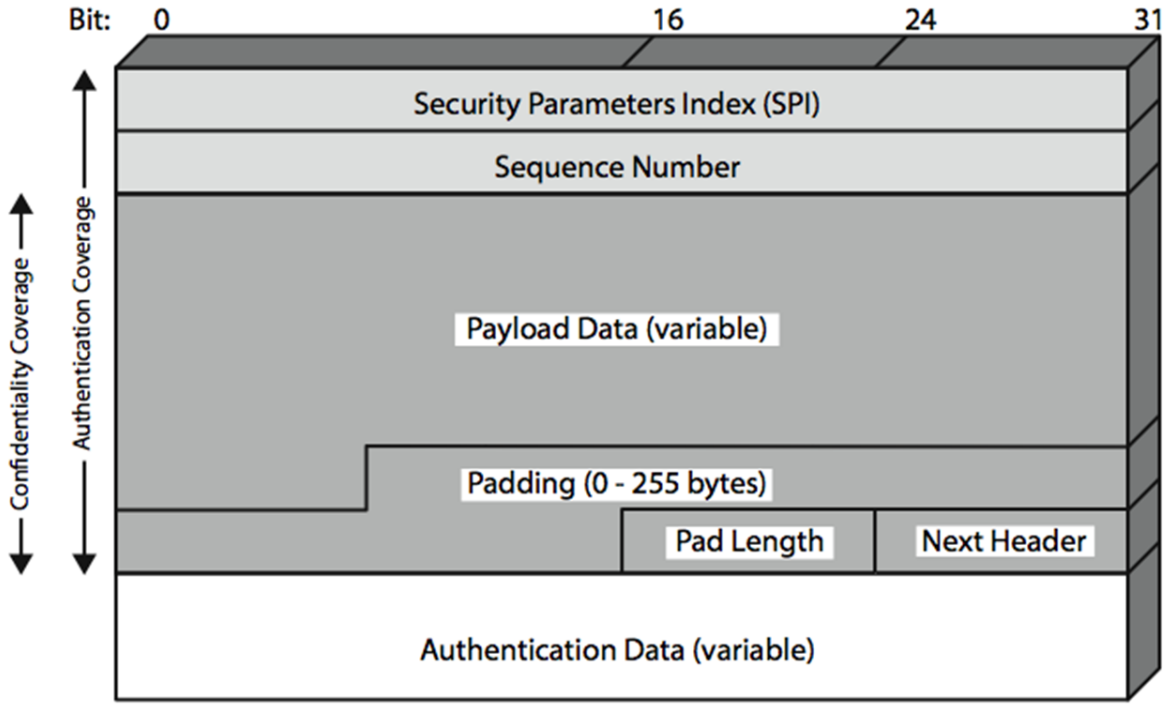




Encapsulating Security Payload (ESP)

- ทำหน้าที่หลักในการ **เข้ารหัสข้อมูล** เพื่อรักษาความลับของข้อมูล
- มีความสามารถในการปกป้องบางส่วนของการไหลของทราฟฟิก (Traffic Flow Confidentiality)
- can optionally provide the same authentication services as AH
- รองรับ algorithm การเข้ารหัสหลายแบบ เช่น
  - DES (Data Encryption Standard)
  - Triple-DES (3DES)
  - RC5
  - IDEA

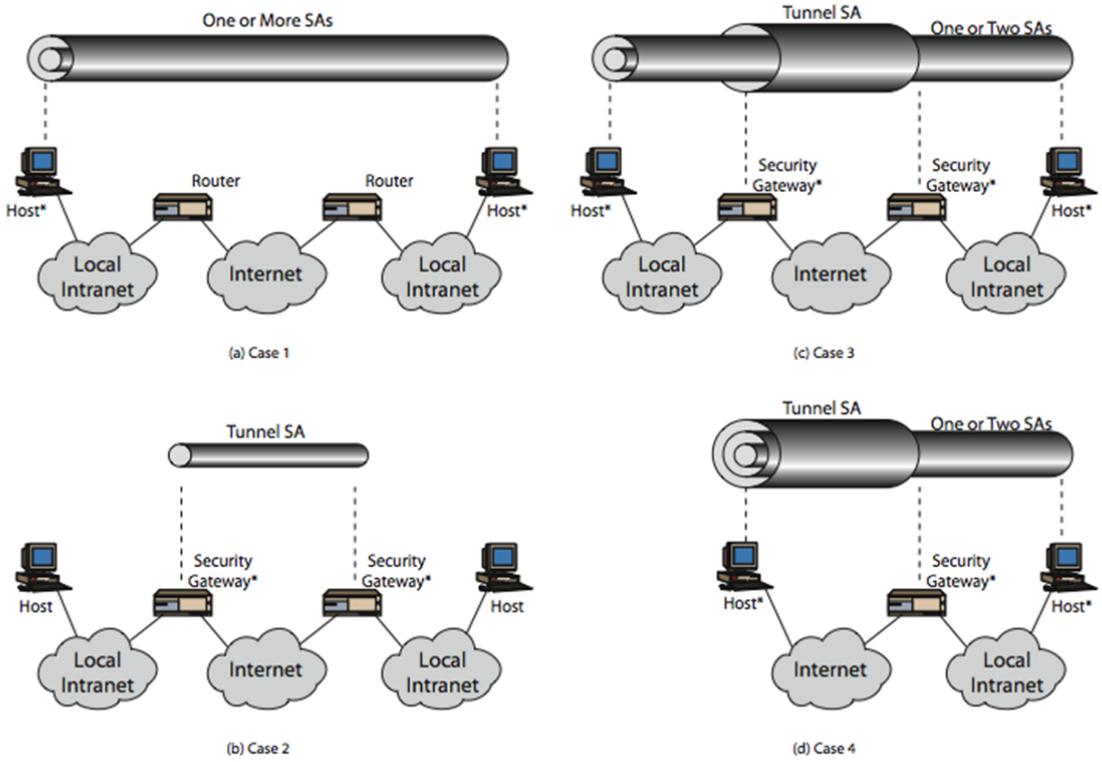
- CAST



Transport Mode vs Tunnel Mode

- Transport Mode
  - เข้ารหัสเฉพาะข้อมูลใน IP Payload แต่ Header ของ IP ก็ยังคง Public
  - สามารถถูกวิเคราะห์ได้ แต่มีประสิทธิภาพสูงกว่า เพราะข้อมูลที่เข้ารหัสมีขนาดเล็กกว่า
  - เหมาะสำหรับ Host-to-Host
- Tunnel Mode
  - **เข้ารหัสทั้ง IP Packet** รวมถึง Header และ Payload
  - สร้าง **Header ใหม่** สำหรับการส่งต่อไปยังปลายทางถัดไป (Next Hop)

- เหมาะสำหรับ VPNs , Gateway-to-Gateway



Web Security

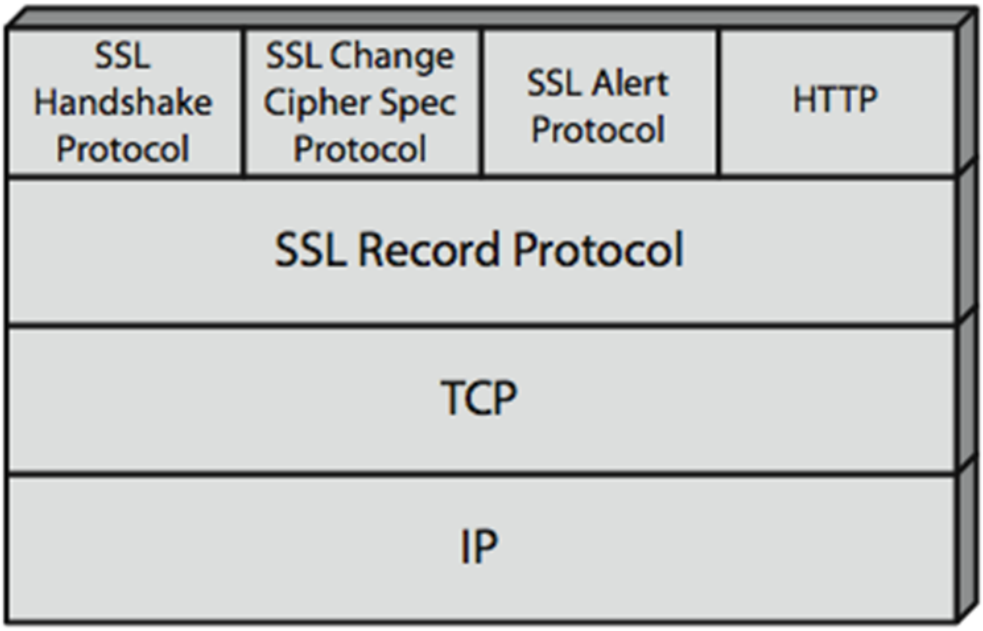
What Is ?

- อย่างที่รู้กันแหละว่า ปัจจุบัน World Wide Web ถูกใช้กันอย่างแพร่หลายและมีความเสี่ยงสูงต่อการถูกบุกรุกในรูปแบบต่าง ๆ เช่น
  - integrity
  - confidentiality
  - denial of service
  - authentication
- เลยจำเป็นต้องมีมาตรการเรื่อง security เพิ่มเติม

SSL (Secure Socket Layer)

- อยู่ใน Transport layer
- พัฒนาโดย Netscape ในตอนแรก ๆ , SSL เวอร์ชั่นที่ 3 พัฒนาและออกแบบจากผู้เชี่ยวชาญภายนอกด้วย ต่อมาเลยกลายเป็น TLS (Transport Layer Security)
- ทำงานร่วมกับ TCP เพื่อการเชื่อมต่อในน่าเชื่อถือของ end-to-end service
- SSL แบ่ง Protocol ออกได้เป็นสอง layer
  - (chatgpt)
  - **Handshake Protocol:** ใช้สำหรับเริ่มต้นการเชื่อมต่อและตกลงวิธีการเข้ารหัส (เช่น การแลกคีย์และการตรวจสอบตัวตน)
  - **Record Protocol:** ใช้สำหรับการเข้ารหัสข้อมูลและรักษาความสมบูรณ์ของข้อมูลระหว่าง

การส่ง



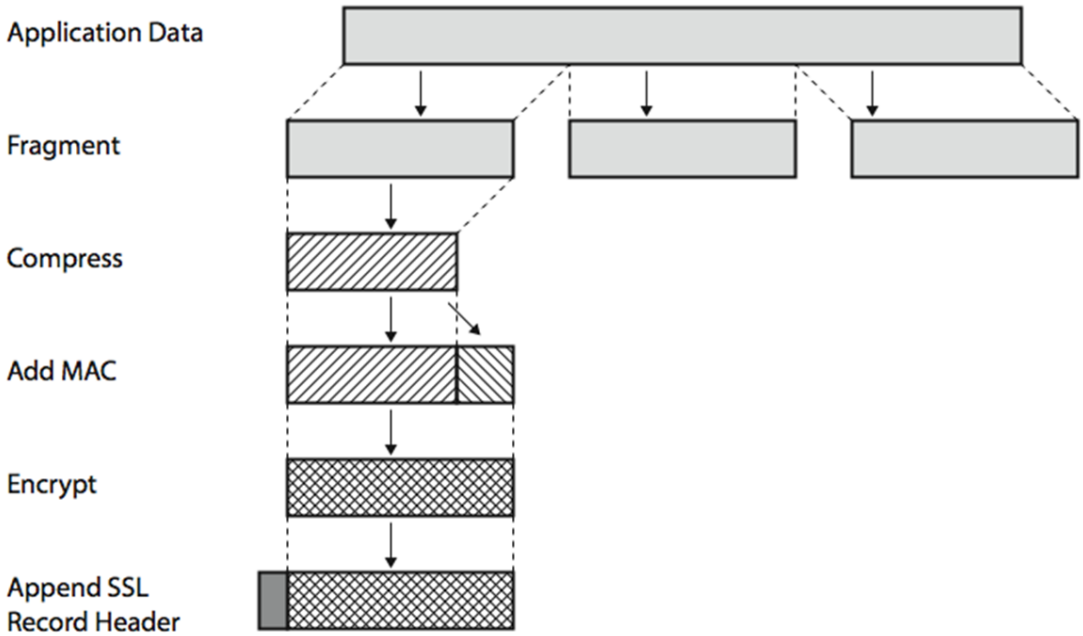
SSL Architecture

- SSL connection
  - เป็นการเชื่อมต่อชั่วคราวแบบ Peer-to-Peer ระหว่างสองฝ่าย
  - เกี่ยวข้องกับ 1 SSL session
- SSL session
  - ความสัมพันธ์ระยะยาว ระหว่าง Client และ Server ถูกสร้างขึ้นจาก HandShake Protocol
  - 1 SSL session ใช้ร่วมกับหลาย ๆ SSL Connections เช่นการเชื่อมต่อกับ server เดิมหลาย ๆ ครั้ง โดยใช้ parameter เดิม

SSL Record Protocol Services

- **Integrity**
  - ใช้ MAC โดยใช้ Shared Secret Key
  - คล้าย ๆ HMAC แต่ต่างกันแค่ Padding
- **Confidentiality**
  - ใช้ Symmetric Encryption ด้วย Shared Secret Key ที่ถูกกำหนดระหว่าง Handshake Protocol
  - รองรับ algorithm ตามนี้
  - AES, IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128

- ข้อความจะถูกบีบอัดก่อนเริ่มการเข้ารหัส



SSL Change Cipher Spec Protocol

- ใช้งานร่วมกับ **SSL Record Protocol**
- มีแค่ 1 Message (Single Message) และทำหน้าที่เดียวคือเปลี่ยนชุดการเข้ารหัส (Cipher Suite) หรือ ทำให้สถานะที่กำหนดไว้ล่วงหน้า (**Pending State**) กลายเป็นสถานะปัจจุบัน (**Current State**)

SSL Alert Protocol

- ใช้สำหรับส่งสัญญาณเตือนเกี่ยวกับปัญหาหรือเหตุการณ์ต่าง ๆ ที่เกิดขึ้นระหว่างการเชื่อมต่อ SSL/TLS
- SSL จะถูกบีบอัดและเข้ารหัสเช่นเดียวกับข้อมูล SSL อื่น ๆ
- แบ่งระดับการแจ้งเตือนได้สองระดับ คือ
  - Fatal Alert → แสดงถึงข้อผิดพลาดร้ายแรงที่ทำให้การเชื่อมต่อต้องสิ้นสุดทันที เช่น ข้อความที่ไม่คาดคิด, MAC ของบันทึกข้อมูลไม่ถูกต้อง , พารามิเตอร์ไม่ถูกต้อง
  - Warning Alert → ปัญหาที่อาจไม่ทำให้การเชื่อมต่อสิ้นสุดทันที แต่ต้องได้รับการแก้ไข เช่น แจ้งการปิดการเชื่อมต่อ, ไม่มีใบรับรอง, ใบรับรองไม่ถูกต้อง

SSL Handshake Protocol

- มีหน้าที่สร้างการเชื่อมต่อระหว่าง server และ client สำหรับ SSL และ TLS
- มีขั้นตอนการทำงานคร่าว ๆ ดังนี้

  1. Establish Security Capabilities

  - server กับ client จะแลกเปลี่ยนข้อมูลเกี่ยวกับความสามารถด้านความปลอดภัย เช่น
  - algorithm การเข้ารหัสที่รองรับ
  - algorithm การสร้าง MAC
  - เวอร์ชันของ SSL/TLS

2. Server Authentication and Key Exchange

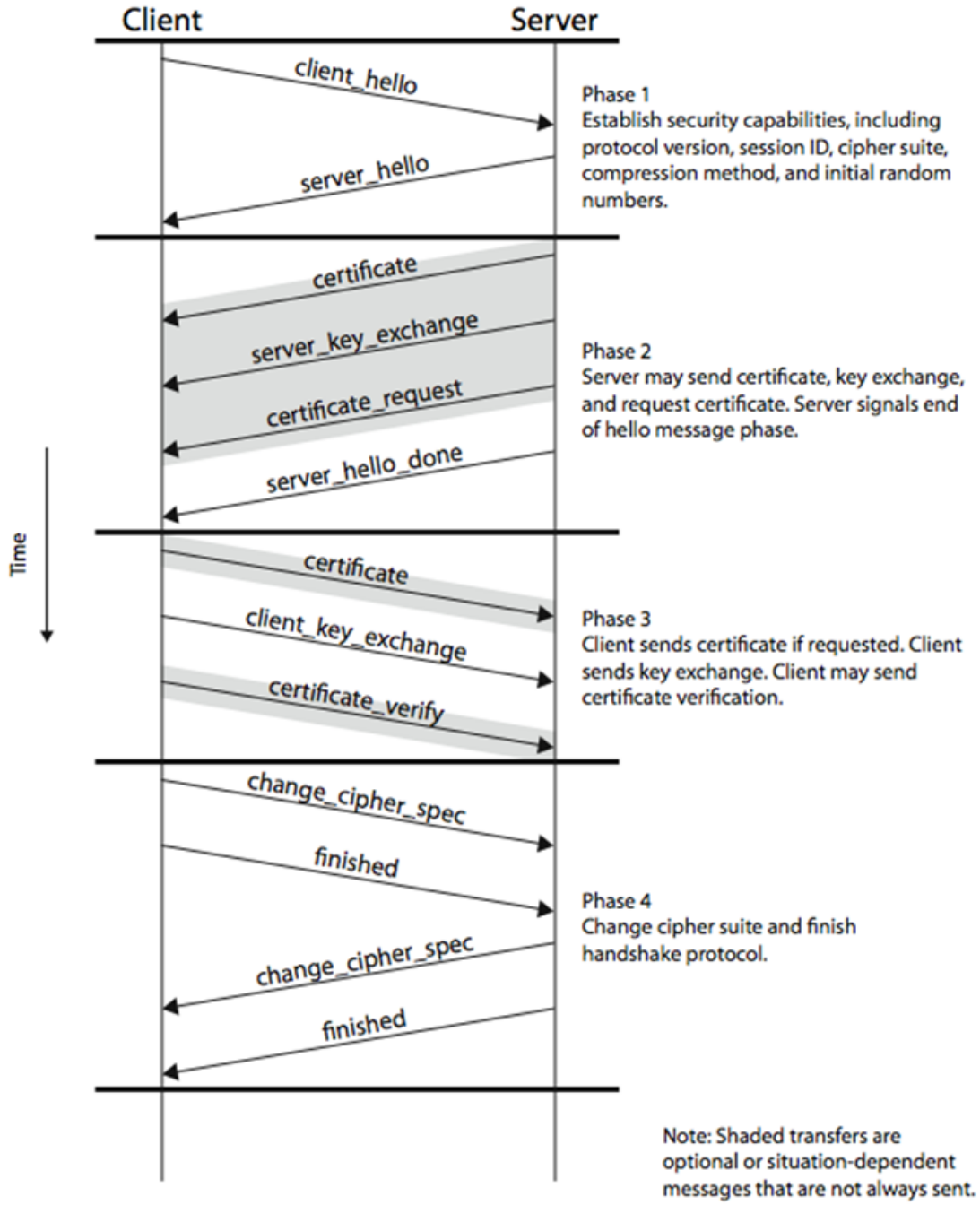
- เซิร์ฟเวอร์จะส่งใบรับรองของตนเองให้กับไคลเอ็นต์
- ไคลเอ็นต์จะตรวจสอบความถูกต้องของใบรับรอง
- เซิร์ฟเวอร์และไคลเอ็นต์จะสร้างคีย์ร่วมกันสำหรับการเข้ารหัสและ MAC

3. Client Authentication and Key Exchange

- หากจำเป็น ไคลเอ็นต์จะส่งใบรับรองของตนเองให้กับเซิร์ฟเวอร์
- เซิร์ฟเวอร์จะตรวจสอบความถูกต้องของใบรับรอง
- เซิร์ฟเวอร์และไคลเอ็นต์จะสร้างคีย์ร่วมกันสำหรับการเข้ารหัสและ MAC

4. Finish

- เซิร์ฟเวอร์และไคลเอ็นต์จะส่งข้อความ "Finish" เพื่อระบุว่าขั้นตอนการจับมือเสร็จสิ้น
- จากนี้ไป การสื่อสารระหว่างเซิร์ฟเวอร์และไคลเอ็นต์จะถูกเข้ารหัสและตรวจสอบความถูกต้องด้วยคีย์ร่วมกัน



TLS (Transport Layer Security)

- เป็น Protocol มาตรฐานของ IETF ที่กำหนดไว้ใน RFC 2246 เป็นการพัฒนาต่อจาก SSLv3 โดยมีการปรับปรุงและแก้ไขข้อบกพร่องบางประการ
- ความแตกต่างหลักระหว่าง TLS และ SSLv3
  - Record Format
  - Version Number
  - **การใช้ HMAC สำหรับ MAC :** TLS ใช้ HMAC (Hash-based Message Authentication Code)
  - **Pseudo-Random Function** : TLS ใช้เพื่อขยาย secrets
  - Additional Alert Codes : TLS มีรหัสการแจ้งเตือนเพิ่มเติม
  - Supported Ciphers : TLS รองรับรหัสการเข้ารหัสที่แตกต่างจาก SSLv3
  - Certificate Types & Negotiations : TLS มีการเปลี่ยนแปลงในประเภทและการเจรจาเกี่ยวกับใบรับรอง
  - Crypto Computations & Padding : TLS มีการเปลี่ยนแปลงในวิธีการคำนวณและการเติมข้อมูล

Server Security

Threats to Hosts

The Problem

- บางครั้งการโจมตีก็มุ่งเป้าหมายไปที่ Host อย่างเลี่ยงไม่ได้ ทำให้จำเป็นต้องทำให้แข็งแกร่ง (hardened)

What is Host?

- อะไรก็ตามที่มี IP (เพราะสามารถถูกโจมตีได้)
- เช่น Servers , Clients (including mobile) , Routers (including home access routers) and sometimes switches , Firewalls

Elements of Host Hardening (องค์ประกอบ)

- Backup
- Restrict physical access to hosts
- Install the operating system with secure configuration options
- Change all default passwords, etc.
- Minimize the applications that run on the host
- Harden all remaining applications on the host
- Download and install patches for operating system vulnerabilities
- Manage users and groups securely
- Manage access permissions for users and groups securely
- Encrypt data if appropriate

- Add a host firewall
- Read operating system log files regularly for suspicious activity
- Run vulnerability tests frequently

Security Baselines and Systems Administrators

มาตรฐานความปลอดภัยและผู้ดูแลระบบ

Security Baselines Guide the Hardening Effort

- Specifications for how hardening should be done → ระบุขั้นตอนและวิธีการที่จะนำไปใช้ Hardening
- Needed because it is easy to forget a step → มาตรฐาน security ช่วยให้มั่นใจว่าไม่มีขั้นตอนไหนถูกข้าม
- Different baselines for different operating systems and versions → มาตรฐาน security จะแต่งต่างกันไปตาม OS กับ เวอร์ชัน
- Different baselines for servers with different functions
- Used by systems administrators
- Disk Images
    - เวลาเรามีหลาย ๆ เครื่องเซิฟเวอร์ เราก็สร้างการใช้งานที่ปลอดภัยและผ่านการทดสอบแล้ว บันทึกเป็น Disk Images แล้วก็เอาไปโหลดใส่ Server อีกเครื่อง

Virtualization

- เทคโนโลยีที่ช่วยให้สามารถรันระบบปฏิบัติการหลายระบบอย่างอิสระบนเครื่องเดียวกัน
- Multiple operating systems running independently on the same physical machine → ทำให้สามารถทำประโยชน์จากฮาร์ดแวร์ได้เยอะกว่าเดิม
- System resources are shared → แบ่ง resources ข้าม vm ได้
- Increased fault tolerance → เพราะสามารถย้าย OS ข้าม Host ได้ทันที
- Rapid and consistent deployment → สามารถสร้าง template os แล้ว copy ไปวางเพื่อ deploy งานเพิ่มเติมได้เลย
- Reduced labor costs → ช่วยลดความซับซ้อนในการจัดการระบบและลดต้นทุนแรงงาน

Windows Server Operating Systems

Windows Server Security

- Intelligently minimize the number of running programs and utilities by asking questions during installation
- Simple (and usually automatic) to get updates
- Still many patches to apply, but this is true of other operating systems

Vulnerabilities and Exploits

Vulnerabilities

- Security weaknesses that open a program to attack → ช่องโหว่คือจุดอ่อนในโปรแกรมที่สามารถถูกใช้โจมตีได้
- An exploit takes advantage of a vulnerability → exploit หรือการโจมตีคือการกระทำที่ใช้ประโยชน์จากช่องโหว่เพื่อเข้าถึงระบบหรือข้อมูล
- Vendors develop fixes → เมื่อพบช่องโหว่แล้ว ผู้ที่ขายซอฟแวร์จะพยายามแก้ไขเพื่อปิดช่องโหว่
- Zero-day exploits → exploits ที่เกิดขึ้นก่อนผู้ขายจะแก้ไขช่องโหว่
  - https://youtu.be/yi8X6qfT1-0?si=ZOeeHuF5TFRh-fC9
- Exploits often follow the vendor release of fixes within days or even hours → ผู้โจมตีมักจะค้นหาและใช้ประโยชน์จากช่องโหว่ทันที หลังจากที่ผู้ขายปล่อยการแก้ไข
- Companies must apply fixes quickly

Fixes

- Work-arounds (วิธีแก้ไขปัญหาชั่วคราว)
  - การดำเนินการที่ผู้ดูระบบหรือผู้ใช้ทำเพื่อบรรเทาผลกระทบ ก่อนที่จะมีการปล่อยแพตช์แก้ไขทางการออกมา
  - ใช้แรงงานมาก จึงมีต้นทุนสูงและเสี่ยงต่อข้อผิดพลาด
- Patches
  - โปรแกรมขนาดเล็กที่แก้ไขช่องโหว่
  - มักดาวน์โหลดและติดตั้งได้ง่าย
- Service packs
- Version upgrades

Problems with Patching

- Must find OS patches
  - Windows server จะทำเองโดยอัตโนมัติ
  - LINUX often use rpm (RedHat Package Manager)
- Companies get overwhelmed by number of patches
  - ผู้พัฒนาปล่อย Patch หลายตัวต่อโปรแกรม
  - Especially a problem for a firm’s many application programs
- Risks of patch installation
  - function บาง function อาจจะหายไป
  - อาจทำให้เครื่องค้างหรือเสียหาย บางครั้งไม่สามารถถอนการติดตั้งได้
  - แก้ปัญหาด้วยแก้นำไปลงที่เซิฟเวอร์จำลองก่อนลงเซิฟเวอร์จริง ๆ

Managing Users and Groups

- Account → user แต่ละคนจะต้องมี Account
- Groups → กลุ่มของ Accounts ช่วยให้การให้สิทธิง่ายขึ้นไม่จำเป็นต้องไปให้ทีละคน เช่น กลุ่มของนักเรียนสามารถเข้าถึงโปรแกรมนี้ได้ ก็แค่แอด Account นักเรียนเข้ากลุ่ม แล้วตั้ง Permission ให้ Group อีกที

Resource

- (pptx) 05 IP Security
- (pptx) 06-07 Server Security
- https://aws.amazon.com/th/what-is/ipsec/