Thinking Inside the Box

Modelling the Insider Threat

James Bore

July 6, 2018

What?

Threat modelling is a toolkit for attempting to predict and mitigate threats to a system.

Why?

Security by design is a popular buzzword, and cannot be achieved without effective threat modelling.

Threat Model Toolbox

- OWASP Top 10
- STRIDE
- DREAD
- CVSS
- Trike
- MIL-STD-882E
- OCTAVE

and many, many others

Insider Threat

Some mitigations against external threats work against the insider threat. Most do not.

Motivations

Motivations for insider threats are not universal, and can be broadly categorised. Each type is more or less likely depending on business and culture and requires different mitigations.

Negligence Not technically a motivation, but lack of knowledge, expertise, or training can turn a trustworthy insider into a threat with a couple of bad clicks.

Perceived Injury People have their own perceptions, and may act out if they feel they have been treated badly.

Malice In some cases the insider threat is a deliberate, carefully planned campaign.

Damage

With the insider threat we should always assume that we have trusted the wrong person, meaning they are permitted through all access controls and intend harm.

Destruction Deleting data, discarding backups, unplugging systems.

Disclosure Revealing or making use of sensitive data for detrimental or selfish reasons.

Modification Modifying data or systems for detrimental or selfish reasons.

Mitigations

- Training and treatment
- Surveillance, logging and monitoring
- Effective and efficient recovery mechanisms
- Least privilege

Summary

- Security by design requires threat modelling
- The insider threat requires a different method to categorize
- Mitigations must include non-traditional remedies such as training, along with classics like resilience, least privilege, and surveillance

Questions?