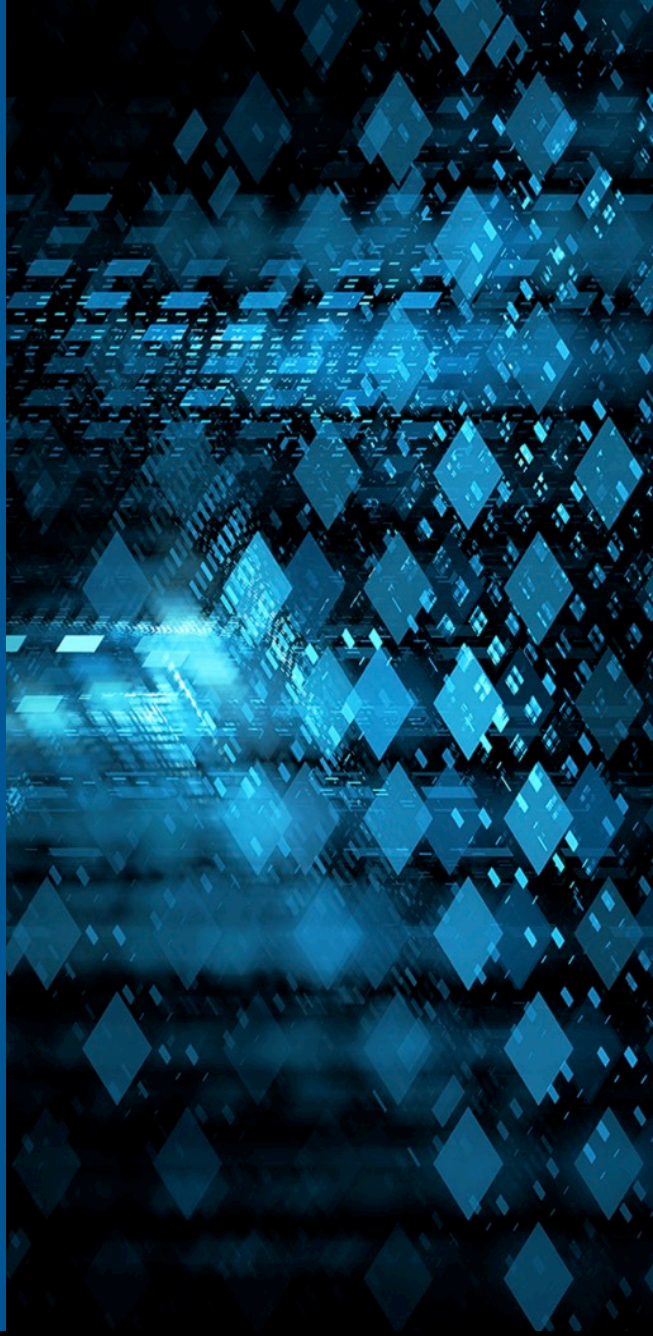
Threat Modeling and Risk Analysis for Developers and Testers

Matt Trevors

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



Threat Modeling and Risk Analysis for Developers and Testers

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Operationally Critical Threat, Asset, and Vulnerability Evaluation℠

DM-0004042

Agenda

- Who am I
- Why
- Terms
- OWASP Top 10
- STRIDE Threat Modeling
- OCTAVE Allegro Risk Analysis
- Mitigation Strategies
- Summary

When, What, and Why?

- Sooner rather than later
- Functional vs. Security Testing

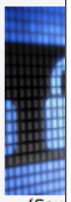
Hack that targeted Arizona voter (was easy to prevent, expert says

Posted: Sep 01, 2016 1:58 AM EDT
Updated: Sep 01, 2016 3:49 PM EDT

By Derek Staahl CONNECT

PHOENIX (KPHO/KTVK) - The FBI is warning every state across the country to shore up cyber defenses on voter databases after hacks in Arizona and Illinois, according to an FBI memo leaked online this week.

[READ MORE: Officials: Hackers breach election systems in Arizona, Illinois]



(Sou

The FBI Flash Bulletin, first obtained by Yahoo News, reveals hackers used a simple method to break into the voter registration databases – a method that cyber security experts say is easy to prevent.

"They used a method called SQL Injection. SQL Injection is a very popu a database. It's actually pretty easy," said Jamie Winterton, director of initiatives at Arizona State University's Global Security Initiative.

August 14, 2015

Cross-site scripting vulnerability uncovered in Salesforce cloud

Share this content:

Cross-Site Scripting (XSS) vulnerability within a Salesforce subdomain now patched

Researchers at cloud application security vendor Elastica have published details of a Cross-Site Scripting (XSS) vulnerability within a Salesforce subdomain providing the potential for attackers to use a trusted Salesforce application as a platform for end-user credential gathering attacks.

Disclosed in early July, Salesforce finally patched the vulnerability on Monday just two days before Elastica went public with the disclosure. Admittedly, XSS vulnerabilities are not the most exciting of attack vectors, but that doesn't mean they are not dangerous. Nor does it mean that organisations shouldn't know better when it comes to detecting them.

Millions of Salesforce users targeted by Dyre malware

Terms

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

The Open Web Application Security Project

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

OWASP Top 10 Web (2013)

A1 - Injection

A2 - Broken Authentication and Session Management

A3 - Cross-Site Scripting (XSS)

A4 - Insecure Direct Object Reference

A5 - Security Misconfiguration

A6 - Sensitive Data Exposure

A7 - Missing Function Level Access Control

A8 - Cross-Site Request Forgery (CSRF)

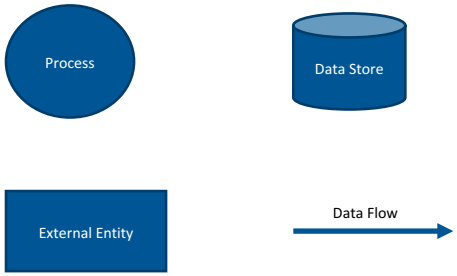
A9 - Using Components with Known Vulnerabilities

A10 - Unvalidated Redirects and Forwards

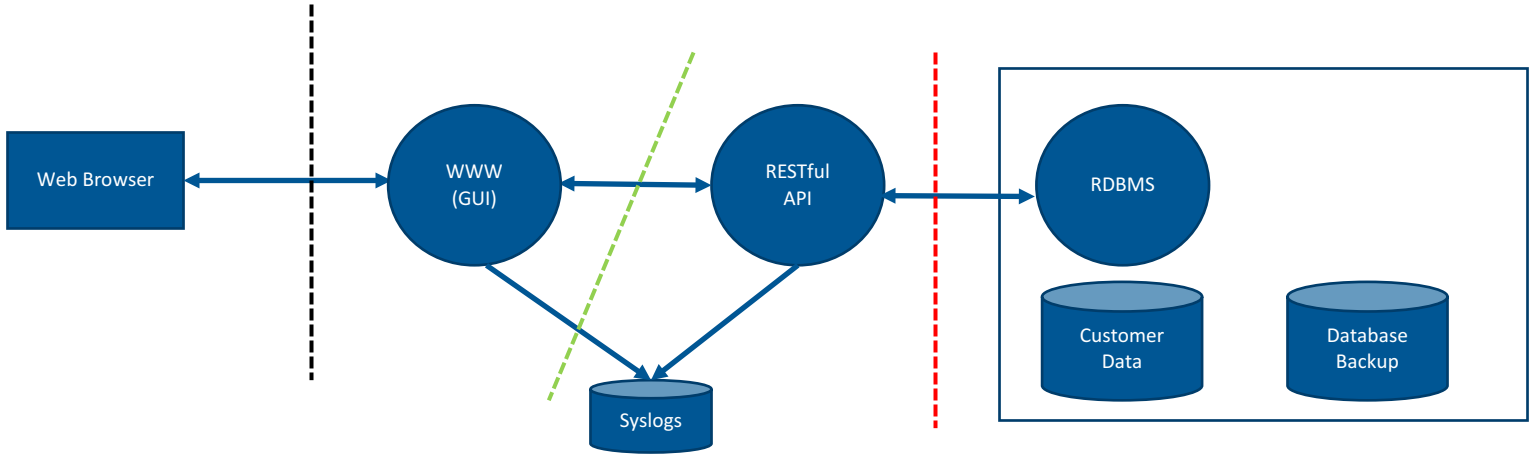
Threat Modeling with STRIDE

	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)



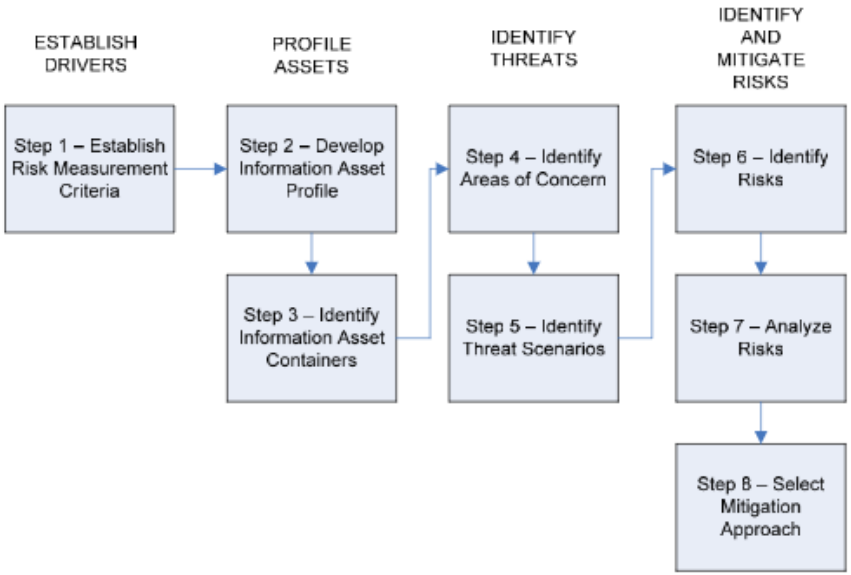
Threat Modeling with STRIDE



	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?

OCTAVE Allegro

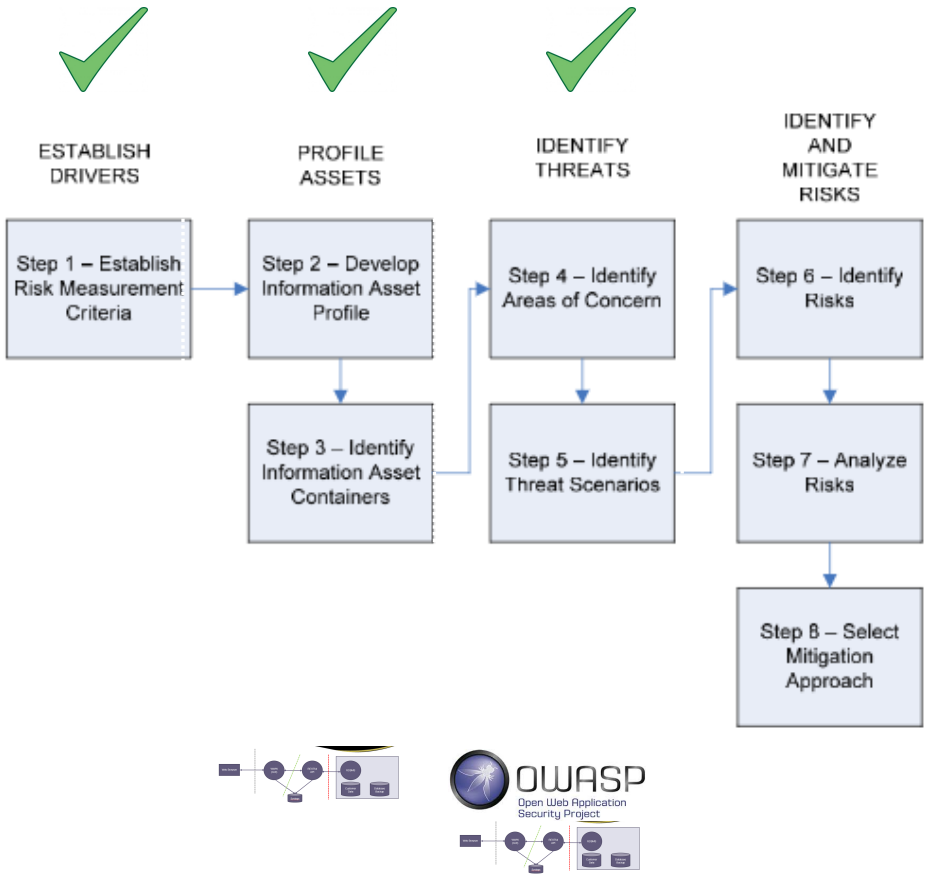


- Qualitative Risk Analysis (pinch of quantitative)
- Helps prioritize work
- 8 Steps

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 = 5
  - Total Risk Score = 30
  - Complete for each applicable STRIDE category/STRIDE entity
  - Order from highest to lowest Risk Score

Mitigation

- NIST SP 800-53 Controls Catalog
- ISO 27000 series (27002, 27034, etc.)
- FIPS 140-2
- IETF standards (OAuth 2.0, TLS, PBKDF2)

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

Summary

- Familiarize with OWASP
- Create STRIDE DFD
- Define OCTAVE Allegro Risk Measurement Criteria
- Complete OCTAVE Allegro spreadsheets (STRIDE/OWASP)
- Calculate Risk Scores
- Sort/Rank based on Risk Scores (highest to lowest)
- Identify industry standard mitigations
- **Calculate effort (for planning purposes)**
- Practice, Practice, Practice… Training, Training, Training

The End

Thank You!