

Hotmodeller

Del av kursen ETE352 Cybersäkerhet - grunder och medvetenhet
som ges vid Linköpings universitet

Mikael Asplund

Varför hotmodeller?

- Behöver förstå hoten
 - Precis som att vi behöver förstå systemet
- Går inte att skydda mot allt, måste fokusera och prioritera
- Få med det som annars kanske missas

Begreppsförvirring

Hotmodellering (threat modeling)

- En process för att analysera hot
- Liknar riskanalys
- Vanliga metoder: PASTA, STRIDE, OWASP

Hotmodell (threat model)

- Antaganden om hotagentens förmåga och kapacitet
- Vanligt begrepp i vetenskaplig litteratur

Attackmodell

- Används inom kryptoanalys (antaganden)
- Används för att beskriva struktur och beteende för attacker (tex ATT&CK)

STRIDE

- Utvecklad vid Microsoft (Kohnfelder and Garg 1999)
- Sex grundläggande hot och motsvarande egenskaper som de hotar

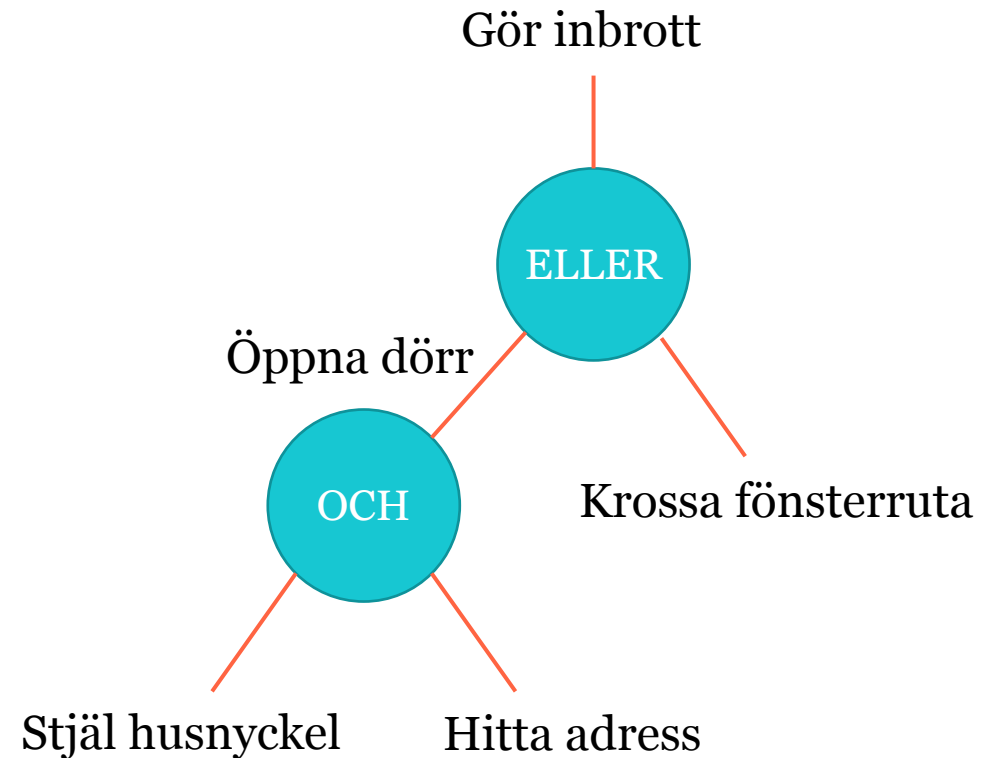
Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

PASTA

- Process for Attack Simulation and Threat Analysis (PASTA)
- Innefattar 7 steg (fritt översatt)
 - Fastställ affärsmål
 - Fastställ tekniskt omfång (systemmodell)
 - Analysera flöden och aktörer
 - Hotanalys
 - Sårbarhetsanalys
 - Attackmodellering
 - Riskanalys

Attackträd

- Formell beskrivning av en sammansatt attack
- Ibland endast ”eller”-noder
- För att skydda
 - Förhindra alla ”eller”-grenar
 - Minst en ”och”-gren



MITRE ATT&CK Framework

- <https://attack.mitre.org/>

- Taktiker – grundläggande mål för attacken, exempel

- Initial access
- Undvika upptäckt
- Command&control

- Tekniker – för varje taktik ett antal specifika tekniker

Initial Access 9 techniques	Execution 13 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 14 techniques	Credential Access 14 techniques	Discovery 16 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 15 techniques	Exfiltration 9 techniques	Impact 13 techniques
Drive-by Compromise Exploit Public-Facing Application	Command and Scripting Interpreter (7) Exploitation for Client Execution	Account Manipulation (4) BITS Jobs Boot or Logon Autostart Execution (11) Boot or Logon Initialization Scripts (3)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (3) BITS Job Boot or Logon Autostart Execution (11) Boot or Logon Initialization Scripts (3)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (3) BITS Job Disable/Enable/Decode Files or Information Forced Authentication Direct Volume Access	Block Folders (4) Credentials From Password Stores (3) Exploitation for Credential Access Forced Authentication Input Capture (4)	Account Discovery (4) Application Window Discovery Browser Bookmark Discovery Cloud Service Dashboard Cloud Service Discovery Domain Trust Discovery	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (6)	Active Collected Data (3) Audio Capture Automated Collection Clipboard Data Data from Cloud Storage Object Data from Information Repositories (2) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2) Email Collection (2) Input Capture (4) Man-in-the-Browser Man-in-the-Middle (1) Screen Capture Video Capture	Application Layer Protocol (4) Communication Through Removable Media Data Encoding (2) Data Obfuscation (2) Dynamic Resolution (3) Encrypted Channel (2) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Traffic Signaling (1) Web Service (2)	Automated Exfiltration Data Transfer Size Limits Data Destruction Data Encrypted for Impact Data Manipulation (3) Defacement (2) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking Service Stop System Shutdown/Reboot	Account Access Removal Data Destruction Data Manipulation (3) Defacement (2) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking Service Stop System Shutdown/Reboot

Zero trust

- Egentligen ett sätt att skydda
- Baseras på en föreställning om en hotmodell
- Utgå ifrån att hotet finns inne i systemet



Det här fotot av Okänd författare licensieras enligt [CC BY-SA-NC](#)

<https://cybersakerhet-grund.ida.liu.se>