Threat Modeling for Security Professionals

BSidesPGH 2019

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Threat Modeling for Security Professionals

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0641

Agenda

- **Who Am I?**
- **Terms**
- **When, What, Why**
- **OWASP Top 10**
- **STRIDE Threat Modeling**
- **OCTAVE Allegro Risk Analysis**
- **Mitigation Strategies**
- **Alternate Sources of Threats**
- **Summary**

Matt Trevors - CERT Division | Software Engineering Institute | Carnegie Mellon

Carnegie Mellon University

Technical Manager – Cybersecurity Assurance Team

CERT Division – Anticipating and solving our nation's cybersecurity challenges

- Largest technical division at the SEI
- Focused on Internet security, digital investigation, secure systems, insider threat, operational resilience, vulnerability analysis, network situational awareness, and coordinated response

Software Engineering Institute (SEI)

- Federally funded research and development center based at Carnegie Mellon University
- Basic and applied research in partnership with government and private organizations
- Helps organizations improve development, operation, and management of software-intensive and networked systems

Terms

- Threat
- Vulnerability
- Asset
- Risk
- Qualitative
- Quantitative
- STRIDE
- OCTAVE

When, What, and Why?

- Sooner rather than later
- Functional vs. Security Testing
- Add Value to the Business (ROI ↑ TCO ↓)

  (and maybe avoid some embarrassment)

The Open Web Application Security Project

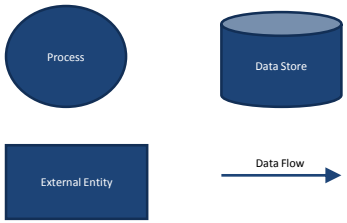
- International Community
- Top 10 Lists (Web, Mobile, Proactive Controls)
- Tools (Zed Attack Proxy)
- Software Assurance Maturity Model (SAMM)

OWASP Top 10 Web

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	X	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	X	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

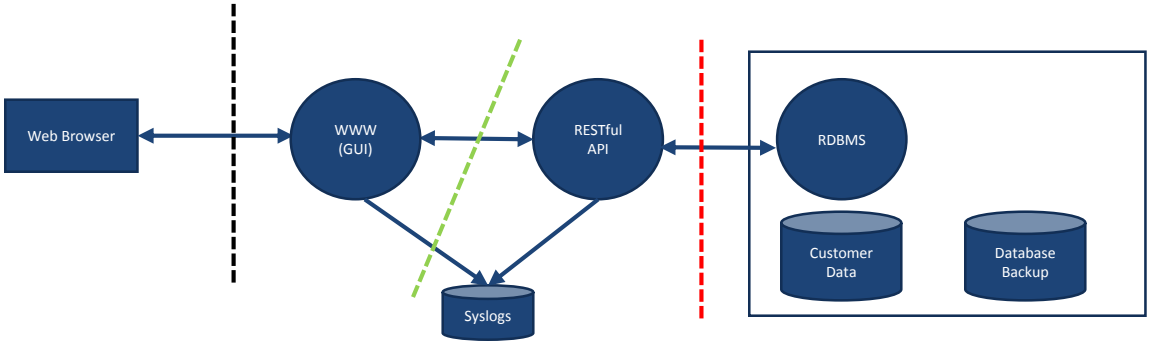
Threat Modeling with STRIDE

	S	T	R	I	D	E
External Entity	X		X			
Process	X	X	X	X	X	X
Data Flow		X		X	X	
Data Store		X	X	X	X	



- Spoofing (Authentication)
- Tampering (Integrity)
- Repudiation (Non-repudiation)
- Information Disclosure (Confidentiality)
- Denial of Service (Availability)
- Elevation of Privilege (Authorization)

Threat Modeling with STRIDE



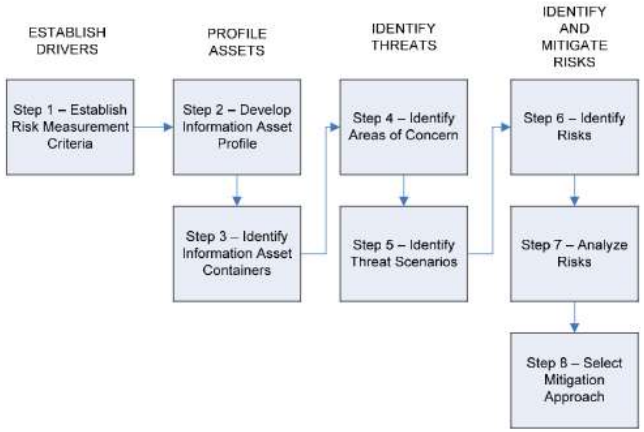
	S	T	R	I	D	E
External Entity	X		X			
Process	X	X	X	X	X	X
Data Flow		X		X	X	
Data Store		X	X	X	X	

Is there a threat of a threat actor {S|T|R|I|D|E} a(n) {EE|Proc|DF|DS} by exploiting a(n) {A[1-10]} vulnerability?

OWASP/STRIDE Association

OWASP Top 10 2017 – STRIDE Category/Entity Association										
	OWASP TOP 10									
STRIDE Category/Entity	A1 inj	A2 ba	A3 sde	A4 xxe	A5 bac	A6 mis	A7 xss	A8 des	A9 vul	A10 log
Spoofing/External Entity	X	X	X			X	X		X	
Repudiation/External Entity	X	X	X	X	X	X	X		X	X
Spoofing/Process						X			X	
Tampering/Process	X				X	X	X	X	X	X
Repudiation/Process				X		X			X	X
Information Disclosure/Process	X	X	X		X	X	X	X	X	
Denial of Service/Process						X			X	
Elevation of Privilege/Process	X	X		X	X	X	X	X	X	
Tampering/Data Flow						X			X	X
Information Disclosure/Data Flow			X			X			X	
Denial of Service/Data Flow						X			X	
Tampering/Data Store				X		X			X	X
Repudiation/Data Store						X			X	X
Information Disclosure/Data Store						X			X	X
Denial of Service/Data Store						X			X	

OCTAVE Allegro

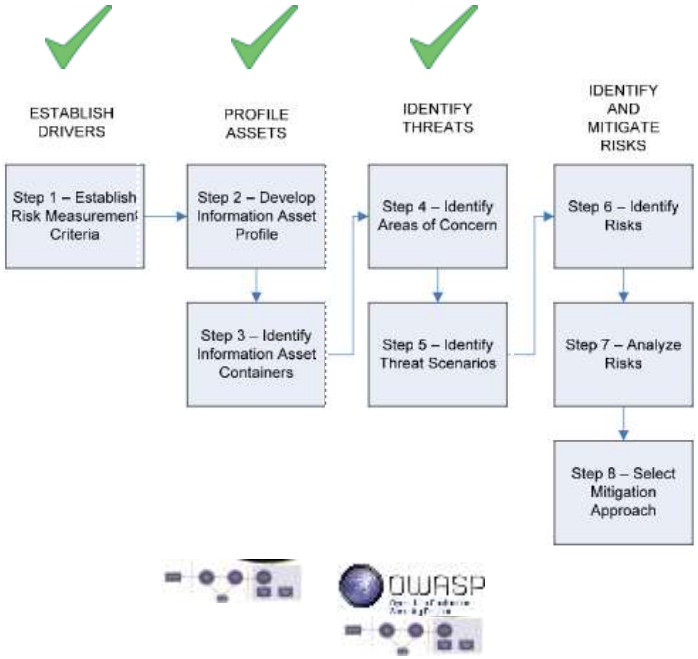


- Qualitative Risk Analysis
- Helps prioritize work
- 8 Steps

OCTAVE Allegro - Risk Measurement Criteria

Impact Area	Low	Moderate	High
Patient Safety	No, or negligible impact on patient treatment. Delay is less than ___ hours	Treatment of the patient aided by system components has been delayed more than ___ hours	Treatment of the patient aided by system components has been delayed more than ___ hours or delayed indefinitely
Regulatory/Legal Issue	No, or negligible impact on regulatory or legal standing	Issue requires legal and/or regulatory review requiring agencies and/or customers and/or the public to be notified	The issue requires legal and/or regulatory review requiring agencies and/or the public to be notified. The issue also requires corrective and preventative action that affects more than ____% of existing customers.
Brand Damage	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense are required to recover.	Reputation is irrevocably destroyed or damaged.
Loss of Productivity	Loss of less than _____% of development time to address issue over a period of ____ days	Loss of between _____% and _____% development time to address issue over a period of _____ days	Loss of greater than _____% development time to address issue over a period of ____ days
Customer Confidence	Less than _____% reduction in customers due to loss of confidence	_____to _____% reduction in customers due to loss of confidence	More than _____% reduction in customers due to loss of confidence

OCTAVE Allegro



OCTAVE Allegro

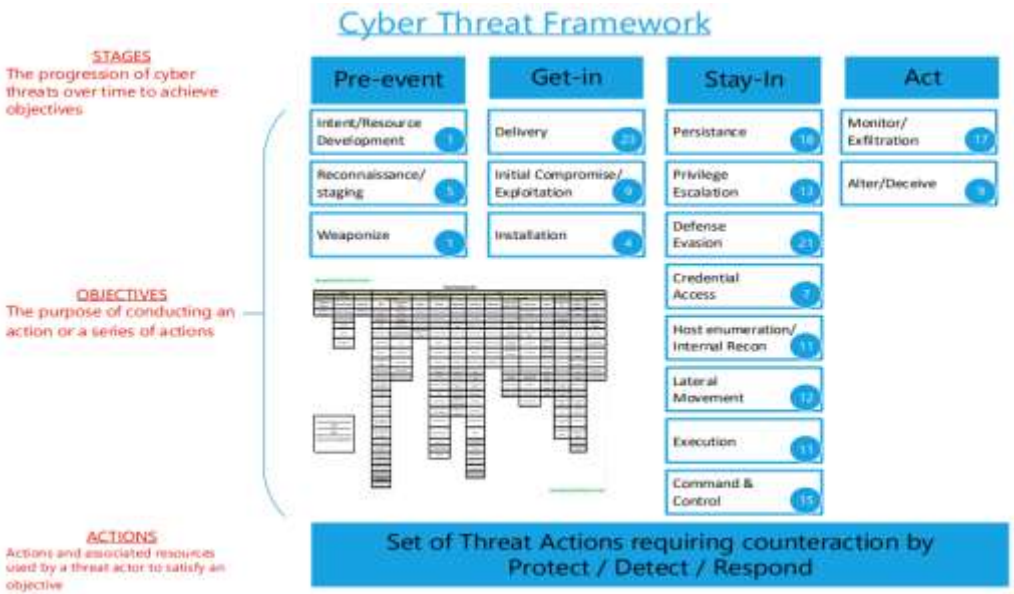
- Example
  - Spoofing -> External Entity
  - Multiply L/M/H damage for each Risk Measurement Criteria (L = 1, M = 2, H = 3)
    - Patient Safety (5) x L = 5
    - Regulatory/Legal (4) x H = 12
    - Brand Damage (3) X M = 6
    - Productivity (2) x L = 2
    - Confidence (1) x H = 3
  - Total Risk Score = 28
  - Complete for each applicable STRIDE category/STRIDE entity
  - Order from highest to lowest Risk Score

Mitigations

- **CSA Cloud Control Matrix**
- **IETF standards (OAuth 2.0, TLS, PBKDF2)**
- **CIS Critical Security Controls**
- **NIST SP 800-53 Controls Catalog**
- **NIST SP 800-171 – Controlled Unclassified Info**
- **ISO 27000 series (27002, 27018, etc.)**

DO NOT ROLL YOUR OWN!!!!!!!

Alternate Sources of Threats - DoDCAR/.govCAR Threat Framework



DoDCAR/.govCAR Threat Framework

Threat Action Heat Ma

Administer	Phase 1 - Prepare		Phase 2 - Engage		
Intent/Resource Development	Reconnaissance/ Staging	Weaponization	Delivery	Initial Compromise/ Exploitation	Installation
Intent/Resource Development	Crawling Internet Websites	Add Exploits to Application Data Files	Spear-phishing Emails w/ Attachments	Targets Application Vulnerability	Writing to Disk
	Network Mapping (e.g. NMAP)		Spear-phishing email w/Malicious Link	Target Operating System Vulnerability	In Memory Malware
	Social Media		Websites	Targets Application Vulnerability Remotely	Interpreted Scripts
	Mid-Points		Removable Media (i.e. USB)	Targets Web Application Vulnerabilities (ex. XSS, CSRF)	Replace legitimate binary with Malicious (ex: Havex)

DoDCAR/.govCAR Threat Framework

Security Capability Coverage (Pr

Threat Framework v2.0

Administer	Phase 1 - Prepare		Phase 2 - Engage			Phase 3 - Propagate		
Intent/Resource Development	Reconnaissance/ Staging	Weaponization	Delivery	Initial Compromise/ Exploitation	Installation	Persistence	Privilege Escalation	Defense Evasion
	Crawling Internet Websites		Spear-phishing Emails w/ Attachments		Writing to Disk			
	Network Mapping (e.g. NMAP)		Spear-phishing email w/Malicious Link	Target Operating System Vulnerability	In Memory Malware			
	Social Media		Websites	Targets Application Vulnerability Remotely	Interpreted Scripts		Automatic Loading at Startup	
	Mid-Points		Removable Media (i.e. USB)	Targets Web Application Vulnerabilities (ex. XSS, CSRF)	Replace legitimate binary with Malicious (ex: Havex)			Library Search Hijack

Summary

- **Familiarize with threat sources**
- **Create STRIDE DFD**
- **Define OCTAVE Allegro Risk Measurement Criteria**
- **Complete OCTAVE Allegro worksheets (STRIDE/OWASP)**
- **Calculate Risk Scores**
- **Sort/Rank based on Risk Scores (highest to lowest)**
- **Identify industry standard mitigations**
- **Practice makes perfect! (well… almost perfect)**

Resources

- **OWASP –** http://www.owasp.org
- **OCTAVE -** http://www.cert.org/resilience/products-services/octave/index.cfm
- **STRIDE -** http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118809998.html
- **CSA -** https://cloudsecurityalliance.org/group/cloud-controls-matrix/
- **CIS -** https://www.cisecurity.org/critical-controls.cfm
- **DoDCAR/.govCAR -** https://csrc.nist.gov/CSRC/media/Projects/cyber-supply-chain-risk-management/documents/SSCA/Fall_2018/WedPM2.2-STARCAR%20SCRM%20FINAL%20508.pdf
- **NSA Threat Framework v2 -** https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threat-framework.pdf