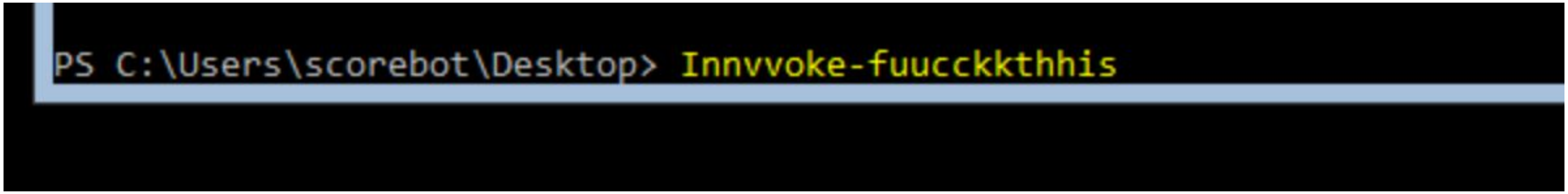
Mason Competitive Cyber

Threat Modeling

Recent Competitions

- CCDC
  - CND, VMs + impossible IT tasks + Red Team
- Issues
  - Room
  - Wifi
  - Start time
  - Services
  - Vsphere web console

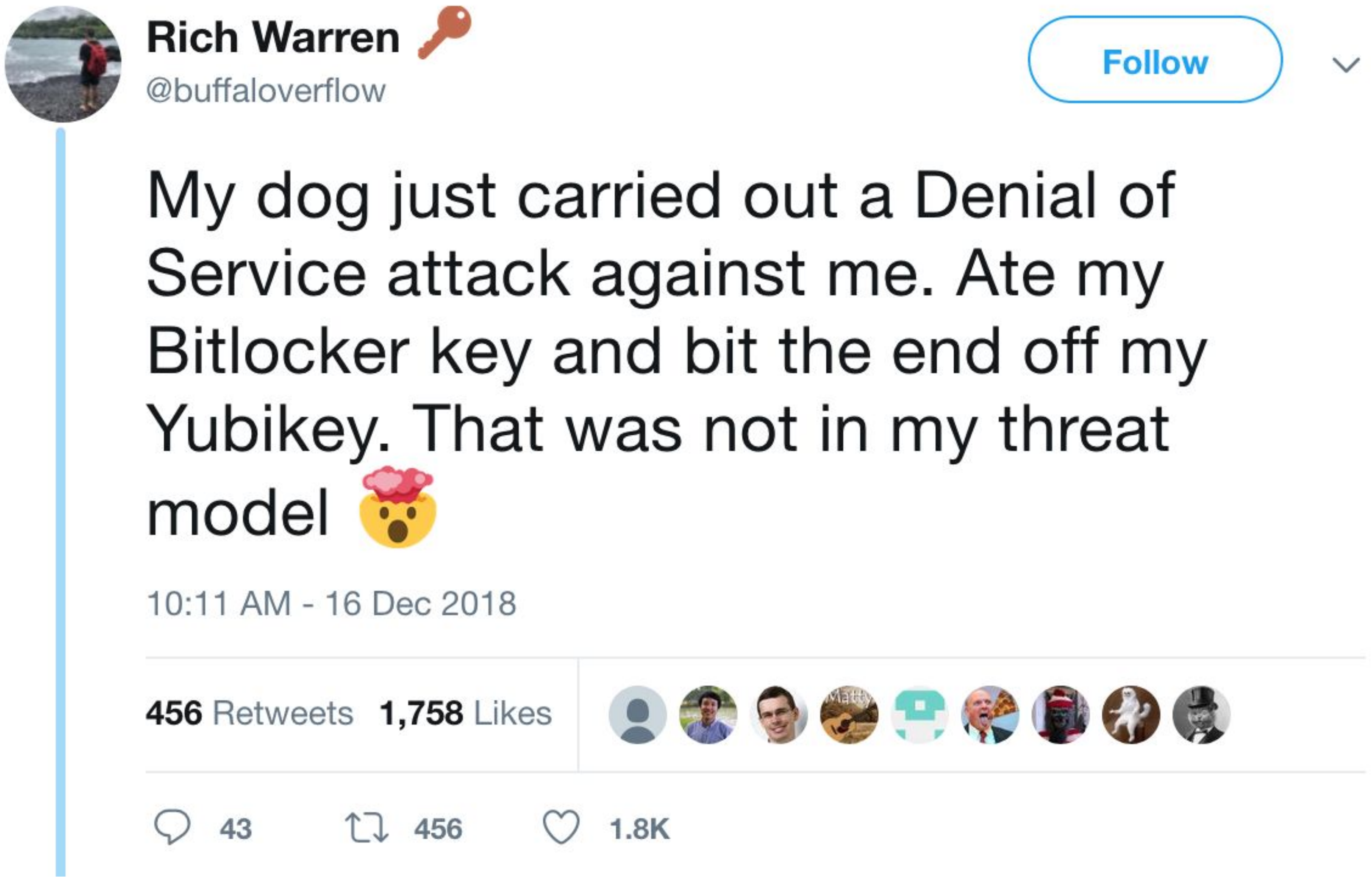


```
PS C:\Users\scorebot\Desktop> Innvvoke-fuucckkthhis
```

Upcoming Competitions & Events

- Cybersecurity Industry Advisory Board Meeting
  - Paul & Michael giving 15min talk
- VA Cyber Fusion
  - In person @ VMI
  - Feb 22-23
- Cyberdawg CTF
  - In person @ UMBC
  - March 2
- BSides Nova
  - March 2

What is Threat Modeling?



Rich Warren 🔑

@buffaloverflow

My dog just carried out a Denial of Service attack against me. Ate my Bitlocker key and bit the end off my Yubikey. That was not in my threat model 🤯

10:11 AM - 16 Dec 2018

456 Retweets **1,758** Likes

43 456 1.8K

What is Threat?

- A neckbeard in a black hoodie?
- When your mom tells you that you’ll be grounded if you don’t do the dishes?

What is Threat?

- A neckbeard in a black hoodie?
- When your mom tells you that you'll be grounded if you don't do the dishes?
- Threats are the things that can go wrong with your system

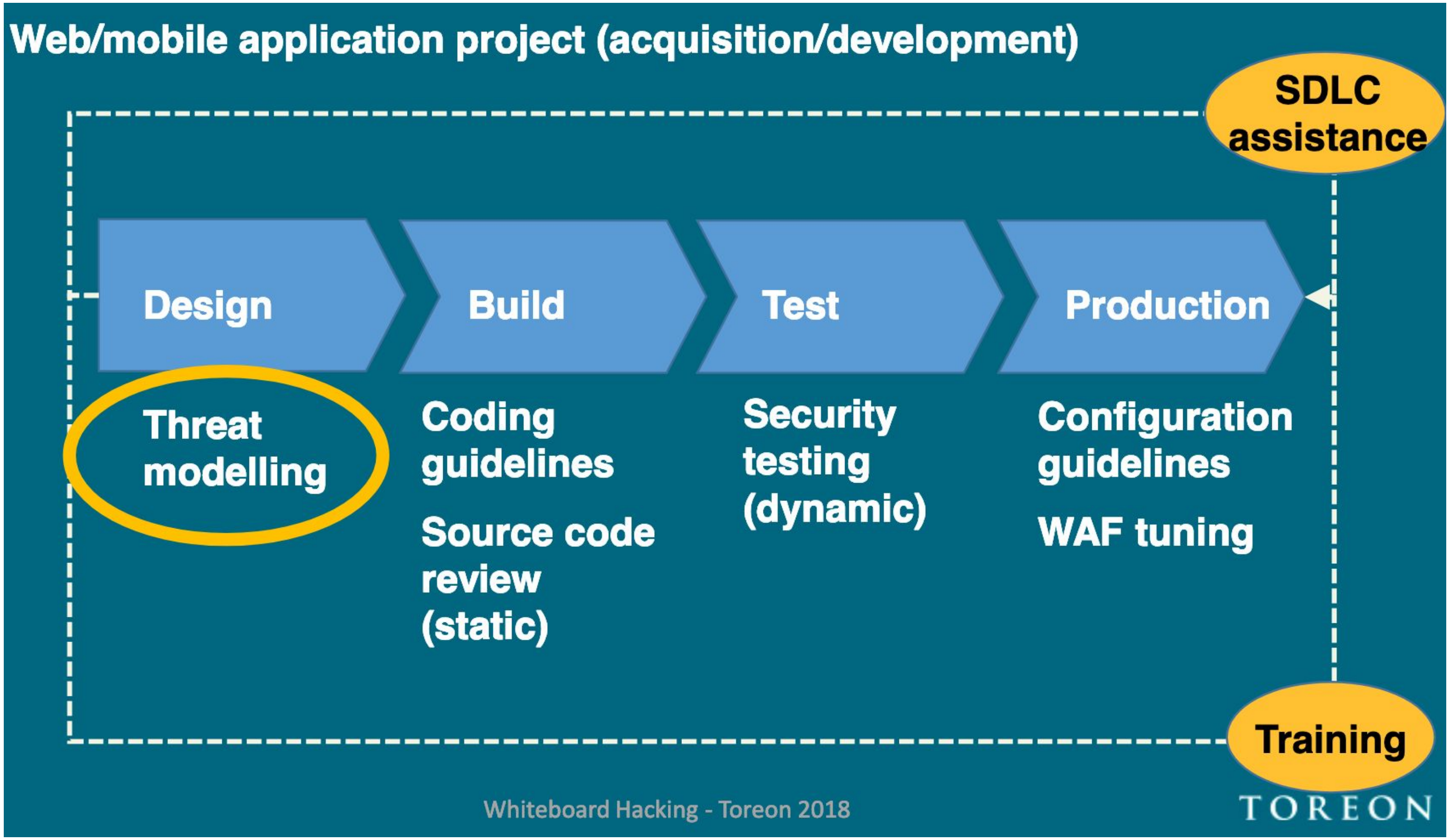
Why threat model?

Threat modeling AKA *Architectural Risk Analysis*

- Prevent security design flaws
  - Flaws != coding bugs
  - Can't all be solved with static code review
- Identify and prioritize risks
- Cost justification

When to threat model?

- Start at beginning of secure development lifecycle
- When system changes or threats change



Web/mobile application project (acquisition/development)

SDLC assistance

Design

Threat modelling

Build

Coding guidelines

Source code review (static)

Test

Security testing (dynamic)

Production

Configuration guidelines

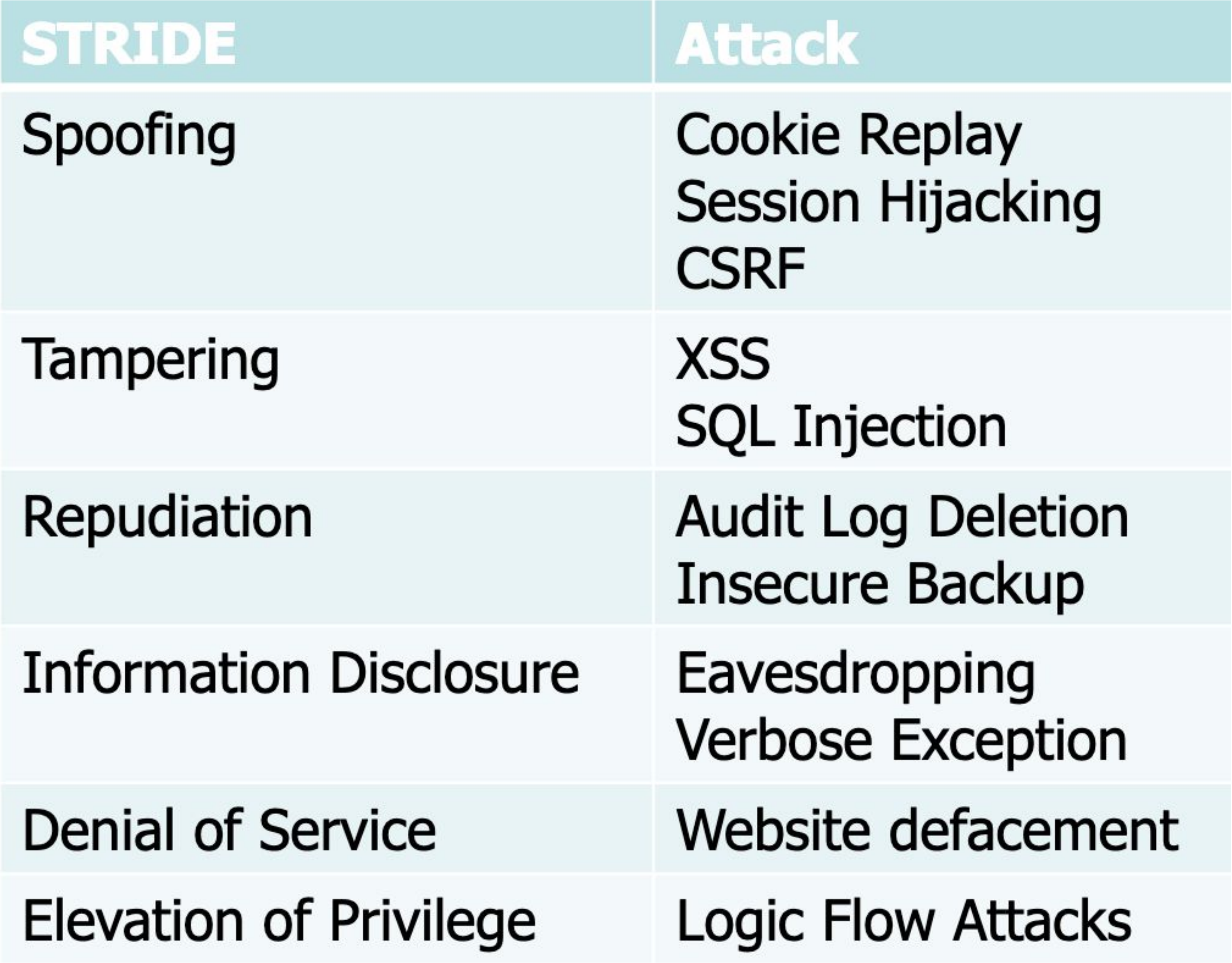
WAF tuning

Training

Whiteboard Hacking - Toreon 2018

TOREON

STRIDE



STRIDE	Attack
Spoofing	Cookie Replay Session Hijacking CSRF
Tampering	XSS SQL Injection
Repudiation	Audit Log Deletion Insecure Backup
Information Disclosure	Eavesdropping Verbose Exception
Denial of Service	Website defacement
Elevation of Privilege	Logic Flow Attacks

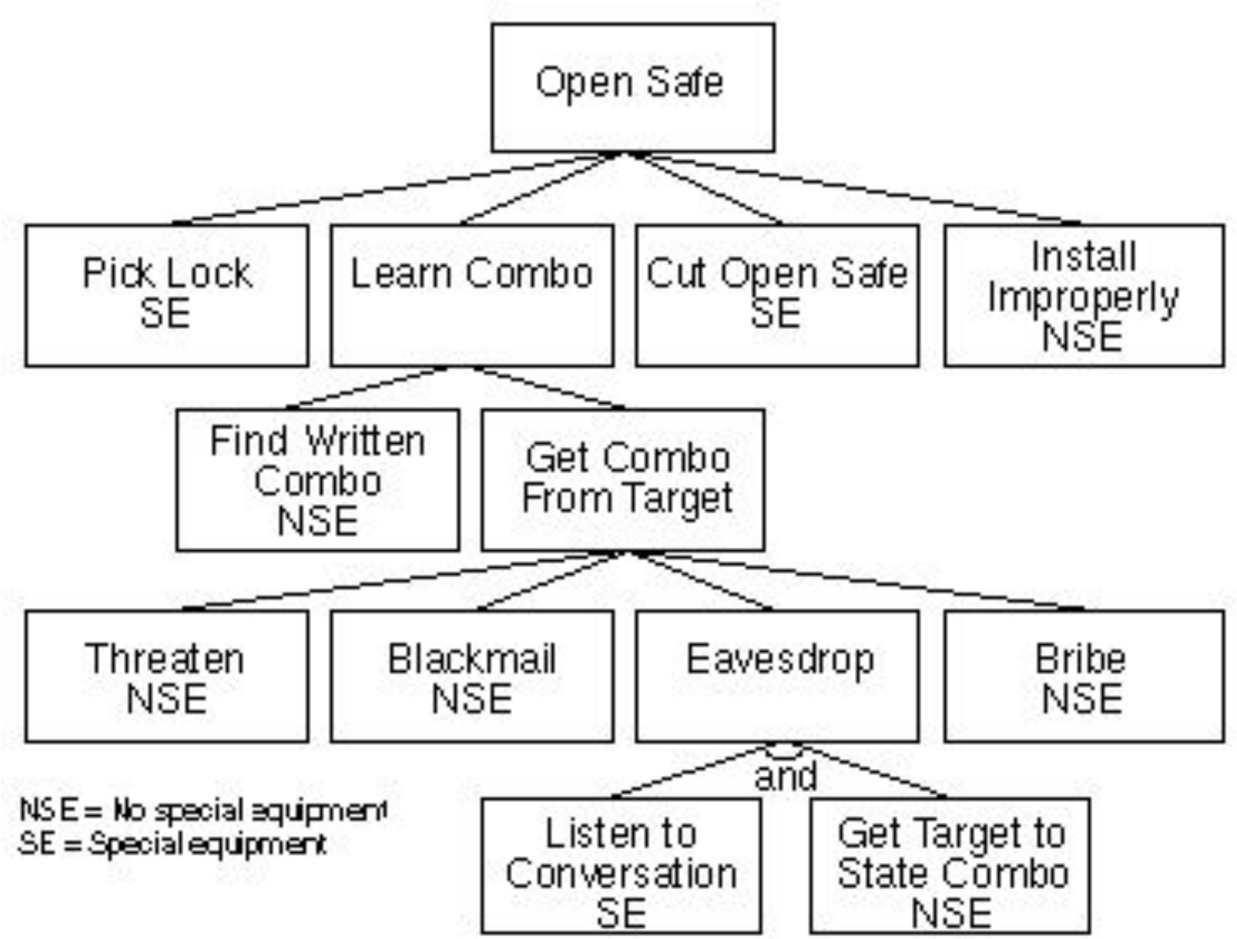
Strategies

- Modeling attackers
    - Not always easy to predict
- Modeling assets
    - Definition of “assets” is vague
        - Endpoints? Routers?
        - What attackers want?
        - Anything we protect?
- Modeling software
    - Data Flow Diagrams
    - Trust boundaries

- STRIDE-per-interaction

Attack Trees

- Diagram showing how attacks relate to each other



Attack Libraries

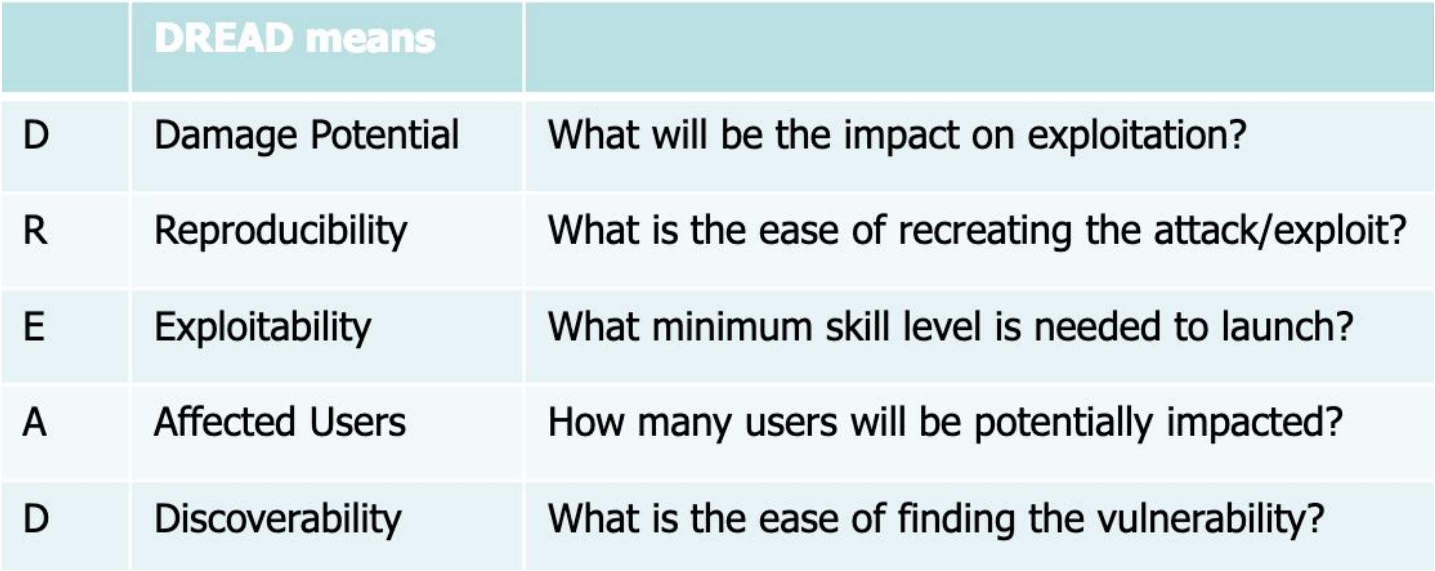
- Lists of attacks
    - Useful for people less familiar with security
- OWASP Top 10
- MITRE CAPEC
    - Common Attack Pattern Enumeration and Classification

- Problem: people thinking these lists are complete

Risk Management

- Risk = Probability * Impact

- DREAD ranking



	DREAD means	
D	Damage Potential	What will be the impact on exploitation?
R	Reproducibility	What is the ease of recreating the attack/exploit?
E	Exploitability	What minimum skill level is needed to launch?
A	Affected Users	How many users will be potentially impacted?
D	Discoverability	What is the ease of finding the vulnerability?

Risk Management

- Avoid risk
  - Don’t build that feature
- Addressing risk
  - Add crypto to mitigate
- Accepting risk
  - “Eh whatever. It’s unlikely”
  - Don’t do this for products because then you’re transferring risk to customers
- Transferring risk
  - Insurance
- Ignoring risk
  - Laws may not make this possible (PCI, GDPR, etc.)

Fuzzing is not a mitigation

- Fuzzing = Sending random data to a program
- Method of finding bugs / testing mitigations
  - Esp. effective with parsers
- NOT a mitigation itself

Practical Exercises

- None related to Threat Modeling
- Wargame
  - https://www.azcwr.org/remote/access/
- TCTF
  - tctf.competitivecyber.club

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™

CRYPSIS™