Threat Modeling for Everyone

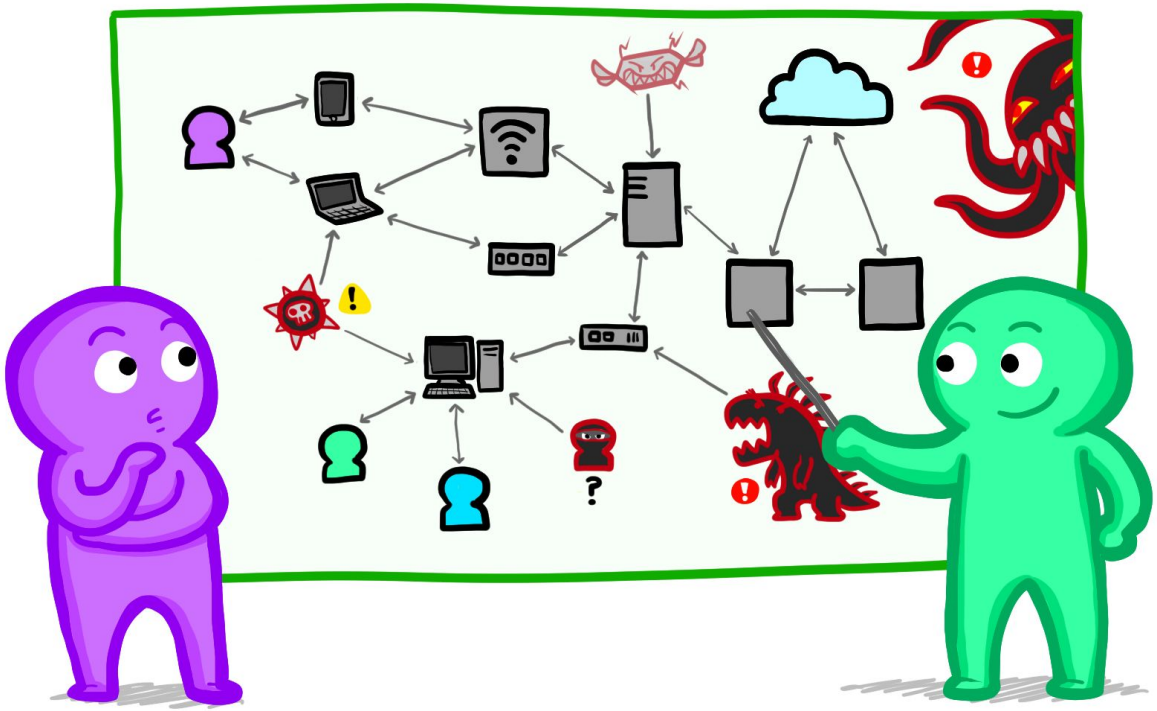
The earlier the better. (2021)

Sanjeev Jaiswal (Jassi)

Agenda

- What and Why Is Threat Modeling
- When We should use Threat Model
- How to implement Threat Model
- STRIDE Hands-On
- What’s Next

Mindset plays an important role here!



What is Threat Modeling

- Design/Model of a system/application from security point of view
- A list of potential threats
- A list of action to mitigate each threat
- Validating the threats and verifications of action taken.

Why Threat Modeling

- To build a secure system/application
- Define and build required controls
- Identify threats early and evaluate their risk
- Document threats, controls, risks & Mitigations
- .Security test cases to be performed by pentesters

Curious case of Helmet

Does using helmet is enough?

- Types of helmets, which one?
- Having helmet is enough?
- Low quality helmet is ok?
- Wearing helmet just to avoid fine?
- What about helmet expiry date?
- Do we need helmet upgrade?

When to use Threat Modeling

- The sooner the better
- Ideally at design phase
- Whenever system changes
- After an incident
- Possibly at CI/CD ?

Threat Modeling Methodologies

Start with these 4 Questions

1. What are we building?
2. What can go wrong?
3. What are we going to do about it?
4. Did We do a good enough job?

Threat Modeling Types

Basically 3 types:

1. Attacker Centric
2. Application Centric
3. Asset Centric

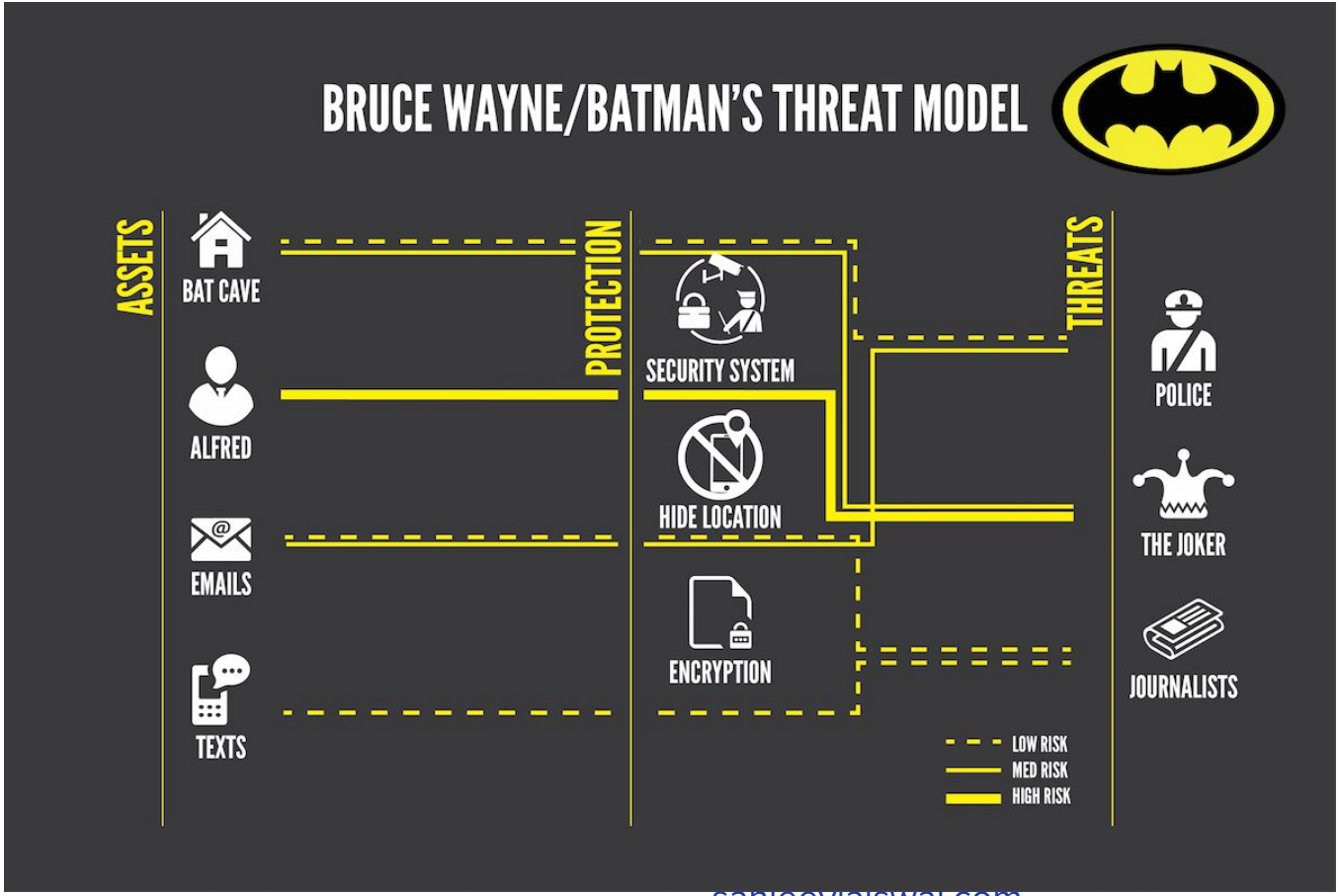
STRIDE (Developer Focused)

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

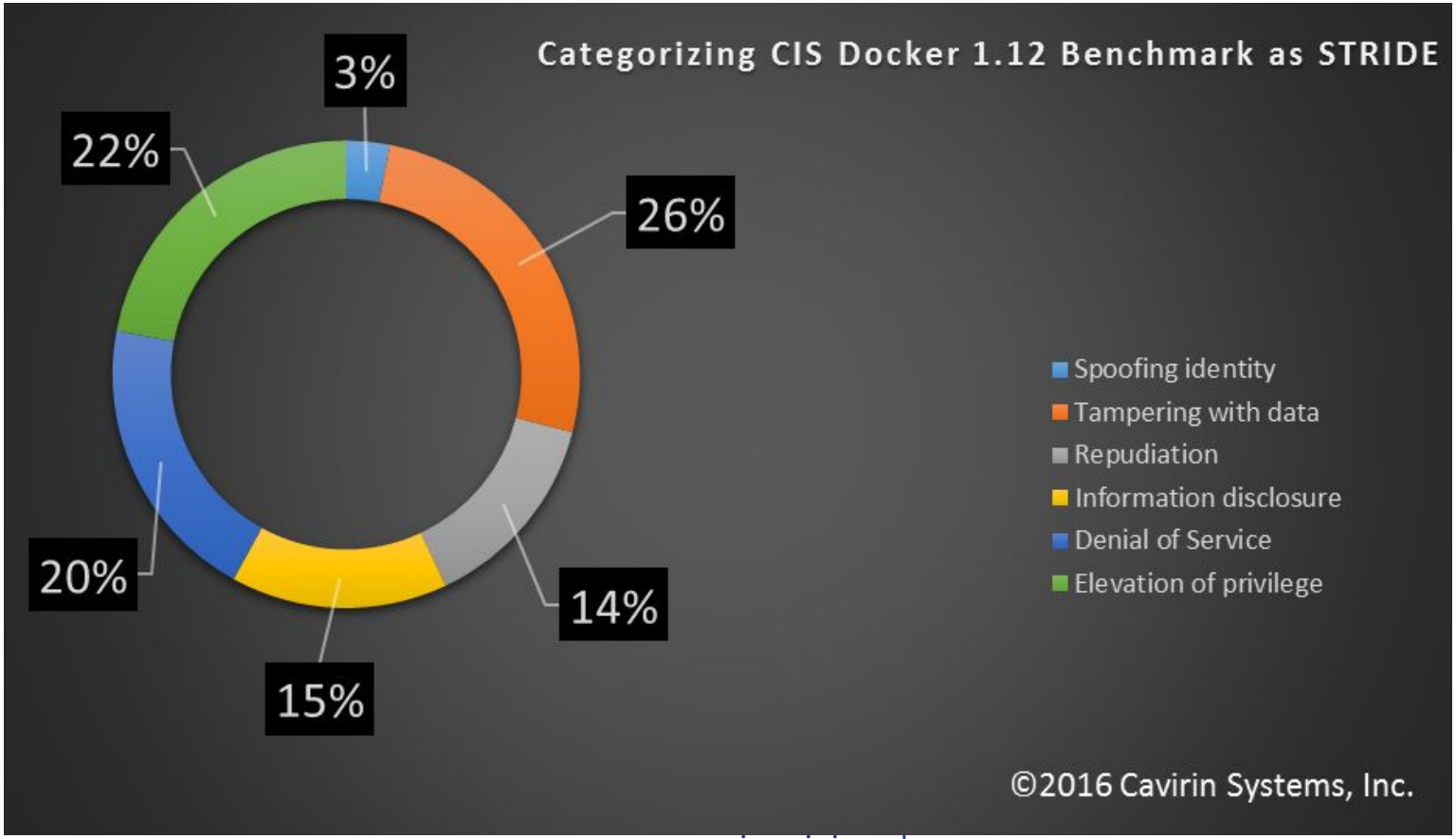
What can go wrong

Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Batman needs Threat Model



STRIDE for Docker



DFD for Threat Model

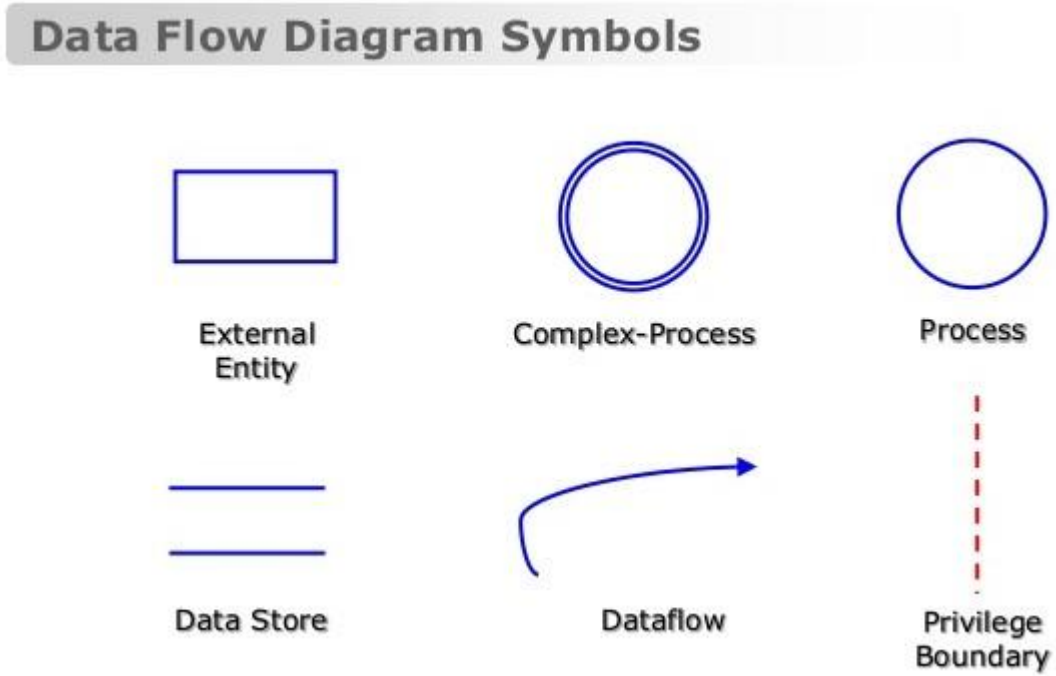
Terms that you will use

- **Asset**: What do you want to protect?
- **Threat**: What's a potential negative impact or outcome?
- **Vulnerability**: Spotted Weakness? Threat can be sensed?
- **Attack:** How to take advantage of the Vulnerability?
- **Mitigation**: How can we reduce the damage?

DFD for Threat Model

Elements

- Process
- Multi-Process
- Data Flow
- Trust Boundary
- Data Store
- External Entity

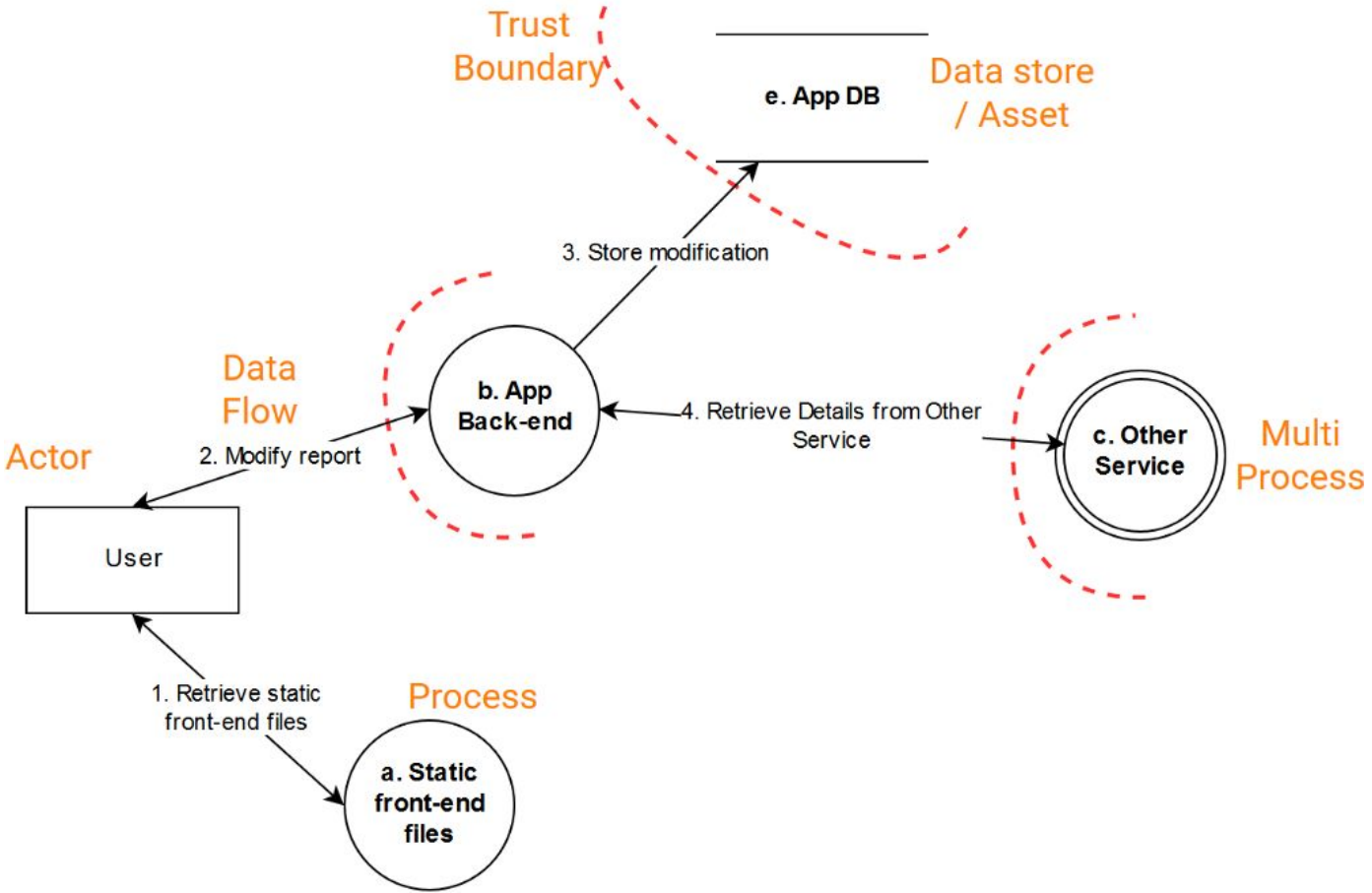


DFD for Threat Model Continued ...

How to Perform

- Identify Entry/Exit Points
- Decompose the Application
- Identify the assets
- Identify the trust levels

Sample Threat Model



Common Threat Model mistakes

- Thinking like an attacker while threat modeling
- This process is only for experts or for Architects
- Only inflow, no outflow and reverse as well
- Thinking one size fits all
- Neglecting business impact
- Focusing on vulnerabilities not the threats

Demo

Implement Threat Model: Tools

- **MS Threat Modeling tool**
- OWASP Threat Dragon Project
- Draw.io
- IriusRisk
- SecuriCAD by foreSeeti
- SD Elements

What's Next

- DevSecOps Threat Model
- Infra Threat Model
- PASTA (Attacker Focused)
- OCTAVE (Practice Focused)
- VAST (Enterprise Focused)

Must READ Resources

- Threat Modeling Book by Adam Shostack
- Learn Threat Modeling for Security Professionals
- OWASP Application Threat Modeling
- Threat Modeling CheatSheet
- Threat Playbook by we45 (Interesting One)
- Docker Container Security and STRIDE

Useful Resources Continued ...

- Microsoft Secure-SDL: Threat Modeling
- OWASP Application Threat Modeling
- Threat Modeling why how when (Nice Article)
- Kubernetes Threat Model (pdf)
- Docker Security: Threat Modeling
- Container as a Service Threat Analysis (pdf)

Thank you

Happy Learning.
Share if you care.

sanjeevjaiswal.com