

Advanced Encryption Standard

010

4

AES

Sub Shift Mix Add

1 Plaintext

128	10
192	12
256	14

ເຄື່ອນຈາກຫັນໄປໃນເລົ່ງ
ທີ່ລະຫວ່າງນີ້ມາດີ

2.1 Key

2.2 ① ⊕ ②.1

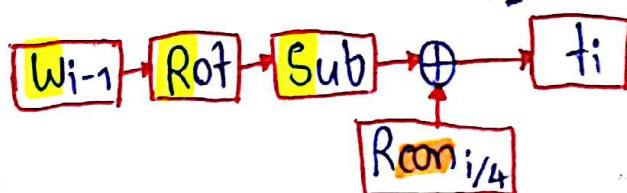
3 SubBytes [ແປສູ່ຢັ້ງຕົວຍັກເຊີງ ຈາກຕາງໆ]

4 Shift Rows [ແກ້ວແຮກເລື່ອນ 0 ແລ້ວ ລົດກ່າຍເລື່ອນ 3]

5 MixColumns [④ × $\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$ ດັກກິນ % modulus]

6.1 Round key [$t_i = \text{Sub}(\text{Rot}(w_{i-1})) \oplus Rcon_{i/4}$]

6.2 Add Round Key [⑤.1 ⊕ ⑥.1])



* Structure.

state 2.2

SubBytes

state 3

Shift Rows

Rcon i/4

state 4

MixColumns

state 5

AddRoundKey

state 6.2

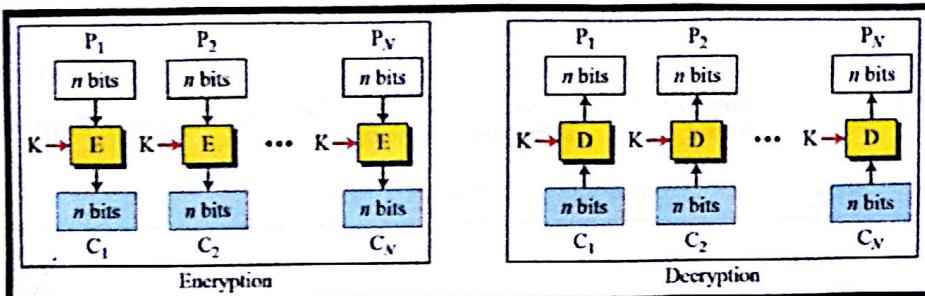
- SubBytes : ແປສູ່ຢັ້ງຕົວຍັກເຊີງ
- ShiftRows : ແປສູ່ຢັ້ງໂຄງລຽງ
- MixColumns : ແປສູ່ຢັ້ງຄວາມກົງ
- AddRoundKey : ຍັດຄົ່ງໄຂໝາລີໃນປົກກາມ

๑๑

Modes of Operation

① ECB

โครงสร้างการเข้ารหัสข้อมูลที่มีขนาดหน้างานหลาย
เพริ: AES รองรับที่ 128 Bit / Block



- ▶ เป็น Block cipher กัน ถ้าเหลือไว้ล่วงไม่ครบ (Pad)
- ▶ ถ้ามี Bit ใน Block ไหน เสียหายจำนวน n Bit
ผู้รับจะรับเสียหายเป็น n Bit ใน Block นั้นๆ ก็ได้น

ข้อดี

- ▶ ง่าย, สะดวก, ผู้รับเสียหายแค่ Bit ที่เสียหายก็พอ

ข้อเสีย

- ▶ ไม่เชิงลับ สำหรับการใช้งานที่บังคับความลับมากๆ เพรา จะใช้ Key เดียวในปัจจุบันมากเกินไป

- ▶ ข้อความใช้ฟอร์แมต Block ซึ่งไม่มีความเชื่อมโยงกัน
อาจส่งผลให้คนร้ายตั้งงบของความไว้ เนื่องจาก

▶ อาจจะแบบลénช์ (Replay attack)

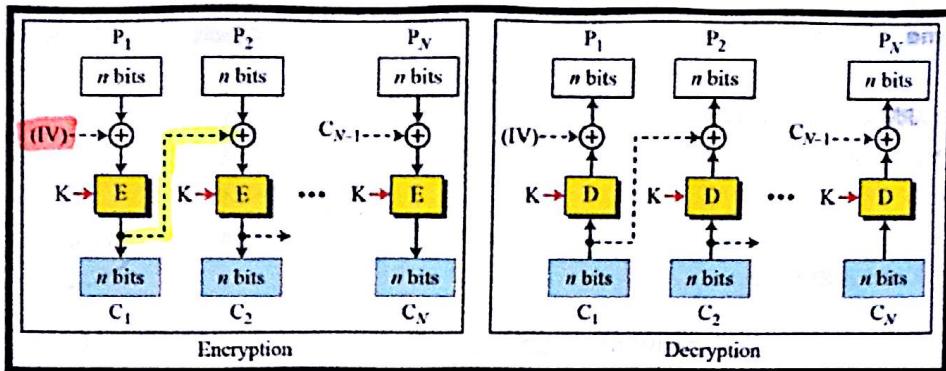
▶ อาจจะพยายามแทรกไฟล์ (Packet injection attack)

ข้อดี

- ▶ ข้อความต้นฉบับตรง มีขนาดสั้น สามารถบรรจุลงในข้อความ
บล็อกได้หมด
- ▶ Ciphertext สามารถแปลผลส่วนๆ ได้หากร้าห์มาก
Plaintext ทั้งหมด key นั้น

๐๑๖

② CBC * Popular กันมาก !!



- ▶ สร้างความสัมพันธ์ รับฟังกุบัน | C ก่อนหน้า ถ่าย ④
- ▶ Block แรกต้องใช้ เวลาต่อรองไว้เมื่อครั้งแรก นั่นจะไม่มี ค่าก่อนหน้า

ข้อดี

- ▶ ความสัมพันธ์ระหว่างบล็อก ลับๆ ให้ยากต่อการแบบ C
- ▶ เนื่องจากส่วนใหญ่ของข้อมูลที่มีการเข้ารหัสงานมากๆ และมี ข้อมูลเพียงกรุณาเข้ารหัสล่วงหน้า

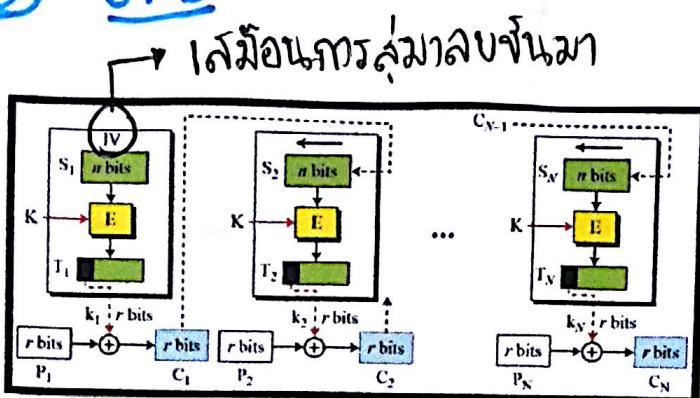
ข้อเสีย

- ▶ ไม่สามารถเข้ารหัสชิ้นๆ ของแต่ละหน้าได้
 - ▶ หากต้องดึงผลลัพธ์ของลักษณะการเข้ารหัส 1 Block จำเป็นต้องรับรู้ถึงการถูกตัดเป็น Plaintext ที่ 2 Block
- Ex ก้า [2] เสีย => [2] เสียมากสุด เพราะเราผิดตัวเสีย
มาเข้ารหัส ก้าในเมืองซึ่งมีอยู่หลายเมือง ॥ และ [3] เสีย ก้า นิติ เพราะเราผิดตัวเสีย ④ ก้าบบังต้าเสีย ก้า

ข้อรุม

- ▶ CBC ถูกประยุกต์ใช้สำหรับการ Authentication ถ่าย
- ▶ ចั่ง ค่า CRC คือค่าใช้โน้มถ่วง

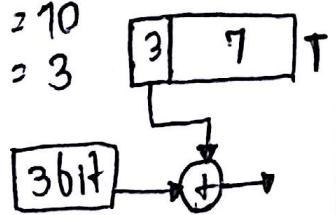
③ CFB



ล่มชั่วโมง

$$k = 10$$

$$r = 3$$



- $r \leq k$, ต้องให้หลักการทั่วไป
- รองรับกรณีที่ PlainText (x Bit) มีขนาดเล็กกว่า Block ของผลลัพธ์ที่รับเข้าร่วม (y Bit) มาก
- ใช้มีดผู้ส่งไม่สามารถคาดเดา PlainText บล็อกถัดไป
มาร่วมกันจนได้ PlainText ขนาด Bit น้อย ($stream$)

ข้อดี

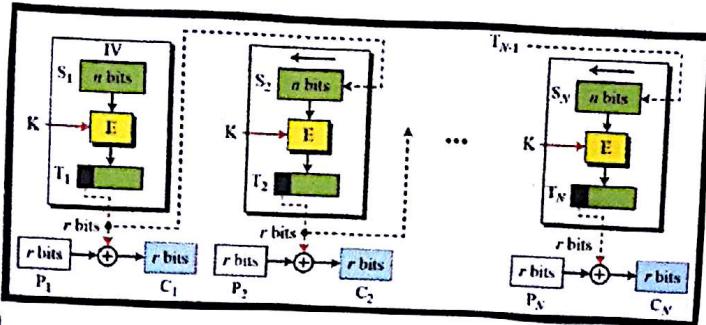
- สามารถถ่ายทอดข้อมูลแบบ Stream ได้ (เนื่องจาก)
- เช่น สำหรับการยืนยันตัวตน

ข้อเสีย

- ถ้ามี Bit เสีย จะล่งผลกระทบต่อการถอดรหัสทั้งหมดใน Block นั้นๆ แล้ว Block ถัดไปจะเก็บ Bit ก่าเสีย
จากการ Shift ลงมาไปจนหมด
- ข้อดีที่ 2 หมายความว่า Bit

๐๑๖

④ OFB (บางครั้งเรียก Internal feedback)



- แก้ปัญหาค่าผิดผลลัพธ์แพร์กราจายของไนน์ด CFB
- นำผลลัพธ์จากการเข้ารหัส IV ที่มีมาต่อไปรับ Plaintext มาบรรจุใน IV แทน
- ฝ่ายรับท่องฝ่ายส่งตรง Synchronization ร้าน เชื่อมโยงการถอดรหัสกับการผิดพลาด

ข้อดี

- กระบวนการซ่อนทางลับสาร มีประสิทธิภาพกว่า CFB
Ex กรณีลับสัญญาณด้วยความเร็วของโทรศัพท์มือถือ
- ลดผลกระทบของการผิดพลาดลง

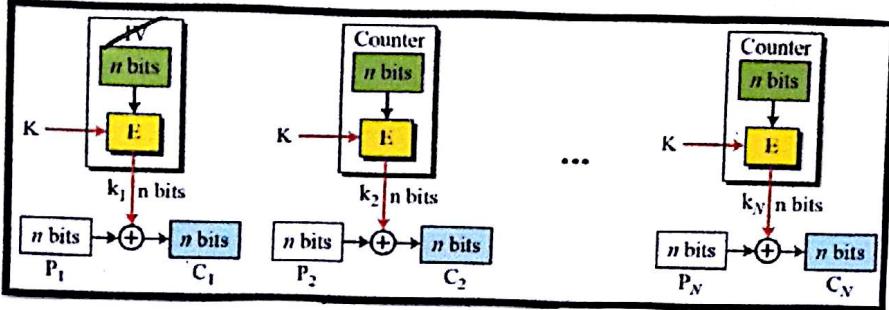
ข้อเสีย

- เนื่องจากไม่มีความสมบูรณ์ที่สุด: อาจมีข้อมูลที่ไม่ถูกรหัส化มากกว่าหนึ่ง比特 CFB

๐๑๐

⑤ CTR

Counter



- คล้าย OFB แต่เปลี่ยน IV เป็น Counter แทน
- Counter จะเน้นที่จะใช้ในการเข้ารหัส Plaintext ใน Block ต่อไป
- ในความหมายของเครื่องหมาย
- Ex: IPSec, ATM network

ข้อดี

- กระบวนการเข้ารหัสและการถอดรหัสสามารถทำแบบขนานได้,
- ขั้นตอนสั้น
- มีประสิทธิภาพดีกว่า OFB

7

Chapter: Network Security

๑๑

Firewalls

- ▶ แนวคิดการของร่างดินเผาไม่ต้องอ่านล่า
NP ก็คือไม่ปลอดภัยๆ
- ทำหน้าที่ควบคุมการเข้าถึงระหว่าง Network ภายในและภายนอก
-
- ▶ NP ก็จะเป็นภัย
เรื่องของ

ชนิดของ Firewalls

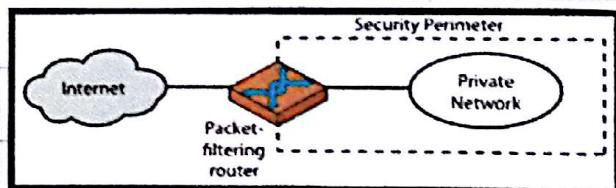
① Packet filter !!!

- ▶ เป็น router ที่ทำการเลือกและส่งต่อเดินทางไป
- โดยตรวจสอบ header ของ packet ที่เข้ามา เกี่ยวกับกฎที่กำหนดไว้
 - ↳ อาจจะเป็น Allow หรือ Drop ??
 - ↳ อย่าลืมกำหนดกฎ Default ไว้ด้วย
เมื่อรับการอนุญาตอยู่แล้วก็ต้องยกเว้น

▶ ข้อดี: ง่ายและเร็ว
ในชั้นกัน Application

▶ ข้อเสีย: ความปลอดภัยสูง

http : 80
https : 443



①	Can a HTTP connection reach the web server?
②	Can a HTTPS connection reach the web server?
③	Can a Telnet connection reach the company server at 202.6.7.10?
A	Allow TCP anyIP:anyPort [out] to 202.6.7.8:80 [in]
B	Drop any anyIP:anyPort to 202.6.7.8: anyPort [in]
C	Allow TCP anyIP:anyPort [out] to 202.6.7.8:443 [in]

- ① A Allow
② B Drop
③ ไม่เข้าอยู่ในลิสต์

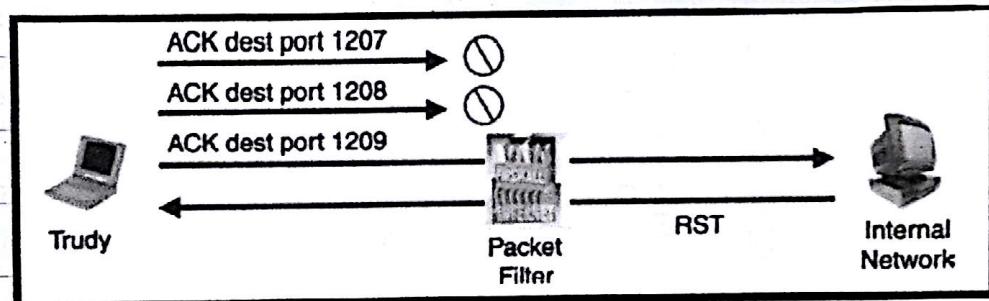
Drop any anyIP:anyPort to anyIP:anyPort ← Default
[out] [in]

↳ Attacks on Packet Filters

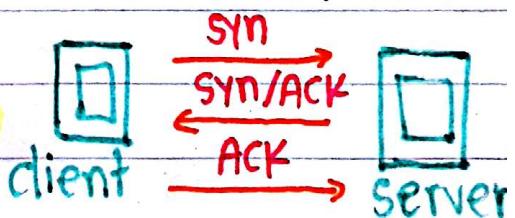
- สร้าง IP ปลอมเข้ามา
- ท่าทาง routing เอง
- พยายามยกเว้นหน่วยงาน packets

↳ พยายาม Drop ไปบางส่วน บางส่วนยังคงอยู่

↳ TCP ACK scan attack



- เป็นการทดสอบเชื่อมต่อ Port ไหนเปิดอยู่บ้าง?
 - ↳ ถ้ามี Port ไหนเปิด RST จะตอบกลับ
 - ↳ ถ้าไม่มี Port ไหนเปิดก็จะไม่ส่ง回包 Packet นั้น
- เป็นการตรวจสอบว่า Firewalls ตั้งค่าไว้ตามค่าที่ควรจะค่าของ Packet อย่างถูกต้องหรือไม่
- ใช้คลิก TCP three-way handshake



ข้อสังเคราะห์: * เมื่อเราไม่มีการจัดการ state ลังก์กี้จะเป็น Attack แบบนี้ได้

ที่ให้รู้ว่า Packet นั้น เป็น Packet ที่เข้ามายังช่องทางเดียว

② Stateful packet filter !!!

- เพิ่มข้อมูลของ State เข้าไป เนื่องจากใช้สำหรับ stateless
↳ แก้ปัญหา TCP ACK scan attack (ข้อส่อ)
- ทำได้แค่ชั้น Transport layer จึงทำให้...
 - ↳ ไม่สามารถดูชั้นข้อมูลจากชั้น Application layer
เนื่องจากชั้น Application layer ไม่สามารถเข้าถึงชั้น Transport layer ได้ (ข้อเสีย)
- ต้องเนื้อหนึ่งใน RAM ในการเก็บชั้นข้อมูลแล้วกันการตรวจสอบจึง..
↳ ทำงานช้ากว่า packet filtering firewall ปกติ (ข้อเสีย)

③ Proxy servers !!!

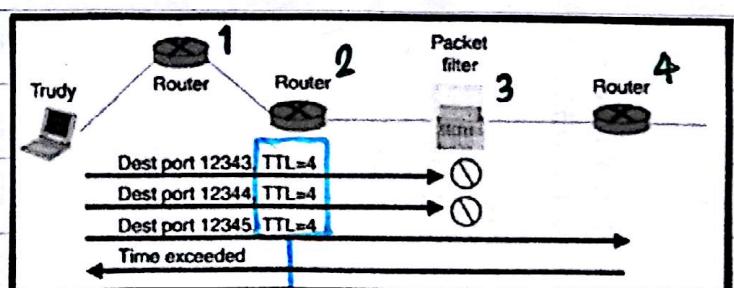
- มีการตรวจสอบข้อมูลที่ในชั้น Application layer
- ตรวจสอบความถูกต้องของ packet, รู้ว่า packet มาจากไหนบ้าง
- เช่นมาสั่งรับ Application ที่สำคัญมากๆ
- อุปกรณ์ security และ performance ได้ดีและยังดี

ข้อส่อ : มีความปลอดภัยสูง | สามารถป้องกัน Firewall ได้
รู้จักข้อมูลในชั้น Application layer

ข้อเสีย : ทำงานช้า

↳ Firewall

- มี ICMP คือยังคงติดต่อ
packet อยู่ก่อนถึง Server



↳ วิ่งได้ 4 hop

DMZs

↳ Demilitarized zone

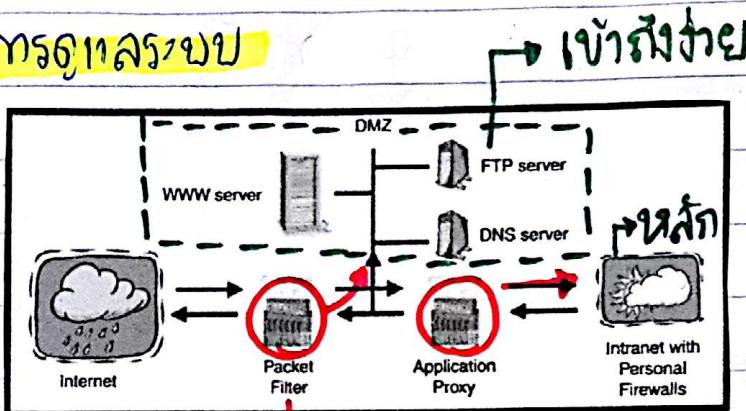
- คุณภาพสามารถท้าทาย Ex Web servers, mail servers

↳ Defense in depth

- เป็นวิธีการที่ดีที่สุดในการต่อต้านภัย

- ต้องมีชั้นหลายชั้น

- ป้องกันในลักษณะที่ต้อง



เข้าร่อง่าย

หลบ

หลบ

เข้าร่อง่าย

Intrusion detection systems (IDS)

- เป็นระบบที่ใช้ตรวจสอบการบุกรุก เพื่อไม่ให้ภัยทางภายนอก
ที่ไม่ได้ผ่านเครือข่ายและต้องต่อเนื่องกัน

- Future : IPS (ป้องกัน)

- มี 2 methods

↳ Signature-Based IDS [detect known]

↳ Anomaly-based IDS [detect unknown]

- มี 2 basic architectures

↳ Host-based IDS [ดูการบุกรุกในเซิร์ฟเวอร์]

↳ Network-based IDS [ดูการบุกรุกในเครือข่าย]

↳ Methods

① Signature-Based IDS ??

- ตรวจสอดโดยใช้ Signature ของป้อมล หรือ patterns
- ถ้าคุณเขียนการโจมตีไว้แล้ว จะสามารถป้องกันได้

ข้อดี : ง่าย

ข้อเสีย : ไม่สามารถป้องกันการโจมตีที่ไม่รู้จัก (Detect unknown attacks)

② Anomaly-Based IDS ??

- สามารถ Detect unknown attacks ได้
 - ↳ ต้องแยกระหว่าง normal กับ abnormal ใช้เกณฑ์
 - กฎการทำงานปกติ ↳ การทำงานไม่ปกติ

↳ Basic architectures

① Host-based ??

- ระบบที่ค่อยเฝ้าระวังและตรวจสอบความผิดปกติที่จะบุกรุกได้
- ไม่สนใจ network activities

Ex ไม่ให้เข้ามาแต่ดำเนินไปเฉยๆ

② Network-based ??

- ระบบที่ค่อยตรวจดู Packet ที่วิ่งอยู่ในเครือข่าย ภัยการบุกรุกหรือไม่
- ไม่ค่อยถูก host-based attacks (ไม่สนใจ)

Ex การพยานทางลักษณะ Port ต่างๆ

ข้อเสีย : ต้องฝ่ายต่อแหล่งเนื้อหาหนึ่งของตนเอง
ในส่วนที่ฐานะของดูแลอยู่ เก่านั้น

Honeypots

↳ เป็นเครื่องมือที่ใช้ส่อ Attacker (Hacker)

- ทำจากบุคคลที่ประสงค์จะเข้ามาในระบบ เพื่อฟังกลับยไว้ส่อ Attacker
- เผ่าตู้ๆ Attacker สามารถปะน้ำหน้าให้รับซื้อโดยหุ่นใจล้วงๆ แล้วนำไปปลูกจุดติดตามได้ง่ายขึ้น
- ส่วนใหญ่จะใช้ใน Production และ Research

ข้อควรระวัง : ไม่ควรใช้รันเน็ตใน Server หลัก

Sessions vs connections

↳ sessions : มีหน่วย connection 7 ตัว

↳ connections : ลักษณะเป็นตัวชี้วัดของเครือข่ายที่สำคัญมาก

Ex ตัวอย่างเช่น con... หมาย พลายนี้บลําย เน็ตเวิร์กเดือนต่อเดือน
เพรา sessions มีการรีบบังคับไว้

security at the Transport Layer

- end-to-end security

↳ Entity authentication : ทำการผูกจัดตั้งงานกัน

↳ message integrity : ข้อมูลที่ส่งมาต้องครบถ้วน

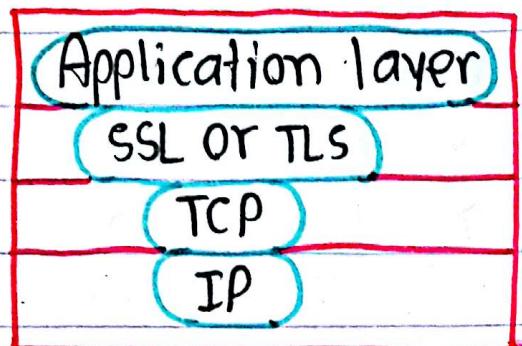
↳ confidentiality : ต้องมีการบันทึก

- SSL & TLS

↳ SSL } https = http + SSL & TLS

↳ TLS }

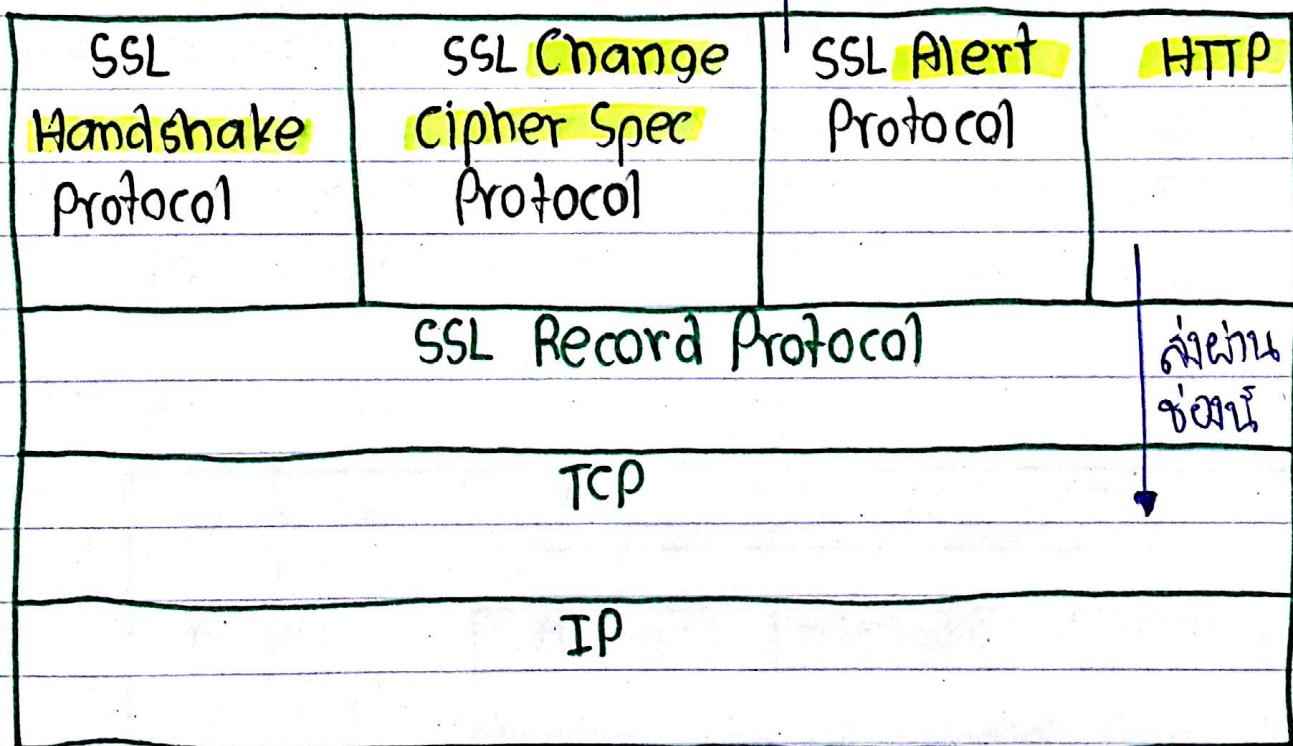
Secure Sockets Layer Protocol



→ รับ Data จาก Application layer
แล้วส่งไป TCP

SSL Protocol Stack

→ รู้ Errror ที่ไม่ค่อยต่อตัน



SSL provides

- ใช้ symmetric-key ในกระบวนการเข้ารหัส
- ใช้ asymmetric-key ในกระบวนการเข้ารหัส
- มีการ check ตรวจสอบความถูกต้องของข้อมูล

ทุกข้อ
[เต่า]

SSL

- Record protocol สำคัญ... จะล่องดูไปเช่นกันฯ ไม่ใช่
- Handshake protocol สำคัญ... client/server และการเปลี่ยน
- ChangeCipherSpec สำคัญ... จะมีการระบุว่าใช้งานไห้หรืออย่าง
- Alert protocol สำคัญ... จะไม่ทราบมาเมื่อเกิดการ Errors ของทาง
การส่งข้อมูล

ข้อมูลกินໄมไว้

SSL Record Protocol

- รับงานครุภัณฑ์จาก Application layer ที่แล้ว รวมถึงข้อมูลมีมาจากการ

Application layer ด้วย

- // → มีการเข้ารหัส (Confidentiality) } 2 บรรทัด
- // → มีการสร้าง MAC (Message Authentication) } ไม่เจ้า !!
- Confidentiality : ในกรอบเดียว } มีการต่างๆ กัน Key
- Message integrity : ที่ใส่ใน MAC } ที่ใช้ร่วมกัน ...

SSL Record Protocol Operation

ยก

Application Data

ต่อ

Fragment

ข้อมูลที่รับมาจากชั้น Application

ปั๊บ

Compress

214 bytes

แบบ

Add MAC

หัวอนุญาติ

เข้า

Encrypt

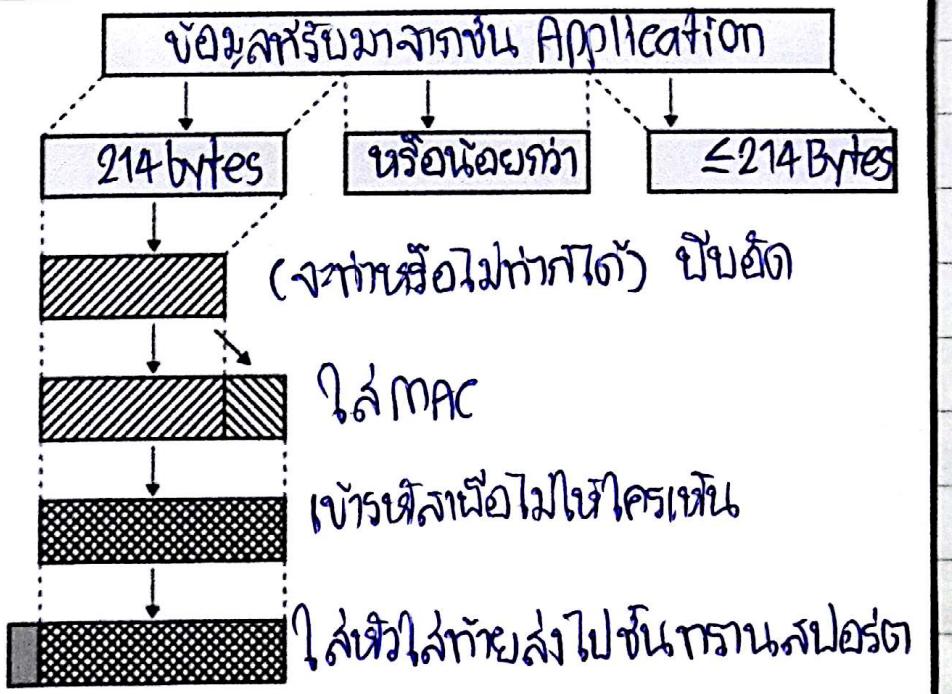
ใส่ MAC

ส่ง

Append SSL
Record Header

เข้ารหัสไม่ให้ใครเห็น

ใส่เข้าไปก่อนไปเชื่อมต่อ



SSL Handshake Protocol

- ทางลงที่สถาปัตย์ parameters ที่นิยมใช้ระหว่าง Client/Server
- // ↳ Phase 1 : Client / Server ทางลงที่สถาปัตย์ที่มีอยู่ในรากน้ำ
- ↳ Phase 1 : ครึ่ง Client/Server ที่อยู่ในรากน้ำ ทางลงที่สถาปัตย์
 - ↳ Phase 2 : ข้อมูล Parameter จาก Server → Client
 - ↳ Phase 3 : ข้อมูล Parameter จาก Client → Server
 - ↳ Phase 4 : ห้องลงส์ Data ให้กันเพื่อใช้ในการเข้ารหัส, เลือก

Change Cipher Spec Protocol

- ใน SSL Record Protocol
- เก็บ State ของลูกค้าสำหรับใช้งานต่อไปแล้ว

Open SSL "Heartbleed" Bug

- ↳ เกิดจากบัญชี Buffer over-read
- ↳ กรณุจุดที่ใน memory ที่ content อยู่ภายในตัวตัด
โดยรอบๆ ไปขนาด 64K
 - ↳ 64K ที่อยู่ภายในอาจจะได้ key หรือ session ไปได้ !!

Transport Layer Security

- ไม้ร่องรุ้ง Fortezza
- ซึ่งรองรับ SSL
- ใช้ Pseudorandom function

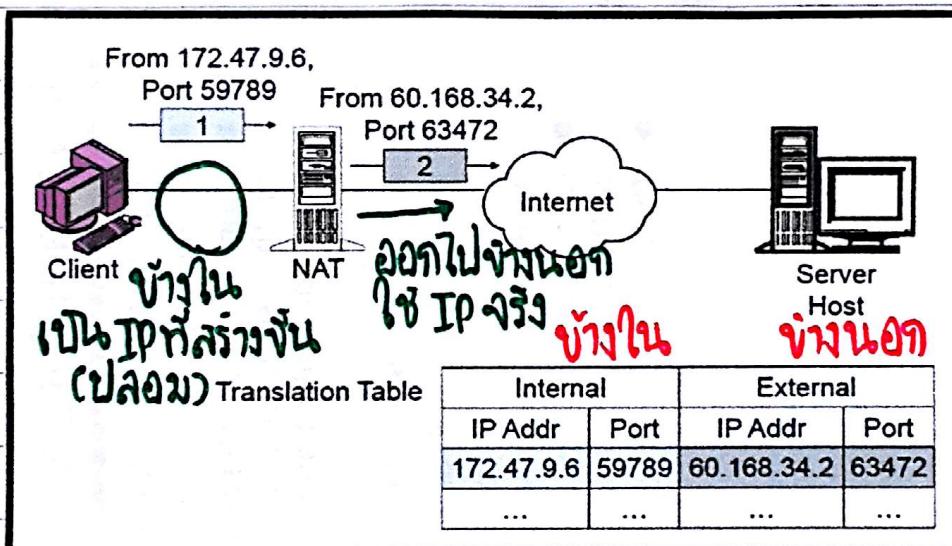
Security at the Network Layer

- เพิ่มภาระต่อไปยังเครือข่ายที่น่าเชื่อถือ เช่น การเข้ารหัสก่อนส่ง

Virtual Private Networks (VPN)

- เป็นการสร้างสื่อสารทางการซึ่งมีต่อที่มีความลับและปลอดภัย
ข้อดี : ถูก, ง่าย (public network)
มีความปลอดภัย, มีความน่าเชื่อถือ (private network)

Network Address Translation (NAT)



- ▶ ด้านนอก : ต้องติดตั้งมาตราฐานเครือข่าย, port ไหน
จะต้องเปิดให้เข้า, port ไหนปิดให้
- ▶ ด้านใน : ต้องติดตั้งตัวตัดหน้าที่ควบคุมการทำงาน

*** สำคัญมากที่สุด โปรต์ที่ต้องบล็อก
สำหรับ IP ภายในทุกๆ เครื่องที่ผ่านไม้กรองด้วย
ซึ่งปัจจุบันมีภัยคุกคามของไวรัสที่มาก

IPSec

- ↳ ชุดของโปรโตคอลที่มีไว้สำหรับ Network Layer โดยเน้นไปที่
- ↳ เมื่อต้องมีส่วนของ Networking Device with IPSec ป้องกันจาก User เลย

- มี 2 modes

↳ Transport mode [จะไม่ยุ่งกับ IP-H]

↳ Tunnel mode [พิ้น IP-H ไปทางล่าง]

- มี 2 security protocols

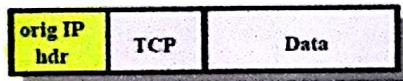
↳ AH [Check ตรวจสอบเปลี่ยนแปลงของข้อมูล]

↳ ESP [มีการเข้ารหัส]

Original

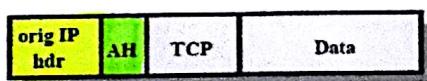
AH

IPv4



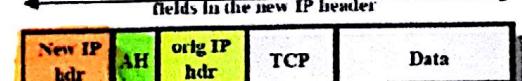
← authenticated except for mutable fields →

IPv4



authenticated except for mutable fields in the new IP header

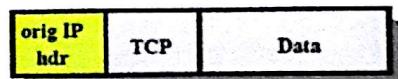
IPv4



Transport
Mode

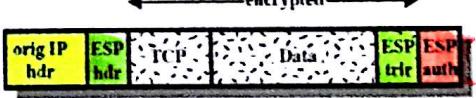
ESP

IPv4



← authenticated → ← encrypted →

IPv4



← authenticated → ← encrypted →

IPv4



Tunnel
Mode