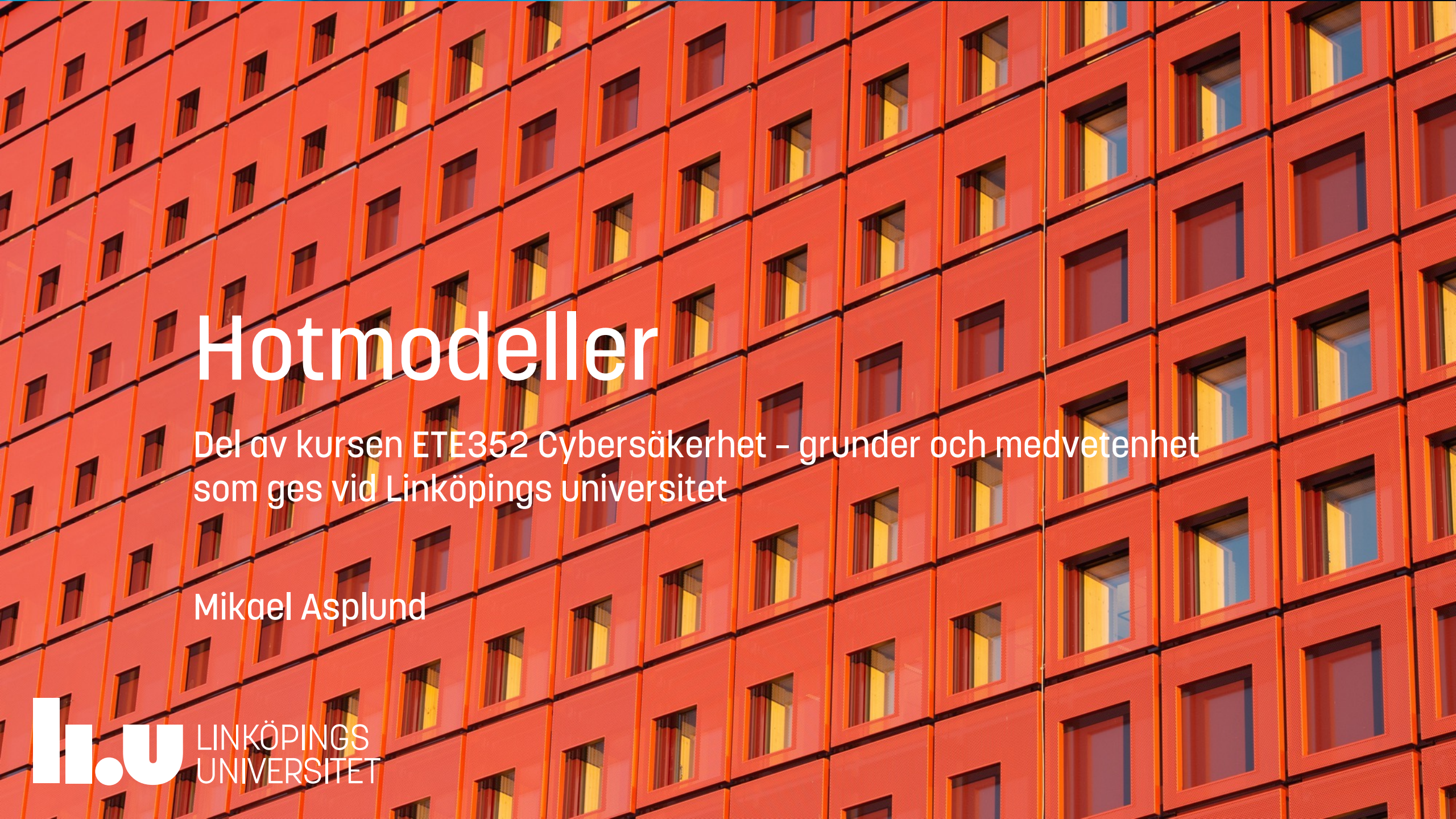


Hotmodeller

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

Mikael Asplund

LINKÖPINGS UNIVERSITET

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

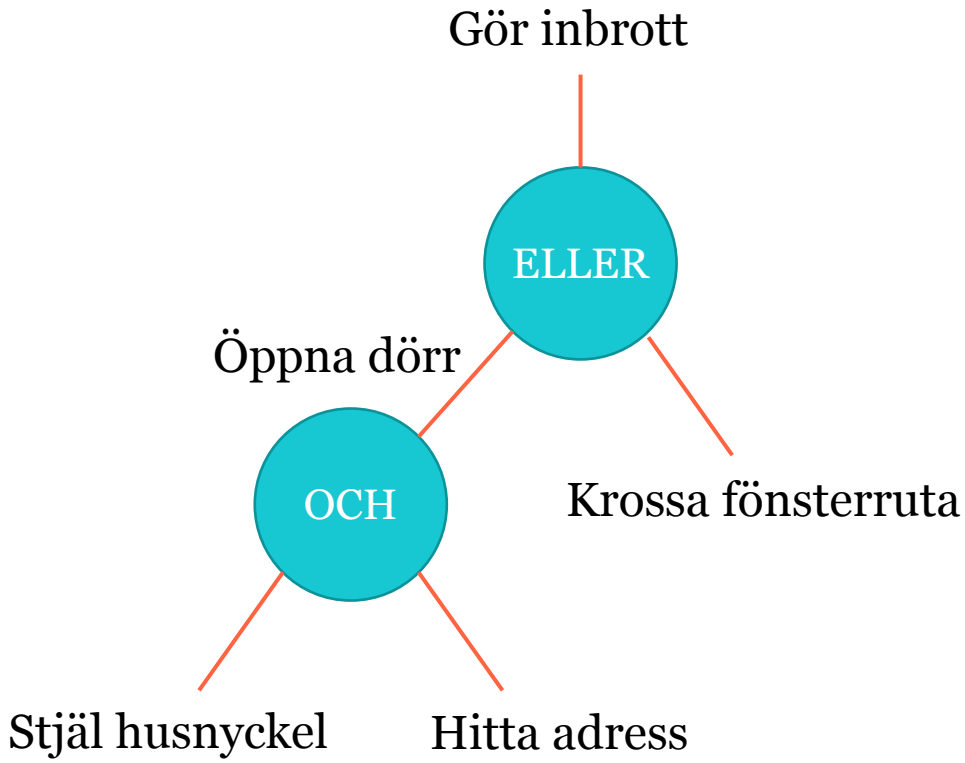
PASTA

- 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

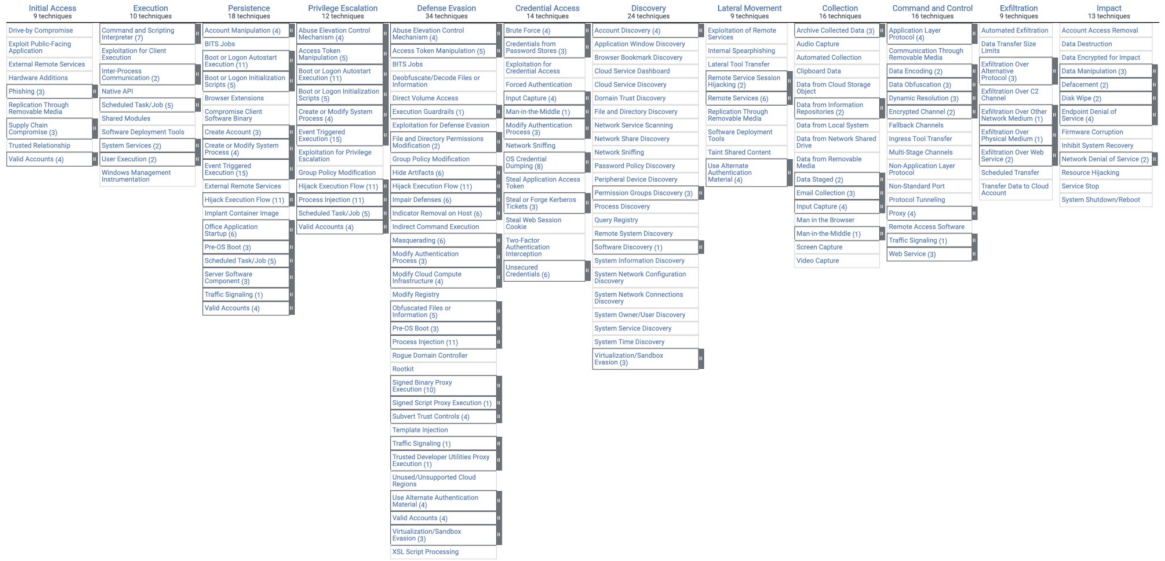
Attackträd

- 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

Zero trust

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

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

LINKÖPINGS UNIVERSITET