**Computer System Security**

**cryptographic tools**

|  |  |
| --- | --- |
| **Word** | **Meaning** |
| Security | Security is the state of being protected against harm or threats (ความปลอดภัยหมายถึงสถานะที่ได้รับการปกป้องจากอันตรายหรือภัยคุกคาม) |
| cryptography | Cryptography refers to the practice and study of techniques for securing communication (การเข้ารหัสหมายถึงการศึกษาและปฏิบัติเทคนิคในการป้องกันการสื่อสาร) |
| plaintext | Plaintext is the original, readable text before encryption (ข้อความต้นฉบับที่สามารถอ่านได้ก่อนการเข้ารหัส) |
| ciphertext | Ciphertext is the encrypted text that is unreadable without decryption (ข้อความที่ถูกเข้ารหัสซึ่งไม่สามารถอ่านได้โดยไม่มีการถอดรหัส) |
| key | A key is secret information used to encrypt and decrypt data (คีย์คือข้อมูลลับที่ใช้ในการเข้ารหัสและถอดรหัสข้อมูล) |
| encryption | Encryption is the process of converting plaintext into ciphertext (การเข้ารหัสคือกระบวนการแปลงข้อความต้นฉบับให้เป็นข้อความรหัส) |
| decryption | Decryption is the process of converting ciphertext back into plaintext (การถอดรหัสคือกระบวนการแปลงข้อความรหัสกลับเป็นข้อความต้นฉบับ) |

|  |  |
| --- | --- |
| hash function | A hash function generates a fixed-size output (digest) from an input message (ฟังก์ชันแฮชคือกระบวนการที่สร้างผลลัพธ์ขนาดคงที่จากข้อความต้นฉบับ) |
| digital signature | A digital signature is a cryptographic method for verifying the authenticity of a message or document (ลายเซ็นดิจิทัลคือวิธีการเข้ารหัสที่ใช้ยืนยันความแท้จริงของข้อความหรือเอกสาร) |
| RSA | RSA is an asymmetric encryption algorithm using two keys: public and private (RSA คืออัลกอริทึมการเข้ารหัสแบบอสมมาตรที่ใช้คีย์สองตัวคือคีย์สาธารณะและคีย์ส่วนตัว) |
| symmetric encryption | Symmetric encryption uses the same key for both encryption and decryption (การเข้ารหัสแบบสมมาตรใช้คีย์เดียวกันในการเข้ารหัสและถอดรหัส) |
| asymmetric encryption | Asymmetric encryption uses a pair of keys: public for encryption and private for decryption (การเข้ารหัสแบบอสมมาตรใช้คีย์คู่หนึ่ง คีย์สาธารณะสำหรับเข้ารหัส และคีย์ส่วนตัวสำหรับถอดรหัส) |
| message authentication | Message authentication ensures a message’s integrity and source authenticity (การยืนยันข้อความช่วยให้มั่นใจว่าข้อความไม่ถูกดัดแปลงและมาจากแหล่งที่แท้จริง) |
| hash | Hashing is converting data into a fixed-size value for authentication or integrity checks (การแฮชคือการแปลงข้อมูลให้เป็นค่าขนาดคงที่เพื่อการยืนยันหรือการตรวจสอบความสมบูรณ์) |

|  |  |
| --- | --- |
| key management | Key management is the process of handling and safeguarding encryption keys (การจัดการคีย์คือกระบวนการจัดการและปกป้องคีย์เข้ารหัส) |
| man-in-the-middle attack | A cyberattack where an attacker intercepts communication between two parties (การโจมตีแบบคนกลางคือการที่ผู้โจมตีสอดแทรกการสื่อสารระหว่างสองฝ่าย) |

**Malicious software**

|  |  |
| --- | --- |
| **Word** | **Meaning** |
| Malware | |  | | --- | | Software designed to disrupt, damage, or gain unauthorized access to a computer system. (มัลแวร์คือซอฟต์แวร์ที่ถูกออกแบบมาเพื่อรบกวน ทำลาย หรือเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต) |  |  | | --- | |  | |
| Virus | |  |  |  | | --- | --- | --- | | |  | | --- | | Attaches to programs and replicates, causing damage when executed. (ไวรัสคือซอฟต์แวร์ที่แทรกตัวเข้ากับโปรแกรมและแพร่กระจาย โดยจะสร้างความเสียหายเมื่อถูกใช้งาน) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Worm |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Self-replicating program spreading across networks. (เวิร์มคือโปรแกรมที่แพร่กระจายตัวเองผ่านเครือข่าย) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Trojan Horse |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Malicious program disguised as legitimate software. (โทรจันคือโปรแกรมอันตรายที่ปลอมตัวเป็นซอฟต์แวร์ที่ถูกต้อง) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Logic Bomb |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Code that triggers malicious actions when conditions are met. (ลอจิกบอมบ์คือโค้ดที่ทำงานเพื่อสร้างความเสียหายเมื่อเงื่อนไขบางอย่างถูกต้อง) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Backdoor/Trapdoor |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Hidden access points allowing unauthorized access. (ช่องโหว่ลับ/ดักบอมบ์คือทางเข้าที่ซ่อนอยู่ที่อนุญาตให้เข้าถึงระบบโดยไม่ได้รับอนุญาต) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Spyware |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Software that collects and transmits user data without consent. (สปายแวร์คือซอฟต์แวร์ที่รวบรวมและส่งข้อมูลของผู้ใช้โดยไม่ได้รับอนุญาต) |  |  | | --- | |  | |  |  | | --- | |  | |
| Adware | |  |  |  | | --- | --- | --- | | |  | | --- | | Software that shows unwanted advertisements. (แอดแวร์คือซอฟต์แวร์ที่แสดงโฆษณาที่ไม่พึงประสงค์) |  |  | | --- | |  | |  |  | | --- | |  | |
| Ransomware | |  |  |  | | --- | --- | --- | | |  | | --- | | Encrypts or locks systems, demanding payment for access. (แรนซัมแวร์คือซอฟต์แวร์ที่เข้ารหัสหรือล็อกระบบ และเรียกค่าไถ่เพื่อเข้าถึง) |  |  | | --- | |  | |  |  | | --- | |  | |
| Keylogger | |  |  |  | | --- | --- | --- | | |  | | --- | | Captures and records keystrokes. (คีย์ล็อกเกอร์คือซอฟต์แวร์ที่บันทึกการพิมพ์แป้นพิมพ์) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Rootkit |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Tools that provide stealthy admin-level access to a system. (รูทคิทคือเครื่องมือที่ช่วยเข้าถึงระบบในระดับผู้ดูแลแบบซ่อนเร้น) |  |  | | --- | |  | |  |  | | --- | |  | |
| Zombie | |  |  |  | | --- | --- | --- | | |  | | --- | | Infected device controlled to perform malicious activities. (ซอมบี้คืออุปกรณ์ที่ถูกติดไวรัสและควบคุมเพื่อทำกิจกรรมที่เป็นอันตราย) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Polymorphic Virus |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Changes its code to avoid detection. (ไวรัสโพลีมอร์ฟิกคือไวรัสที่เปลี่ยนโค้ดของตัวเองเพื่อหลีกเลี่ยงการตรวจจับ) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Zero-Day Attack |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Exploits vulnerabilities unknown to the vendor. (การโจมตีช่องโหว่ใหม่คือการใช้ประโยชน์จากช่องโหว่ที่ยังไม่มีการแก้ไข) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Blended Attack |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Combines multiple attack methods for maximum effect. (การโจมตีแบบผสมคือการรวมวิธีการโจมตีหลายรูปแบบเพื่อเพิ่มผลกระทบสูงสุด) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Auto-rooter |  |  | | --- | |  | | |  | | --- | | Tool for exploiting vulnerabilities and gaining root access. (เครื่องมือเจาะระบบคือเครื่องมือที่ใช้เจาะช่องโหว่เพื่อเข้าถึงสิทธิ์ระดับผู้ดูแล) | |

**Non malicious software**

|  |  |
| --- | --- |
| **Word** | **Meaning** |
| Buffer Overflow | |  | | --- | | When input exceeds the allocated memory buffer size, leading to memory corruption. (บัฟเฟอร์โอเวอร์โฟลว์คือการที่ข้อมูลนำเข้าเกินขนาดหน่วยความจำที่กำหนดไว้ ทำให้เกิดความเสียหายต่อหน่วยความจำ) |  |  | | --- | |  | |
| |  | | --- | | Defensive Programming |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Programming approach to ensure software remains functional under unexpected conditions. (การเขียนโปรแกรมป้องกันคือวิธีการเขียนโปรแกรมเพื่อให้ซอฟต์แวร์ยังคงทำงานได้ในสถานการณ์ที่ไม่คาดคิด) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Input Validation |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Ensuring external data conforms to expectations before processing. (การตรวจสอบความถูกต้องของข้อมูลนำเข้าคือการยืนยันว่าข้อมูลจากภายนอกเป็นไปตามข้อกำหนดก่อนการประมวลผล) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | SQL Injection |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Maliciously injecting SQL queries into an application to manipulate databases. (การโจมตีแบบ SQL Injection คือการแทรกคำสั่ง SQL ที่เป็นอันตรายเพื่อควบคุมฐานข้อมูล) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Cross-Site Scripting (XSS) |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Injecting scripts into web applications to attack users or systems. (การโจมตี Cross-Site Scripting คือการแทรกสคริปต์ในเว็บแอปพลิเคชันเพื่อโจมตีผู้ใช้หรือระบบ) |  |  | | --- | |  | |  |  | | --- | |  | |
| Shellcode | |  |  |  | | --- | --- | --- | | |  | | --- | | Malicious low-level code executed on a vulnerable system. (โค้ดเชลล์ที่เป็นอันตรายคือโค้ดระดับต่ำที่ใช้โจมตีระบบที่มีช่องโหว่) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Code Injection |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Including unauthorized code into a system's execution flow. (การแทรกโค้ดที่ไม่ได้รับอนุญาตคือการใส่โค้ดเข้าไปในกระบวนการทำงานของระบบ) |  |  | | --- | |  | |  |  | | --- | |  | |

|  |  |
| --- | --- |
| Stack Overflow | Overflowing data onto a program stack, potentially altering program flow. (สแต็กโอเวอร์โฟลว์คือการที่ข้อมูลล้นเข้าสู่สแต็กของโปรแกรม ซึ่งอาจเปลี่ยนแปลงการทำงานของโปรแกรม) |
| Safe Temporary Files | |  | | --- | | Temporary files with random, secure names and limited access permissions. (ไฟล์ชั่วคราวที่ปลอดภัยคือไฟล์ชั่วคราวที่มีชื่อสุ่มและกำหนดสิทธิ์การเข้าถึงอย่างปลอดภัย) |  |  | | --- | |  | |
| Good Design Principles | Security-focused design strategies, e.g., least privilege and open design. (หลักการออกแบบที่ดีคือกลยุทธ์การออกแบบที่เน้นความปลอดภัย เช่น การให้สิทธิ์น้อยที่สุดและการออกแบบแบบเปิด) |

**Operating system security authentication and access control**

|  |  |
| --- | --- |
| **Word** | **Meaning** |
| |  | | --- | | Operating System (OS) |  |  | | --- | |  | | |  | | --- | | Software that manages hardware and software resources, ensuring security and efficient operation. (ระบบปฏิบัติการคือซอฟต์แวร์ที่จัดการทรัพยากรฮาร์ดแวร์และซอฟต์แวร์ เพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพและปลอดภัย) |  |  | | --- | |  | |
| |  | | --- | | User Authentication |  |  | | --- | |  | | |  | | --- | | Software that manages hardware and software resources, ensuring security and efficient operation. (ระบบปฏิบัติการคือซอฟต์แวร์ที่จัดการทรัพยากรฮาร์ดแวร์และซอฟต์แวร์ เพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพและปลอดภัย) |  |  | | --- | |  | |
| |  | | --- | | Access Control |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Restricting resource usage to authorized users or processes. (การควบคุมการเข้าถึงคือการจำกัดการใช้งานทรัพยากรให้เฉพาะผู้ใช้หรือกระบวนการที่ได้รับอนุญาต) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Memory Protection |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Mechanisms to prevent one process from accessing another’s memory. (การป้องกันหน่วยความจำคือกลไกที่ป้องกันไม่ให้กระบวนการหนึ่งเข้าถึงหน่วยความจำของอีกกระบวนการหนึ่ง) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Mandatory Access Control (MAC) |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Restricting access based on security labels and clearances, independent of user discretion. (การควบคุมการเข้าถึงแบบบังคับคือการจำกัดการเข้าถึงตามระดับความปลอดภัยและการอนุญาต โดยไม่ขึ้นกับการตัดสินใจของผู้ใช้) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Discretionary Access Control (DAC) |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Access determined by the resource owner, who decides permissions. (การควบคุมการเข้าถึงแบบยืดหยุ่นคือการที่เจ้าของทรัพยากรเป็นผู้กำหนดสิทธิ์ในการเข้าถึง) |  |  | | --- | |  | |  |  | | --- | |  | |
| Kernel | |  |  |  | | --- | --- | --- | | |  | | --- | | Core component of the OS responsible for managing security, processes, and hardware. (แกนหลักของระบบปฏิบัติการคือส่วนสำคัญที่รับผิดชอบการจัดการความปลอดภัย กระบวนการ และฮาร์ดแวร์) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Trusted Path |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Mechanism ensuring secure communication between user and system to prevent tampering. (เส้นทางที่เชื่อถือได้คือกลไกที่รับรองการสื่อสารที่ปลอดภัยระหว่างผู้ใช้และระบบ เพื่อป้องกันการดัดแปลงข้อมูล) |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Reference Monitor |  |  | | --- | |  | | |  | | --- | | Abstract system that mediates all access requests to objects, ensuring policy compliance. (ตัวควบคุมการอ้างอิงคือระบบนามธรรมที่ทำหน้าที่ตรวจสอบคำขอเข้าถึงทั้งหมดเพื่อให้สอดคล้องกับนโยบาย) |  |  | | --- | |  | |
| |  | | --- | | Role-Based Access Control (RBAC) |  |  | | --- | |  | | Access permissions based on user roles rather than individual identity. (การควบคุมการเข้าถึงแบบอิงบทบาทคือการกำหนดสิทธิ์การเข้าถึงตามบทบาทของผู้ใช้แทนที่จะเป็นตัวตนส่วนบุคคล) |

**Database security**

|  |  |
| --- | --- |
| **Word** | **Meaning** |
| Database | |  | | --- | | A structured collection of data stored for use by applications. (ฐานข้อมูลคือชุดของข้อมูลที่ถูกจัดเก็บอย่างมีโครงสร้าง) |  |  | | --- | |  | |
| Database Security | |  | | --- | | Measures to protect databases from unauthorized access or threats. (ความปลอดภัยของฐานข้อมูลคือมาตรการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือภัยคุกคาม) |  |  | | --- | |  | |
| |  | | --- | | Relational Database |  |  | | --- | |  | | |  | | --- | | A database structured with tables, where each table has unique identifiers. (ฐานข้อมูลเชิงสัมพันธ์คือฐานข้อมูลที่จัดโครงสร้างด้วยตาราง และแต่ละตารางมีตัวระบุที่ไม่ซ้ำกัน) |  |  | | --- | |  | |
| SQL (Structured Query Language) | |  | | --- | | A standardized language used for managing and querying relational databases. (SQL คือภาษามาตรฐานที่ใช้จัดการและค้นหาข้อมูลในฐานข้อมูลเชิงสัมพันธ์) |  |  | | --- | |  | |
| |  | | --- | | Access Control |  |  | | --- | |  | | |  | | --- | | Restricting access to data based on user roles and permissions. (การควบคุมการเข้าถึงคือการจำกัดการเข้าถึงข้อมูลตามบทบาทและสิทธิ์ของผู้ใช้) |  |  | | --- | |  | |
| |  | | --- | | Inference |  |  | | --- | |  | | |  | | --- | | The ability to deduce sensitive information from authorized data. (การอนุมานคือความสามารถในการสรุปข้อมูลที่ละเอียดอ่อนจากข้อมูลที่ได้รับอนุญาต) |  |  | | --- | |  | |
| Encryption | |  | | --- | | The process of encoding data to prevent unauthorized access. (การเข้ารหัสคือกระบวนการเข้ารหัสข้อมูลเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต) |  |  | | --- | |  | |
| |  | | --- | | Data Mining |  |  | | --- | |  | | |  | | --- | | The process of analyzing large datasets to discover patterns or relationships. (การทำเหมืองข้อมูลคือกระบวนการวิเคราะห์ชุดข้อมูลขนาดใหญ่เพื่อค้นหารูปแบบหรือความสัมพันธ์) |  |  | | --- | |  | |
| Auditability | |  | | --- | | The ability to track who or what has accessed the database. (ความสามารถในการตรวจสอบคือความสามารถในการติดตามว่าใครหรือสิ่งใดที่เข้าถึงฐานข้อมูล) |  |  | | --- | |  | |
| |  | | --- | | Role-Based Access Control (RBAC) |  |  | | --- | |  | | A system of access control based on user roles. (การควบคุมการเข้าถึงตามบทบาทคือระบบที่จำกัดการเข้าถึงตามบทบาทของผู้ใช้) |