การจัดการความมั่นคงปลอดภัยทางข้อมูล

Information Security Management

Chapter 4 : Access Control

เนื้อหา

- การควบคุมการเข้าถึง (Access Control)
- การระบุตัวตน (Identification)
- การพิสูจน์ตัวตน (Authentication)
- การอนุญาต (Authorization)
- การตรวจสอบได้ (Accountability)

การควบคุมการเข้าถึง (Access Control)

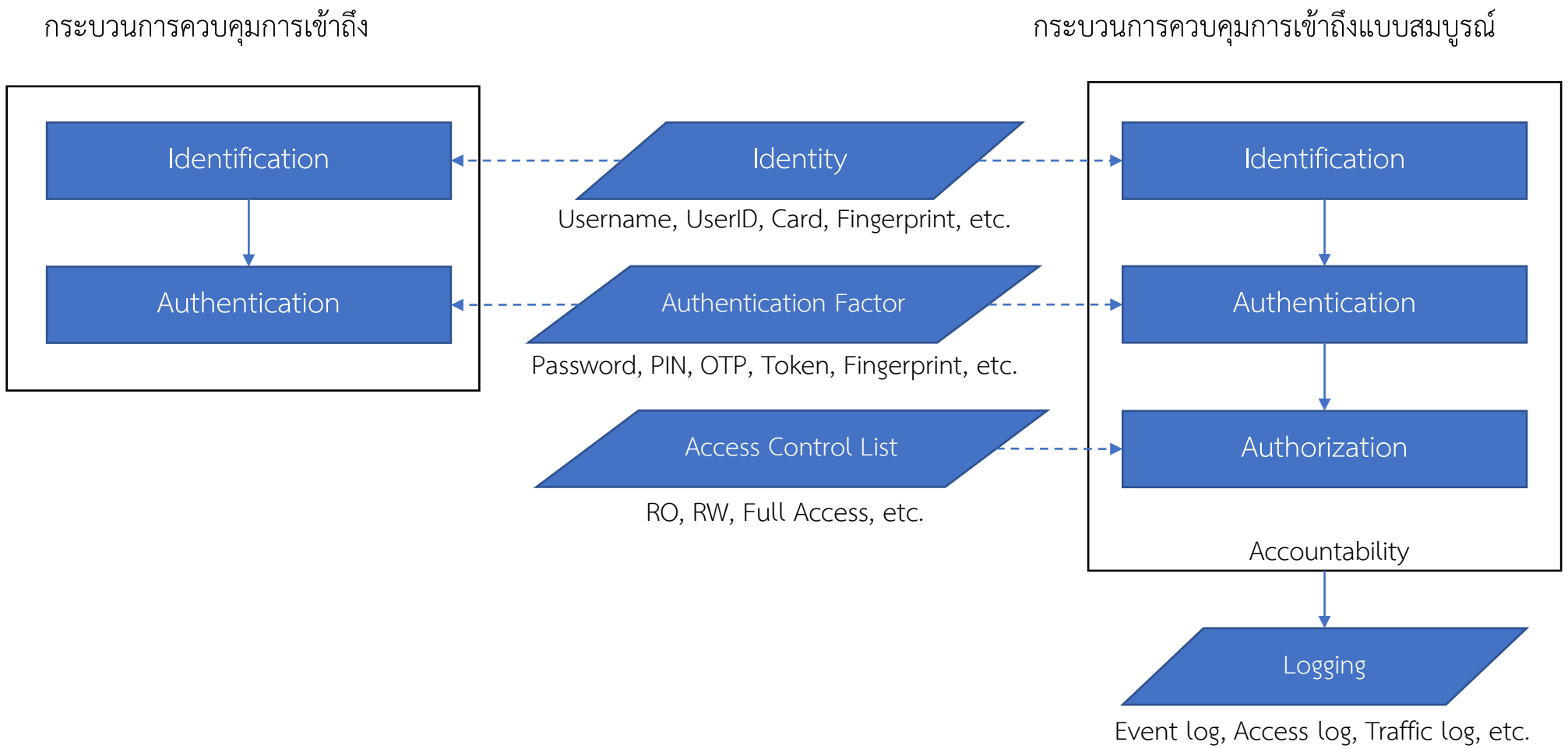
Access Control คือ กระบวนการที่ช่วยควบคุมสิทธิ์ในการเข้าถึงทรัพยากร เพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้ามาลบ แก้ไข หรือขโมยข้อมูลไปใช้จนเกิดความเสียหายกับองค์กร ซึ่งเป็นสิ่งที่กำหนดว่าใครคือผู้ที่จะสามารถเข้ามากระทำการใดๆ ภายในเครือข่ายหรือพื้นที่ขององค์กรได้ และสามารถระบุว่าบุคคลเหล่านั้นจะเข้าถึงทรัพยากรใดได้บ้าง

การควบคุมการเข้าถึง (Access Control)

ขั้นตอนการควบคุมสิทธิ์ในการเข้าถึงข้อมูลของแต่ละบุคคล มีกระบวนการต่างๆ ดังนี้

- การระบุตัวตน (Identification)
- การพิสูจน์ตัวตน (Authentication)
- การอนุญาต (Authorization)
- การตรวจสอบได้ (Accountability)

การควบคุมการเข้าถึง (Access Control)



ประเภทของ Access Control

Access Control สามารถแบ่งเป็น 4 ประเภทหลัก ๆ ได้แก่

1. Discretionary access control (DAC)
2. Mandatory access control (MAC)
3. Role-based access control (RBAC)
4. Attribute Based Access Control (ABAC)

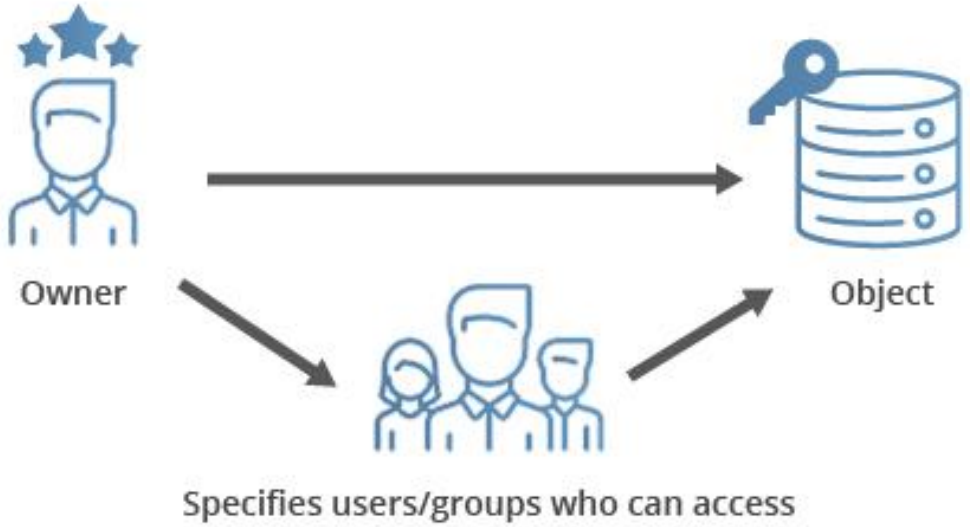
Discretionary access control (DAC)

เป็นการควบคุมการเข้าถึงทรัพยากรที่เจ้าของเป็นผู้ควบคุมอย่างสมบูรณ์ โดยผู้เป็นเจ้าของสามารถกำหนดสิทธิ์การเข้าถึงของผู้ใช้รายอื่น เช่น

การอนุญาตให้เข้าไปอ่าน หรือแก้ไขข้อมูล และเมื่อมีการร้องขอเพื่อเข้ามาในระบบ เจ้าของทรัพยากรสามารถอนุญาตคำร้องของผู้ใช้รายนั้นได้ทันที นอกจากนี้ยังสามารถโอนสิทธิ์ความเป็นเจ้าของให้กับผู้อื่นได้อีกด้วย

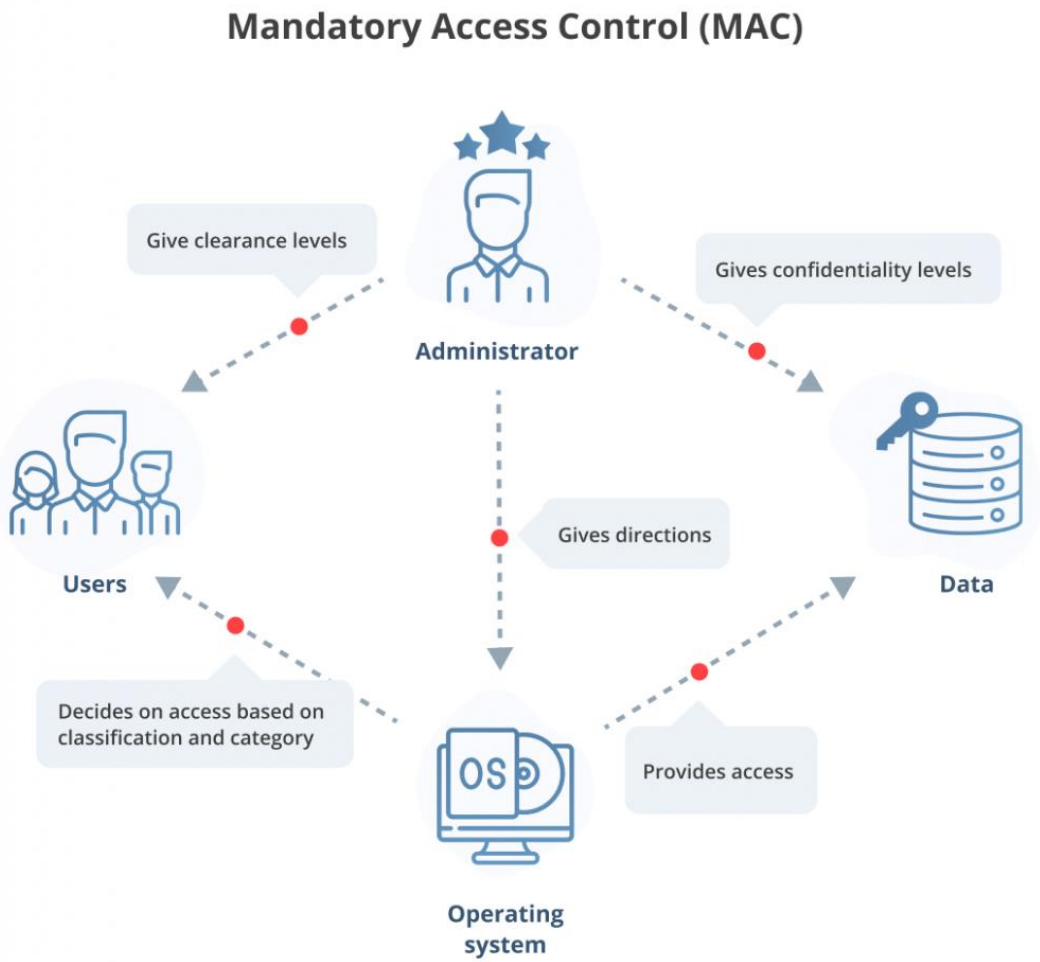
ทำให้ DAC เป็นวิธีการควบคุมที่มีความยืดหยุ่น แต่จะไม่เหมาะหากนำไปใช้กับการปกป้องข้อมูลที่เป็นความลับ หรือทรัพยากรที่ต้องการความปลอดภัยสูง

Discretionary access control (DAC)



Mandatory access control (MAC)

เป็นการควบคุมแบบส่วนกลาง ซึ่งจะกำหนดการเข้าถึงทรัพยากรตามนโยบาย หรือตามระดับชั้นความปลอดภัยที่วางไว้ เป็นการควบคุมโดยระบบไม่ใช่โดยเจ้าของ ทำให้ผู้ใช้ไม่สามารถเปลี่ยนแปลงนโยบายต่าง ๆ เหล่านั้นได้ วิธีการควบคุมแบบนี้มักใช้กับระบบที่มีความอ่อนไหวสูง เช่น ระบบของรัฐบาล



Role-based access control (RBAC)

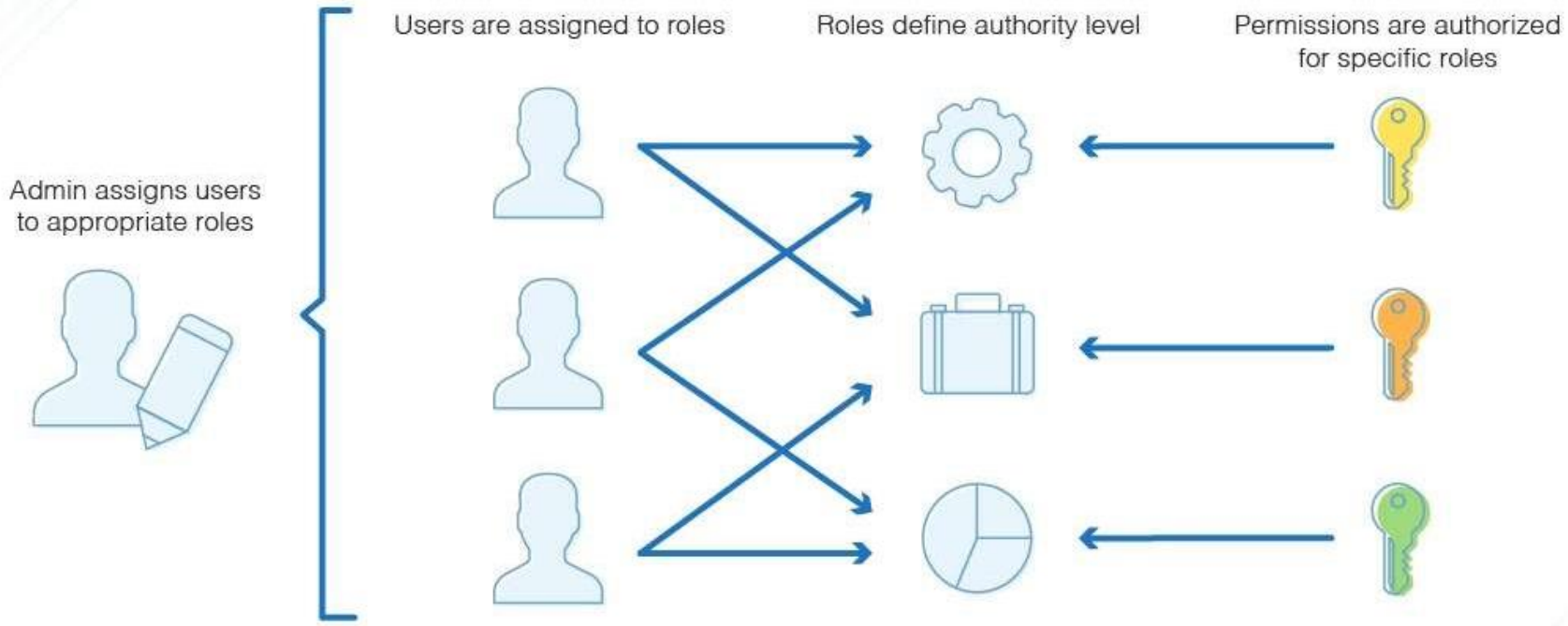
เป็นการจัดการสิทธิ์ในการเข้าถึงระบบ โดยจะเป็นตัวกำหนดบทบาทว่าผู้ใช้รายใดสามารถเข้าถึงส่วนใดได้บ้าง เช่น

ผู้ใช้ A สามารถเข้าไปลบ แก้ไขข้อมูล และติดตั้งซอฟต์แวร์ใหม่ได้ ขณะที่ผู้ใช้ B ทำได้เพียงแค่ลบหรือแก้ไขข้อมูล แต่ไม่สามารถติดตั้งซอฟต์แวร์ได้ ส่วนคนที่เหลืออาจได้สิทธิ์แค่เข้าไปอ่านข้อมูลเท่านั้น

นอกจากนี้ผู้ใช้งานหนึ่งคนยังสามารถมีได้หลายบทบาท เช่น ได้บทบาทเป็น Admin ของระบบหนึ่ง แต่เป็นแค่ User ของอีกระบบหนึ่งก็ได้เช่นกัน

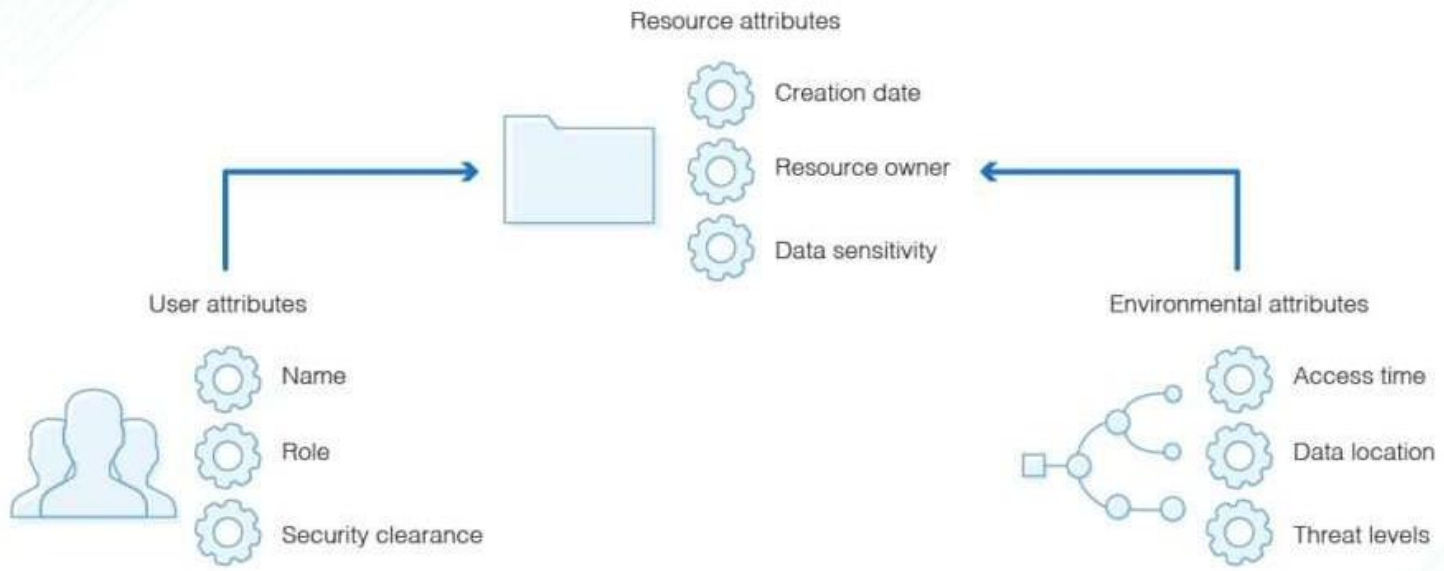
นั่นทำให้วิธีการควบคุมแบบ RBAC มีการนำไปใช้อย่างกว้างขวาง และยังสามารถนำไปใช้ร่วมกับการควบคุมทั้งแบบ DAC และ MAC ได้อีกด้วย

Role-based access control (RBAC)

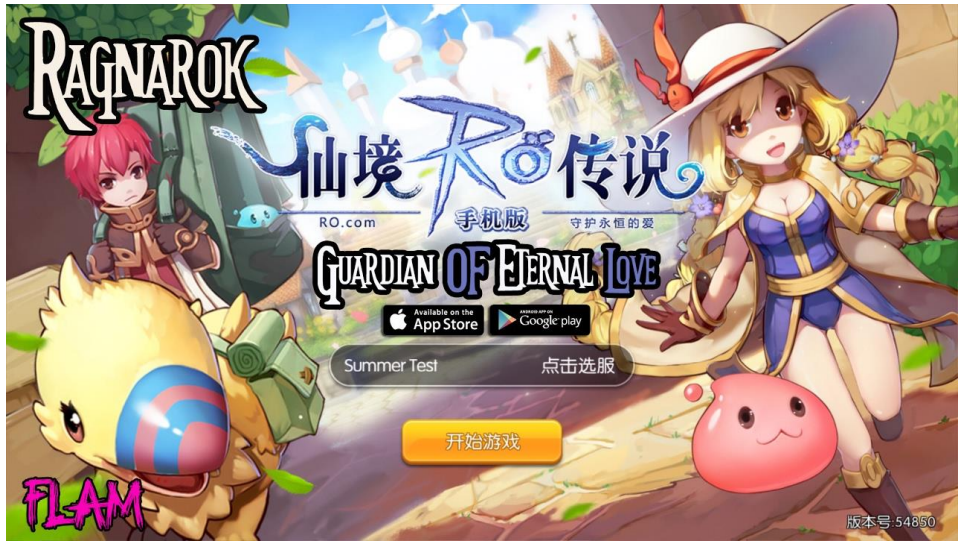


Attribute Based Access Control (ABAC)

เป็นการควบคุมการเข้าถึงทรัพยากรโดยการคัดกรองจากคุณสมบัติของผู้ใช้บางประการ เช่น หากผู้ใช้เป็นพนักงานของบริษัท และอยู่ฝ่าย IT ด้าน Security จะสามารถเข้าถึงอุปกรณ์ Firewall ได้ หรือกำหนดให้ผู้ใช้ที่เป็น Manager เท่านั้นที่มีสิทธิ์เข้าไปแก้ไขข้อมูลที่มีความอ่อนไหว



การระบุตัวตน (Identification)



ความพยายามที่จะพิสูจน์ว่าผู้ใช้เป็นมนุษย์ หรือเป็นผู้ที่มีสิทธิ์ในการใช้งาน พยายามพิจารณาว่าผู้ใช้คนนั้นเป็นใครเพื่อให้คุณสามารถป้องกันไม่ให้ผู้อื่นใช้งานแอปพลิเคชันของคุณได้

Who Are the Abusers? : Spammers

เป็นรูปแบบการละเมิดข้อมูลที่พบมาก เกิดจากผู้ใช้ที่พยายามทำการตลาด หรือบริการของผลิตภัณฑ์ หรือพยายามเพิ่มการจัดอันดับของเว็บไซต์โดยการหว่านลิงก์ในเว็บไซต์อื่น ๆ แรงจูงใจหลักของผู้ส่งอีเมลขยะเป็นเชิงพาณิชย์ ดังนี้

- โพสต์โฆษณา
- การโพสต์รีวิวสินค้าปลอม สำหรับผลิตภัณฑ์ของตนเอง หรือต่อคู่แข่ง
- เริ่มต้นธุรกิจพีระมิด (Pyramid Schemes)
- ขายผลิตภัณฑ์ในตลาดมืด

Who Are the Abusers? : Scammers

การหลอกลวงทางอินเทอร์เน็ตอีกแบบหนึ่ง มีกลเม็ดมากมายเพื่อหลอกเอาผลประโยชน์และหลีกเลี่ยงทางกฎหมาย แรงจูงใจหลักของสแกมเมอร์ ดังนี้

- การหลอกให้ติดตั้ง botnet หรือ keylogger ที่เป็นอันตรายบนคอมพิวเตอร์
- การโพสต์แบบฟอร์มที่ใช้ในการหลอกลวงแบบฟิชชิ่ง
- การหลอกให้โพสต์ไฟล์ขนาดใหญ่หรือเป็นที่นิยมเพื่อหลีกเลี่ยงทางกฎหมาย
- การโพสต์เนื้อหาลามกอนาจารเพื่อหลีกเลี่ยงกฎหมาย
- การหลอกขอบริจากเงิน

Who Are the Abusers? : Griefers and Trolls

เป็นการเอาเปรียบคนอื่น การสร้างความเดือดร้อนรำคาญให้แก่ผู้ใช้งานอื่นด้วย หรือดึงความสนใจของผู้ใช้งานอื่น มีลักษณะต่างๆ ดังนี้

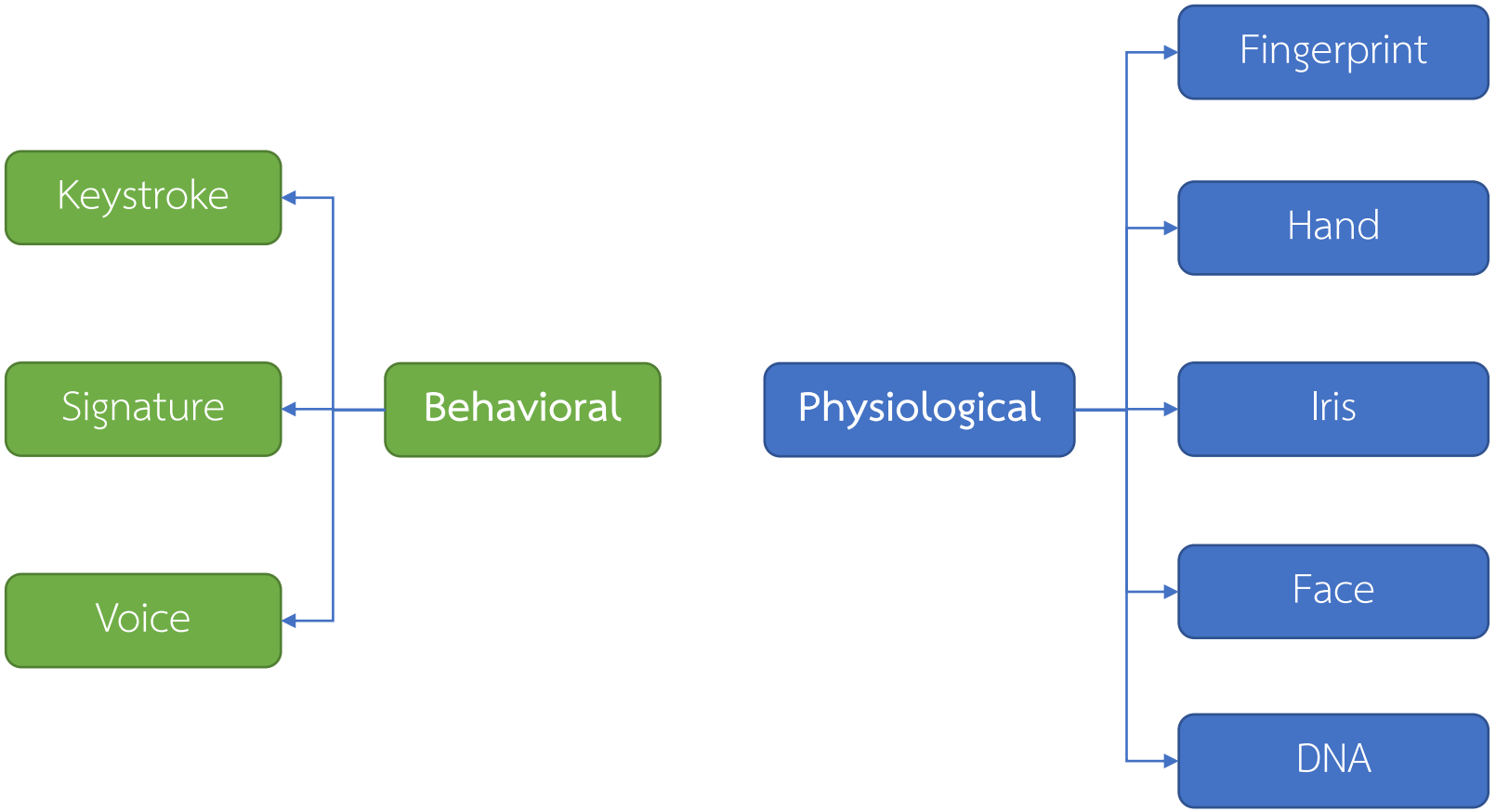
- การโพสต์ดูหมิ่น ใส่ร้ายหรือหมิ่นประมาท
- การโพสต์เนื้อหาที่ไม่เหมาะสม
- ก่อกวนผู้ใช้รายอื่นอย่างต่อเนื่อง

การพิสูจน์ตัวตน (Authentication)

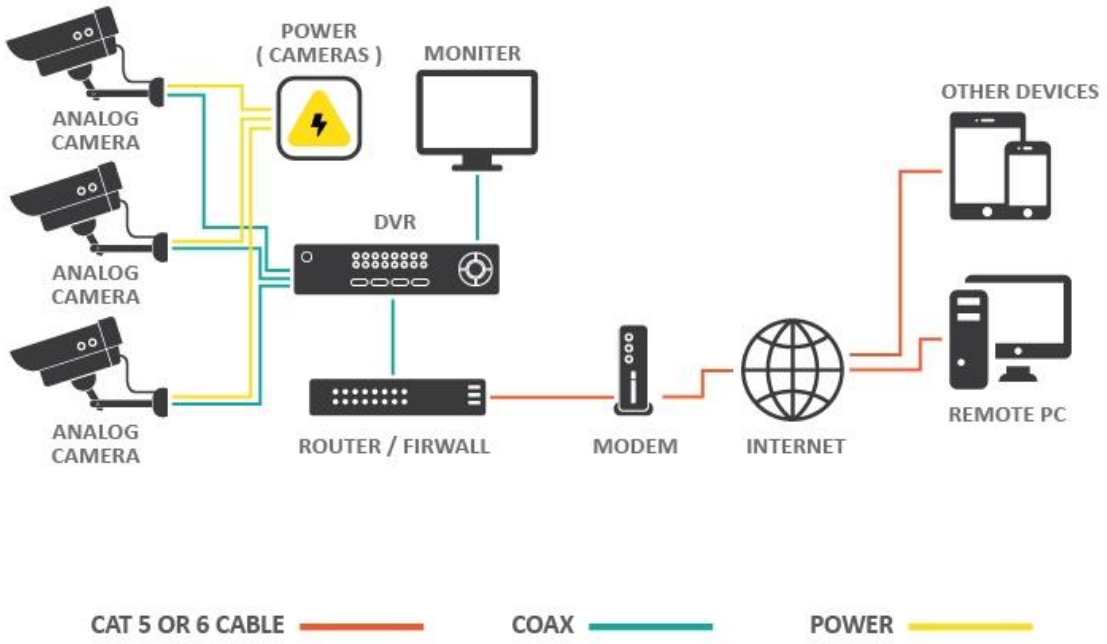
การพิสูจน์ตัวตนของผู้ใช้งานในระบบ สามารถทำได้จากการตรวจสอบคุณสมบัติ 3 อย่างของผู้ใช้ คือ

- สิ่งที่ผู้ใช้รู้ (Something you know) เช่น Password
- สิ่งที่ผู้ใช้มี (Something you have) เช่น Smart Card
- สิ่งที่ผู้ใช้เป็น (Something you are) เช่น Biometrics (ลายนิ้วมือ ใบหน้า ม่านตา เสียงพูด)

คุณลักษณะเฉพาะตัวที่ใช้งานการพิสูจน์ทราบตัวตน



ปัญหาการกำหนดและรักษารหัสผ่าน



เรือนจำป่วน! แฮกเกอร์เจาะระบบกล้องวงจรปิด ไลฟ์สดชีวิตนักโทษในคุก

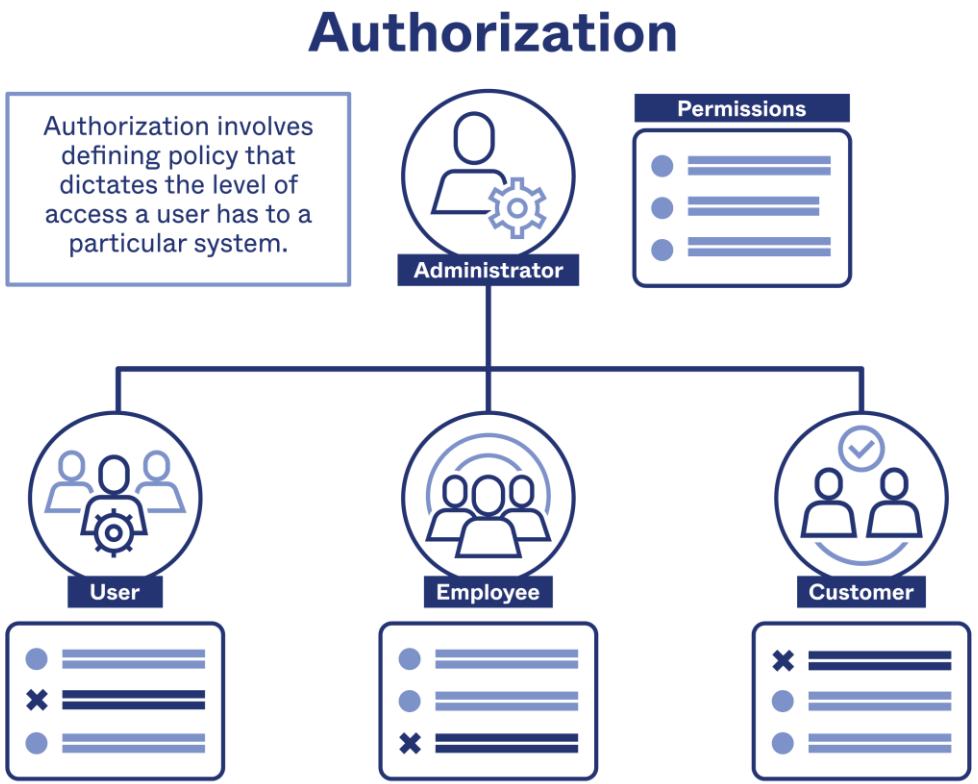
25 ธ.ค. 62 (11:00 น.) ความคิดเห็น 7

กดฟัง

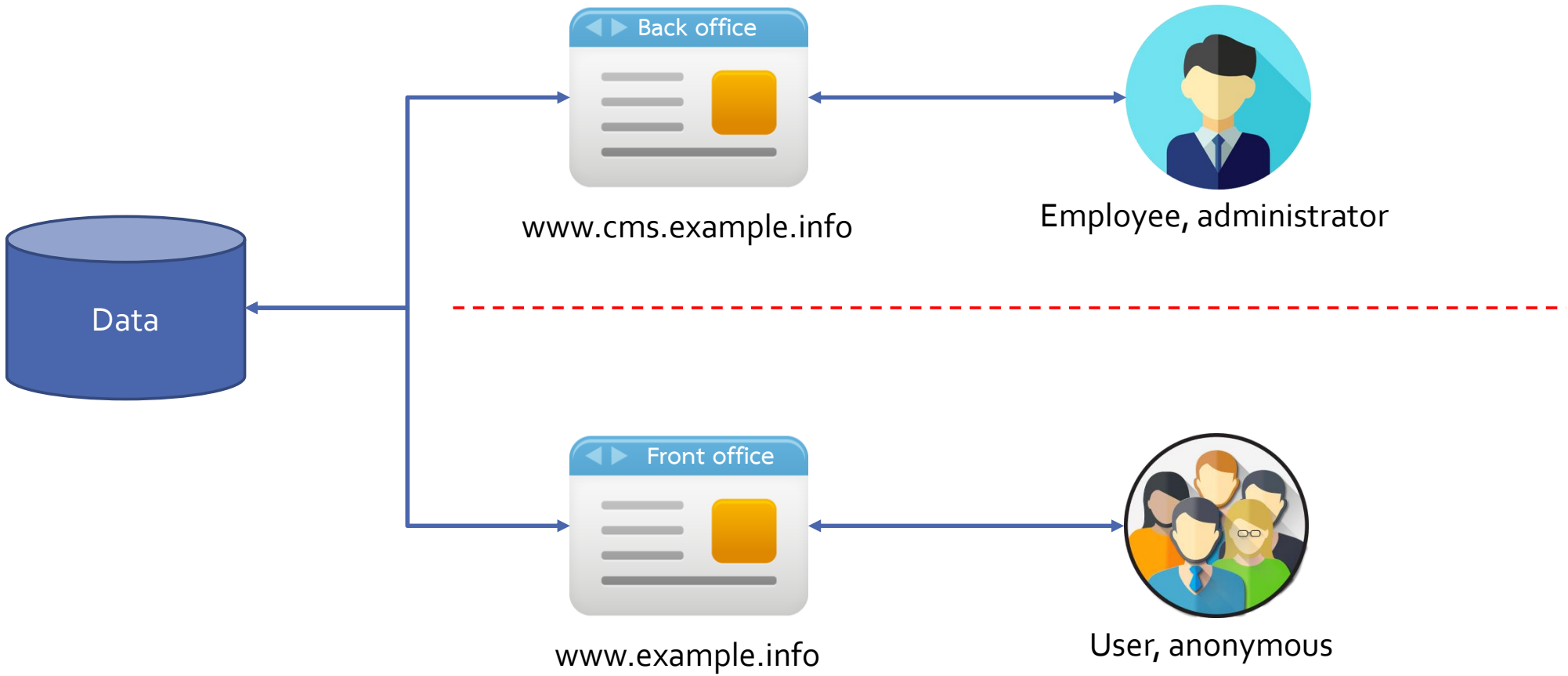
Add @Sanook.com

การอนุญาต (Authorization)

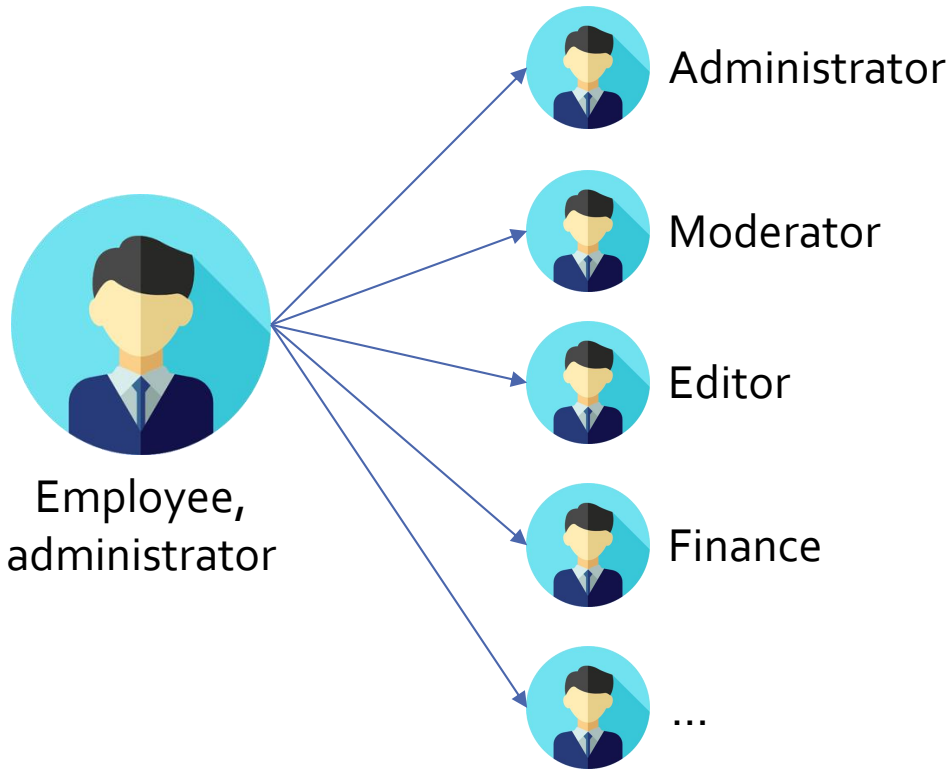
เป็นกลไกการอนุญาตหรือให้สิทธิ์ในการเข้าถึงระบบและเข้าใช้ข้อมูลในระบบของผู้ใช้ที่ผ่านการพิสูจน์ตัวตนมาแล้ว โดยกลไกจะพิจารณาว่าผู้ใช้แต่ละคนได้รับอนุญาตให้เข้าถึงระบบในระดับใดบ้าง และเข้าใช้ข้อมูลส่วนใดได้บ้าง (ARE you allow to do that ?)

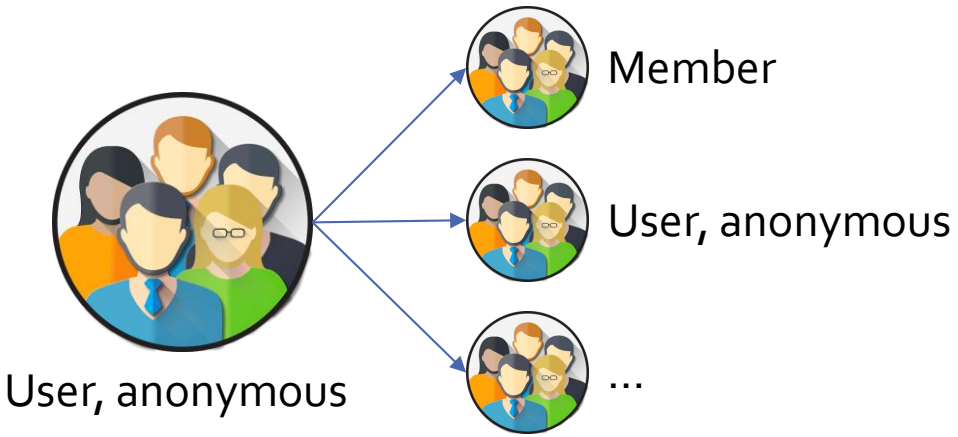


Authorization : Separate Interfaces

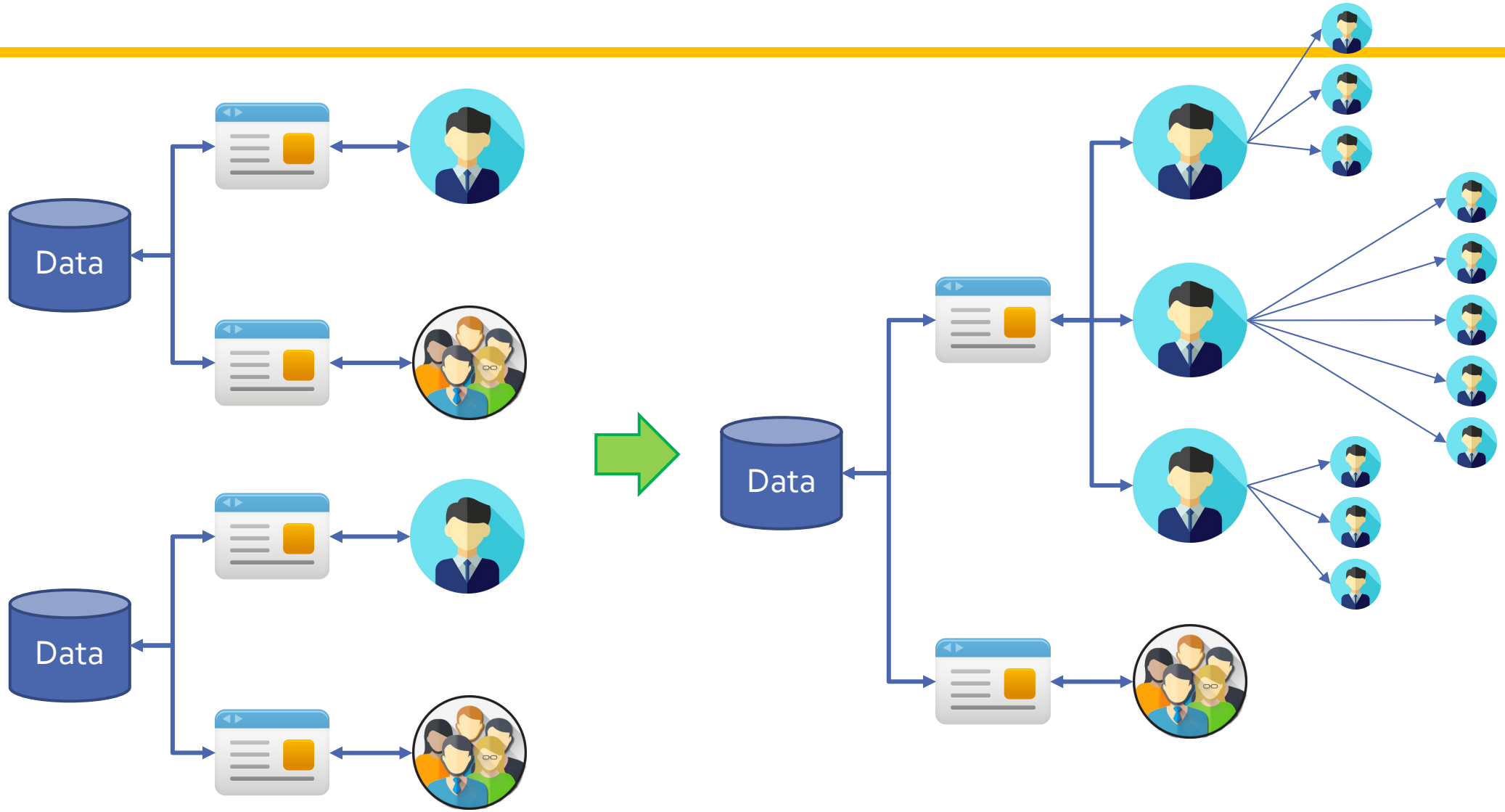


Authorization : User Types

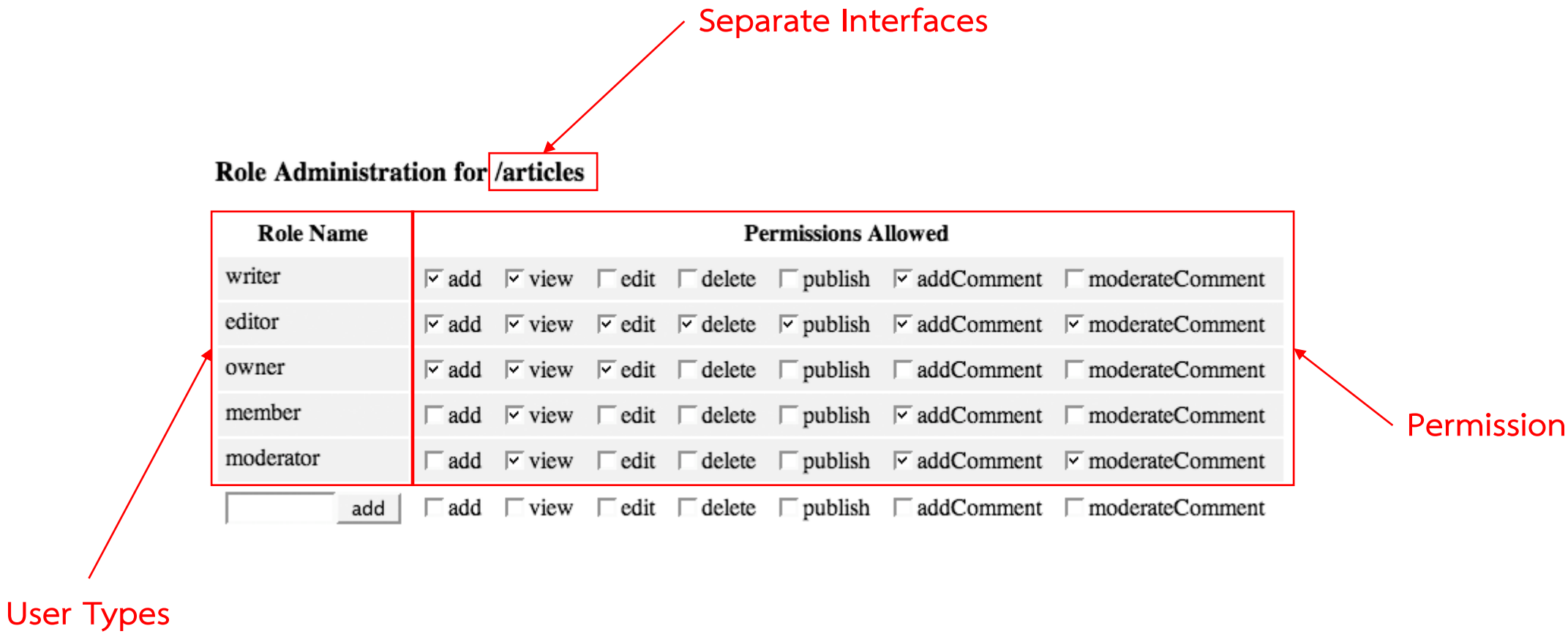




Authorization : User Groups



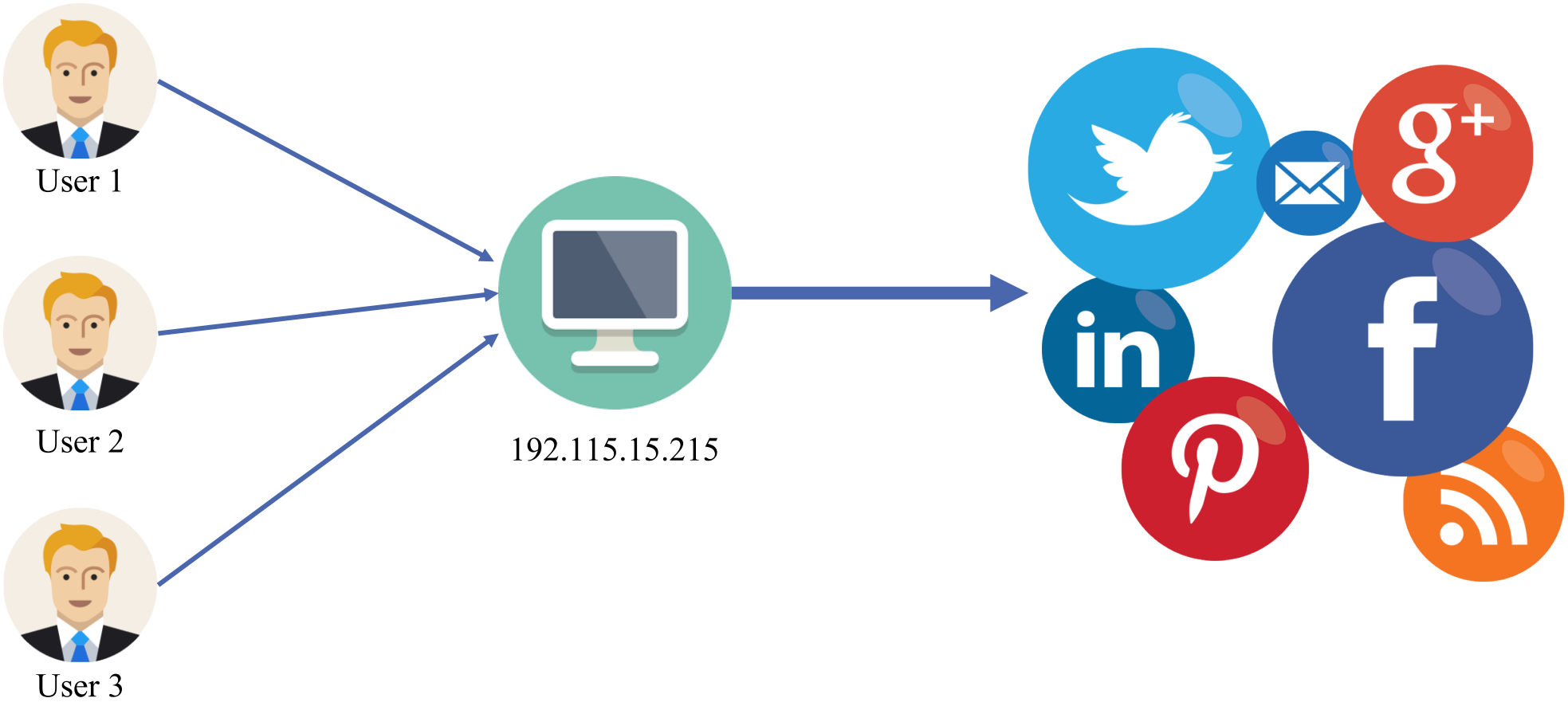
Authorization : The manage Roles User Interface



การตรวจสอบได้ (Accountability)

ในขั้ยตอนสุดท้าย ของการควบคุมการเข้าถึง คือ การตรวจสอบย้อนกลับเกี่ยวกับสิ่งที่ได้เกิดขึ้นในระบบคอมพิวเตอร์ หรือเครือข่ายไปแล้ว การตรวจสอบจะเกิดขึ้นไม่ได้ถ้าไม่มีหลักฐานที่เชื่อถือได้ ซึ่งหลักฐานที่เก็บบันทึกเหตุการณ์ที่เกิดขึ้นเราจะเรียกว่า ล๊อก (Log)

ทำไมต้องมี Log file



ทำไมต้องมี Log file

พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

"**มาตรา ๒๖** ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใด เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปี เป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้"

หน้า ๒๔
เล่ม ๑๓๔ ตอนที่ ๑๐ ก ราชกิจจานุเบกษา ๒๔ มกราคม ๒๕๖๐

พระราชบัญญัติ
ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒)
พ.ศ. ๒๕๖๐

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร

ให้ไว้ ณ วันที่ ๒๓ มกราคม พ.ศ. ๒๕๖๐
เป็นปีที่ ๒ ในรัชกาลปัจจุบัน

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร มีพระราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐"

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ให้ยกเลิกความในมาตรา ๔ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

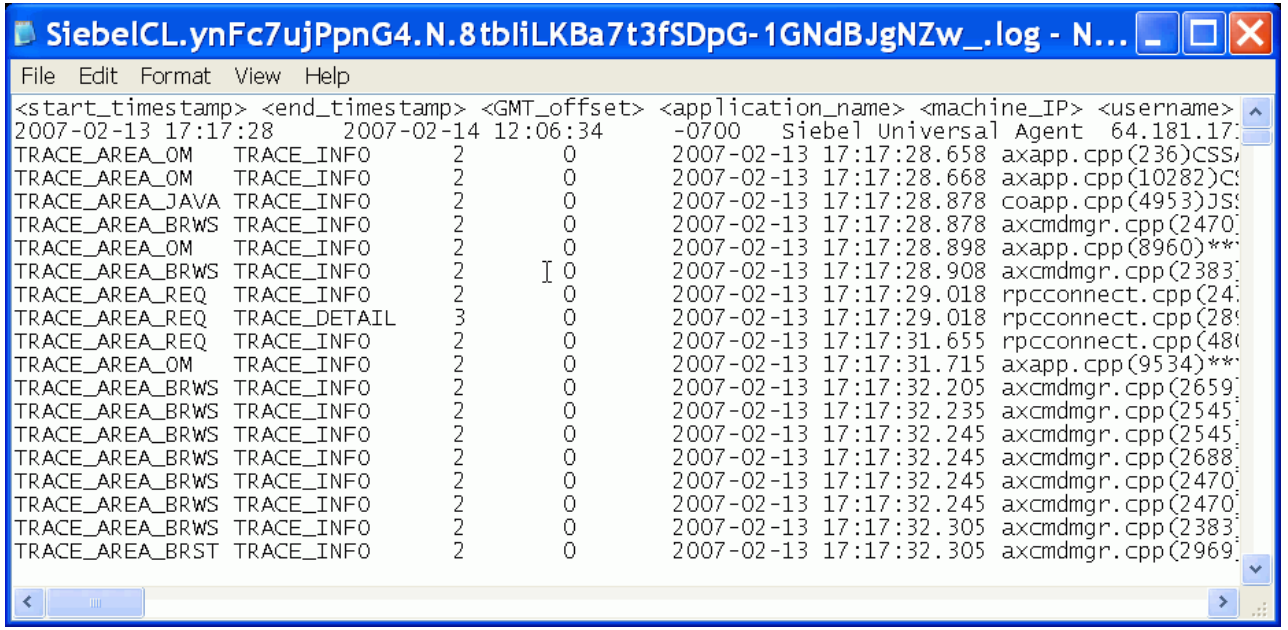
"มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจแต่งตั้งพนักงานเจ้าหน้าที่กับออกกฎกระทรวงและประกาศเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงและประกาศนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้"

มาตรา ๔ ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา ๑๓ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

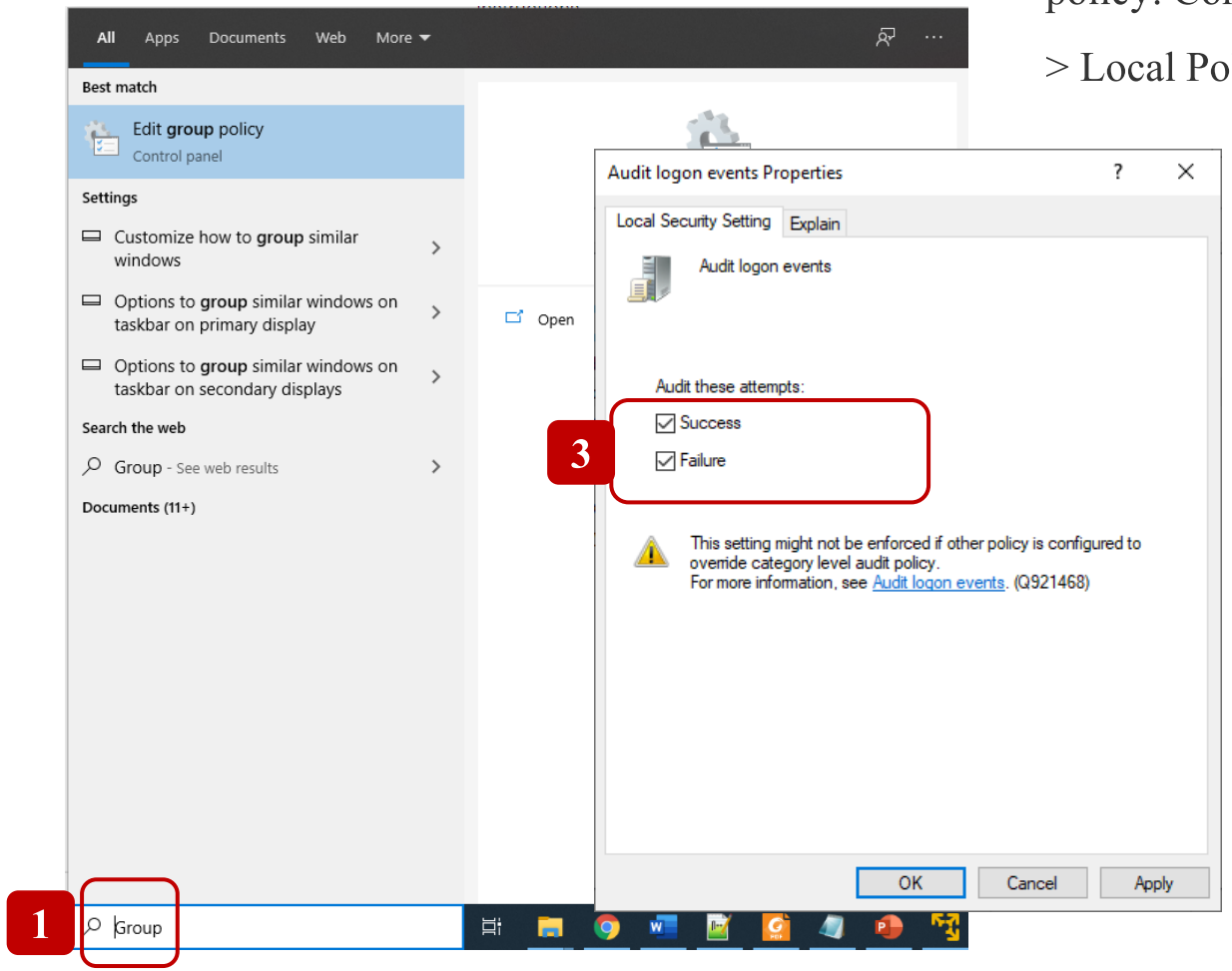
Logging Data

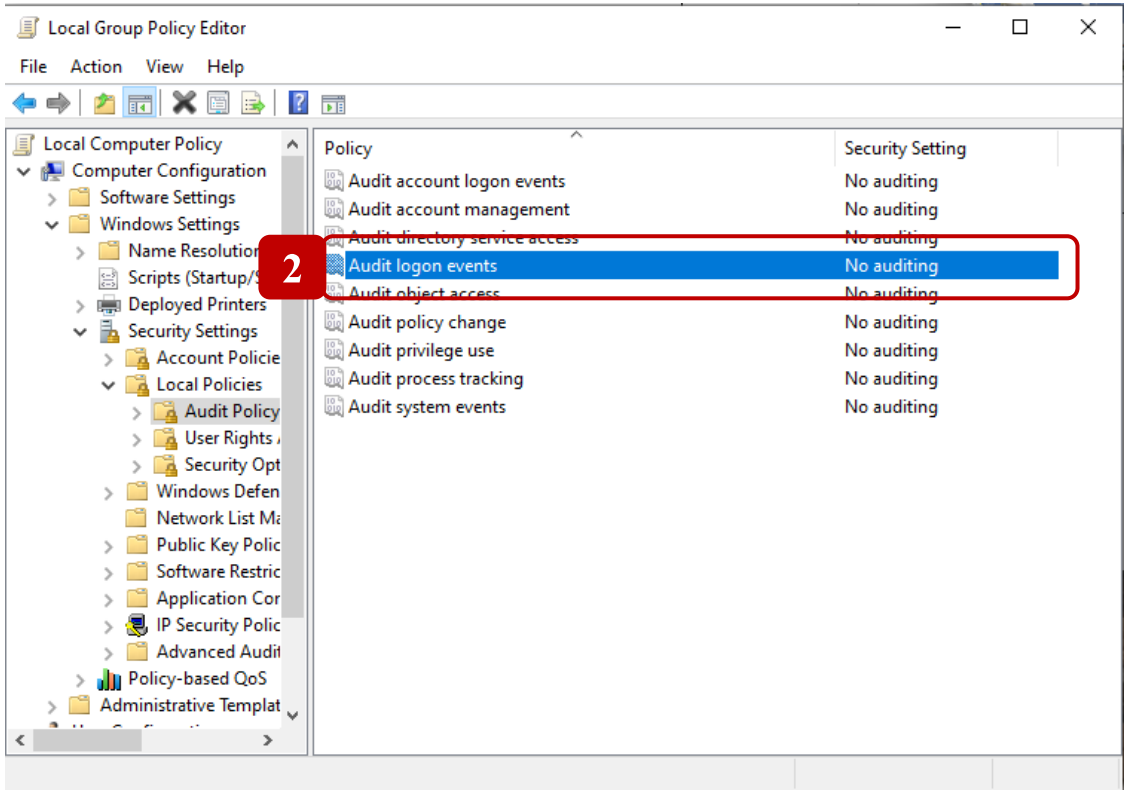
ไฟล์การจราจรทางข้อมูล ใช้เพื่อตรวจสอบกิจกรรมบนเซิร์ฟเวอร์ สามารถวิเคราะห์วิธีการที่ผู้ใช้งานใช้โปรแกรม และค้นหาหลักฐานของปัญหาด้านความปลอดภัย รวมถึงความสามารถในการบอกว่าใครทำอะไรและที่ไหนและเมื่อใดที่ทำไปแล้วนั้นอนุญาตให้ผู้ใช้ที่รับผิดชอบต่อการกระทำของพวกเขา



Enable get Log file in Windows 10 (System Log)

policy: Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy





View Log file in Windows 10

Windows Logs > Security > Event Id : 4624