Software Engineering Methodology
Lecture 14 - Threat Models

Gregory S. DeLozier, Ph.D.

gdelozie@kent.edu

Threat Models

- Structure for thinking about security
- Lists of things that might go wrong
- Lists of questions to ask

Wikipedia - Threat Model

https://en.wikipedia.org/wiki/Threat_model

“Where are the high-value assets?”

“Where am I most vulnerable to attack?”

“What are the most relevant threats?”

“Is there an attack vector that might go unnoticed?”

STRIDE Model

A list of things to think about (Microsoft, 1999)

- Spoofing of user identity
- Tampering
- Repudiation
- Information disclosure (privacy breach, data leak)
- Denial of service (D.o.S)
- Elevation of privilege

https://en.wikipedia.org/wiki/STRIDE_(security)

Microsoft on STRIDE

- Specific discussion of each threat

https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

- See also discussion of application

https://msdn.microsoft.com/en-us/library/ee798544(v=cs.20).aspx

DREAD Model

- Model for each type of potential attack
  - Damage - how bad would an attack be?
  - Reproducibility - how easy is it to reproduce the attack?
  - Exploitability - how much work is it to launch the attack?
  - Affected users - how many people will be impacted?
  - Discoverability - how easy is it to discover the threat?
- No longer in use at MS, used elsewhere
- Worries about discoverability

https://en.wikipedia.org/wiki/DREAD_(risk_assessment_model)

Guidelines for Action

- There are guidelines for securing various things

(DO tutorials are excellent.)

https://www.digitalocean.com/community/tutorials/7-security-measures-to-protect-your-servers

(This one is pretty silly looking but has good advice…)

https://www.hostgator.com/blog/3-easy-steps-that-protect-your-website-from-hackers/

Homework:

- Read the threat model pages

- Analyze threats against your product

- Prepare some risk mitigation steps

- Execute them