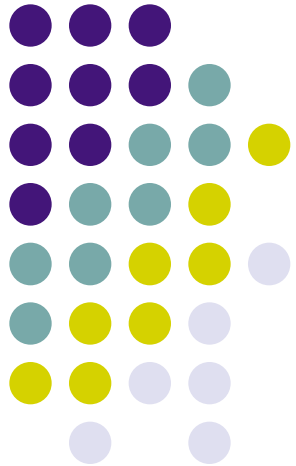
Authentication System

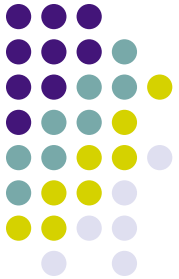
Mr.Jantapong Boodluck

Electronic Computer Technology

King Mongkut's University of Technology North Bangkok



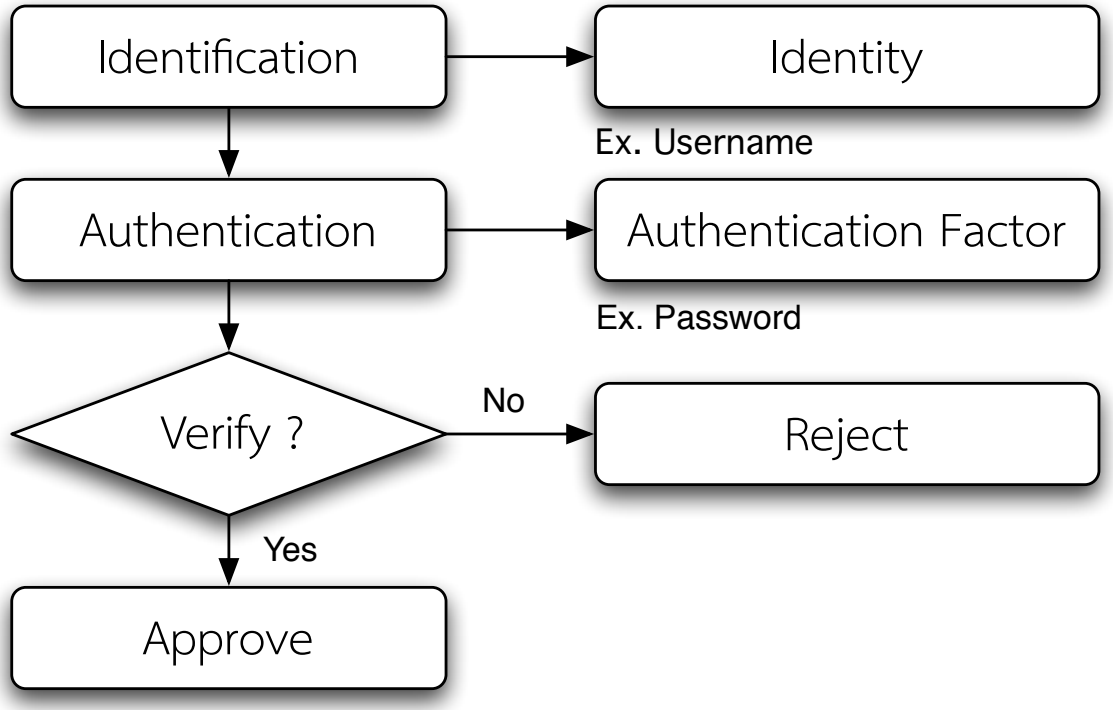
Outline



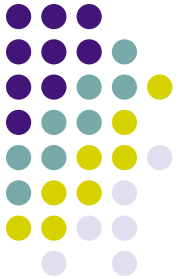
- Authentication Flow
- Authentication Types
- Compare Authentication Types
- Authentication Protocol

Authentication Flow

- การระบุตัวตน (Identification)
- การพิสูจน์ตัวตน (Authentication)



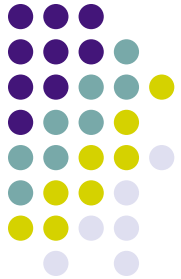
Authentication Types



- ไม่มีการพิสูจน์ตัวตน (No Authentication)
- การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Authentication by Passwords)
- การพิสูจน์ตัวตนโดยใช้ PIN (Authentication by PIN)
- การพิสูจน์ตัวตนโดยใช้ Password Authenticators หรือ Tokens (Authentication by Password Authenticators or Tokens)
- การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล (Authentication by Biometric Traits)
- การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว (One-Time Password: OTP)
- การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-key Cryptography)
- การพิสูจน์ตัวตนโดยการใช้ลายเซ็นอิเล็กทรอนิคส์ (Digital Signature)
- การพิสูจน์ตัวตนโดยใช้การถาม - ตอบ (Zero-Knowledge Proofs)

Authentication Types

No Authentication

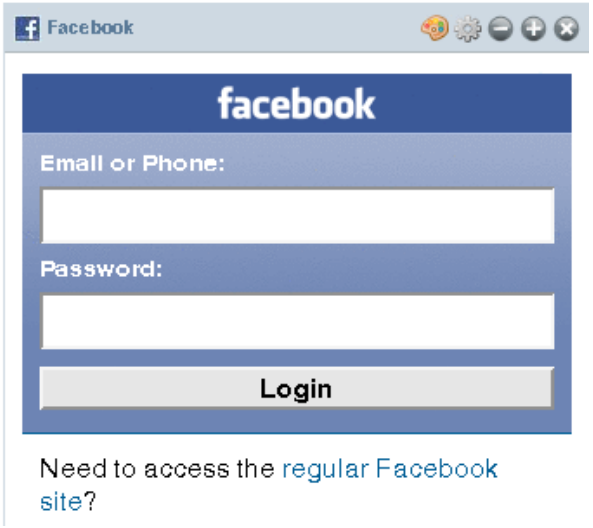


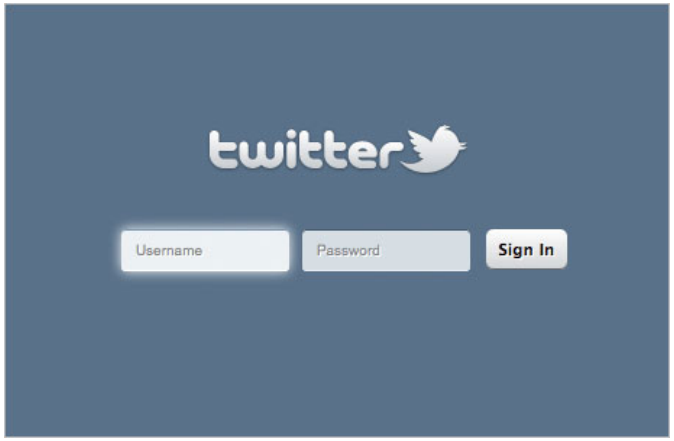
- ข้อมูลเหล่านั้นเป็นข้อมูลสาธารณะ ที่อนุญาตให้ทุกคนเข้าใช้บริการและเปลี่ยนแปลงได้ หรือ
- ข้อมูลข่าวสารหรือแหล่งของข้อมูลนั้นๆ สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

Authentication Types

Authentication by Passwords

- รหัสผ่านเป็นวิธีการที่ใช้มานานและนิยมใช้กันแพร่หลาย
- การใช้แค่รหัสผ่านไม่มีประสิทธิภาพมากพอ
- วิทยาการและความรู้ที่ก้าวหน้าทำให้รหัสผ่านอาจจะถูกขโมย





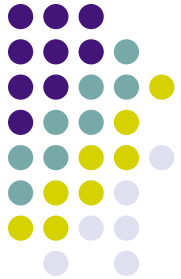
Authentication Types

Authentication by PIN

- ใช้อย่างแพร่หลายโดยเฉพาะการทำธุรกรรมทางด้านธนาคาร
- PIN ถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัส
- ใช้ฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะและถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งในการถอดรหัส

Authentication Types

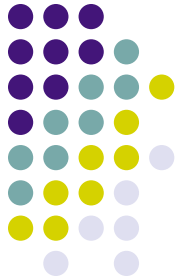
Authentication by Password Authenticators or Tokens



- Authenticator หรือ Token เป็นฮาร์ดแวร์พิเศษที่ใช้สร้าง "รหัสผ่านซึ่งเปลี่ยนแปลงได้ (Dynamic Password)"
  - ซิงโครนัส
    - *การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับสถานการณ์ (Event-synchronous authentication)*
    - *การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับเวลา (Time-synchronous authentication)*
  - อะซิงโครนัส

Authentication Types

Authentication by Password Authenticators or Tokens



- *การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับสถานการณ์*

  (Event-synchronous authentication)

  - ผู้ใช้จะต้องกด Token เพื่อให้ Token สร้างรหัสผ่าน
  - นำรหัสผ่านใส่ลงในฟอร์ม เพื่อเข้าสู่ระบบ

- *การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับเวลา*

  (Time-synchronous authentication)

  - สร้างรหัสผ่านโดยมีการกำหนดช่วงระยะเวลาการใช้งาน
  - ผู้ใช้ต้องการเข้าสู่ระบบ โดยใส่รหัสผ่านและเวลาที่รหัสผ่านตัวนั้นถูกสร้างขึ้นมา

Authentication Types

Authentication by Password Authenticators or Tokens

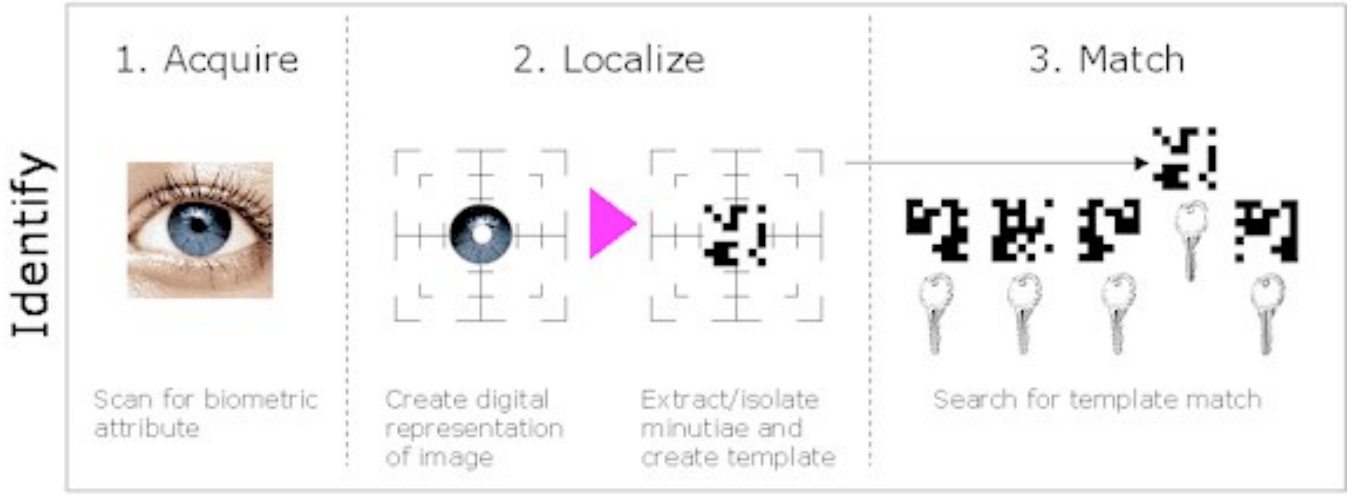
- อะซิงโครนัส
  - ร้องของไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์ก็จะส่ง Challenge String มาให้
  - ใส่ลงใน Token ที่ผู้ใช้ถืออยู่ Token จะทำการคำนวณรหัสผ่าน
  - นำรหัสผ่านนั้นใส่ลงในฟอร์มเพื่อเข้าสู่ระบบ

ตัวอย่าง Authenticators หรือ Token

Authentication Types

Authentication by Biometric Traits

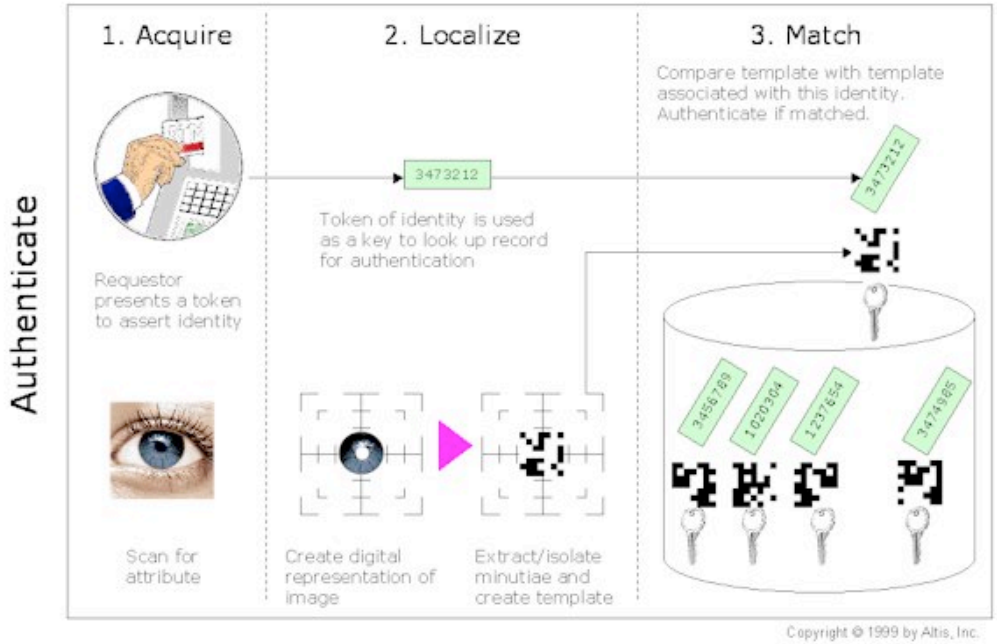
- เก็บหลักฐานทางชีวภาพ
  - เก็บภาพของเรตินาจากบุคคลที่ถือ Token การ์ดหรือสมาร์ทการ์ด
  - นำภาพเรตินาที่ได้มาแยกแยะเพื่อหาลักษณะเด่นเก็บไว้เป็น Template
  - Template ที่ได้จะถูกบันทึกเป็นกุญแจคู่กับรหัสผ่านที่มีอยู่ใน Token การ์ด หรือสมาร์ทการ์ดของแต่ละบุคคล



Authentication Types

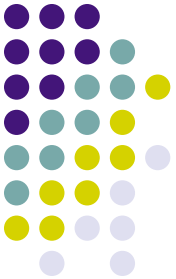
Authentication by Biometric Traits

- ตรวจสอบหลักฐานทางชีวภาพ
  - นำบัตรมาผ่านเครื่องอ่านบัตรและแสดงเรตินาให้เครื่องเก็บภาพ เพื่อหากุญแจและสร้าง Template
  - นำ Template ที่ได้ไปตรวจสอบกับ Template ที่เก็บไว้เพื่อหากุญแจ และนำกุญแจที่ได้มาเปรียบเทียบกันว่าตรงกันหรือไม่

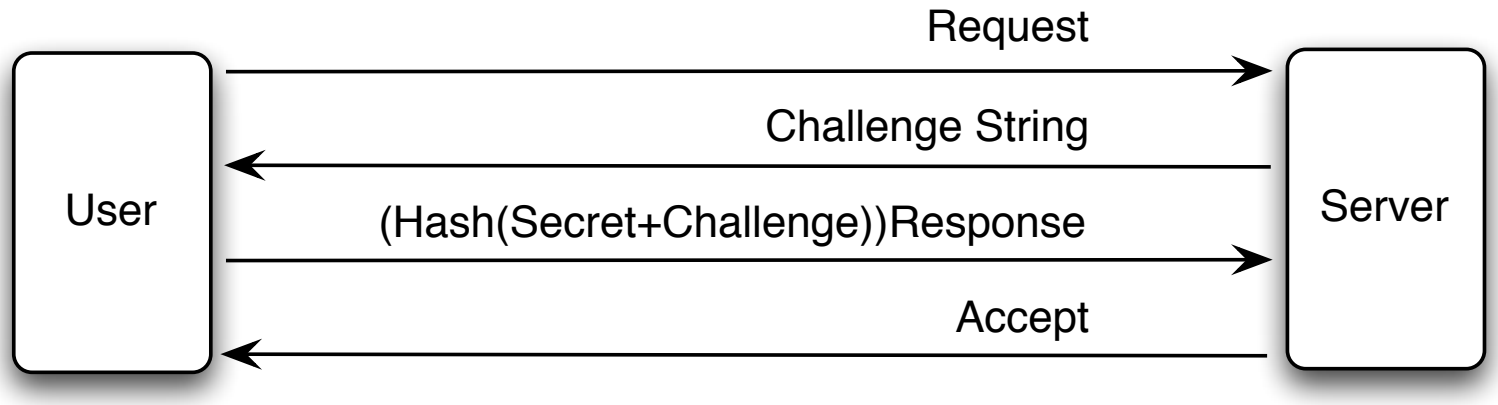


Authentication Types

One-Time Password (OTP)

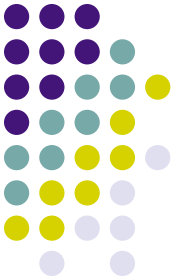


- ผู้ใช้จะทำการร้องขอไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์จะส่ง Challenge String กลับมาให้
- จากนั้นผู้ใช้จะนำ Challenge String และรหัสลับที่มีอยู่กับตัวของผู้ใช้นำไปเข้าแฮชฟังก์ชันได้ Response
- ส่งค่านั้นกลับไปยังเซิร์ฟเวอร์ ทำการตรวจสอบค่าที่ผู้ใช้ส่งมาเปรียบเทียบกับค่าที่เซิร์ฟเวอร์คำนวณ



Authentication Types

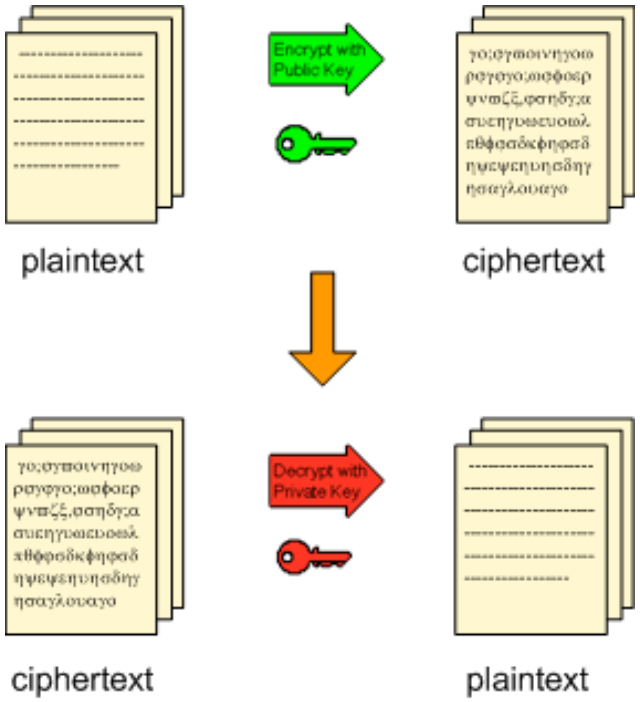
Public-Key Cryptography



- ประกอบไปด้วยกุญแจ 2 ชนิด ที่ต้องใช้คู่กันเสมอในการเข้ารหัสและถอดรหัส
  - กุญแจสาธารณะ (Public Key) เป็นกุญแจที่ผู้สร้างจะส่งออกไปให้ผู้ใช้อื่นๆ ทราบหรือเปิดเผยได้
  - กุญแจส่วนตัว (Private Key) เป็นกุญแจที่ผู้สร้างจะเก็บไว้ โดยไม่เปิดเผยให้คนอื่นรู้
- นำข้อมูลที่จะส่งไปยังผู้รับมาเข้ารหัสด้วยกุญแจสาธารณะของผู้รับ และเมื่อผู้รับได้รับข้อความนั้นแล้วจะถอดรหัสออกมาด้วยกุญแจส่วนตัว มีเพียงผู้รับเท่านั้นที่จะสามารถถอดรหัสออกมาได้

Authentication Types

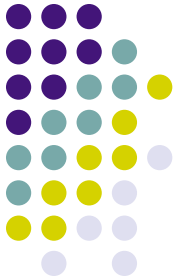
Public-Key Cryptography



ระบบของการเข้ารหัสแบบใช้คู่รหัสกุญแจ

Authentication Types

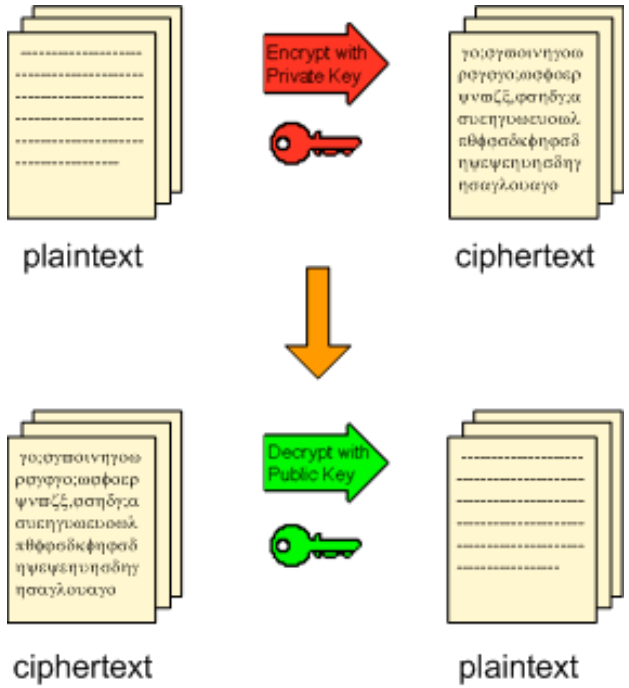
Public-Key Cryptography



- การประยุกต์ใช้ในการพิสูจน์ตัวตน (Authentication)
  - นำข้อมูลที่ผู้ส่งต้องการส่งมาเข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่ง
  - ผู้รับจะใช้กุญแจสาธารณะซึ่งเป็นคู่รหัสกันถอดรหัส
  - ผู้รับก็สามารถรู้ได้ว่าข้อความนั้นถูกส่งมาจากผู้ส่งคนนั้นจริง ถ้าสามารถถอดรหัสข้อมูลได้อย่างถูกต้อง

Authentication Types

Public-Key Cryptography



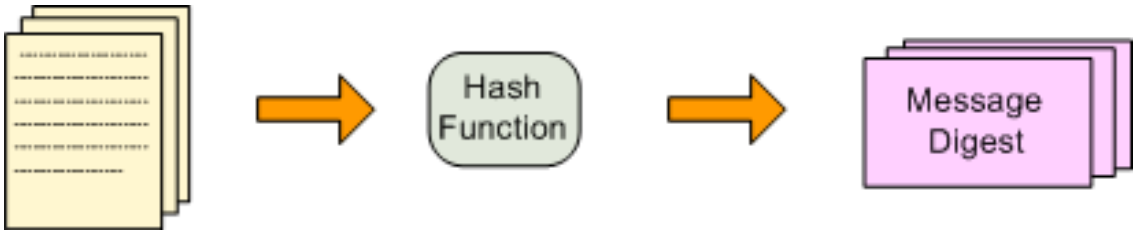
ระบบของการเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการพิสูจน์ตัวตน

Authentication Types

Digital Signature

- เป็นการนำหลักการของการทำงานของระบบการเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการพิสูจน์ตัวตนมาประยุกต์ใช้ ระบบของลายเซ็นดิจิตอลสามารถแบ่งเป็นขั้นตอนได้ดังนี้

1. นำข้อมูลไปเข้าฟังก์ชั่นทางคณิตศาสตร์ที่เรียกว่า "แฮชฟังก์ชัน" ได้เมสเซสไดเจสต์ (Message Digest) ออกมา



Authentication Types

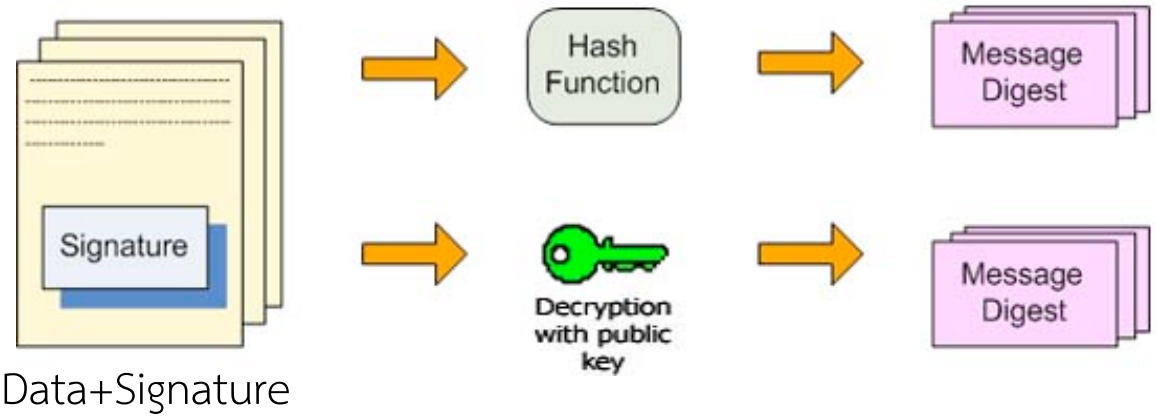
Digital Signature

2. การใช้กุญแจส่วนตัวเข้ารหัสข้อมูล หมายถึงว่าผู้ส่งได้ลงลายเซ็นดิจิตอล ยินยอมที่จะให้ผู้รับสามารถทำการตรวจสอบด้วยกุญแจสาธารณะของผู้ส่งเพื่อพิสูจน์ตัวตนของผู้ส่งได้

Authentication Types

Digital Signature

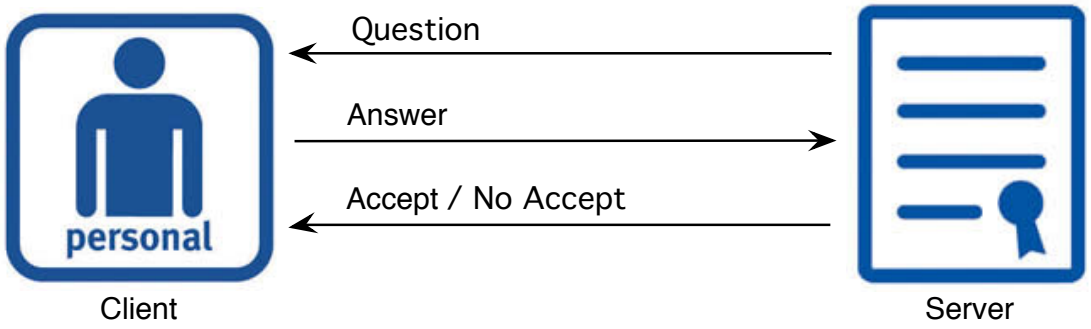
3. การตรวจสอบข้อมูลว่าถูกส่งมาจากผู้ส่งคนนั้นจริงในด้านผู้รับ
   - นำข้อมูลมาผ่านแฮชฟังก์ชันเพื่อคำนวณหาค่าเมสเซจไดเจสต์
   - ถอดรหัสลายเซ็นอิเล็กทรอนิคส์ด้วยกุญแจสาธารณะของผู้ส่ง
   - ถ้าข้อมูลเมสเซจไดเจสต์ที่ได้จากการถอดรหัสเท่ากันกับค่าเมสเซจไดเจสต์ในตอนต้นที่ทำการคำนวณได้ จะถือว่าข้อมูลดังกล่าวนั้นถูกต้อง



Authentication Types

Zero-Knowledge Proofs

- เป็นวิธีการพิสูจน์ตัวตนโดยใช้การถาม - ตอบ
- คำถามและคำตอบผู้ใช้เป็นคนสร้างขึ้นมา
- ระบบจะสุ่มคำถามเหล่านั้นที่ผู้ใช้คนนั้นๆ สร้างขึ้นมา
- การให้ใช้ระบบจะได้รับการยินยอมก็ต่อเมื่อการตอบคำตอบที่ผู้ใช้ตอบนั้นสัมพันธ์กับคำตอบที่มีอยู่ในเซิร์ฟเวอร์
- มีการนำความรู้ด้าน AI (Artificial Intelligence)



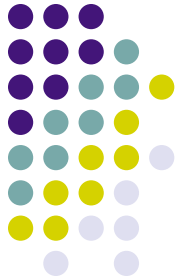
Compare Authentication Types

การพิสูจน์ตัวตน	ข้อดี	ข้อเสีย
ไม่มีการพิสูจน์ตัวตนตน	ง่ายต่อการใช้งานและค่าใช้จ่ายต่ำ	ความปลอดภัยของข้อมูลจะขึ้นอยู่กับผู้ใช้ว่าจะนำข้อมูลเหล่านั้นไปใช้ในทางที่ควรหรือไม่
การพิสูจน์ตัวตนโดยใช้รหัสผ่าน	สามารถใช้ได้กับทุกระบบ	จะไม่ปลอดภัยเมื่อมีการส่งข้ามระบบเครือข่ายที่เป็นสาธารณะหรือไม่มีการเข้ารหัสข้อมูล
การพิสูจน์ตัวตนโดยใช้ PIN	- ง่ายต่อการจำและความปลอดภัยค่อนข้างดี (บัตร ATM) - สามารถสื่อสารข้ามเครือข่ายสาธารณะได้อย่างปลอดภัย	- ต้องใช้ฮาร์ดแวร์เฉพาะในการอ่าน PIN - ไม่สามารถใช้กับต่างระบบกันได้ - ราคาแพง

Compare Authentication Types

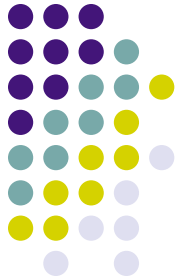
การพิสูจน์ตัวตน	ข้อดี	ข้อเสีย
การพิสูจน์ตัวตนโดยใช้ password authenticators หรือ tokens แบบซิงโครนัส	- มีความปลอดภัยมากกว่าการใช้การจำรหัสผ่านแบบธรรมดา - ไม่ต้องใช้เครื่องอ่านการ์ด - ผู้ที่ละเมิดเข้ามาไม่สามารถจะเข้ามาจู่โจมได้	- การใช้งานยุ่งยากกว่าแบบจำรหัสผ่าน - authenticator เป็นวัตถุจึงง่ายต่อการสูญหายและการถูกขโมยได้
กการพิสูจน์ตัวตนตนโดยใช้ password authenticators หรือ tokens แบบอะซิงโครนัส	- มีความปลอดภัยมากกว่าการใช้การจำรหัสผ่าน แบบธรรมดา - ไม่ต้องใช้เครื่องอ่านการ์ด - เป็นวิธีการป้องกันที่ดีที่สุดเมื่อเปรียบเทียบกับ วิธีการใช้การพิสูจน์ตัวตนโดยใช้ password authenticators หรือ tokens	- การใช้งานยุ่งยากกว่าแบบจำรหัสผ่าน - authenticator เป็นวัตถุจึงง่ายต่อการสูญหาย และการถูกขโมยได้ไม่สามารถป้องกันผู้ที่ละเมิดเข้ามาในระบบได้ - การใช้งานค่อนข้างยุ่งยากกว่าวิธีการใช้ "รหัสผ่านซึ่งเปลี่ยนแปลงได้ (dynamic password)" วิธีอื่นๆ

Compare Authentication Types



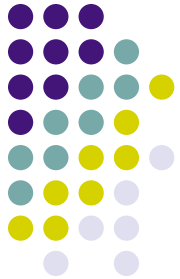
การพิสูจน์ตัวตน	ข้อดี	ข้อเสีย
การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล	มีความปลอดภัยสูงเพราะเลียนแบบกันได้ยาก	- ระบบมีความซับซ้อนสูง - ยังไม่ได้รับความนิยมกันอย่างแพร่หลาย - ค่าใช้จ่ายสูง
การพิสูจน์ตัวตนโดยวิธี One-Time Password	ทำให้การเดาหรือขโมยรหัสผ่านเป็นไปได้ยาก	- ไม่สะดวกต่อการใช้งาน เพราะผู้ใช้ต้องจำรหัสผ่านหลายตัว - ถ้าผู้ใช้จำรหัสผ่านไม่ได้ หรือ ทำรหัสผ่านสูญหาย ก็ไม่สามารถเข้าใช้ระบบได้
การพิสูจน์ตัวตนโดยการเข้ารหัสแบบคู่รหัสกุญแจ	- การจัดการกุญแจทำได้ปลอดภัย เพราะ ใช้กุญแจในการเข้ารหัส และถอดรหัสต่างกัน - สามารถระบุผู้ใช้โดยการใช้ร่วมกับลายมือชื่อ อิเล็กทรอนิกส์	- ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก - ต้องใช้ระบบที่สนับสนุนการทำงาน

Compare Authentication Types



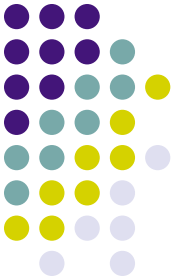
การพิสูจน์ตัวตน	ข้อดี	ข้อเสีย
การพิสูจน์ตัวตนโดยการใช้ลายเซ็นดิจิตอล	- สามารถระบุตัวผู้ส่งได้ชัดเจน - ป้องกันข้อมูลถูกแก้ไขระหว่างการส่งได้ หรือสามาถตรวจสอบข้อมูลได้ว่าผ่านการแก้ไขมาหรือไม่	ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก
การพิสูจน์ตัวตนโดยวิธี zero-knowledge proofs	ความปลอดภัยค่อนข้างสูง เพราะคำถามและคำตอบจะมีเพียงผู้ใช้และเซิร์ฟเวอร์เท่านั้นที่ทราบ	ความซับซ้อนของระบบเพิ่มขึ้นตามความฉลาดของระบบ

โพรโตคอลในการพิสูจน์ตัวตน (Authentication Protocol)



- Secure Socket Layer (SSL)
- Secure Shell (SSH)
- Internet Security (IPSEC)
- Kerberos

Authentication Protocol
Secure Socket Layer (SSL)

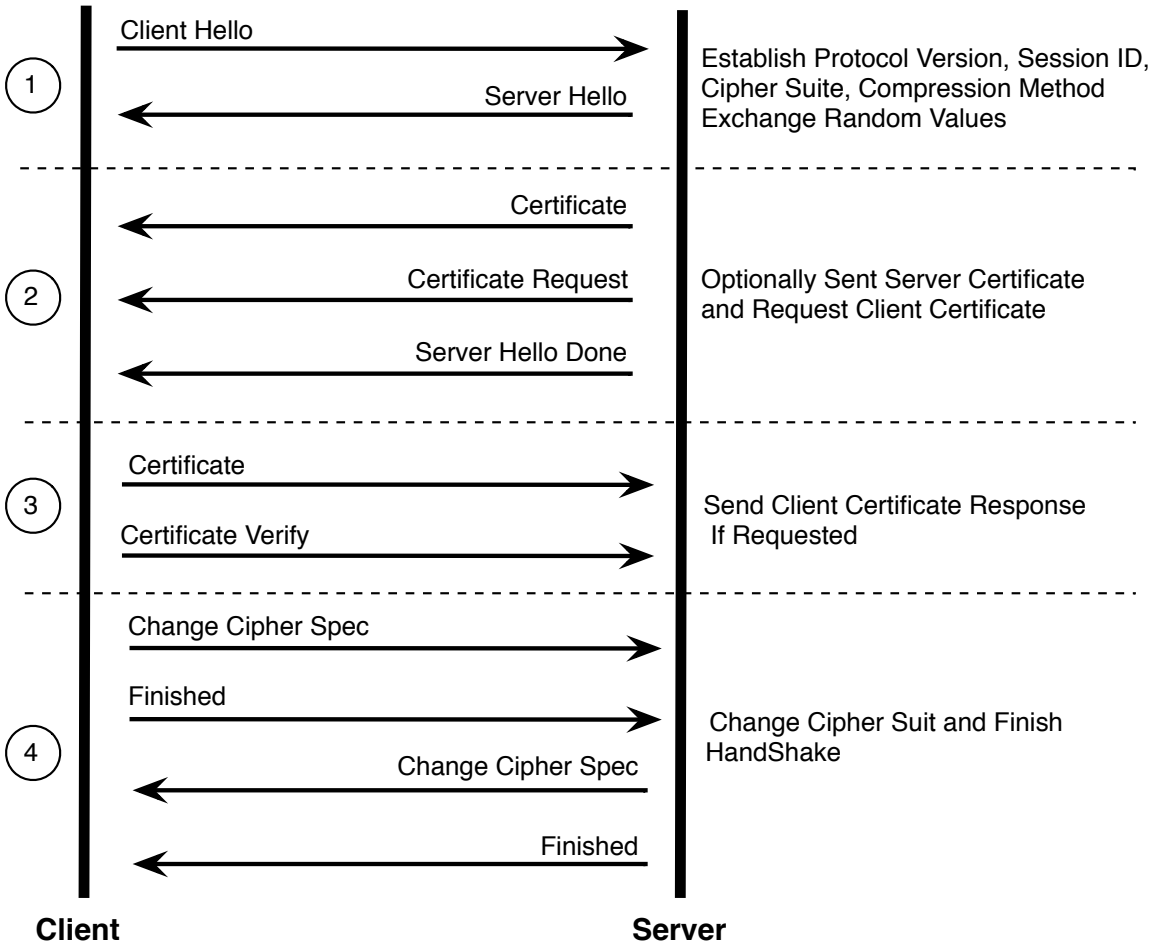


- Secure Sockets Layer (SSL) เพื่อใช้ในโพรโตคอลระดับแอพพลิเคชันคือ Hypertext Transfer Protocol (HTTP)
- SSL ทำให้เกิดการสื่อสารอย่างปลอดภัยระหว่างไคลเอ็นต์และเซิร์ฟเวอร์ โดยการอนุญาตให้มีกระบวนการพิสูจน์ตัวตนรวมกับการใช้งานลายเซ็นดิจิตอลสำหรับการรักษาความถูกต้องของข้อมูลและการเข้ารหัสข้อมูลเพื่อป้องกันความเป็นส่วนตัวระหว่างการสื่อสารข้อมูล

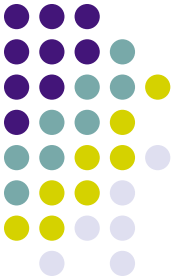
Authentication Protocol

Secure Socket Layer (SSL)

- กระบวนการในการเริ่มต้นการสื่อสารผ่านชั้น SSL แบ่งเป็น 4 ขั้นตอนคือ



Authentication Protocol
Secure Socket Layer (SSL)



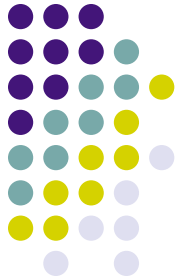
ขั้นตอน 1 : ประกาศชุดวิธีการเข้ารหัส ไดเจสต์ และลายเซ็นดิจิตอลที่สนับสนุนของทั้งไคลเอ็นต์และเซิร์ฟเวอร์

- วิธีการเข้ารหัสที่เว็บเซิร์ฟเวอร์และไคลเอ็นต์สนับสนุน หมายเลขระบุการสื่อสาร (Session identifier) รวมถึงวิธีการบีบอัดข้อมูล

ขั้นตอน 2 : การพิสูจน์ตัวตนของเซิร์ฟเวอร์ต่อไคลเอ็นต์

- ไคลเอ็นต์จะทำการตรวจสอบ Certificate กับผู้ให้บริการ Certificate Authority เพื่อยืนยันความถูกต้องของ Certificate ของเซิร์ฟเวอร์

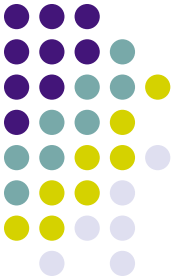
Authentication Protocol
Secure Socket Layer (SSL)



ขั้นตอน 3 : การพิสูจน์ตัวตนของไคลเอ็นต์ต่อเซิร์ฟเวอร์ ถ้าจำเป็น เซิร์ฟเวอร์สามารถร้องขอ Certificate จากไคลเอ็นต์เพื่อตรวจสอบความถูกต้องของ Client ด้วยก็ได้

ขั้นตอน 4 : ไคลเอ็นต์และเซิร์ฟเวอร์ตกลงชุดวิธีการเข้ารหัส การสร้างไดเจสต์ และการใช้ลายเซ็นดิจิตอล

Authentication Protocol
Secure Shell (SSH)

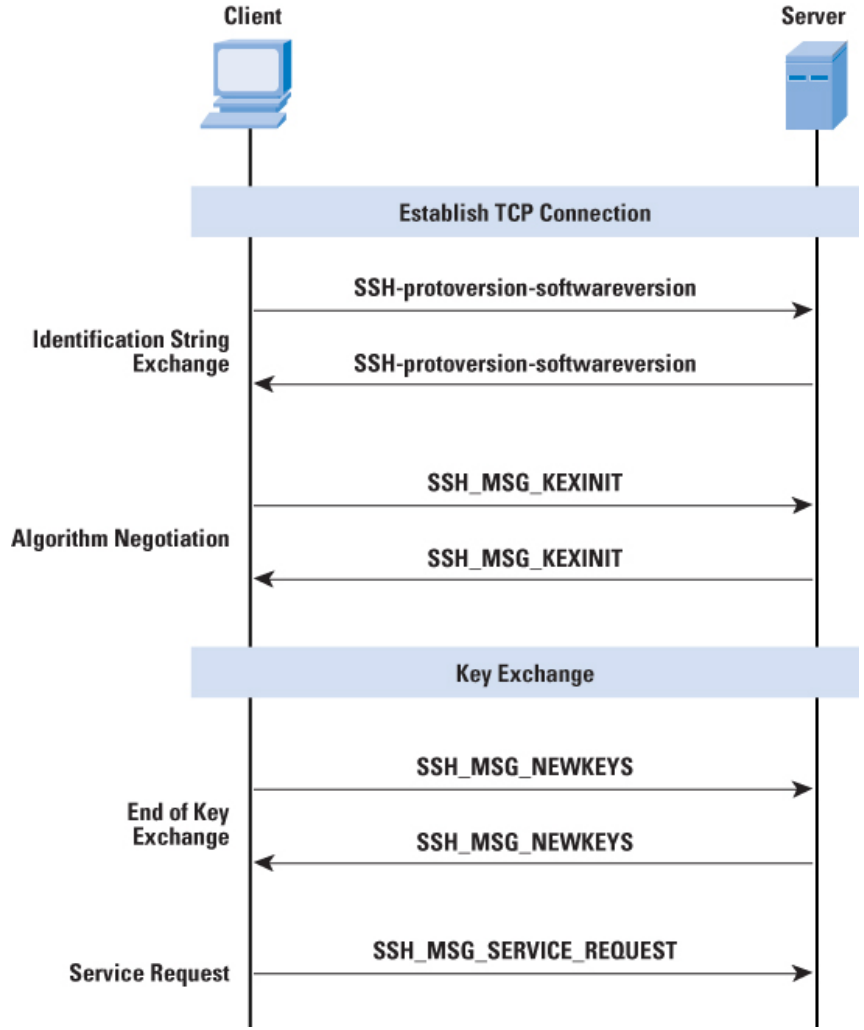


- SSH เป็นการติดต่อสื่อสารโดยใช้การพิสูจน์ตัวตนรวมกับลายเซ็นดิจิตอล และมีการเข้ารหัสการสื่อสาร ตรงกันข้ามกับการสื่อสารแบบเก่าเช่น Telnet หรือ R Utilities เป็นต้น

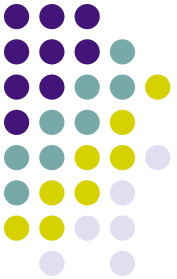
	มาตรฐานตาม SSH เวอร์ชัน 1	มาตรฐานตาม SSH เวอร์ชัน 2
การเข้ารหัสแบบ Public key	RSA	DSA, DH
การสร้างไดเจสต์	MD5, CRC-32	MD5, SHA-1
การเข้ารหัสด้วยกุญแจสมมาตร	3DES, IDEA, ARCFOUR, DES	3DES, Blowfish, Twofish, CAST-128, IDEA, ARCFOUR
การบีบอัดข้อมูล	zlib	zlib

Authentication Protocol

Secure Shell (SSH)



Authentication Protocol
Secure Shell (SSH)



- **การเริ่มต้นการติดต่อสื่อสารตามโพรโตคอล SSH เป็นไปตามขั้นตอนสรุปได้เป็น**

  1. ไคลเอ็นต์เริ่มถามเวอร์ชันของโพรโตคอล SSH บนเซิร์ฟเวอร์ ถ้าใช้ SSH เวอร์ชันเดียวกันถือว่าสื่อสารกันได้

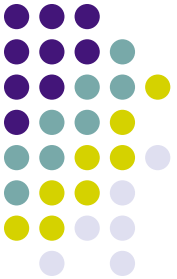
  2. ไคลเอ็นต์จะประกาศวิธีการเข้ารหัส วิธีการสร้างไดเจสต์ และการแลกเปลี่ยนกุญแจในการเข้ารหัสที่สนับสนุน

  3. เซิร์ฟเวอร์จะทำหน้าที่เลือกชุดวิธีการทั้งหมดที่ไคลเอ็นต์สนับสนุน

  4. ไคลเอ็นต์และเซิร์ฟเวอร์เริ่มต้นแลกเปลี่ยนกุญแจในการเข้ารหัส

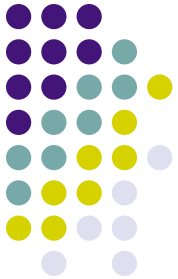
  5. ไคลเอ็นต์และเซิร์ฟเวอร์เริ่มต้นติดต่อสื่อสารด้วยการเข้ารหัสและสามารถใช้การบีบอัดข้อมูลร่วมได้

Authentication Protocol Internet Security (IPSEC)

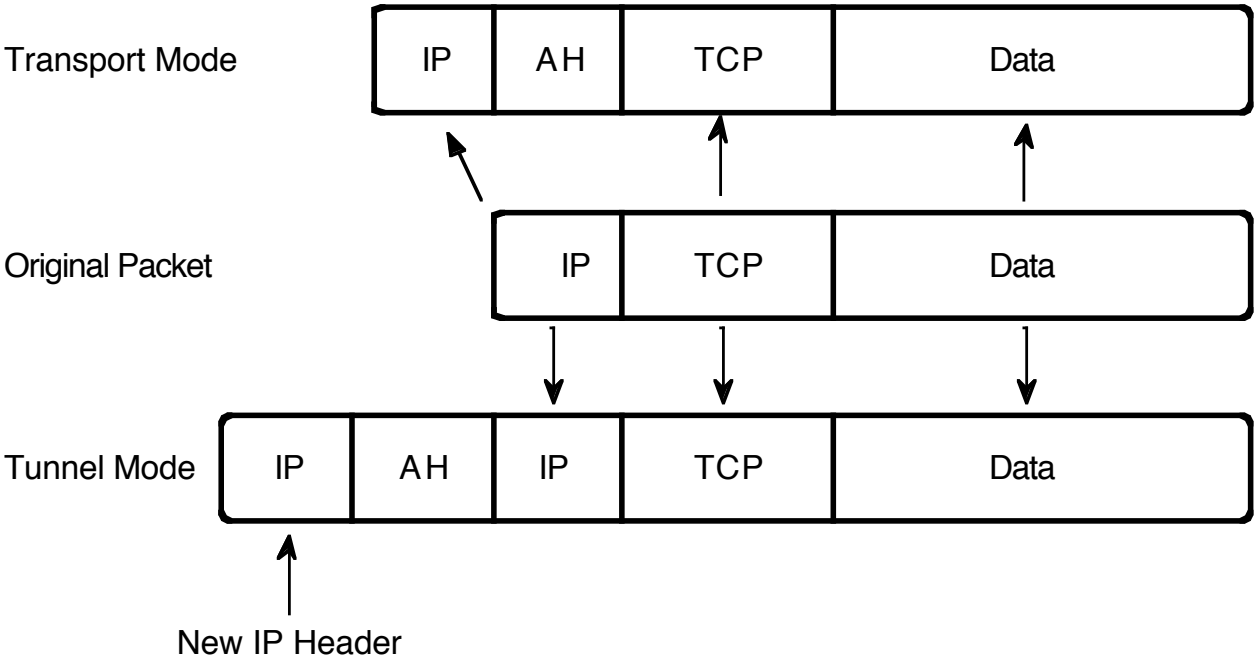


- IPsec เป็นส่วนเพิ่มขยายของ Internet Protocol (IP) ในชุดโพรโตคอล TCP/IP พัฒนาเพื่อเป็นส่วนหนึ่งของมาตรฐานของ IPv6
- IPsec ใช้โพรโตคอล 2 ชุดคือ Authentication Header (AH) และ Encapsulated Security Payload (ESP)
- รองรับการพิสูจน์ตัวตน(Authentication) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความลับ (Confidentiality) ในระดับชั้นของ IP

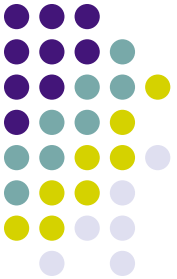
Authentication Protocol Internet Security (IPSEC)



- การใช้งานสามารถเลือกใช้ได้สองรูปแบบ

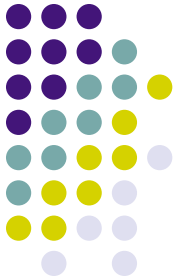


Authentication Protocol Internet Security (IPSEC)



- Transport mode นำเฉพาะข้อมูลของโพรโตคอล IP ซึ่งจะประกอบด้วยข้อมูลของชั้น Transport (TCP หรือ UDP) และชั้นแอพพลิเคชันโดยเพิ่มโพรโตคอล AH และเพิ่มข้อมูลใน IP เดิมให้เหมาะสมตามมาตรฐาน IPsec
- Tunnel mode เป็นการนำส่วนแพ็กเก็ตเดิมทั้งหมดมาครอบด้วย IP โพรโตคอลชุดใหม่ที่เป็นไปตามชุดโพรโตคอล IPsec สังเกตได้จากมีการเพิ่มเฮดเดอร์ IP และ AH เข้าไปข้างหน้าแพ็กเก็ตชุดเดิม

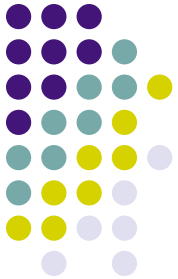
Authentication Protocol Internet Security (IPSEC)



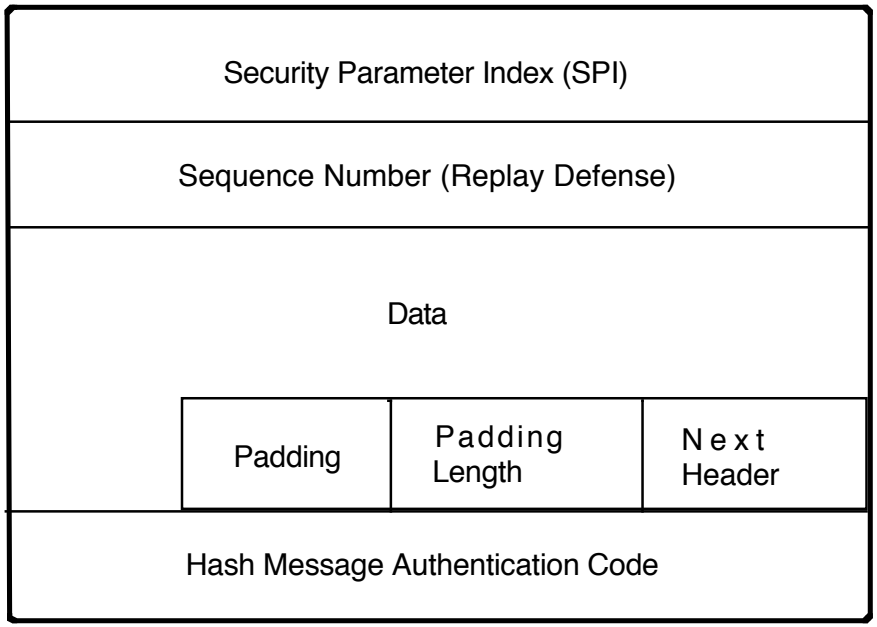
- AH หรือ Authentication Header ทำหน้าที่รักษาความถูกต้องของ IP ดาตาแกรม โดยการคำนวณ HMAC กับทุก IP ดาตาแกรม

Next Header	Payload Length	Reserved
Security Parameter Index (SPI)		
Sequence Number (Replay Defense)		
Hash Message Authentication Code		

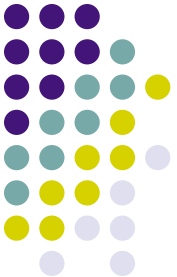
Authentication Protocol Internet Security (IPSEC)



- ESP หรือ Encapsulated Security Payload ใช้สำหรับรักษาความถูกต้องของแพ็กเก็ตโดยใช้ HMAC และการเข้ารหัสร่วมด้วย



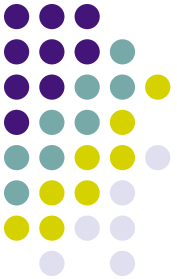
Authentication Protocol Kerberos



- **ระบบ Kerberos ประกอบขึ้นจากสองส่วนหลักคือ**
  - Ticket ใช้สำหรับการพิสูจน์ตัวตนของผู้ใช้ในระบบและการเข้ารหัสข้อมูล
  - Authenticator ใช้ในการตรวจสอบ Ticket ว่าเป็นผู้ใช้คนเดียวกันที่ใช้ Ticket เป็นใบเบิกทางเข้าสู่ระบบและเป็นผู้ใช้ที่ระบบสร้างให้อย่างถูกต้อง
- **Kerberos เซิร์ฟเวอร์ มีสองส่วนบริการในการใช้งานคือ**
  - Authentication service (AS) สำหรับการพิสูจน์ตัวตนของผู้ใช้กับ Kerberos เซิร์ฟเวอร์ก่อนการเข้าใช้บริการ
  - Ticket Granting Service (TGS) เป็นบริการที่ออก Ticket เพื่อให้ผู้ใช้นำไปใช้กับเซิร์ฟเวอร์ที่ต้องการ

Authentication Protocol

Kerberos



กระบวนการใช้งานระบบ Kerberos มีลำดับดังนี้

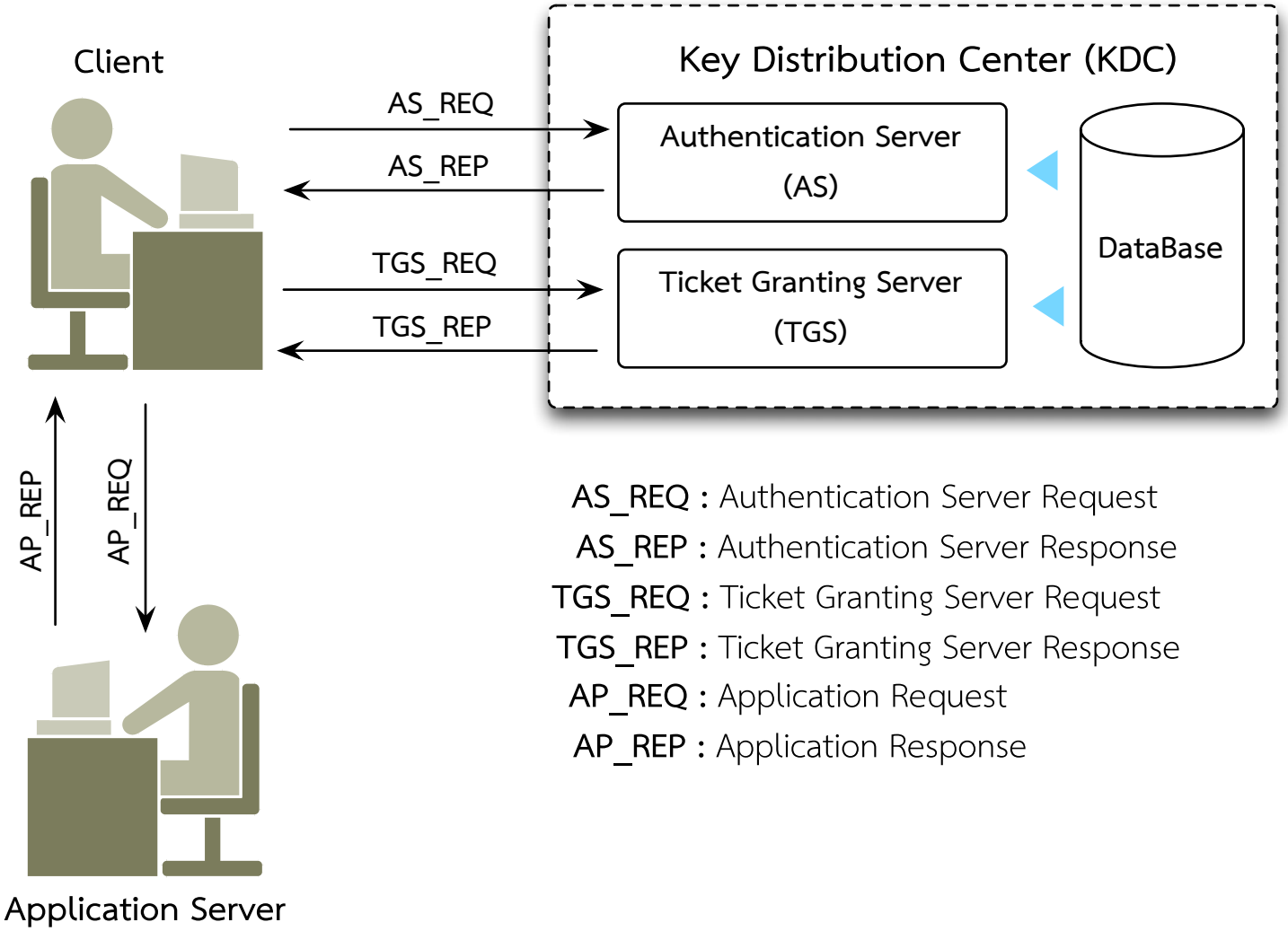
1. พิสูจน์ตัวตนกับ Authentication Service ของ Kerberos ซึ่งจะได้กุญแจสมมาตรซึ่งจะใช้ในการเข้ารหัสข้อมูลในการติดต่อสื่อสาร

2. ติดต่อไปที่ Ticket Granting Service เพื่อให้ออก Ticket

3. ผู้ใช้นำ Ticket ไปใช้กับการร้องขอบริการจากเซิร์ฟเวอร์ในระบบ

Authentication Protocol

Kerberos



AS_REQ : Authentication Server Request

AS_REP : Authentication Server Response

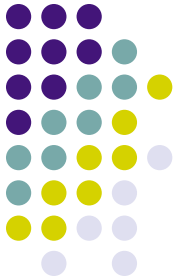
TGS_REQ : Ticket Granting Server Request

TGS_REP : Ticket Granting Server Response

AP_REQ : Application Request

AP_REP : Application Response

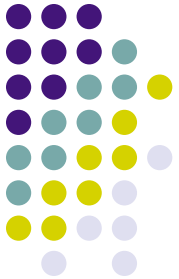
Summary



การรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ หรือ ระบบเครือข่ายคอมพิวเตอร์เป็นสิ่งที่ควรตระหนักเป็นอย่างยิ่งในปัจจุบัน เพราะโลกในยุคปัจจุบันเป็นโลกแห่งข้อมูลข่าวสาร การเก็บรักษาข้อมูลให้ปลอดภัยจึงเป็นสิ่งสำคัญกับตัวบุคคลและองค์กร

เพราะฉะนั้นการที่จะอนุญาตให้บุคคลใดบุคคลหนึ่งสามารถเข้าถึงข้อมูลจึงเป็นสิ่งที่ควรระมัดระวัง เพราะข้อมูลบางอย่างของบุคคลและองค์กรมีความสำคัญและไม่สามารถเปิดเผยต่อบุคคลภายนอกได้

Resources



- Computer Security Division Computer Security Resource Center / National Institute of Standard and Technology (CSRC/NIST)
  - csrc.nist.gov
- Computer Emergency Response Team(CERT)
  - www.cert.org
- SANS
  - www.sans.org
- อาจารย์ ธนัญชัย ตรีภาค สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
- สิริพร จิตต์เจริญธรรม, เสาวภา ปานจันทร์ และ เลอศักดิ์ ลิ้มวิวัฒน์กุล
- Security Focus
  - www.securityfocus.com