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

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

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

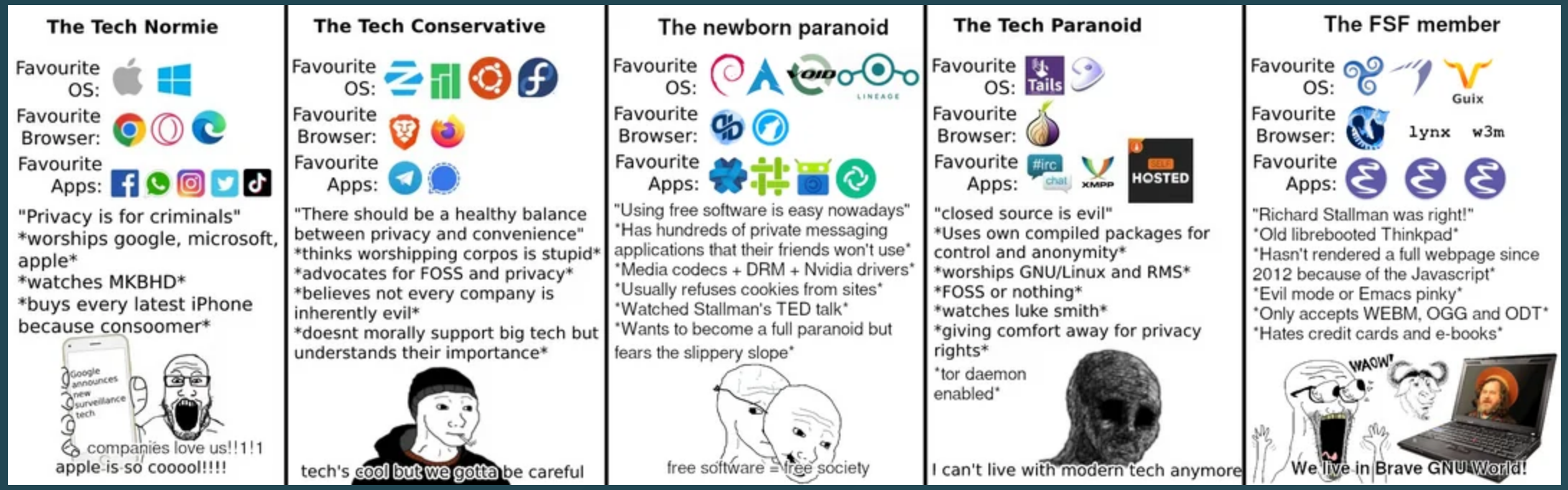
Tools and Techniques for Threat Modeling

- 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



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 from www.flaticon.com'