

2110413 comp security

กิจกรรม

① Introduction to computer security

- security เป็นเรื่องที่ลับๆ ไม่ควรรู้บุคคล
- ผู้คนส่วนใหญ่ ทำการรุกราน Hack
- Social Engineer : การใช้กลยุทธ์ทางมนุษย์ ทางความรู้ เช่น identity ล้วง password
- BotNet : Network of bot computers (remote control)
- Warez : Software ผิดกฎหมาย

The protection of resources from being accessed by an unauthorized person at a particular time

10 security principles

- 1) Least privilege ต้อง access + grant
- 2) Defense in depth ~ may password หลายชั้น
- 3) Secure failure
- 4) Secure the weakest link
- 5) Compartmentalization แบ่งส่วน จำกัดพื้นที่ในส่วนๆ ให้
- 6) Simplicity
- 7) It's hard to hide secret ถ้าเป็นความลับ ก็ยากจะซ่อน
- 8) Promote privacy
- 9) Don't extend trust easily
- 10) Trust the community

Security

- = Free from risk of loss
- = ปลอดภัย ไม่เสี่ยงภัย

Privacy

- = the freedom to control access to our personal information

② Security components

Privacy is depending on intent

ปัญหา security อาจจะไม่เป็นปัญหา privacy ขึ้นอยู่กับว่ามีความต้องการหรือไม่

Solution: make an agreement

No privacy without security

security component (the AAA of security) ต้องมี 3 หลักการรองรับ security

- Authentication รู้ตัว
 - Authorization รับได้
 - Accounting (Auditing)
- หลัก 3 หลักการรองรับ → Supporting Concepts
- Integrity Authenticity
 - software engineering & Threat modeling
 - Validation of input

③ Authentication

- ตรวจสอบว่าเข้าร่วมของแท้ ของจริง ของเดิม
- ทำให้ตรวจสอบ validate คุณสมบัติบางอย่าง
 - ผู้ใช้งาน (ตรวจสอบ / สื้อ)
 - ทุกอย่างที่ wrong

ส่วนที่ 1 Prearrange questions, Password, OTP, Challenge and Response

ส่วนที่ 2

ส่วนที่ 3

- การรุกราน Hash / Password hacking

เพรียบเทียบกับ fax → X คือ

- 1) เล่นต่อ X ตาม dictionary จนกว่า find ได้ — dictionary attack
- 2) generate strings every possibility — brute force
- 3) generate strings ด้วยสีรังนองของ hash — rainbow table (lookup table)

④ Authorization อนุญาติ เมื่อ ไม่อนุญาติ

- By Policy (นโยบาย), App-based, to guide and determine present and future decisions
- Type enforcement ~Policeman

Security Policy = ประมวลผลที่แนบมาในรูปแบบ 2 กรณี คือ secure / Insecure (Auth/Unauth)

Secure System = starts in auth state and cannot enter unauth state.

Security Policy

- Confidentiality ผู้ใดที่สามารถอ่านได้ความลับ (who can read)
- Integrity ผู้ใดที่สามารถแก้ไขเปลี่ยนแปลงได้ (who can write/alter)
- Availability (when to access)

Access Control Models - โครงสร้าง Policy

1. MAC : Mandatory Access Control - จำกัดผู้ดูแล ไม่ให้เข้าไปในพื้นที่

- Admins control user
- Multilevel systems
- sensitivity labels

2. DAC : Discretionary Access Control - คนที่มีอำนาจเข้าถึงที่มุ่งรักษา (ไม่ต้องการของคนอื่น)

- Access rights and permission
- ownership
- หัวใจของ MAC

3. RBAC : Role-based Access Control

- least privileges
- ผู้มี Access ที่มีภาระ
- หัวใจสำคัญที่สุด คือ role
- คนที่เข้ามายังระบบจะต้องมี role และมี access ตาม policy

Access Control Matrix

- Product of policy
- Subjects on rows, resources on columns, specify the rules
 - * ACCESS control list - who can do what with this object.
 - * Capability - what I can access (ມຳຈຸດໝາຍ)

implement ທັນທີ admin ອົບຮູບ
ມີກຸງໄດ້ອາດວ່າ

Security Models

1. Multilevel security - MAC, Within organization

- 1.1 Bell-LaPadula, System may leak the information
 - Simple property : No read up (ບໍ່ມີຄວາມເປັນຫຼັງຈາກຫົວໜ້າ)
 - * - property : No write down (ບໍ່ມີຄວາມເປັນຫຼັງຈາກຫົວໜ້າ)
 - Tranquility property : of 2 properties ບະໜົນຫຼັງຈາກການເກີນ (declassify view)
- 1.2 Biba, ເພື່ອງສ່າງໃຫຍ່ດັ່ງນີ້
 - Never read down or write up
 - Info Confidentiality
 - Windows security warning when installation

Usage : Auth uses Bell-LaPadula, Unauth uses Biba

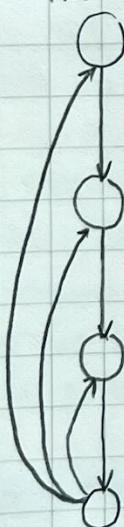
2. Multilateral security - Between departments

- China Walls model : ລັບອັນດັບ ຄ່າວົງວິນາຍົກ (ຈົກຈັງ), ດັກຮູ້ພວກ A ພັນທັນກົງ B
- Reverse engineering

⑤ Log Analysis (Part of Auditing)

- ສະແດງກົດປົງ ເພື່ອຕາມກາຈົບປັນປົວເລັ້ນ

Workflow



Log Collection

syslogs, Eventlogs, App logs, firewall logs, Network logs, Infrastructure logs

Event management

What (All / Filtered) How (Centralized, Backup, Format, Raw / Parsed)

Preprocess (Index, Summaries) Who (Direct / Program / Dashboard, Data sensitivity)

Analysis

How

Manual Alert
Automated Deep dives

Technique

Stat
Anomaly

Association
AI / ML

Time

Real-time
post-Mortem

Response

- Reporting
- Incident response
- Evidence preservation
- Lesson learned

⑥ Physical Security (Defend Against the Dark Arts)

Keyword: ឧបនិងសារអ៊ីកទេសចរណ៍

- និរត្រូវ computer ដែលទទួលទិន្នន័យ នៃ ផែបាយ → minimize the risk to information
- 1) keylogger / ឧគមនុសាការការ keyboard
- 2) ឬ http request និងចំណាំ parameter
- 3) គិតថ្នាក់នៃ network
- 4) គេកស់កំពង់ script

⑦ Integrity and Basic Encryption

Integrity

= ខ្សោយសារនៃព័ត៌មាន ដូចជាបែងចែងនូវការបញ្ជូនមានការបញ្ចូន/យកចំណាំ

= sometimes referred as Authenticity (4th "A" of security)

- require (hardware) supports

Trust (ត្រូវឈរ)

• ត្រូវឈរក្នុង policy ទៅការងារ

- processor - ថែរការ chip ទៅការងារ

- user / dev - ថែរការ user ទៅការងារការងារការងារ

- software / process - ថែរការក្នុងការងារការងារ

• បាន ការបង្រាប់ memory ដែលនឹងបានអង្គភាព នៅក្នុងការងារ និងការងារ memory ដែលនឹង (segmentation)

• ក្នុងគេងតែ → minimize trust

Sandbox

• by Java Applet

If trust → run anywhere

else → run in sandbox (cannot access local files)

• trust នៃការងារបានបញ្ជូន

Domain

• ការបង្រាប់នូវការងារបានបញ្ជូន

• Isolation

Hardware Support for Integrity

Ring by Multics

- memory compartments (page and segmentation)
- Inner ring (kernel) can access outer ring
- Interprocess communication through kernel
- មួយម្រាតឱ្យមាន 2 rings (kernel / non-kernel(user))

Encryption (When no hardware support) - email / network

- Monoalphabetic Substitution Cipher by Julius Caesar
Weakness: បានក្រែងបន្ថែមក្នុងអំពីរាយដែលត្រូវត្រូវជាលើស a,c,s

① Hash digests (short input, long output)

- = Message digest (MD5, SHA1, SHA-256, SHA-512, Tiger-Hash)
 - one-way function
 - vary input to fixed size output
 - collision-free
- integrity CHECK
- sometimes not considered as encryption (no decryption)

② Symmetric Encryption - Scalability?

2.1 Stream Cipher ex. Vigenere

- ម៉ោង key ទូទាត់ក្នុងខ្សោយ
- ឧបតាថ្មី key = lucky
- word = computing
- key' = luckyluck
- នៃសំខាន់ output ជា matrix (ប្រុងរួមរាល់)

- need hardware support vector operation

2.2 Block Cipher ex. Wheatstone-Playfair Cipher

- $n \times n$ cipher blocks
- block size = $k < n$
- តាមឱ្យក្រឡាតាំង ពី ដំឡើងតាមគេងបំពេញក្នុង ក្រឡាតាំងនៅក្នុងប្រុងរួមរាល់
- ចំណេះចំណេះ
- ទូទាត់ក្នុង ឬ bit រារាង Group និង encode

Mode of operation in Block Cipher

- 1) Electronic codebook (ECB)
- 2) Cipher block chaining (CBC) & PCBC
- 3) Cipher feedback (CFB) & Output feedback (OFB)
- 4) Counter

1) input | shift encryption នៅរឿង

2) Initial vector (IV) នៅឯង output នានា IV និង Block ក្នុង

3) IV និង encrypt នៅឯង input និង \oplus (ឲ្យបិនបាន) IV

3) Asymmetric Encryption

- Public key - ចាប់ផ្តើម
 - key-pair, keep private, distributed public
 - ម៉ោងក្រឡាតាំងផ្ទៀងផ្ទាត់ private នូវក្រឡាតាំង public, vice-versa
- Q: Bob នឹង Alice តាមឱ្យក្រឡាតាំង នៃខ្លួនឯងដូចត្រូវការការ Bob
- A: ((message) Bob's private) Alice's public
- *ចាប់ផ្តើមផ្ទៀងផ្ទាត់ Alice តាមឱ្យក្រឡាតាំងនូវ *
- 1) public និង encrypt នៅក្នុង តំបន់ (Alice និង តំបន់បាន)

Security Protocol

- 1) Digital signature នូវ plain text និង hashed + encrypted ឬក្នុង ធម្មតាក្នុងវគ្គភាពវិទ្យាអំពីរាយ
- 2) HTTPS/SSL/TLS Client សរុប key នៃរូបភាព pub key នូវ server និងសំរាប់ឯង និង server នូវវគ្គភាពនូវ key និងនៃការបង្រៀន
Key = symmetric encryption

⑧ Public key Infrastructure

Digital Certificate - a trusted document issued and signed by a trusted third party with digital signature → trustworthy?

(CA)

- Issuer, Subject, Subject public key, Issuer Digital Signature
- Self-Signed Certificate : សំគាល់សំគាល់

Public Key Infrastructure - set of roles, policies, procedures for

1. The registration of public key
2. The management of public key
3. The validation of public key

PKI parties

Certificate Authority (CA) : Gen Key, Revoke, Back-up, Cross certification - among CAs

Verification Authority (VA) : Face-to-Face, Remote, Automatic Registration

Registration Authority (RA) and Local RA

Certificate Distribution System : LDAP (special purpose Databases)

9 Practical Network Security

How systems are hacked

- Remotely : Remote login services + Exploit vulnerabilities / malware / Trojan
- Locally : social engineering + Exploit vulnerabilities

1) Sniffing environment (Sniff the environment)

- Server details (Nginx, Apache) versions
- OS information
- API
- Tools: Wireshark
- ယောက်: ပဲချေခား

1.1 Social Side

- မိန္ဒကိုဖော်လော်စွာ
- of domain name registration

1.2 Network side

- map target-target network
- Tools: Nmap
 - OS fingerprinting (by implementing various protocols' initial sequence number)
 - service fingerprinting

2) Identify possible vulnerabilities in network service

Defense : firewall (network and transport layer)

encryption

IDS, IPS (App layer)

ကာဆုံးလုပ်ငန်းတော်

ဂေါ်မြန် + ပြန်လည်

မျှော်းပျော်ရွေ့ 100%

Identify possible vulnerabilities in network services

Attacker : spoof IP addresses

Spoof MAC addresses - အေး

Distributed denial of services (DDoS) : အေး ပူး

80% Network

1) DoS in DNS, TCP, ICMP

2) TCP SYN Flood attack - spoof fake IP, server ထုတ်ပေါ် connection to ACK အားလုံး (long timeout / no ACK)

3) TLS/SSL Heartbleed - use SSL heartbeat ပုံစံပေးကြမ်းလုံး ၂၃၁ 2 bytes (OK)

ပုံစံပေးကြမ်း ပို့ 65536 bytes ပျော်စွာနှုန်း memory သိန်း ၆၅၅၃၆ bytes

⑩ Buffer Overflow

- กรณีที่มีข้อมูลมากกว่าที่ต้องการ
 - อาจเขียนรหัส return-address หรือคำสั่งที่รันโค้ดจากภายนอก (Remote code execution)
→ stack smashing
 - ใช้ใน shared library และมีชื่อว่า printf

Observation

- Injecting malicious code/data
- Redirect program

Similar Vulnerabilities

- Integer overflow (น้อยกว่า)
- "printf" vulnerability

Protection

1 Static analysis - กันไว้ก่อน ไม่สามารถ detect ได้ทันที

- 1 Lexical analysis - Tokenization
- 2 Semantic analysis - Parser

2 Dynamic solutions

- 1 Address protection → Canary words, Address encode, Copy of address, Tags ตรวจสอบ input ให้ถูกต้อง
- 2 Input protection
- 3 Bounds checking : จำกัด
- 4 Obfuscation : ซ่อนความซับซ้อน ให้เดา ที่เก็บของข้อมูล

3 Isolation

- 1 Non-executable
- 2 Sandboxing

⑪ Digital Forensics (กระบวนการรับหลักฐาน)

การหักดิบหลักฐาน (กระบวนการ)

- IoT → ჩิปเซ็ต เน็ตเวิร์ก ต้องห่วงคุณ
- ซอฟแวร์ที่อยู่บนเครื่อง → ถ้ารู้จักไฟล์หนึ่ง อาจจะนำกลับมาต่อ กันได้
- ต่อไป

การหักดิบหลักฐาน (กระบวนการ)

- ผ่านแม่เหล็ก
- บางชิ้นงานจะเน้นแม่เหล็ก
- เชิงนิพัทธ์ (7 ครั้ง)

Digital Forensics = Law + Computer Science

Collect and analyze data from computer systems, networks, storage devices

- Networks, small scale Digital Devices, storage Media, Code Analysis

Forensics Process (Process กระบวนการ)

- 1) Acquisition or imaging of exhibits - ต้องหักดิบ ไม่ให้ disk รวมตัว write-blocked
- 2) Analysis - Visible, Hidden, Encrypted, Deleted files
- 3) Reporting

• Image Tampering (การเปลี่ยนแปลงภาพ)

- ตัว Metadata หายไป (ทำให้ visible และ deleted file)

(Pen-Test)

⑯ Cyber Security & Penetration Testing Training (Guest)

Introduction to Cyber Security

Cyber Security Track

1) Security Management - Անվայութիւն

- 1. Legislative Track

Հայաստանի Հանրապետության օրենսդրության համար կառավագական օրենսդրությունը՝ անվայութիւնը և անվայութիւնային պահպանը

2) Penetration Test - offensive

- Ինվազիվ Web,
- Red Teaming

3) Monitoring and Detection - defensive

- Blue Team
- SOC/SIEM
- security architecture

4) Incident Response & Threat Hunting - Խոցադր և կրակառ (incident) դրվագաբայր

- Digital forensic
- Malware Analysis
- Threat Intelligence

Security Management պահպանային համակարգեր

- Gap Assessment - զարգացման current state - desired state հաջողություն ունենալու implement
- Risk Assessment - զարգացման համար անվայութիւնը (աշխատանքային պահանջանակներ) է priority ու risk
- IT Audit - մրցանակագրություն

Security Assessment

- 1) Vulnerability Assessment (VVA) : Գործադրային ավտոմատ ալգորիթմ, known vulnerabilities e.g. antivirus (knowledge-based)
- 2) Penetration Test : hacker aspect մասնակիությունը ուժավորացնելու login
- 3) Red Teaming : Կամուրջավորությունը target համար անձնական critical core / sensitive files
- penetration Test Level - Black Box (Malicious փոխադարձություն), Grey Box (user credential), White Box (որոշակի համար user credential փաստաթուղթ)
- penetration Test Process անվայութիւնը առաջարկությունների համար

1 Scope Definition

5 Result Analysis

2 Information Gathering

6 Research

3 Enumeration (Port Scanning, System - OS fingerprint)

7 Exploitation

4 Vulnerabilities Identification (Automatic + Manual)

8 Analysis & Reporting

Monitoring and Detection + Incident Response

- SIEM : centralized system to define threat
- SOC : team

Դրվագաբայր

organization ที่ต้อง standard ของ Web Security

OWASP & Penetration Test

OWASP Web Security Testing Guide (WSTG)

- 1 Information Gathering
- 2 Configuration and Deployment Management Testing
- 3 Identity Management Testing
- 4 Authentication Testing
- 5 Authorization Testing
- 6 Session Management Testing
- 7 Input Validation Testing
- 8 Testing for Error Handling
- 9 Testing for Weak Crypto
- 10 Business Logic Testing (นี้จะทำยากๆ - 100 มาก)
- 11 Client-Side testing
- 12 API Testing

Pentesting Tools

Enumeration : Nmap, DirBuster (DirB), TheHarvester ดูว่ามี server อะไร

Vulnerabilities Identification : Burp Suite, OWASP Zed Attack Proxy, W3af

Exploitation : SQLmap, Metasploit framework, Kali Linux x วิธีการจู่โจมที่มีมาไว้แล้ว (Pre)

⑬ Biometric สร้างบุคคลที่ไม่ซ้ำกัน, make each person unique

Identity Issues

- fake documents
- identity thefts (เช่น การหักดิบ)

ร่องรอย biometric

- ศีรษะ ก้น ตา ใบหน้า
- ร่องรอยนิ้วมือ
- detects multiple enrollments (1 คน / 1 account)
- ป้องกันการฟอกฟื้นตัว

Application

- Forensics
- Government
- Commercial

Good Biometrics - เก็บบันทึกมาตรวจสอบกับการใช้งาน

- Large inter-class similarity - ต่างคนต่างกัน แต่รูปแบบเดียวกัน
- Small intra-class similarity - คนเดียวกัน ควรตัดแล้วได้ค่าใกล้เคียงกัน

Quality of biometrics

- Property ร่องรอยบุคคลเป็น unique
- Image quality รูปดี → ร่องรอยดี , ภาพดีเกิน false match
- Fake biometric ภายนอกดูปั๊บ

บุคคล

- ลักษณะทางกายภาพ, ลักษณะทางกายภาพ, ความหลากหลาย
- ภาษาพูด
- รูป, Heatmap, 3D of face
- รูป
- รูปหน้าครึ่งหนึ่ง - ผู้คนทั่วไป → soft biometric
- เสียง
- ผิวน้ำ

Traits

- unique
- permanent