

Základní bezpečnostní principy. Modelování bezpečnostních rizik, metodiky STRIDE a DREAD.

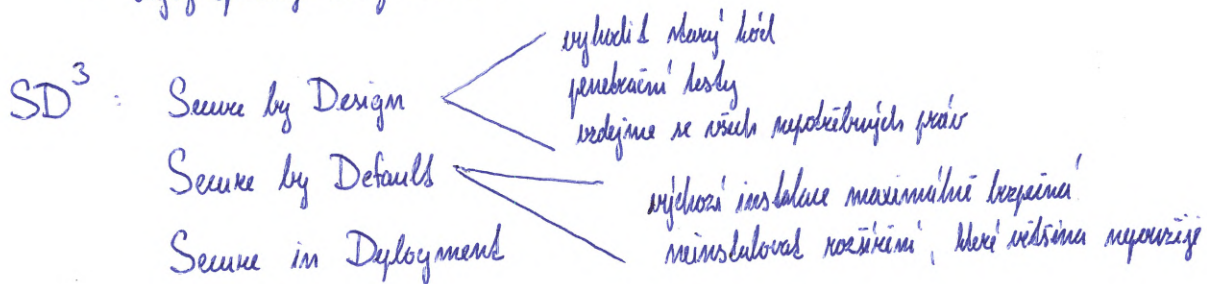
hrozba - ^{přeměnitelná} příčina neúspěšného incidentu (přeměnitelná autentizace hrozbou sílou)

reaktelnost - skutečná možnost, které může být vyvolána hrozbou / hrozbami

Kvalitní roztváření - bezpečný & spolehlivý
↓
chráněná důvěrnost, integriteta a dostupnost dat

- bezpečnost roztváření se musí řídit už v návrhové části

- důležitý operační vztah autor!



další pravidla: myslět jako útočník, minimalizace ploch pro útok, víceúrovňová bezpečnost
externí systémy jsou nebezpečné, bezpečné selhání!
we security through obscurity

STRIDE: (model pro identifikaci bezpečnostních rizik)

Spoofing of Identity - podvržení identity

Tampering with data - neautorizovaná změna dat

Repudiation - popření transakce uživatelem

Information disclosure - únik informací

Denial of service

Elevation of privilege - neautorizovaná vyšší oprávnění

možná řešení:

- lepší autentizace, multi-faktor, ...
- autentizace, hashing, MAC, ...
- digitální podpis, časové odznaky, ...
- autentizace, šifrování, ...
- filtrování, loadbalancing, QoS, ...

• oprávnění uživatelů

modelování hrozeb

- ◦ proces - jednotka zpracování dat [S, T, I, D, E]
- = ◦ uložení [T, R, I, D]
- ◦ hranice - počítací, adresní prostor, hranice sdílení
- ◦ interakce - vstup do systému [S, R]
- ◦ tok dat [T, R, I, D]

- hodnocení rizik: DREAD

- průměrná hodnota je pět kategorií, škála [0, 10]

- Damage potential
- Reproducibility - jak snadno se kopíruje
- Exploitability - jak snadno se využije
- Affected users - množství postihnutých uživatelů
- Discoverability

- vyhlášení: CVSS ~~CVSS~~ - více metrik, méně hodnot (škála)
CWSS - měří se a komplikace měří se