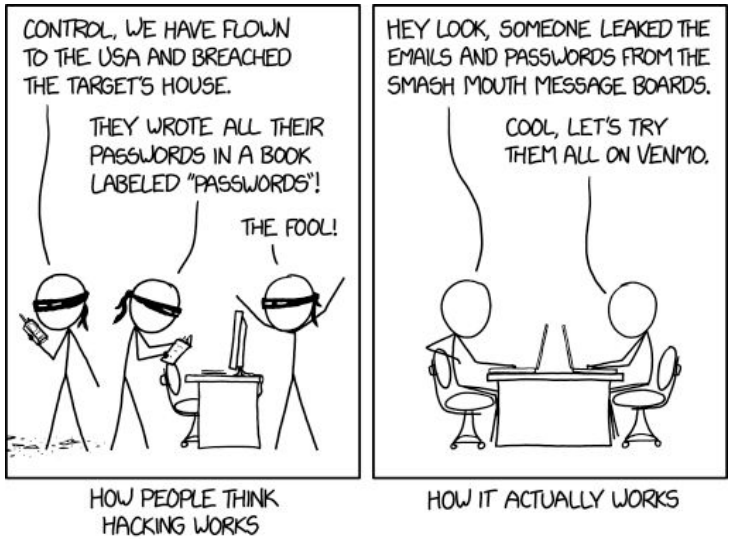
Secure Application Design and Development With Threat Modeling



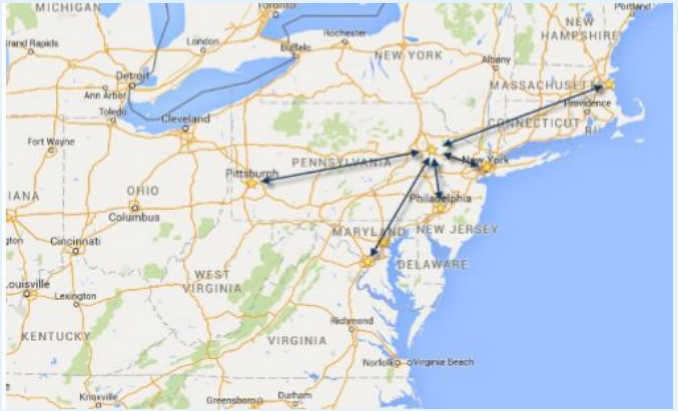
https://xkcd.com/2176/

Joe Kuemerle
joe@kuemerle.com
@jkuemerle

techbash

November 7-10, 2023 | Pocono Manor, PA

- Great speakers with top content
- A fraction of the cost of the more crowded conferences
  - 3-day conference plus lodging for less than $1000
- Full day deep dive preconference sessions available
- Easy to get to from almost anywhere
- In addition to the breakout sessions you get a great hallway track, attendee reception, game night and more
- Full day of kids & family sessions on Friday, free for families of attendees
- Discounted Kalahari Waterpark room nights: stay, learn and play all in one place



https://techbash.com or **@techbash**

https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/

https://www.flickr.com/photos/111692634@N04/11406985424

https://www.flickr.com/photos/23195413@N07/2438941120

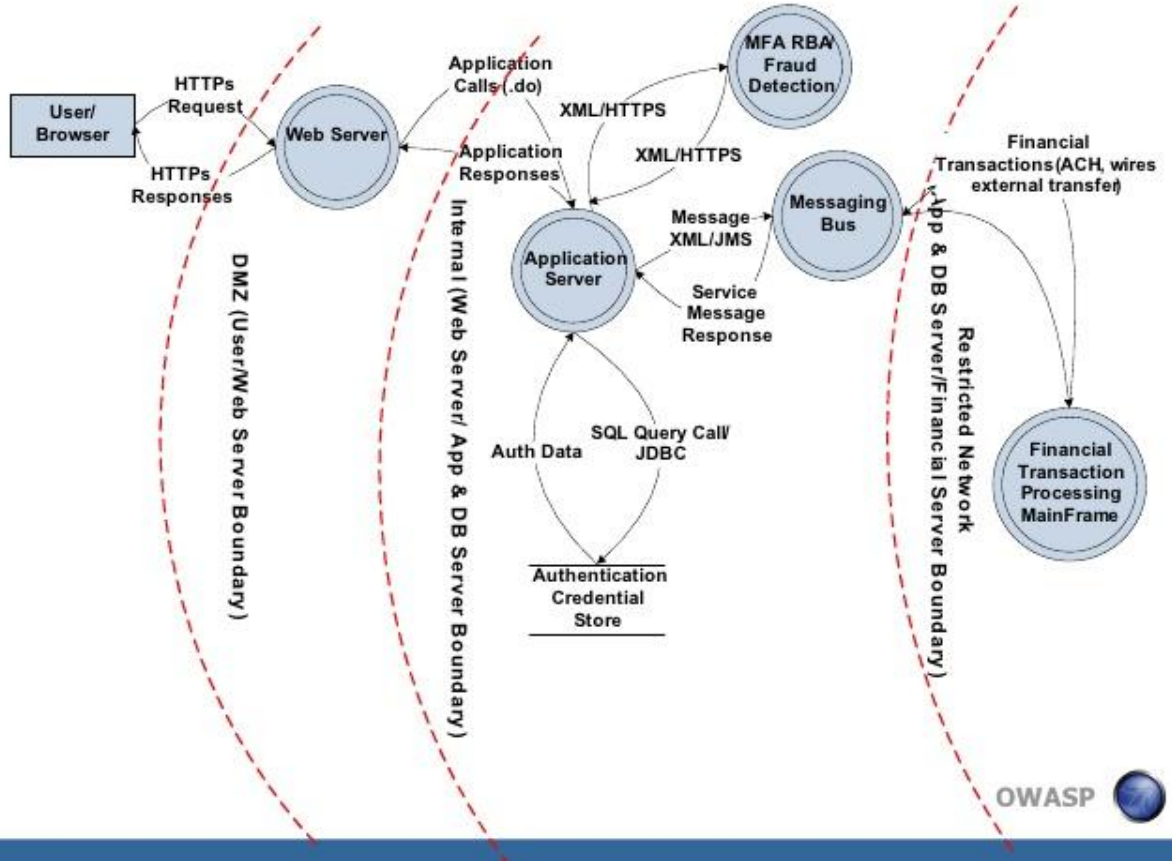
https://www.flickr.com/photos/11946169@N00/15198147976

https://www.flickr.com/photos/9511824@N05/4744861022

https://www.flickr.com/photos/45170709@N06/4167655890

https://www.flickr.com/photos/37804160@N00/3261531583

Data flow diagram-Online Banking Application

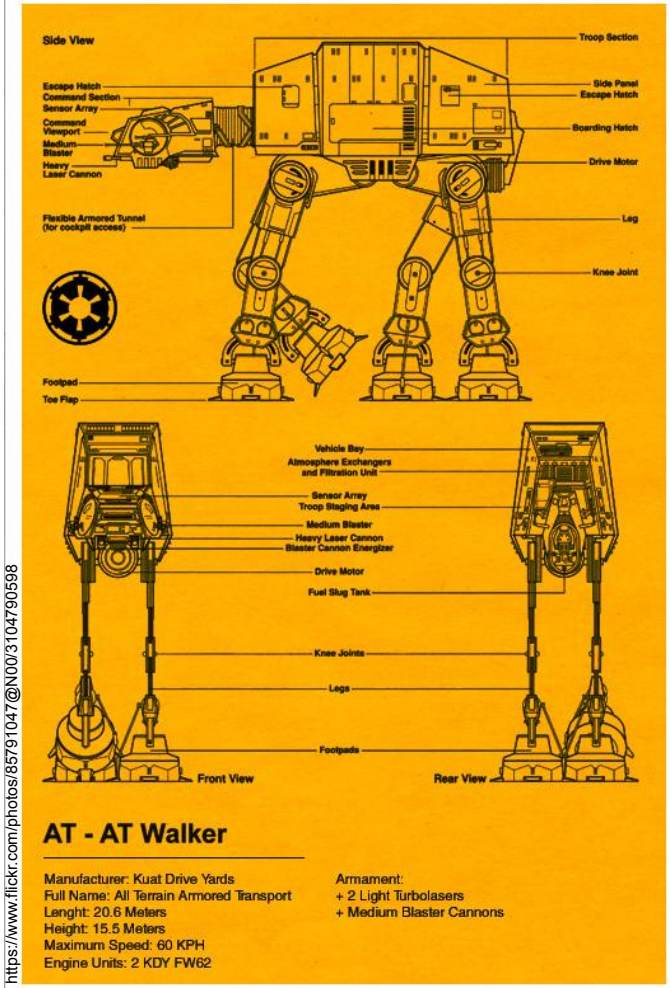


https://commons.wikimedia.org/wiki/File:Data_Flow_Diagram_-_Online_Banking_Application.jpg

https://www.flickr.com/photos/49968232@N00/48436759506

Agenda

- Why
  - Why should you threat model
  - Benefits of threat modeling
- What
  - What is a threat model
  - What are the different types of threat modeling
  - Threat Model All The Things
- How
  - Tooling and techniques
  - Threat modeling and agile development
  - Ongoing updates



https://xkcd.com/2021

HOW SOFTWARE DEVELOPMENT WORKS

https://www.flickr.com/photos/92244916@N00/118407393

https://www.flickr.com/photos/92244916@N00/118407393

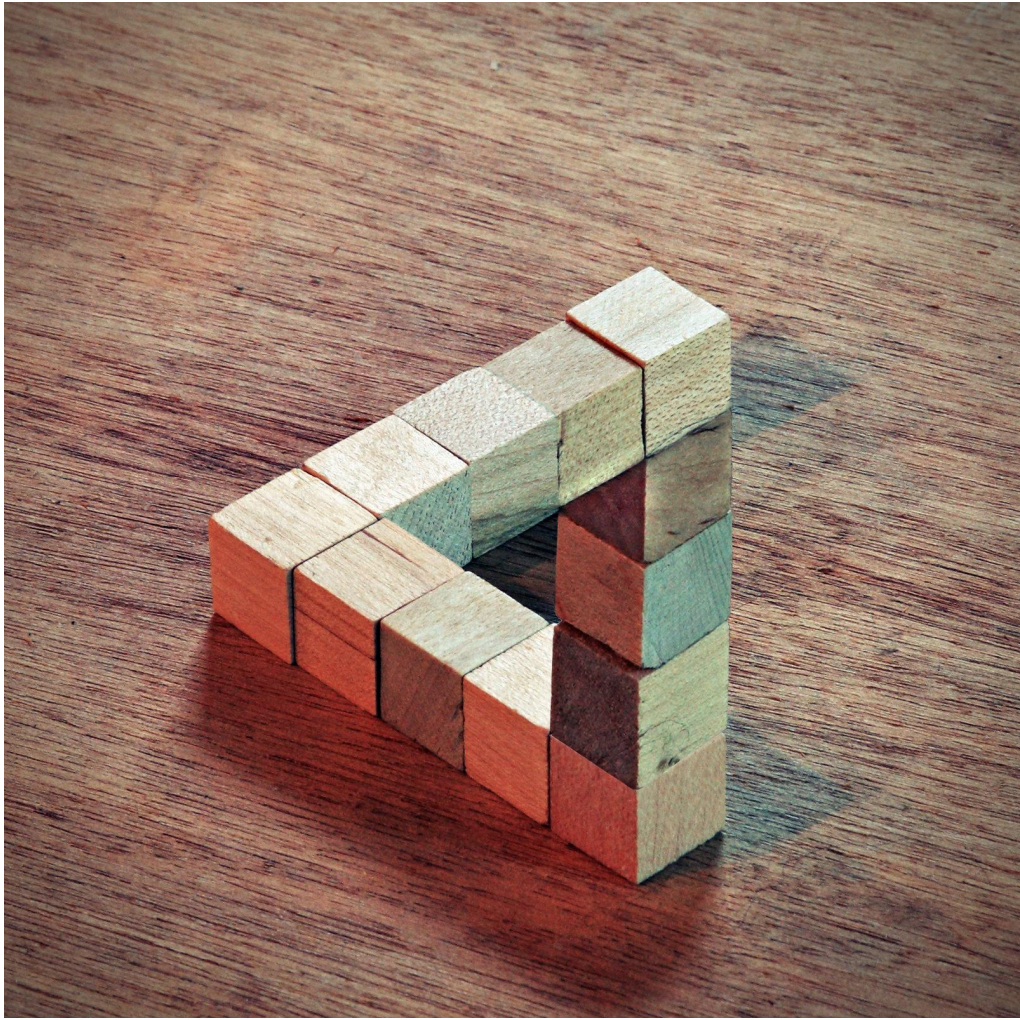
https://www.flickr.com/photos/28634332@N05/31090859297

https://www.flickr.com/photos/53941521@N00/729236991

Confidentiality

Integrity

Availability



https://www.flickr.com/photos/44442915@N00/4667535253

https://www.flickr.com/photos/65447217@N00/13771754114

Spoofing: An intruder posing as another user, component, or other system feature that contains an identity in the modeled system.

Tampering: The altering of data within a system to achieve a malicious goal.

Repudiation: The ability of an intruder to deny that they performed some malicious activity, due to the absence of enough proof.

Information Disclosure: Exposing protected data to a user that isn't authorized to see it.

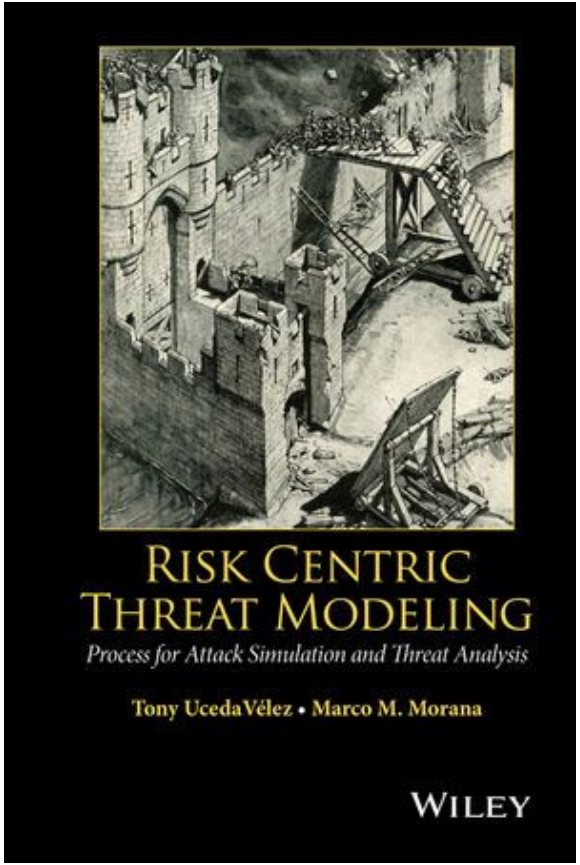
Denial of Service: An adversary uses illegitimate means to exhaust services needed to provide service to users.

Elevation of Privilege: Allowing an intruder to execute commands and functions that they aren't allowed to.

Process for **A**ttack **S**imulation and **T**hreat **A**nalysis

1. Define Objectives	• Identify Business Objectives • Identify Security and Compliance Requirements • Business Impact Analysis
2. Define Technical Scope	• Capture the Boundaries of the Technical Environment • Capture Infrastructure | Application | Software Dependencies
3. Application Decomposition	• Identify Use Cases | Define App. Entry Points & Trust Levels • Identify Actors | Assets | Services | Roles | Data Sources • Data Flow Diagramming (DFDs) | Trust Boundaries
4. Threat Analysis	• Probabilistic Attack Scenarios Analysis • Regression Analysis on Security Events • Threat Intelligence Correlation and Analytics
5. Vulnerability & Weaknesses Analysis	• Queries of Existing Vulnerability Reports & Issues Tracking • Threat to Existing Vulnerability Mapping Using Threat Trees • Design Flaw Analysis Using Use and Abuse Cases • Scorings (CVSS/CWSS) | Enumerations (CWE/CVE)
6. Attack Modeling	• Attack Surface Analysis • Attack Tree Development | Attack Library Mgt. • Attack to Vulnerability & Exploit Analysis Using Attack Trees
7. Risk & Impact Analysis	• Qualify & Quantify Business Impact • Countermeasure Identification and Residual Risk Analysis • ID Risk Mitigation Strategies

https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/



https://www.wiley.com/en-us/Risk+Centric+Threat+Modeling%3A+Process+for+Attack+Simulation+and+Threat+Analysis-p-9780470500965#

Damage Potential: Ranks the extent of damage resulting from an exploited weakness.

Reproducibility: Ranks the ease of reproducing an attack

Exploitability: Assigns a numerical rating to the effort needed to launch the attack.

Affected Users: A value representing how many users get impacted if an exploit becomes widely available.

Discoverability: Measures how easy it is to discover the threat.

https://www.octotrike.org

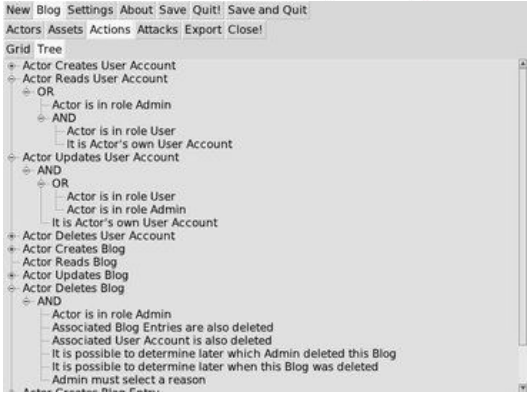
¤ Trike

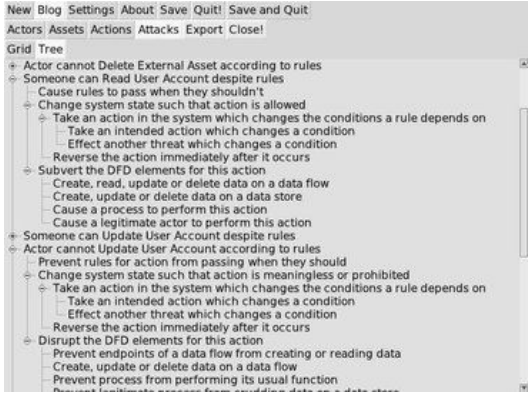
Trike is an open source threat modeling methodology and tool. The project began in 2006 as an attempt to improve the efficiency and effectiveness of existing threat modeling methodologies, and is being actively used and developed.

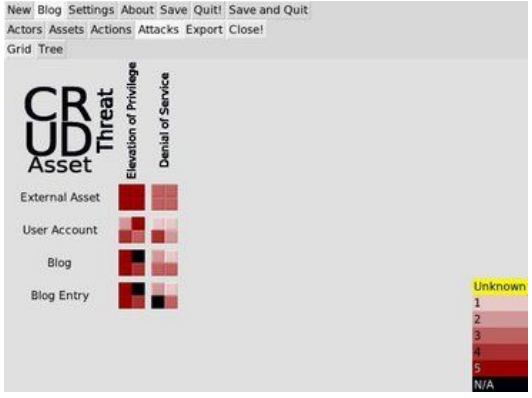
There have been three versions of the Trike methodology:

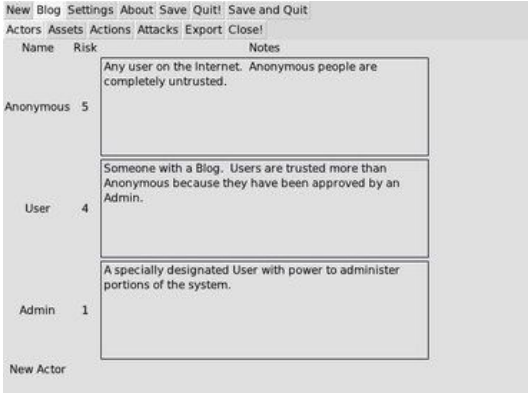
- Version 1 is documented in a white paper. Highlights include automatic threat generation at the requirements level and automatic generation of attack trees.
- Version 1.5 is partially documented in the help spreadsheet for the version 1.5 implementation. It is an interim bridge between version 1 and version 2. Highlights include improved automatic threat generation at the requirements level, security objectives, the complete absence of threat trees, and HAZOP analysis.
- Version 2 is a yet-to-be-documented superset of version 1.5. Additional highlights include semi-automatic threat generation at the architectural level and attack chaining. Version 2 is under active development. Most of our more recent talks give previews of different portions of the version 2 methodology.

There have been several different Trike tools; for the full scoop, see our tools page.







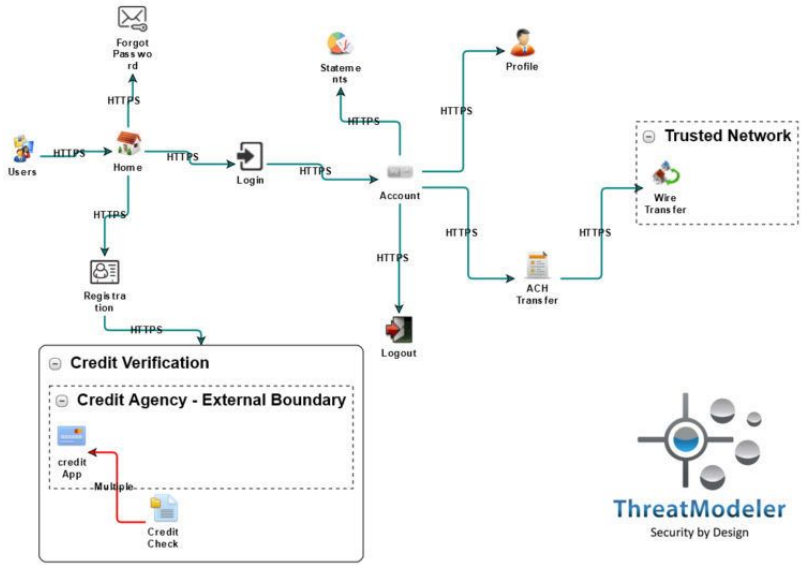


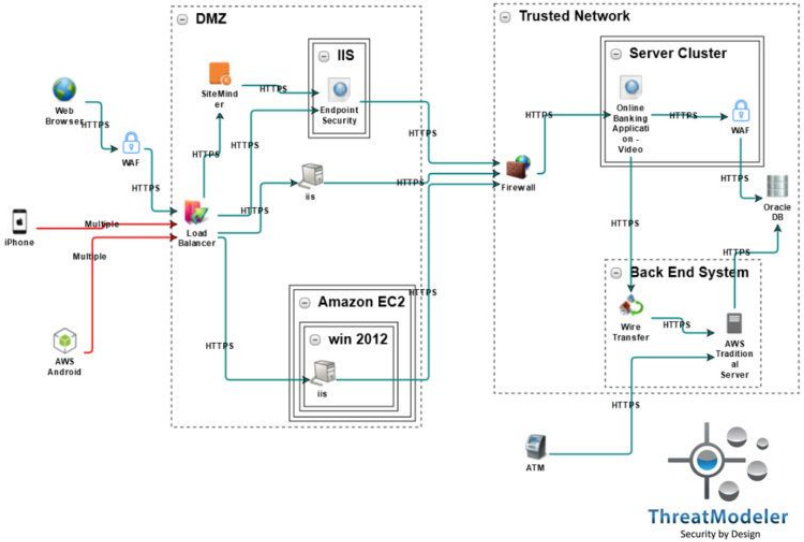
Octopus

Download

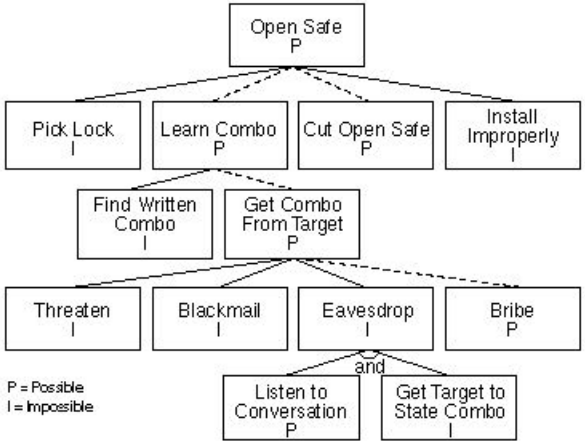
Spreadsheet
Standalone Tool

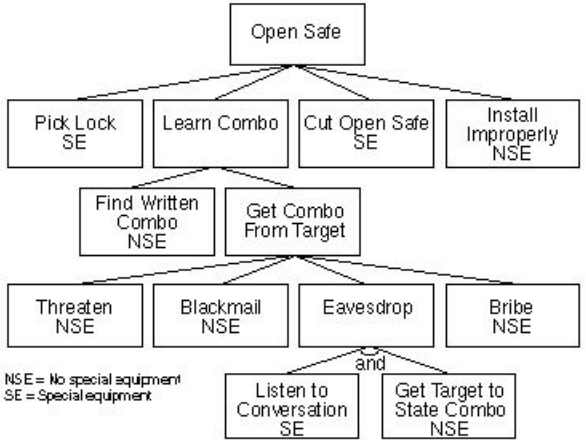
Visual **A**gile **S**imple **T**hreat modeling

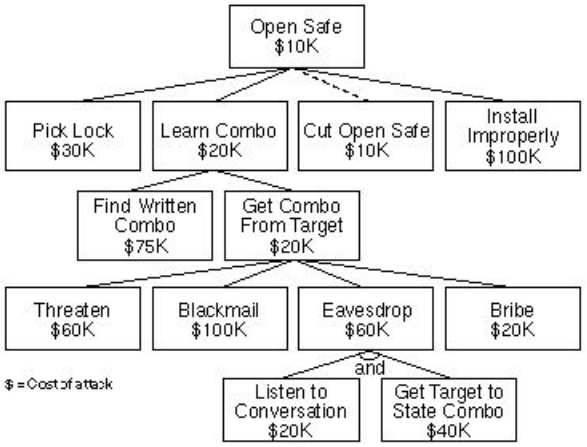


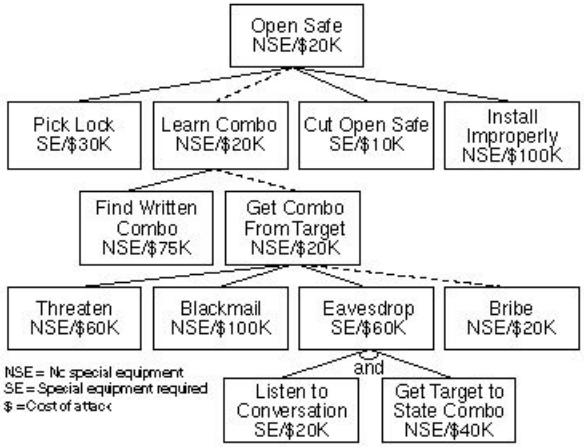


https://threatmodeler.com/operational-application-threat-modeling





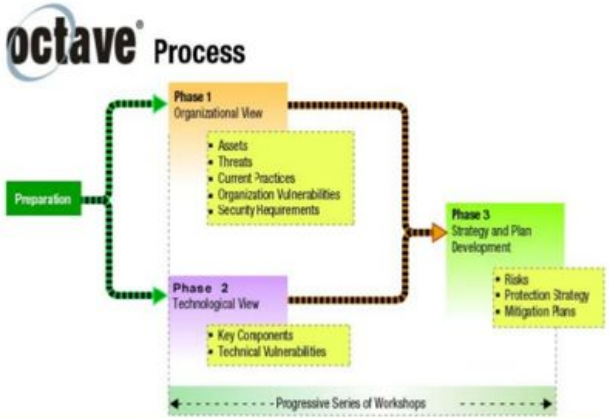




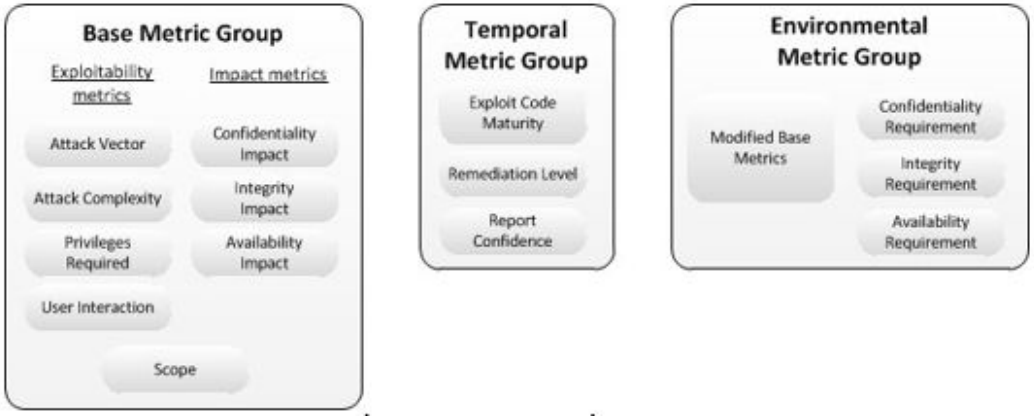
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods

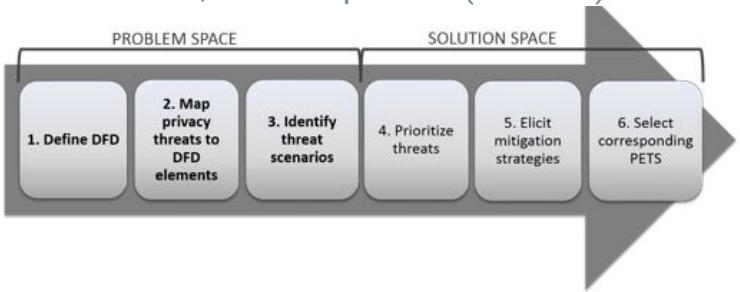
Operationally **C**ritical **T**hreat, **A**sset and **V**ulnerability **E**valuation



Common **V**ulnerability **S**coring **S**ystem



linkability, **i**dentifiability, **n**onrepudiation, **d**etectability, **d**isclosure of information, **u**nawareness, **n**oncompliance (**LIDDUN**)



- Hybrid **T**hreat **M**odeling **M**ethod
- Quantitative Threat Modeling Method
- T-MAP

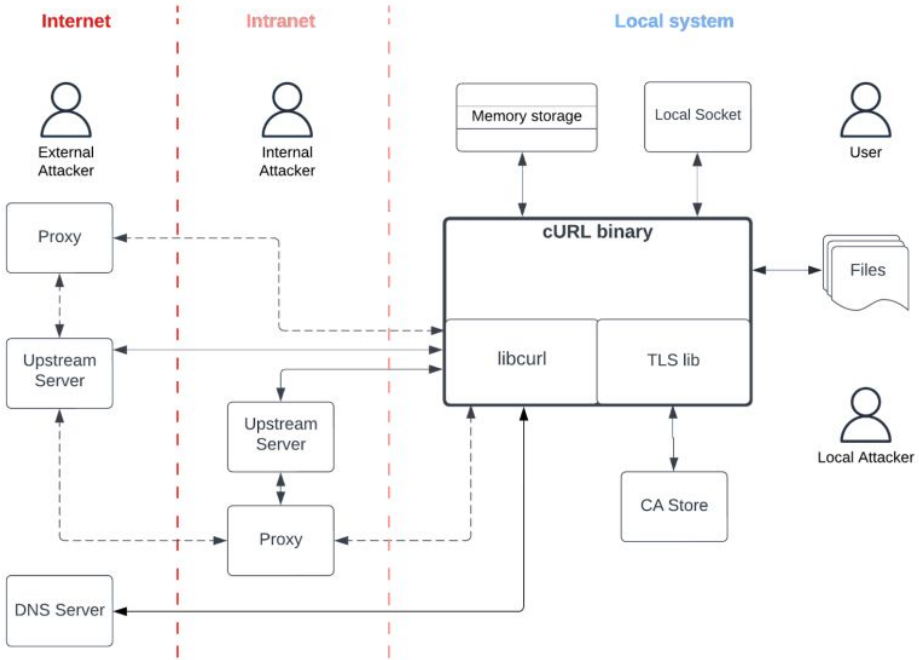
Shostack's 4 Question Frame for Threat Modeling

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

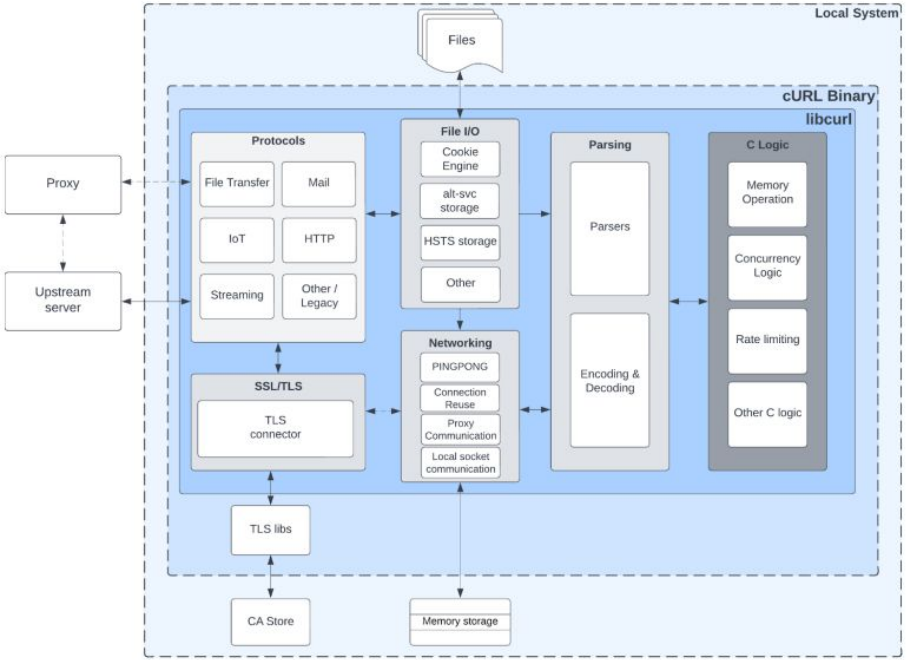
https://github.com/adamshostack/4QuestionFrame

https://www.flickr.com/photos/11629603@N04/8415520966

High-Level Data Flow



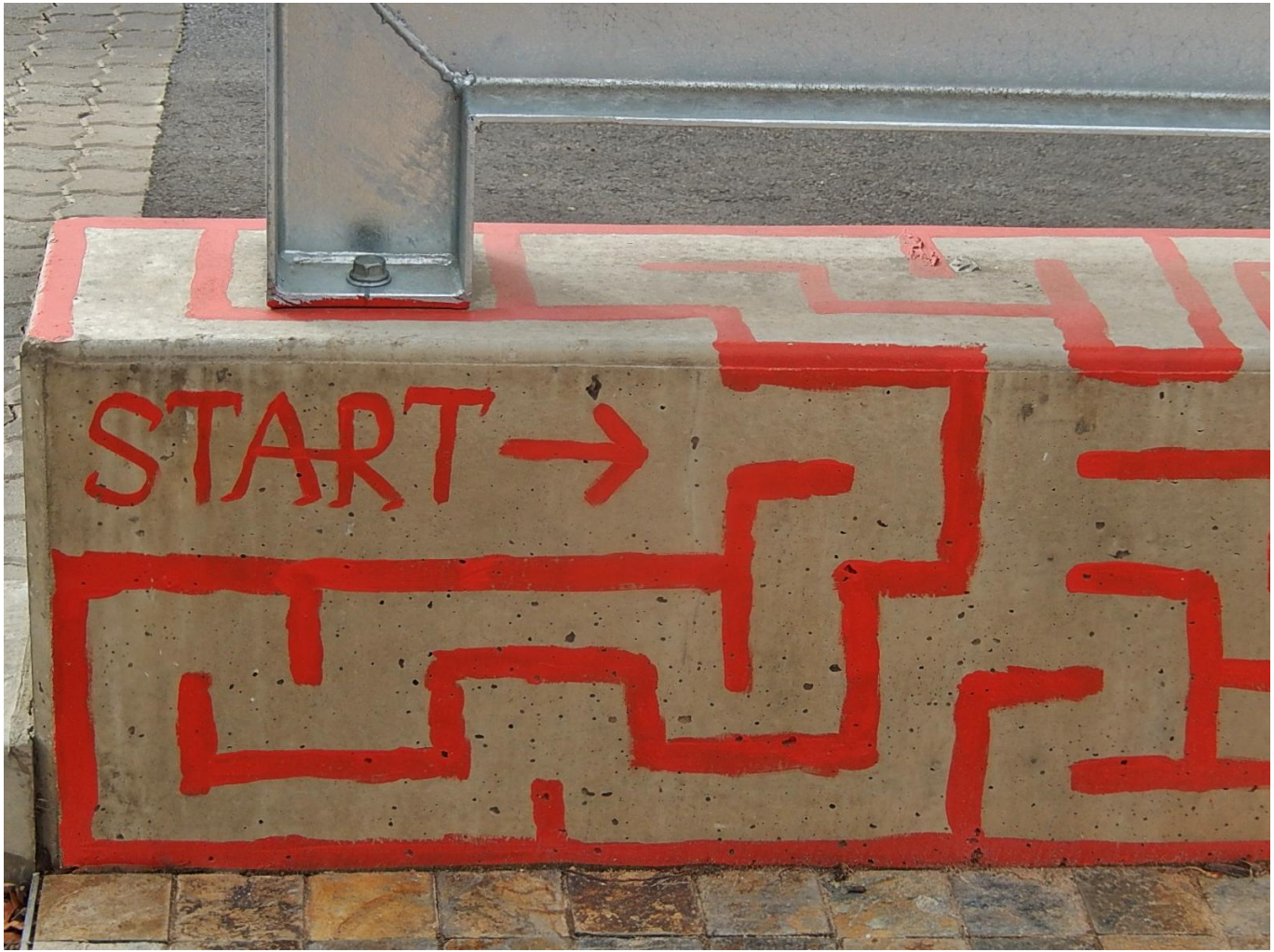
Binary Data Flow



https://github.com/trailofbits/publications/blob/master/reviews/2022-12-curl-threatmodel.pdf

https://daniel.haxx.se/blog/2022/12/21/the-2022-curl-security-audit/

https://www.flickr.com/photos/10816734@N03/9367809606



https://www.flickr.com/photos/89165847@N00/11300349426

Spoofing: An intruder posing as another user, component, or other system feature that contains an identity in the modeled system.

Tampering: The altering of data within a system to achieve a malicious goal.

Repudiation: The ability of an intruder to deny that they performed some malicious activity, due to the absence of enough proof.

Information Disclosure: Exposing protected data to a user that isn't authorized to see it.

Denial of Service: An adversary uses illegitimate means to exhaust services needed to provide service to users.

Elevation of Privilege: Allowing an intruder to execute commands and functions that they aren't allowed to.

https://www.flickr.com/photos/60944636@N00/9559870980

IriusRisk: https://www.iriusrisk.com/

https://www.flickr.com/photos/93332172@N03/14041012886

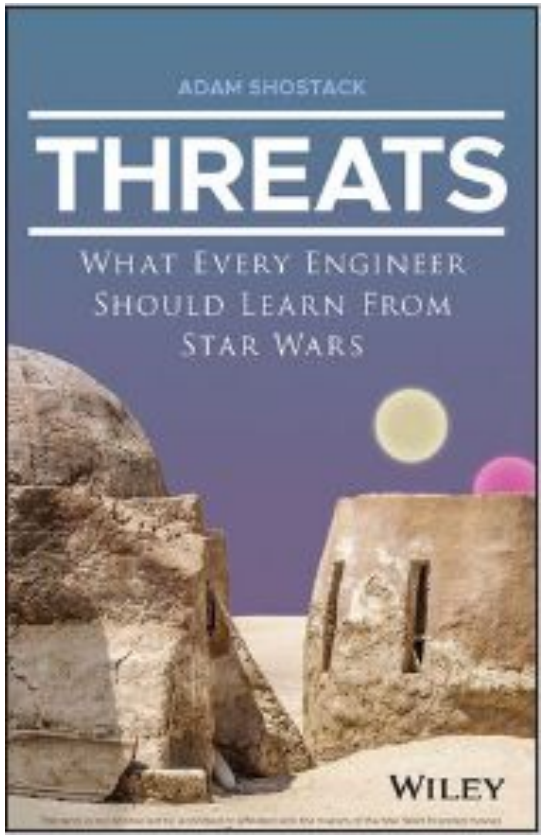
https://www.flickr.com/photos/38478466@N06/3700355684

https://www.flickr.com/photos/53416300@N00/8334277572

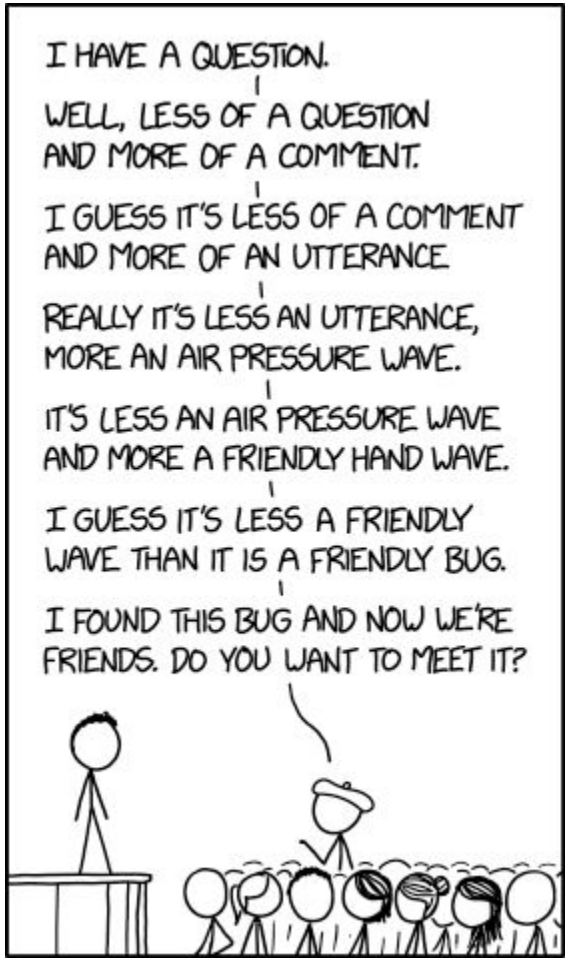
https://www.flickr.com/photos/46944516@N00/15269502297

http://bit.ly/3GZqMo5

https://www.pinterest.com/pin/159948224238201989/



http://bit.ly/3W4ofx8



https://xkcd.com/2191/

Resources

- https://www.threatmodelingmanifesto.org/
- https://github.com/hysnsec/awesome-threat-modelling
- https://github.com/OWASP/threat-model-cookbook
- https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
- https://owasp.org/www-project-threat-dragon/
- https://github.com/geoffrey-hill-tutamantic/rapid-threat-model-prototyping-docs
- https://www.cynance.co/pasta-threat-modelling/
- https://bit.ly/adam-yt
- https://threatmodeler.com/threat-modeling-methodologies-overview-for-your-business/
- https://github.com/adamshostack/4QuestionFrame
- https://about.gitlab.com/blog/2021/07/09/creating-a-threat-model-that-works-for-gitlab/