บทที่ 3 : การป้องกันการเจาะระบบ Part2

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

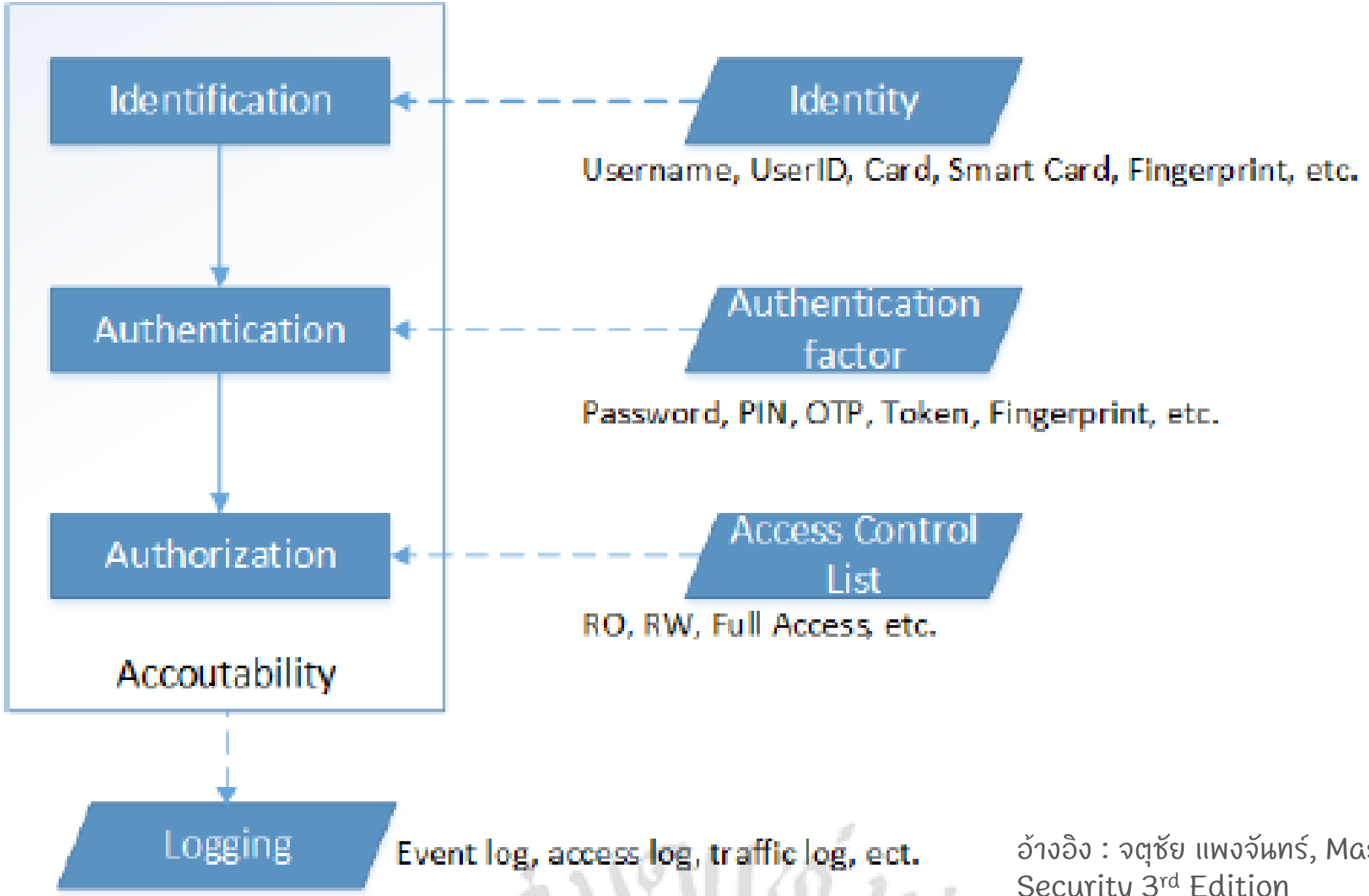
Agenda

- การควบคุมการเข้าถึง (Access Control)

การควบคุมการเข้าถึง (Access Control)

มี 4 ขั้นตอนหลักๆ คือ

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



อ้างอิง : จตุชัย แพงจันทร์, Master in Security 3rd Edition

การระบุตัวตน (Identification)

การระบุตัวตน เป็นสิ่งที่แทนตัวผู้ใช้เพื่อระบุตัวตน ปกติจะไม่ซ้ำกัน มักประกอบไปด้วย

- Username/User ID
- รหัสผ่าน
- ข้อมูลส่วนตัว
- ชื่อหน่วยงาน
- กลุ่มผู้ใช้
- สิทธิ์ในการใช้งาน
- นโยบาย

LDAP
(Lightweight Directory Access Protocol)

- เป็นโปรโตคอลมาตรฐานในการเข้าถึงไดเร็คทอรี
- ในองค์กรจะมีไดเร็คทอรีฐานข้อมูลผู้ใช้งานกลาง ซึ่งจะถูกเรียกใช้งานผ่าน LDAP

LDAP

Lightweight Directory Access Protocol

การพิสูจน์ทราบตัวตน (Authentication)

เป็นสิ่งยืนยันว่าเป็นคนนั้นหรือสิ่งนั้นจริง

ซึ่งต้องผ่านการระบุตัวตนให้ได้ก่อน

การพิสูจน์ทราบตัวตน 3 ประเภท

What you know 

What you have 

What you are 

การเดารหัสผ่าน (Password Guessing)

- ปกติแล้วการพิสูจน์ทราบตัวตนของผู้ใช้ จะใช้ Username และ Password โดย Username จะเป็นส่วนที่เปิดเผย แต่รหัสผ่านจะมีเฉพาะเจ้าของเท่านั้นที่ทราบ
- ผู้ใช้ส่วนใหญ่จะใช้คู่ Username และ Password สำหรับล็อกอินเข้าบัญชีในหลายๆระบบ เนื่องจากเป็นการยากที่คนๆหนึ่งจะจำรหัสผ่านได้มากมาย

Login: admin
Password: admin

Secure enough...

รหัสผ่านที่ถือว่ามีคุณสมบัติง่ายต่อการเดา

- รหัสผ่านที่สั้น เช่น xyz, abcd
- รหัสผ่านเดียวกับ Username
- คำที่รู้จักและคุ้นเคย เช่น password, admin
- มีข้อมูลส่วนตัวในรหัสผ่าน เช่น ชื่อ เบอร์โทร วันเกิด
- ใช้รหัสผ่านเดียวกับทุกระบบที่ใช้
- เขียนรหัสผ่านไว้บนกระดาษแล้วเก็บไว้ในที่ที่ค้นหาได้ง่าย
- ไม่เปลี่ยนรหัสผ่านเป็นประจำ

ระยะเวลาที่ใช้ในการเดารหัสผ่าน

Length	Lowercase	+Uppercase	+Nos. & Symbols
6 characters	10 minutes	10 hours	18 days
7 characters	4 hours	23 days	4 years
8 characters	4 days	3 years	463 years
9 characters	4 months	178 years	44,530 years

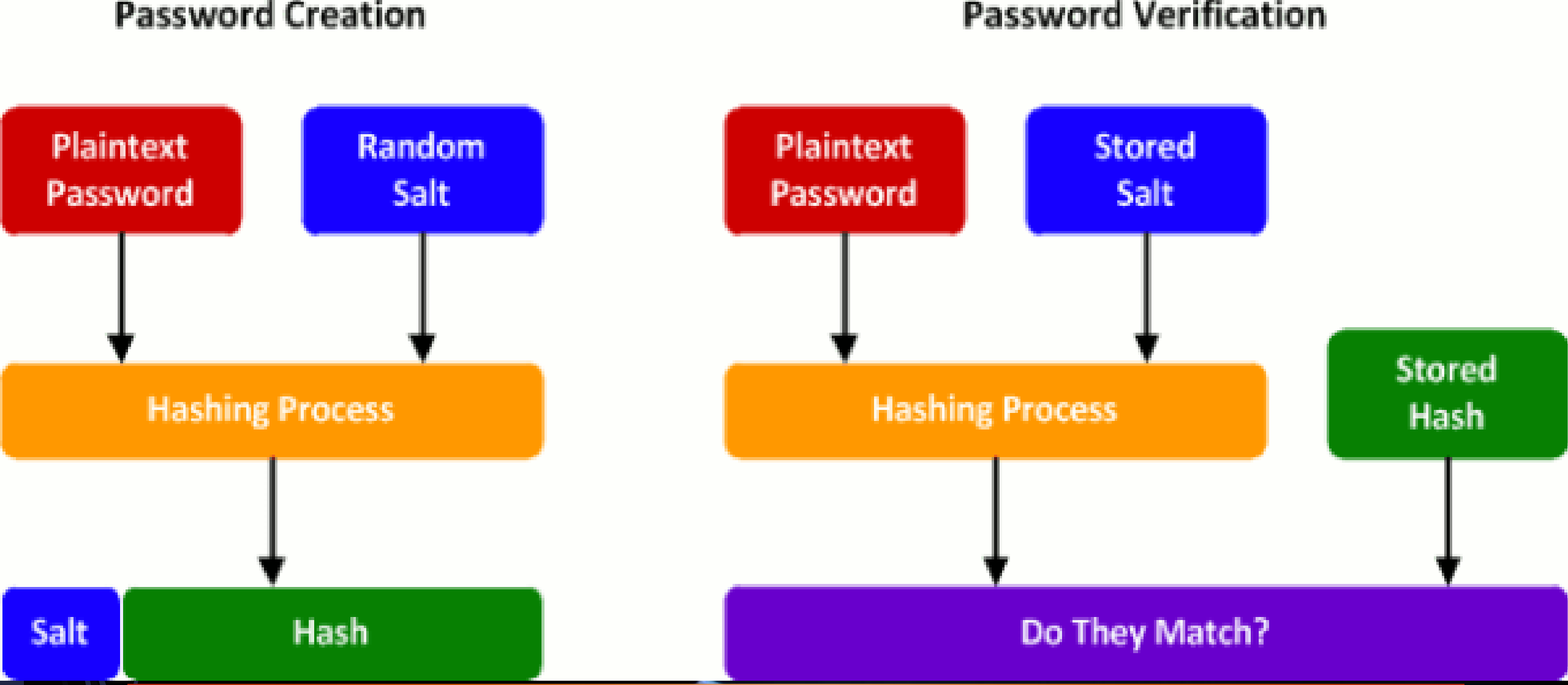
http://randommization.com/2011/02/14/time-a-hackers-computer-takes-to-randomly-guess-your-password/

การป้องกันรหัสผ่าน

- อาจใช้ซอฟต์แวร์จัดการรหัสผ่าน (Password Manager) เข้ามาช่วยในการเก็บและสร้างรหัสผ่าน
- สามารถศึกษาซอฟต์แวร์ดังกล่าวได้จากเว็บไซต์
- http://www.pcmag.com/article2/0,2817,2407168,00.asp

ซอฟต์แวร์ป้องกันรหัสผ่าน

Name	Zoho Vault	Sticky Password Premium	Dashlane 4	LastPass 4.0 Premium	LogMeOnce Password Management Suite Ultimate 5.2	Keeper Password Manager & Digital Vault 10	Password Boss Premium v2.0	AgileBits 1Password 6	RoboForm 8 Everywhere	True Key by Intel Security (2017)
		Sticky Password			LogMeOnce	keeper	PASSWORD BOSS		RoboForm	True Key
Lowest Price	$12.00 Zoho	$14.99 Special Offer	$39.99 Dashlane - Synced		$39.00 LogMeOnce				$19.95 RoboForm	
	SEE IT	SEE IT	SEE IT		SEE IT				SEE IT	
Editors' Rating	●●●◐○	●●●●◐ EC	●●●●● EC	●●●●● EC	●●●●◐ EC	●●●●○	●●●●○	●●●◐○	●●●◐○	●●●◐○
Import From Browsers	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓
Import From Competitors	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Two-Factor Authentication	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓



การเก็บรักษา Password ในฐานข้อมูลให้ปลอดภัยมากขึ้น

Secure Password in PHP: https://secure.php.net/manual/en/function.password-hash.php
And https://secure.php.net/manual/en/function.password-verify.php

OTP (One-Time Password)

- เป็นรหัสผ่านที่จะมีการเปลี่ยนแปลงทุกครั้งที่มีการล็อกอินเข้าสู่ระบบ
- ออกแบบมาเพื่อป้องกันการเดารหัสผ่านและการดักฟัง
- ปกติจะใช้การส่งข้อความไปยังโทรศัพท์มือถือ (What you have) ไม่นิยมส่งทางอีเมลเพราะหากอีเมลโดนแฮ็ก จะทำให้ไม่ปลอดภัย

Token หรือ Authenticator

- เป็นฮาร์ดแวร์หรือแอพพลิเคชั่นที่ใช้สร้างรหัสผ่านขณะใช้งาน และจะเปลี่ยนแปลงไปทุก ๆ ครั้ง

Biometric

ประเภทไบโอเมตริกส์	การใช้งาน	ความแม่นยำ	การยอมรับของผู้ใช้
การลงลายเซ็น	ง่ายมาก	ต่ำ	ปานกลาง
เสียงพูด	ง่ายมาก	ต่ำ	ปานกลาง
รูปโครงหน้า	ปานกลาง	ปานกลาง	ปานกลาง
ลายฝ่ามือ	ปานกลาง	ปานกลาง	สูง
ลายนิ้วมือ	ปานกลาง	สูง	สูง
จอตาและม่านตา	ยาก	สูงมาก	ต่ำ
DNA	ยาก	สูงมาก	ต่ำ

2FA
(Two-factors Authentication)

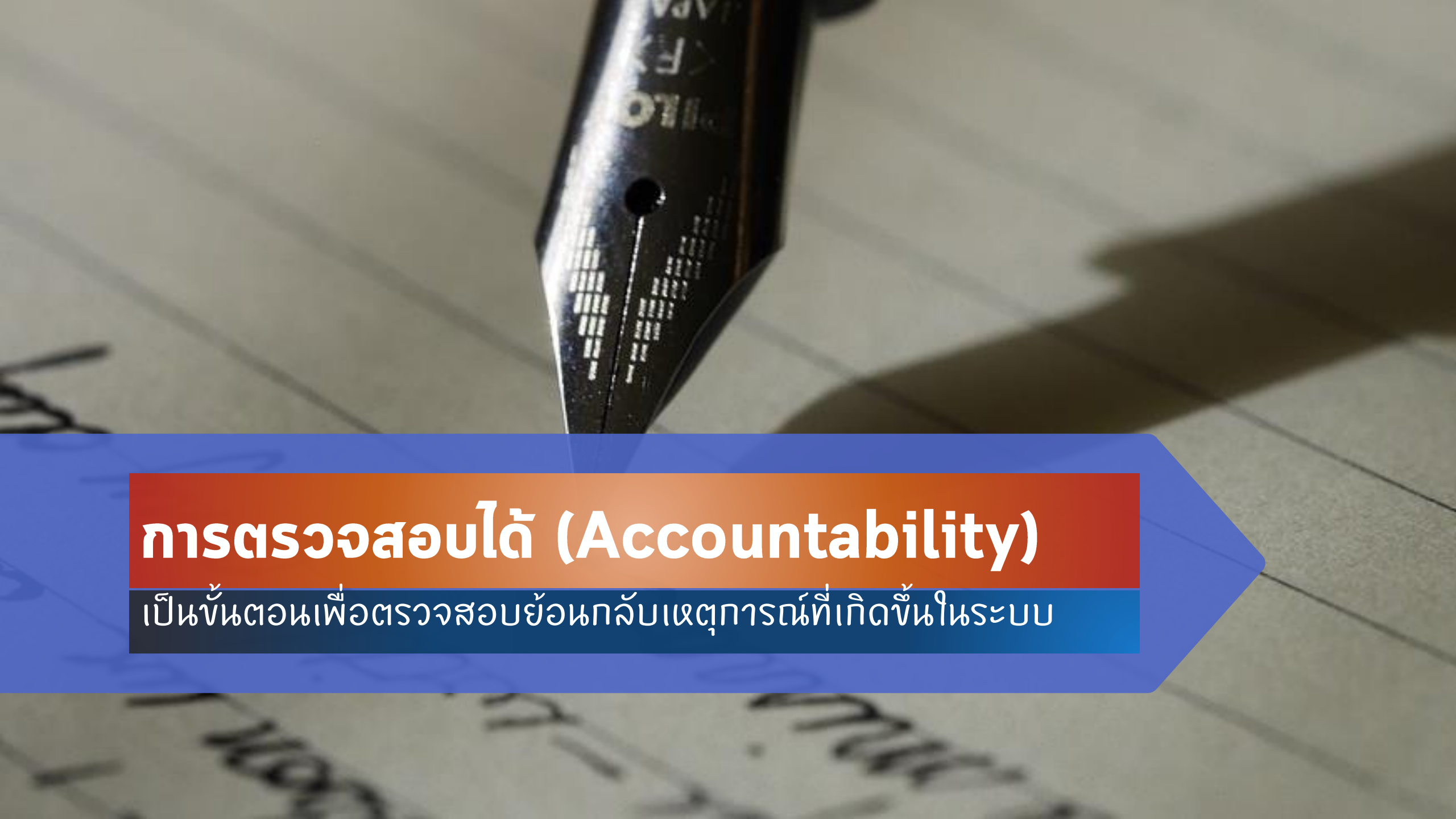
- เป็นการพิสูจน์หลักฐานสองในสามหรือมากกว่า ได้แก่ สิ่งที่รู้ สิ่งที่มี และสิ่งที่เป็น
- เช่นใช้รหัสผ่านคู่กับลายนิ้วมือ หรือรหัสผ่านคู่กับโทเคน

การอนุญาต (Authorization)

เป็นกระบวนการหลังจากที่มีการพิสูจน์ทราบตัวตนแล้ว
โดยอนุญาตตามสิทธิ์ที่ User คนนั้นหรือสิ่งนั้นมี

การอนุญาตแบ่งเป็น 3 ทาง

- อนุญาตเป็นรายๆ (ไม่นิยมใช้)
- อนุญาตเป็นกลุ่ม (นิยมใช้ทั่วไป)
- อนุญาตเข้าใช้หลาย ๆ ระบบ (Single Sign-on) นิยมใช้ในองค์กรที่มีระบบมากๆ

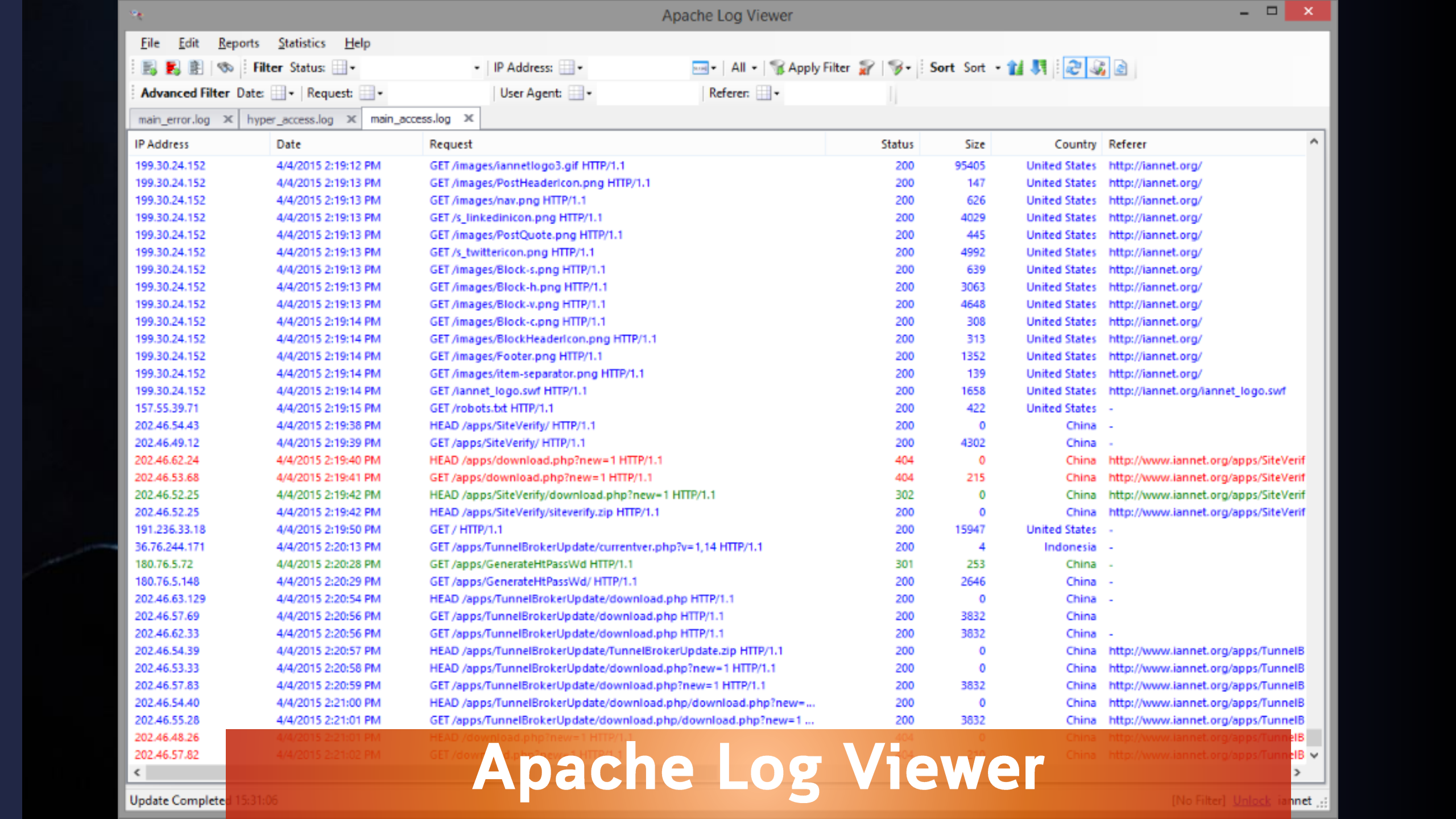


การตรวจสอบได้ (Accountability)

เป็นขั้นตอนเพื่อตรวจสอบย้อนกลับเหตุการณ์ที่เกิดขึ้นในระบบ

การเก็บล็อก (Log)

- ล็อกเป็นการเก็บเหตุการณ์ต่าง ๆ ที่เกิดขึ้นภายในระบบ
- เป็นสิ่งสำคัญมากในการสืบสวนการโจมตี
- ใช้เป็นหลักฐานทางกฎหมายได้
- แฮ็กเกอร์มักทำการลบล็อกเมื่อเข้าโจมตีระบบแล้ว
- ควรมีระบบจัดเก็บล็อกที่ปลอดภัย เช่น ใน Linux จะมีเซิฟเวอร์สำหรับเก็บ Syslog โดยเฉพาะ



Apache Log Viewer