

Threat Modeling 101

Intro to Operational Security

What is Security

"Security is a property (or more accurately a collection of properties) that hold in a given system under a given set of constraints"

- System - anything from hardware, software, firmware, and information being processed, stored, and communicated
- Constraints - define an adversary and their capabilities

What is Operational Security (OpSec)

"Operational security (OPSEC) is a security and risk management process that prevents sensitive information from getting into the wrong hands."^[1]



Why is OpSec Important

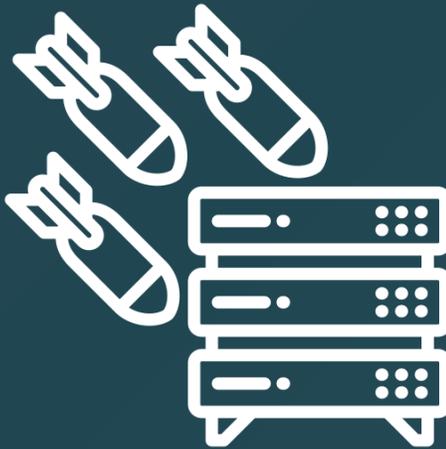
- Protection of Sensitive Information
- Preservation of Privacy
- Mitigation of Threats
- Maintaining Operational Continuity

Core Principles of OpSec

 center

What is Threat Modeling?

"Threat modeling is the process of using hypothetical scenarios, system diagrams, and testing to help secure systems and data." [1]



Purposes of Threat Modeling

- Identifies Potential Risks
- Helps us understand common Attack Vectors
- Prioritizes Security Concerns

Benefits of Threat Modeling

- Proactive Risk Management
- Promotes Continuously Improvement
- Prioritizing risks saves time and \$\$\$

Overview of Threat Modeling Process

There are many different well-defined processes for Threat Modeling



center

Key Concepts in Threat Modeling

- **Assets**
- **Threats**
- **Vulnerabilities**
- **Risks**

Threat Modeling: Assets

- Types of assets
 - data
 - hardware
 - software
 - personnel

Threat Modeling: Threats

- External threats
 - hackers
 - malware
 - phishing attacks
- Internal threats
 - improper access
 - sabotage

Threat Modeling: Vulnerabilities

“A property of a system or its environment which, in conjunction with an internal or external threat, can lead to a security failure, which is a breach of the system’s security policy.”

- Classifications
 - Abstraction level
 - Type of error/condition/bug
 - Age: zero-day vs. known
 - Disclosure process

Assessing Risks

- Vulnerability assessments:
 - penetration testing
 - code reviews
 - attacker reconnaissance
- Risk assessment methodologies
 - qualitative vs. quantitative
 - likelihood and impact

OpSec in Practice

- Access controls to protect assets
- Encrypting sensitive data
 - in transit and at rest
- Conduct regular security audits
- Not all countermeasures are technical

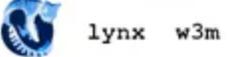
Tools and Techniques for Threat Modeling

- Threat modeling frameworks: STRIDE, DREAD, PASTA
- Threat modeling tools:
 - Microsoft Threat Modeling Tool,
 - OWASP Threat Dragon
- Manual vs. automated threat modeling approaches vs TMaaS

Case Studies: Real-world Examples

- Target data breach
- Stuxnet worm
- Equifax data breach
- <https://www.bleepingcomputer.com/tag/zero-day/>

Threat Modeling for You

The Tech Normie	The Tech Conservative	The newborn paranoid	The Tech Paranoid	The FSF member
<p>Favourite OS: </p> <p>Favourite Browser: </p> <p>Favourite Apps: </p>	<p>Favourite OS: </p> <p>Favourite Browser: </p> <p>Favourite Apps: </p>	<p>Favourite OS: </p> <p>Favourite Browser: </p> <p>Favourite Apps: </p>	<p>Favourite OS: </p> <p>Favourite Browser: </p> <p>Favourite Apps: </p>	<p>Favourite OS: </p> <p>Favourite Browser: </p> <p>Favourite Apps: </p>
<p>"Privacy is for criminals" *worships google, microsoft, apple* *watches MKBHD* *buys every latest iPhone because consumer*</p>	<p>"There should be a healthy balance between privacy and convenience" *thinks worshipping corpos is stupid* *advocates for FOSS and privacy* *believes not every company is inherently evil* *doesn't morally support big tech but understands their importance*</p>	<p>"Using free software is easy nowadays" *Has hundreds of private messaging applications that their friends won't use* *Media codecs + DRM + Nvidia drivers* *Usually refuses cookies from sites* *Watched Stallman's TED talk* *Wants to become a full paranoid but fears the slippery slope*</p>	<p>"closed source is evil" *Uses own compiled packages for control and anonymity* *worships GNU/Linux and RMS* *FOSS or nothing* *watches luke smith* *giving comfort away for privacy rights* *tor daemon enabled*</p>	<p>"Richard Stallman was right!" *Old librebooted Thinkpad* *Hasn't rendered a full webpage since 2012 because of the Javascript* *Evil mode or Emacs pinky* *Only accepts WEBM, OGG and ODT* *Hates credit cards and e-books*</p>
<p></p>	<p> tech's cool but we gotta be careful</p>	<p> free software = free society</p>	<p> I can't live with modern tech anymore</p>	<p> We live in Brave GNU World!</p>

Integrating into Your Security Strategy (Corpos)

- Incorporating threat modeling into the software development lifecycle (SDLC)
- Aligning threat modeling with compliance requirements (e.g., GDPR, HIPAA)
- Building a culture of security awareness and accountability

Challenges and Limitations

- Complexity of systems and evolving threats
- Resource constraints: time, expertise, budget
- Over-reliance on threat modeling as a sole security measure

Future Trends in Threat Modeling

- AI and machine learning for automated threat detection and response
- Integration of threat intel feeds into threat modeling processes
- Emphasis on other proactive and adaptive threat modeling approaches

Thank you

[1] - <https://www.fortinet.com/resources/cyberglossary/operational-security>

<https://www.cisco.com/c/en/us/products/security/what-is-threat-modeling.html>

<https://radiumhacker.medium.com/threat-modelling-frameworks-sdl-stride-dread-pasta-93f8ca49504e>

Presentation made by Kevin Cordero

Icons made by [Dewi Sari](http://www.flaticon.com) from www.flaticon.com