TOREON

Practical Threat Modeling

SecAppDev 2018

Material

tinyurl.com/secappdev2018

TOREON

Sebastien Deleersnyder

- 5 years developer experience
- 15+ years information security experience
- Application security consultant Toreon

- Belgian OWASP chapter founder
- OWASP volunteer
- www.owasp.org

- Co-founder www.BruCON.org

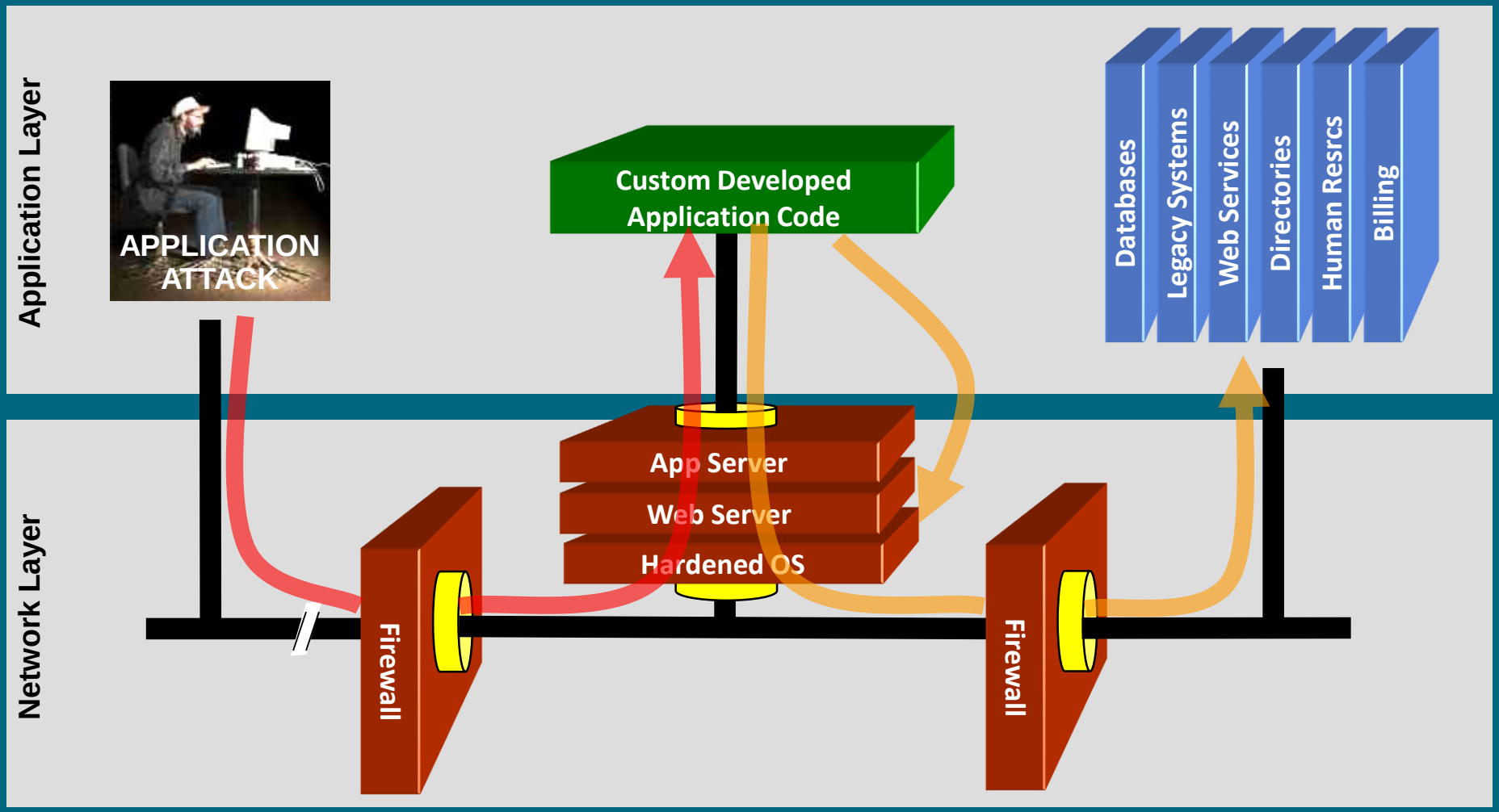
TOREON

Threat modeling introduction

- Threat modeling in a secure development lifecycle
- What is threat modelling?
- Why threat modeling?
- Threat modeling stages
- Diagrams
- Identify threats
- Addressing threats
- Document a threat model
- Tools

TOREON

Your security "perimeter" has huge holes at the application layer

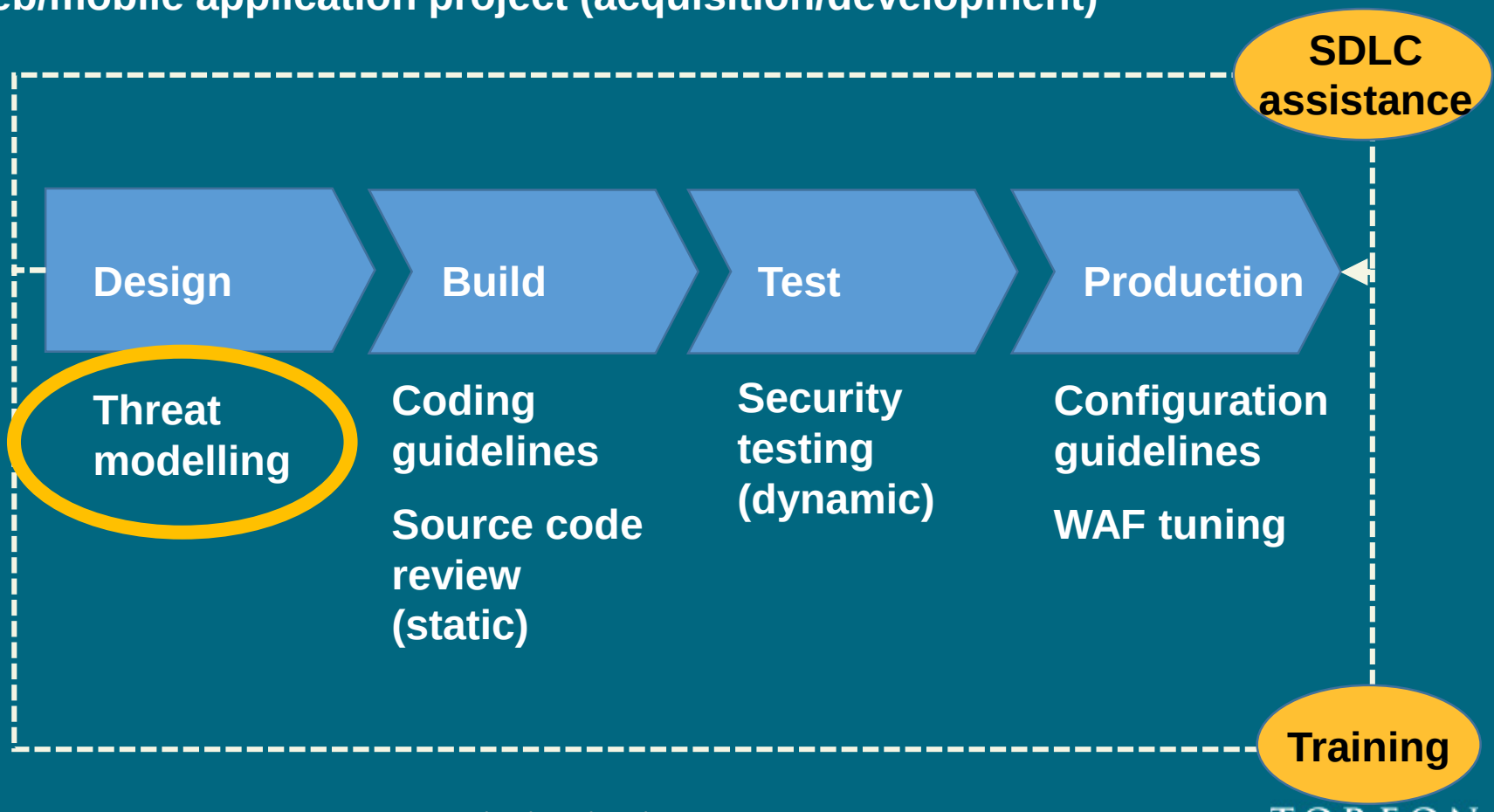


You can't use network layer protection (firewall, SSL, IDS, hardening) to stop or detect application layer attacks

TOREON

Secure development lifecycle

Web/mobile application project (acquisition/development)



TOREON

Flaws versus bugs

Security Design Flaws

- Introduced because of lack of security requirements, errors in design, lack of secure design knowledge, lack of architecture design review
- Cannot be identified by tools since lack contextual knowledge of the application
- Can be identified with threat modeling/secure architecture reviews

Security Coding Bugs

- Coding errors that result in vulnerabilities
- Can be identified with source code analysis and tools
- Requires developers understanding secure coding and following secure coding standards

Threat modeling

- Threat modelling is the activity of identifying and managing application risks
- Threat modelling is also known as Architectural Risk Analysis

TOREON

Why threat modeling?

- Prevent security design flaws when there's time to fix them
- Select mitigation strategy and techniques based on identified, documented and rated threats.
- Identify & address greatest risks
- Ability to prioritize development efforts within a project team based on risk weighting
- Increased risk awareness and understanding
- Mechanism for reaching consensus and better trade-off decisions
- Means for communicating results
- Cost justification and support for needed controls
- Artifacts to document due diligence for each software project

Threat modelling stages

Step 1

Diagram

What are we building?

TOREON

Threat modelling stages

Step 1

Diagram

What are we building?

Step 2

Identify threats

What can go wrong?

TOREON

Threat modelling stages

Step 1	Step 2	Step 3
Diagram	Identify threats	Mitigate
What are we building?	What can go wrong?	What are we doing to defend against threats?

TOREON

Threat modelling stages

Step 1	Step 2	Step 3	Step 4
Diagram	Identify threats	Mitigate	Validate
What are we building?	What can go wrong?	What are we doing to defend against threats?	Validate steps 1-3 Report

TOREON

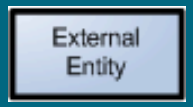
Diagrams

- Define scope
- Good understanding context / objectives
- Understand how the software works
- Who interacts with the software?
- With Data Flow Diagrams, Sequence Diagrams, State diagrams ...
- Identify attack surfaces
- Foundation for threat analysis

Diagramming

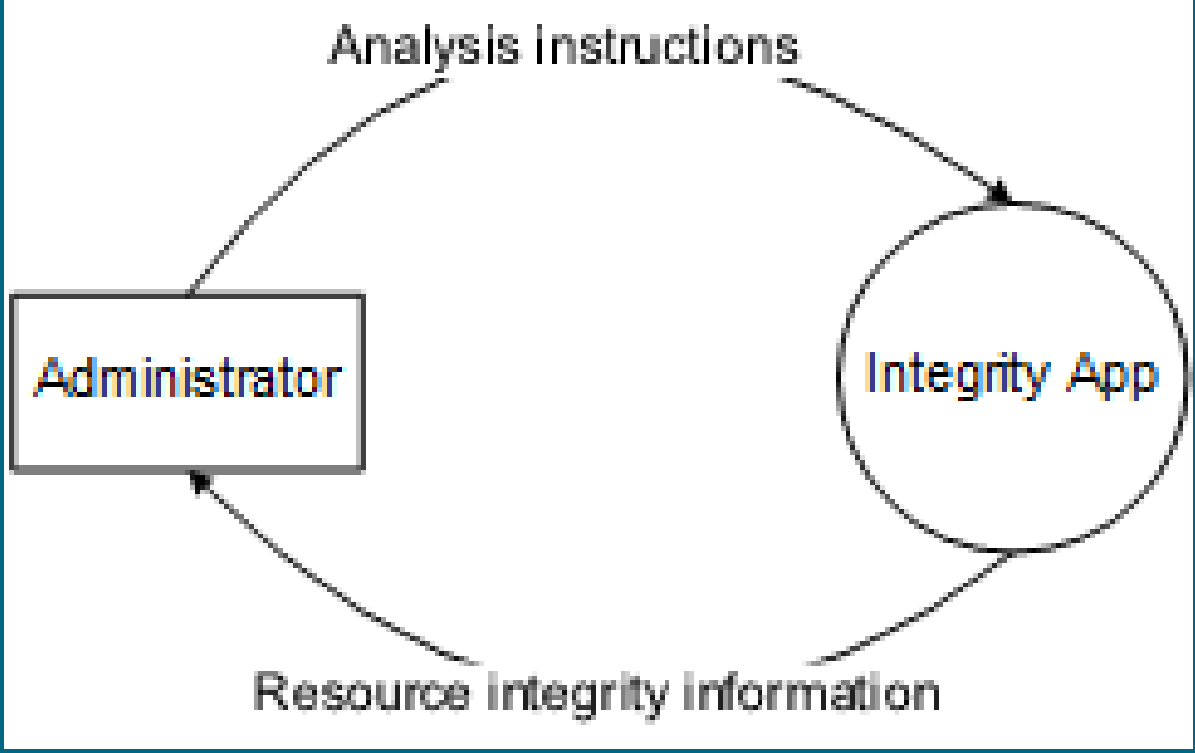
- Use DFDs (Data Flow Diagrams)
  - Include processes, data stores, data flows
  - Include trust boundaries
  - Diagrams per scenario may be helpful
- Update diagrams as web application changes
- Enumerate assumptions, dependencies
- Number everything (if manual)

DFD Basics

Symbol		Description
External Entity		• Represents entities outside the application that interact with the application via an entry point
Process		• Represents tasks that handle data within the application; tasks may process data or perform actions based on the data
Data Store		• Represents locations where data is stored; data stores do not modify data, they only store it.
Data Flow		• Represents data movement within applications; the arrow tells the direction of data movement
Trust Boundary		• Represents the change of trust levels as data flows through the application

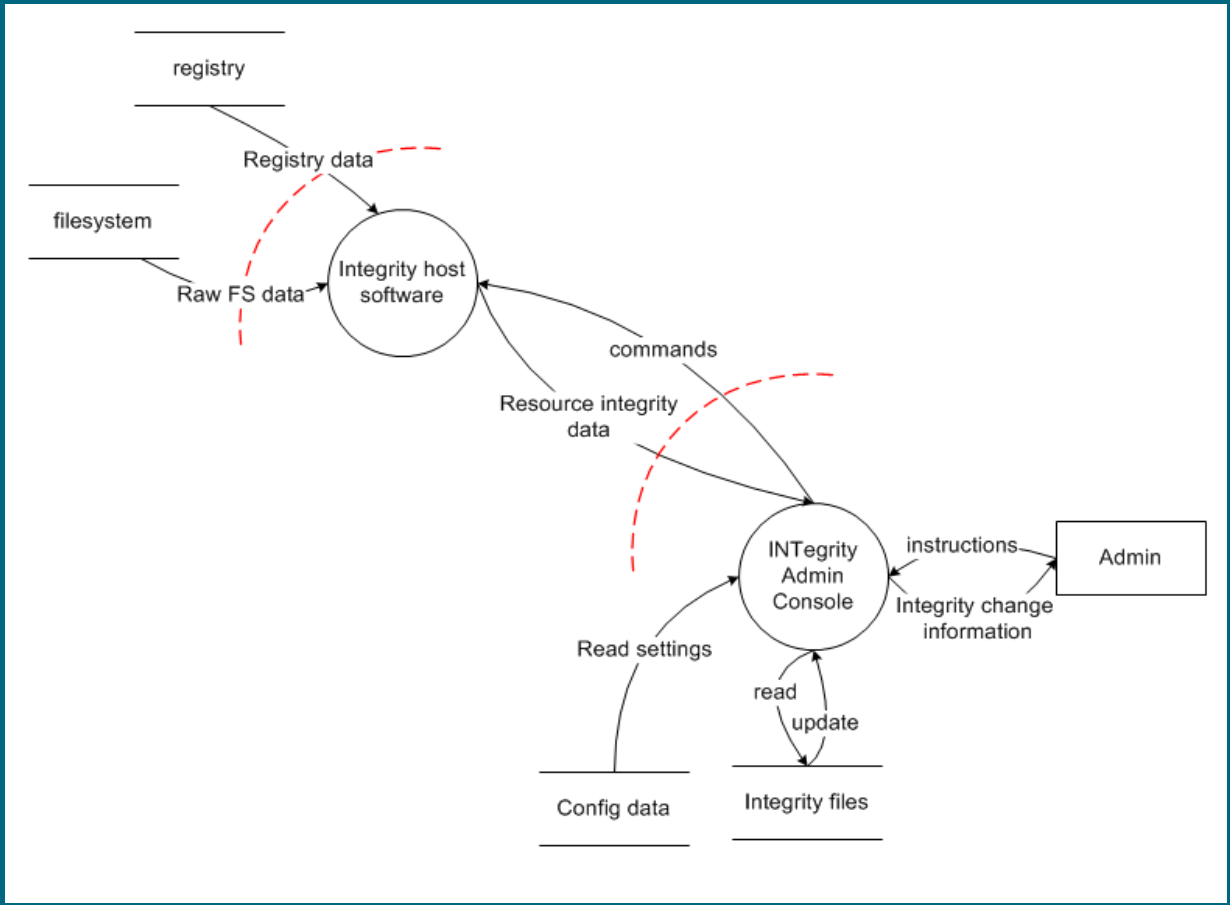
TOREON

Context diagram



TOREON

Level 1 Diagram



TOREON

Identify threats

- Based on diagrams
- STRIDE analysis
- Focus on identifying threats

TOREON

STRIDE

Spoofing	• Can an attacker gain access using a false identity?
Tampering	• Can an attacker modify data as it flows through the application?
Repudiation	• If an attacker denies doing something, can we prove he did it?
Information Disclosure	• Can an attacker gain access to private or potentially injurious data?
Denial of Service	• Can an attacker crash or reduce the availability of the system?
Elevation of Privilege	• Can an attacker assume the identity of a privileged user?

TOREON

Apply STRIDE Threats to Each Element

Apply the relevant parts of STRIDE to each item on the diagram

- External Entity – S, T
- Process – S, T, R, I, D, E
- Data store, data flow – T, I, D
  - Data stores that are logs – T, I, D, and R

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

This is why you number things

TOREON

Example

	Admin		>		Admin Console	
	Mitigations	Vulnerabilities	Mitigations	Vulnerabilities	Mitigations	Vulnerabilities
S	User/PW				SSL Cert	
T			SSL			
R		No audit log				No Audit log
I			SSL			
D						
E						No Access Control

TOREON

Addressing threats

- Cover all threats
- Identify controls already in place
- Handle threats not (completely) covered

TOREON

Addressing each threat

Mitigation patterns

Authentication	• Mitigating spoofing
Integrity	• Mitigating tampering
Non-repudiation	• Mitigating repudiation
Confidentiality	• Mitigating information disclosure
Availability	• Mitigating denial of service
Authorisation	• Mitigating elevation of privilege

TOREON

Mitigation patterns

- Apply appropriate secure design strategies
- Leverage proven best practices
- Reuse organisation security services, e.g.,
  - Single-Sign-On, Log Server
- Do not reinvent the wheel

For threats not (completely) covered

- Redesign to eliminate
- Apply standard mitigations
- Create new mitigations
- Accept vulnerability in design

TOREON

Risk-based Threat Management

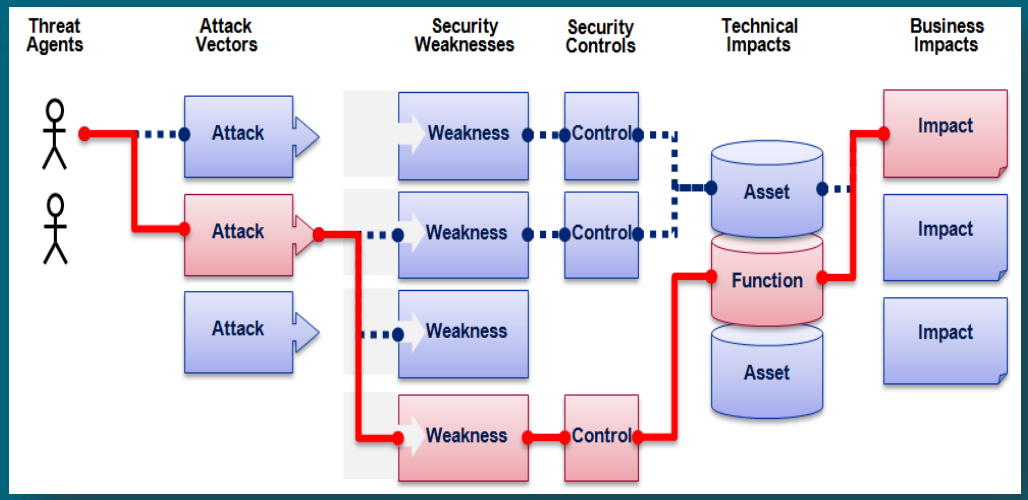
"The only truly secure system is one that is powered off, cast in a block of concrete, and sealed in a lead-lined room with armed guards - and even then I have my doubts. "

Prof Gene Spafford

Source: http://spaf.cerias.purdue.edu/quotes.html

TOREON

OWASP risk rating



Injection Example

Threat Agent	Attack Vector	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact
?	3 Easy	Widespread	Easy	Severe	?
	2 Average	Common	Average	Moderate	
	1 Difficult	Uncommon	Difficult	Minor	
	3	2	2	3	
		2.33	*	3	

7 weighted risk rating

TOREON

Example

Threat	Description	Vector	Prevalence	Detectability	Impact	Rating	Risk
TH – 01	Credentials can be brute forced	2	2	3	3	7.00	High
TH – 02	No security rules on password	2	2	2	3	6.00	Medium
TH – 03	No SSL for Android App	2	3	2	2	4.67	Medium
TH – 04	No SSL active for admin module	1	2	3	2	4.00	Medium
TH – 05	No accountability of Drupal updates	3	2	2	1	2.33	Low
TH – 06	API calls can be tampered with	1	1	1	2	2.00	Low
TH – 07	Fake IDs can be used	1	1	1	2	2.00	Low

Low: 1-3, Medium: 4-6, High: 7-9

TOREON

Communicate Your Threat Model

You cannot just "write and throw out" a security document

- **Recipients often won't understand it**

Communicate Your Threat Model

To increase adoption

- Present the results to the audience, in person
- Discuss the countermeasures – cost vs. impact
- Complete the threat model with a proposed action list that you know is acceptable

Typical audience

Architects

- Should integrate the proposition to update the design

Developers

- Should benefit from the model transparently, through updated specification

Security testing team

- Now know precisely what to test!

Software editor

- If you are acquiring software, you can add the threat model to the software acceptance procedure

TOREON

Update Your Threat Model

- First Threat Model during design
- Update Threat Model during technology decisions
- Review Threat Model before implementation
- Refine and verify Threat Model during security review
- Iterate

TOREON

Free Tools

- Whiteboards!
- Mind-Mapping diagramming tools such as FreeMind
- Microsoft Threat Modeling Tool 2016 https://www.microsoft.com/en-us/download/details.aspx?id=49168 https://www.youtube.com/watch?v=G2reie1skGg (demo)
- Gliffy Adds Dynamic Diagrams to Your Confluence Wiki Pages https://www.gliffy.com/products/confluence-plugin/
- ThreatSpec, developers and security engineers write threat specifications alongside code https://threatspec.org/
- Mozilla SeaSponge, browser-based graphical threat modeling tool http://mozilla.github.io/seasponge
- OWASP Threat Dragon Project https://www.owasp.org/index.php/OWASP_Threat_Dragon
- Elevation of Privilege (EoP) Card Game https://www.microsoft.com/en-us/sdl/adopt/eop.aspx https://www.youtube.com/watch?v=gZh5acJuNVg (Black Hat USA 2010: Elevation of Privilege: The Easy way to Threat Model)
- Trike was introduced as an open source threat modeling methodology and tool introduced in 2006

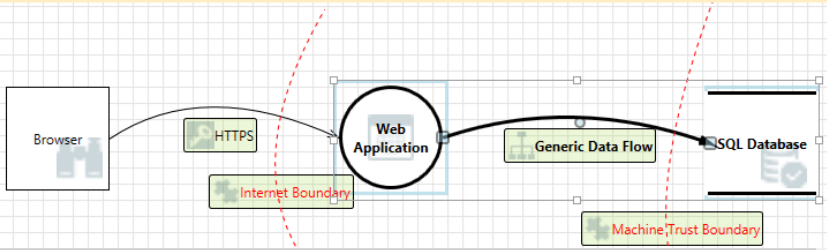
TOREON

Microsoft Threat Modeling Tool 2016

Basic Threat Model - Threat Modeling Tool 2016

File Edit View Settings Diagram Reports Help

Diagram 1



Threat List

ID	Diagram	Changed By	Last Modi	State	Title	Category	Short D	Description	Justificat
0	Diagram 1		Generated	Not Started	Spoofing the Browser External Entity	Spoofing	Spoofing...	Browser may be spoofed by an attacker and this may lead to unauthorized access to Web App...	
1	Diagram 1		Generated	Not Started	Cross Site Scripting	Tampering	Tamperi...	The web server 'Web Application' could be a subject to a cross-site scripting attack because it...	
2	Diagram 1		Generated	Not Started	Elevation Using Impersonation	Elevation Of Pr...	A user su...	Web Application may be able to impersonate the context of Browser in order to gain addition...	
3	Diagram 1		Generated	Not Started	Spoofing of Destination Data Store SQL Datab...	Spoofing	Spoofing...	SQL Database may be spoofed by an attacker and this may lead to data being written to the at...	
4	Diagram 1		Generated	Not Started	Potential SQL Injection Vulnerability for SQL D...	Tampering	Tamperi...	SQL injection is an attack in which malicious code is inserted into strings that are later passed...	
5	Diagram 1		Generated	Not Started	Potential Excessive Resource Consumption for...	Denial Of Servi...	Denial of...	Does Web Application or SQL Database take explicit steps to control resource consumption? R...	
6	Diagram 1		Generated	Not Started	Potential Data Repudiation by Web Application	Repudiation	Repudiat...	Web Application claims that it did not receive data from a source outside the trust boundary....	
7	Diagram 1		Generated	Not Started	Potential Process Crash or Stop for Web Appli...	Denial Of Servi...	Denial of...	Web Application crashes, halts, stops or runs slowly; in all cases violating an availability metric.	
8	Diagram 1		Generated	Not Started	Data Flow HTTPS Is Potentially Interrupted	Denial Of Servi...	Denial of...	An external agent interrupts data flowing across a trust boundary in either direction.	
9	Diagram 1		Generated	Not Started	Web Application May be Subject to Elevation...	Elevation Of Pr...	A user su...	Browser may be able to remotely execute code for Web Application.	

19 Threats Displayed, 19 Total

Threat Properties

ID: 4 Diagram: Diagram 1 Status: Not Started Last Modified: Generated

Title: Potential SQL Injection Vulnerability for SQL Database

Category: Tampering

Description: SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.

Justification:

Interaction: Generic Data Flow

Priority: High

Threat Properties | Notes - no entries

TOREON

Commercial Tools (no particular order)

- Microsoft Visio (Windows)
- ConceptDraw Pro (MacOS)

- MyAppSecurity ThreatModeler http://myappsecurity.com/threatmodeler/

- PTA Technologies http://www.ptatechnologies.com/

- Amenaza SecuriTree (Based on Attack trees vs Software centric approach) http://www.amenaza.com/

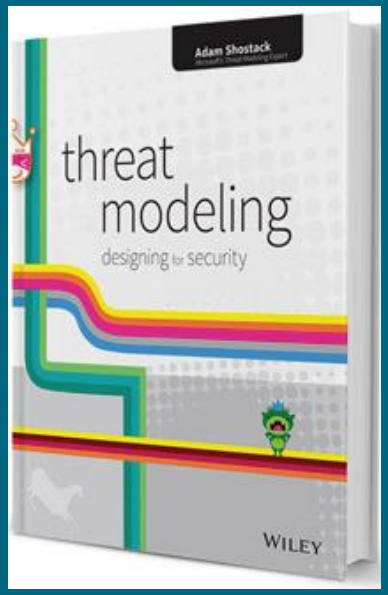
- IriusRisk by Continuum Security https://iriusrisk.continuumsecurity.net/

- Security Compass SD Elements is a Software Security Requirements Management platform that includes automated threat modeling capabilities https://www.securitycompass.com/threatmodeling/

- isograph AttackTree https://www.isograph.com/software/attacktree/

TOREON

Resources



Books

- **Threat Modeling (Adam Shostack, MS)**
- **Threat Modeling (Swiderski, Snyder) – older**
- **Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis (P.A.S.T.A) (Marco Morana and Tony "UV.")**
- **FAIR - Measuring and Managing Information Risk: A FAIR Approach (Jack Freund and Jack Jones)**

Online

- **https://en.wikipedia.org/wiki/Threat_model**
- **https://www.owasp.org/index.php/Application_Threat_Modeling**
- **BruCON 0x06 - Keynote - Adam Shostack - https://www.youtube.com/watch?v=-2zvfevLnp4**

TOREON

OWASP – On-going

- OWASP threat model project creation
- With the summit group, go over all the outcomes
- Publish all outcomes as soon as project is started
- Continue work on the cheat sheets
- Start work on a model to compare all threat methodologies, tools and techniques

Join the discussion at

https://owasp.slack.com/messages/C1CS3C6AF

OWASP Threat Modeling Slack channel

TOREON

Templates for this Workshop

- Template to document a threat model
- Template to calculate risk levels of identified threats
- Threat modeling Visio Stencil

TOREON

That’s All Folks

You can contact me through

- **Toreon seba@toreon.com**
- **OWASP seba@owasp.org**
- **Twitter @SebaDele**
- **OWASP TM Slack channel**

TOREON