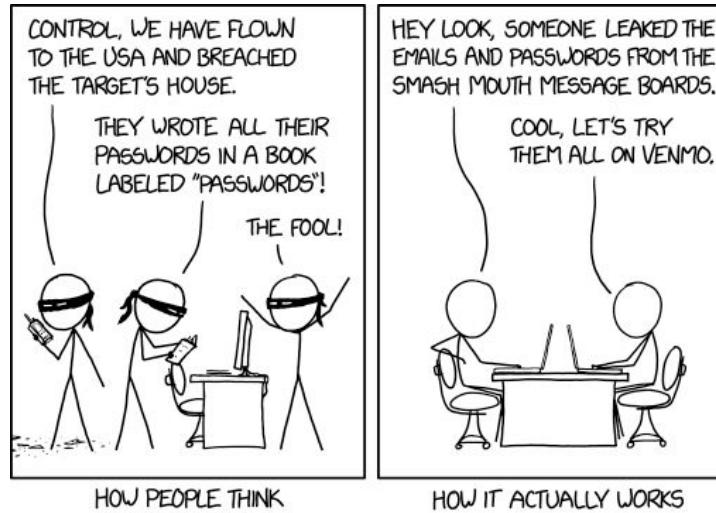
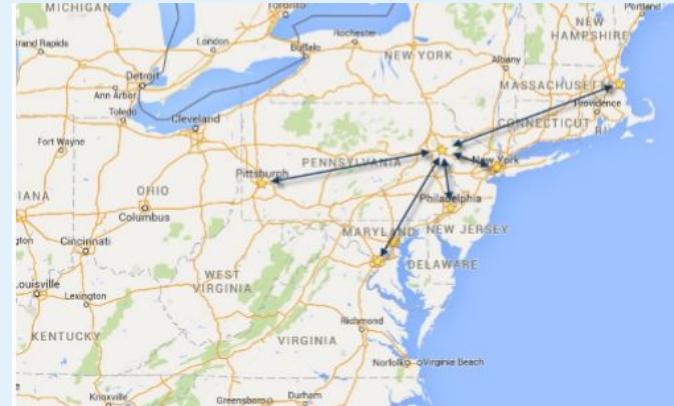


Secure Application Design and Development With Threat Modeling



Joe Kuemerle
joe@kuemerle.com
[@jkuemerle](https://twitter.com/jkuemerle)

- 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/11946169@N00/15198147976>



@jkuemerle@infosec.exchange

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



@jkuemerle@infosec.exchange

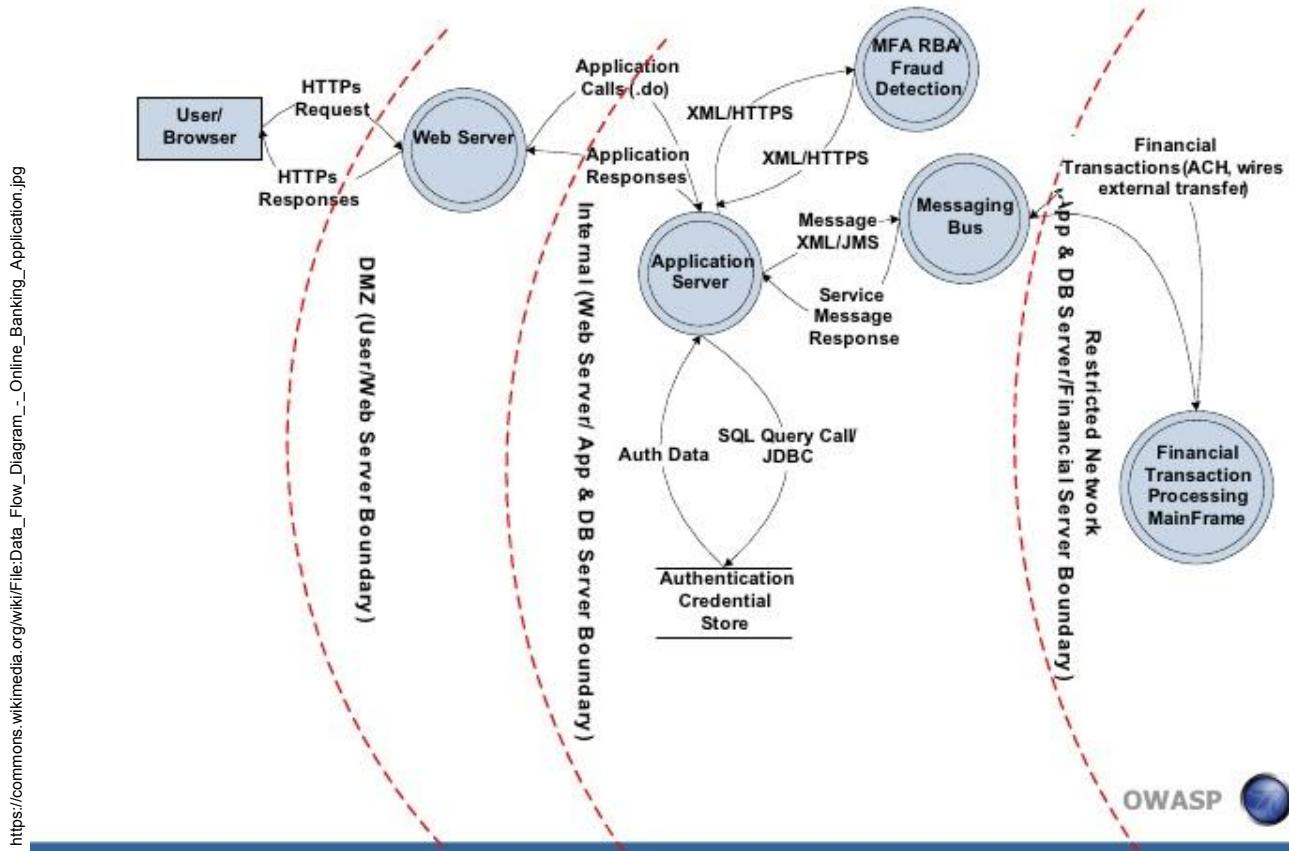


<https://www.flickr.com/photos/45170709@N06/4167655890>

@jkueemerle@infosec.exchange



Data flow diagram-Online Banking Application

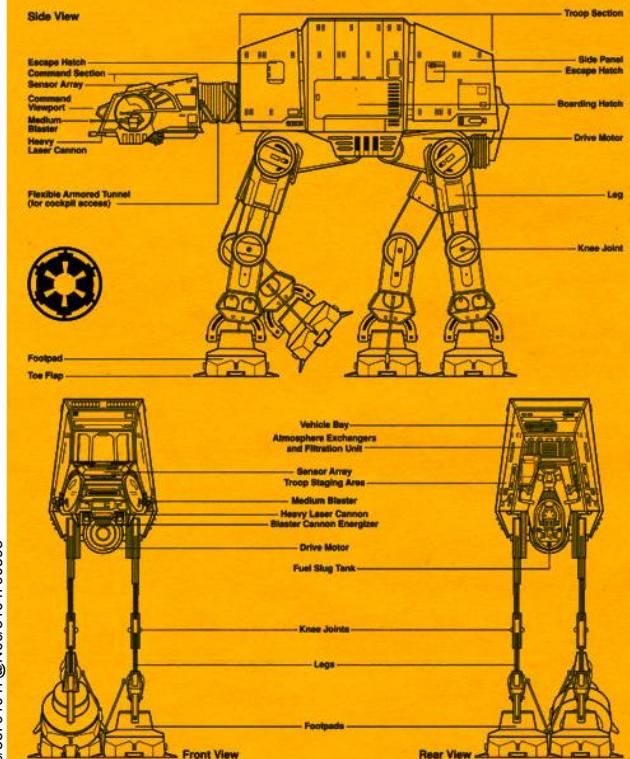




<https://www.flickr.com/photos/49968232@N00/48436759506>

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



AT - AT Walker

Manufacturer: Kuat Drive Yards
Full Name: All Terrain Armored Transport
Length: 20.6 Meters
Height: 15.5 Meters
Maximum Speed: 60 KPH
Engine Units: 2 KDY FW62

Armament:
+ 2 Light Turbolasers
+ Medium Blaster Cannons

WE NEED TO MAKE 500 HOLES IN THAT WALL,
SO I'VE BUILT THIS AUTOMATIC DRILL. IT USES
ELEGANT PRECISION GEARS TO CONTINUALLY
ADJUST ITS TORQUE AND SPEED AS NEEDED.

GREAT, IT'S THE PERFECT WEIGHT!
WE'LL LOAD 500 OF THEM INTO
THE CANNON WE MADE AND
SHOOT THEM AT THE WALL.



HOW SOFTWARE DEVELOPMENT WORKS

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



@jkuemerle@infosec.exchange



INFORMATION

Validations

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

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



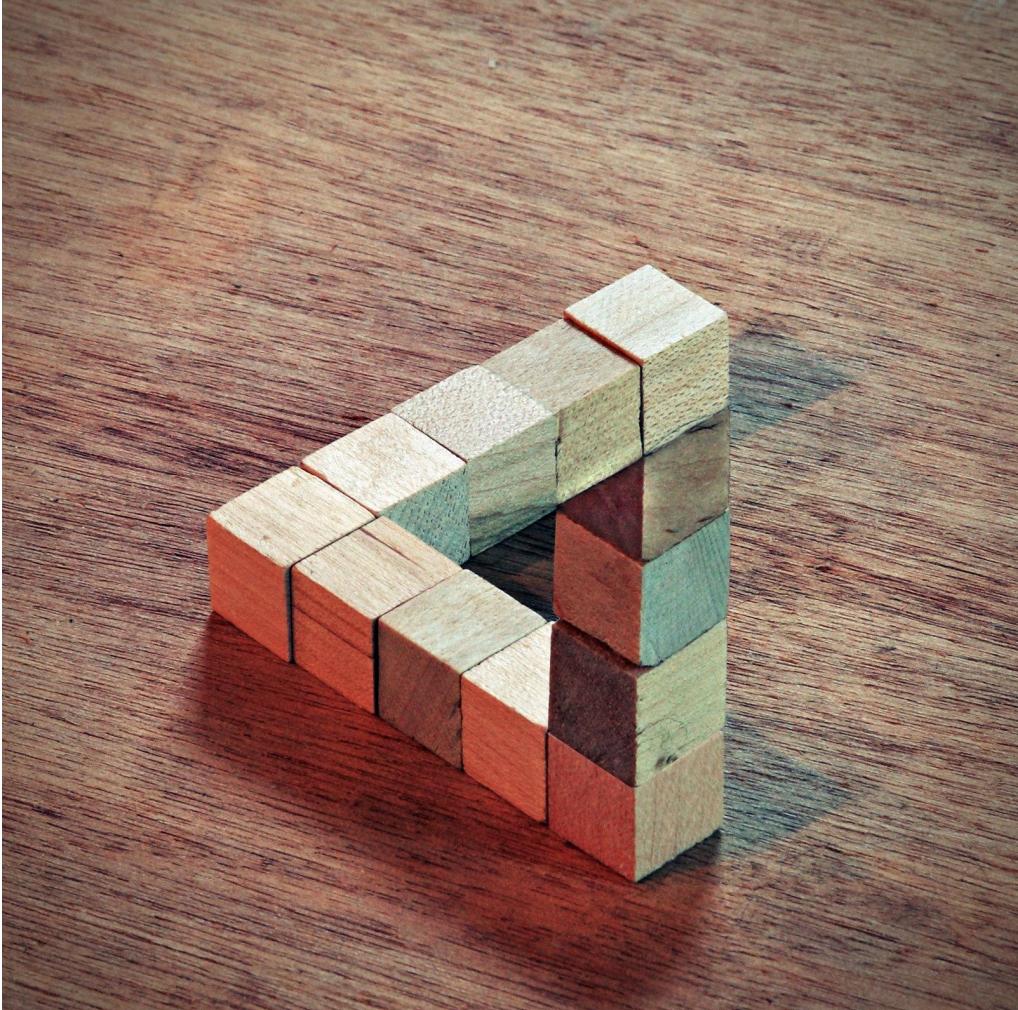
@jkuemerle@infosec.exchange



Confidentiality

Integrity

Availability





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.

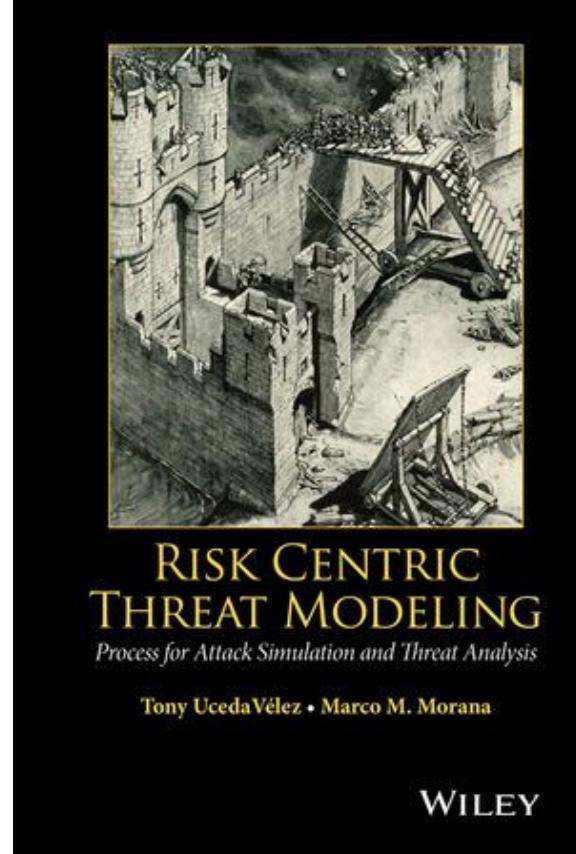
Denial of Service: An adversary uses illegitimate means to exhaust services needed to provide service to users.

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

Process for Attack Simulation and Threat Analysis



<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.

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](#).

The screenshot shows the Trike tool interface with several windows open, illustrating the threat modeling process:

- Top Left Window:** A tree view of threat types:
 - Grid Tree
 - + Actor Creates User Account
 - + Actor Reads User Account
 - OR
 - Actor is in role Admin
 - AND
 - Actor is in role User
 - Actor is in role Admin
 - It is Actor's own User Account
 - + Actor Updates User Account
 - AND
 - OR
 - Actor is in role User
 - Actor is in role Admin
 - It is Actor's own User Account
 - + Actor Deletes User Account
 - + Actor Creates Blog
 - + Actor Reads Blog
 - + Actor Updates Blog
 - + Actor Deletes Blog
 - AND
 - Actor is in role Admin
 - Associated Blog Entries are also deleted
 - Associated User Account is also deleted
 - It is possible to determine later which Admin deleted this Blog
 - It is possible to determine later when this Blog was deleted
 - Admin must select a reason
 - Top Right Window:** A tree view of threat types:
 - Grid Tree
 - + Actor Cannot Delete External Asset according to rules
 - Someone can Read User Account despite rules
 - Cause rules to pass when they shouldn't
 - Change system state such that action is allowed
 - Take an action in the system which changes the conditions a rule depends on
 - Take an intended action which changes a condition
 - Effect another threat which changes a condition
 - Reverse the action immediately after it occurs
 - Subvert the DFD elements for this action
 - Create, read, update or delete data on a data flow
 - Create, update or delete data on a data store
 - Cause a process to perform this action
 - Cause a legitimate actor to perform this action
 - + Someone can Update User Account according to rules
 - Actor cannot Update User Account according to rules
 - Prevent rules for action from passing when they should
 - Change system state such that action is meaningless or prohibited
 - Take an action in the system which changes the conditions a rule depends on
 - Take an intended action which changes a condition
 - Effect another threat which changes a condition
 - Reverse the action immediately after it occurs
 - Disrupt the DFD elements for this action
 - Prevent endpoints of a data flow from creating or reading data
 - Create, update or delete data on a data flow
 - Prevent process from performing its usual function
 - Middle Left Window:** A table view of actors:

| New | Blog | Settings | About | Save | Quit! | Save and Quit! |
|-----------|--------|---|---------|--------|--------|----------------|
| Actors | Assets | Actions | Attacks | Export | Close! | |
| Name | Risk | Notes | | | | |
| Anonymous | 5 | Any user on the Internet. Anonymous people are completely untrusted. | | | | |
| User | 4 | Someone with a Blog. Users are trusted more than Anonymous because they have been approved by an Admin. | | | | |
| Admin | 1 | A specially designated User with power to administer portions of the system. | | | | |
 - Middle Right Window:** A matrix view of threats:

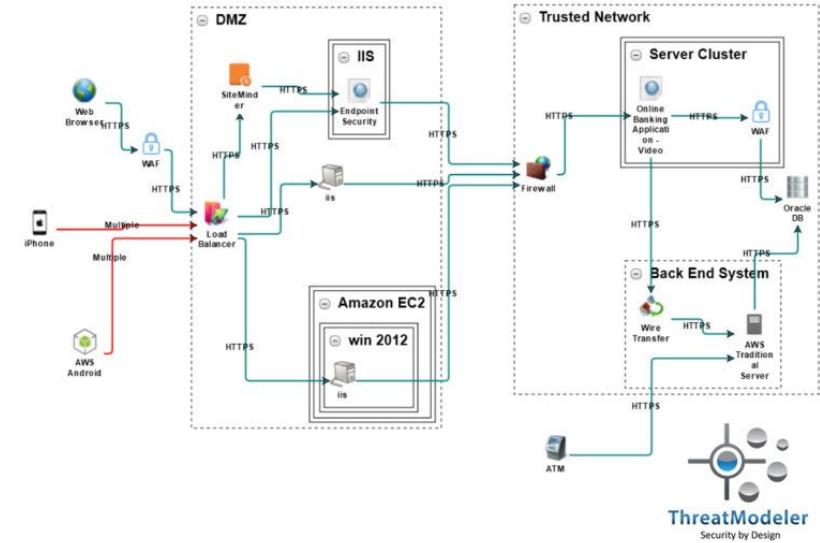
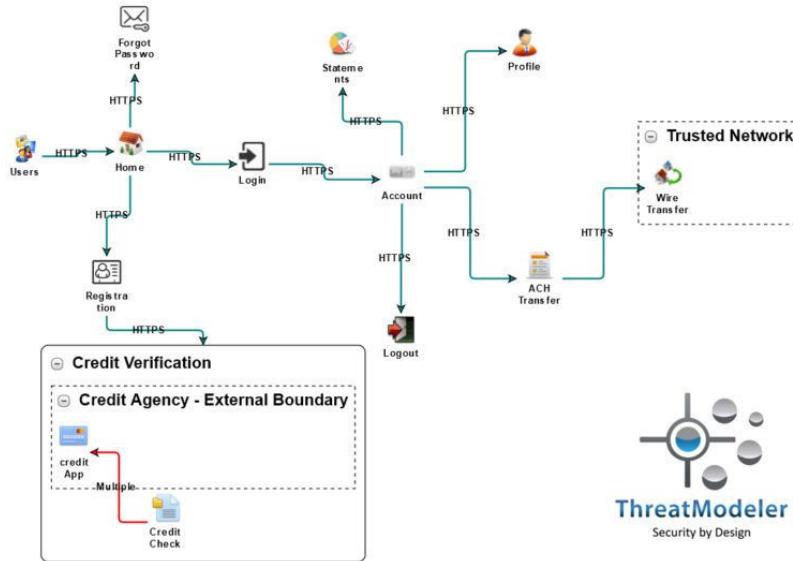
| New | Blog | Settings | About | Save | Quit! | Save and Quit! |
|----------------|--------|----------|------------------------|-------------------|--------|----------------|
| Actors | Assets | Actions | Attacks | Export | Close! | |
| Grid Tree | | | | | | |
| CRUD | Asset | Threat | Elevation of Privilege | Denial of Service | | |
| External Asset | | | | | | |
| User Account | | | | | | |
| Blog | | | | | | |
| Bug Entry | | | | | | |
 - Bottom Left Window:** A matrix view of actors:

| New Actor | | | | | | |
|-----------|----------------|--------------|------|-----------|--|--|
| | External Asset | User Account | Blog | Bug Entry | | |
| Anonymous | | | | | | |
| User | | | | | | |
| Admin | | | | | | |
 - Bottom Right Window:** A matrix view of threats:

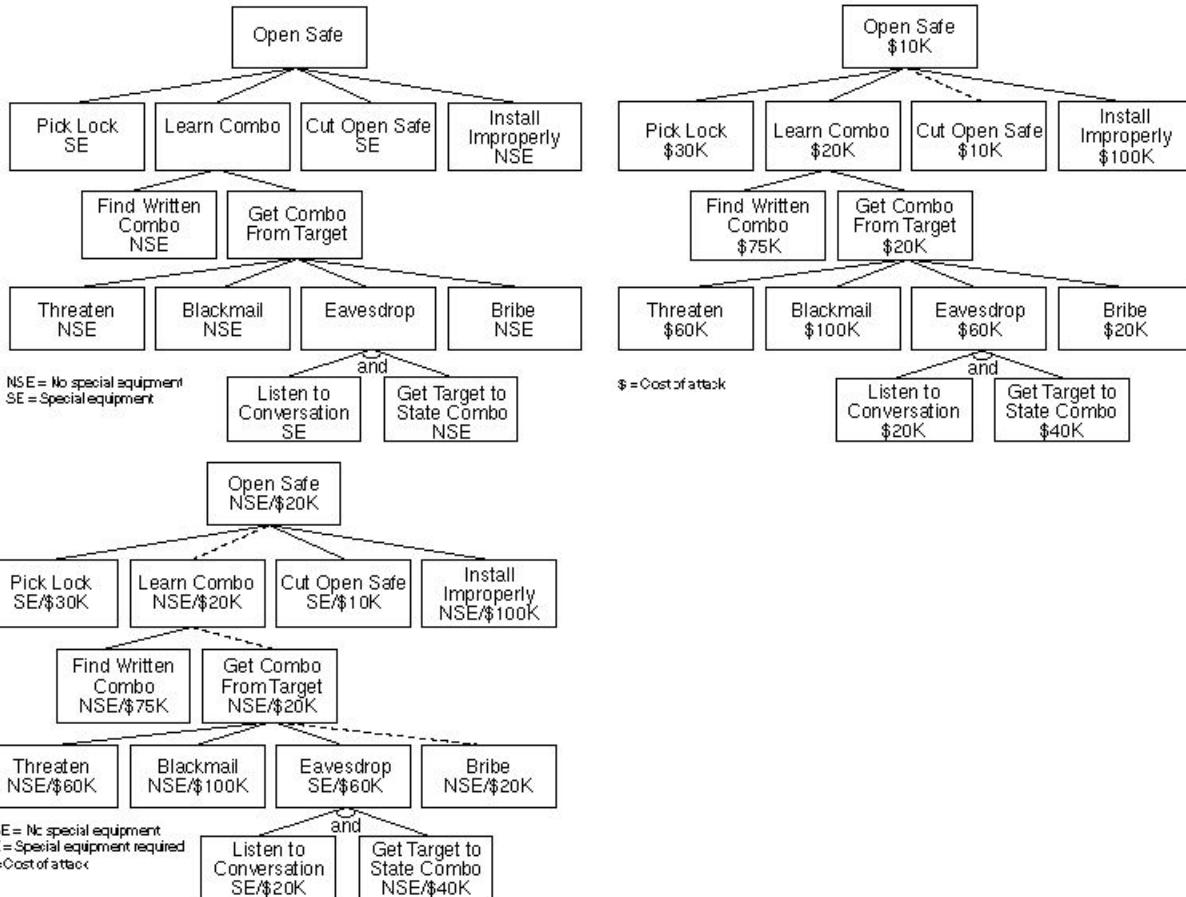
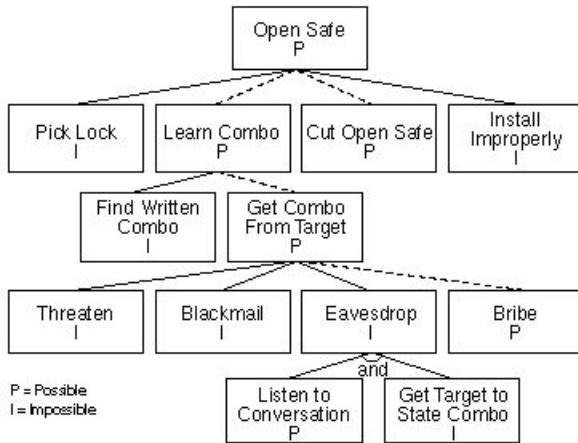
| New | Blog | Settings | About | Save | Quit! | Save and Quit! |
|----------------|--------|----------|------------------------|-------------------|--------|----------------|
| Actors | Assets | Actions | Attacks | Export | Close! | |
| Grid Tree | | | | | | |
| CRUD | Actor | Threat | Elevation of Privilege | Denial of Service | | |
| External Asset | | | | | | |
| User Account | | | | | | |
| Blog | | | | | | |
| Bug Entry | | | | | | |



Visual Agile Simple Threat modeling

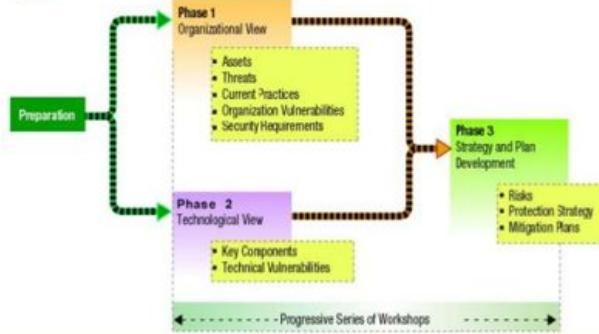


<https://threatmodeler.com/operational-application-threat-modeling>

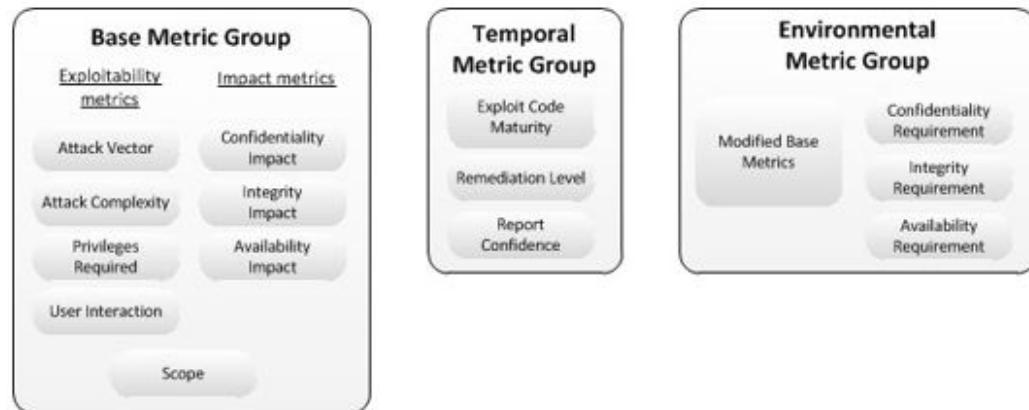


https://www.schneier.com/academic/archives/1999/12/attack_trees.html

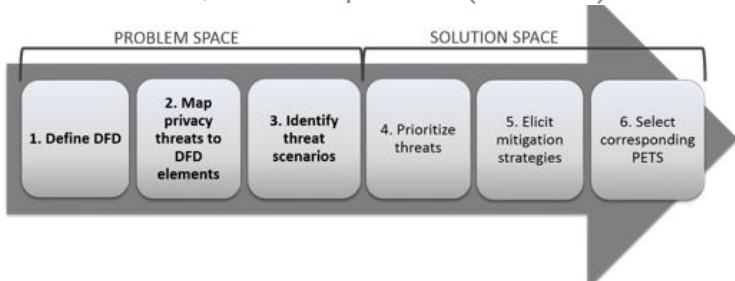
Operationally Critical Threat, Asset and Vulnerability Evaluation



Common Vulnerability Scoring System



linkability, identifiability, nonrepudiation, detectability, disclosure of information, unawareness, noncompliance (**LIDDUN**)



- Hybrid Threat Modeling Method
- Quantitative Threat Modeling Method
- T-MAP

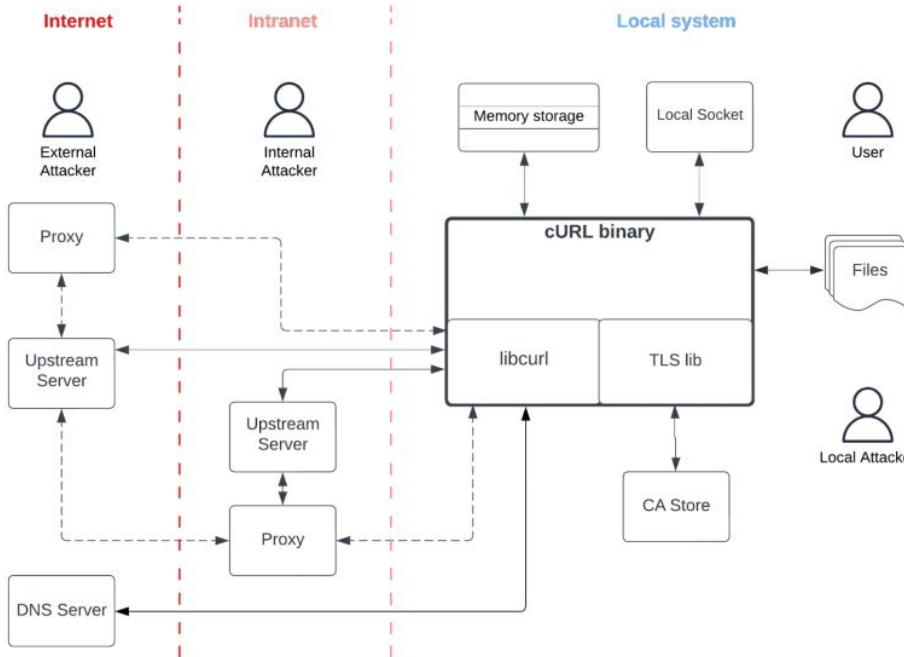
Shostack's 4 Question Frame for Threat Modeling

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?

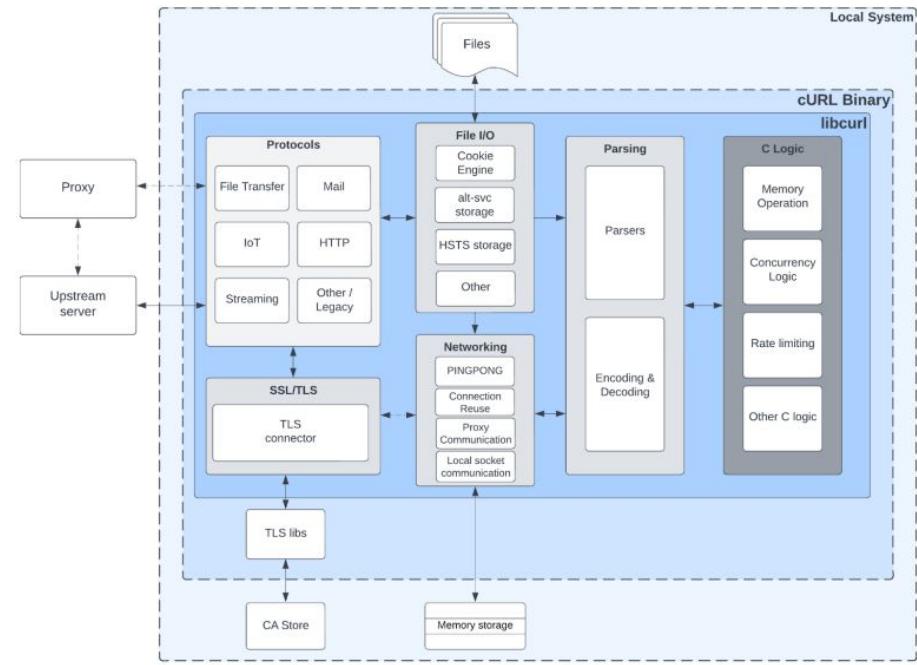
<https://github.com/adamshostack/4QuestionFrame>



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>



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>



@jkuemerle@infosec.exchange

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

**KEEP ON
ILLUSTRATING!**





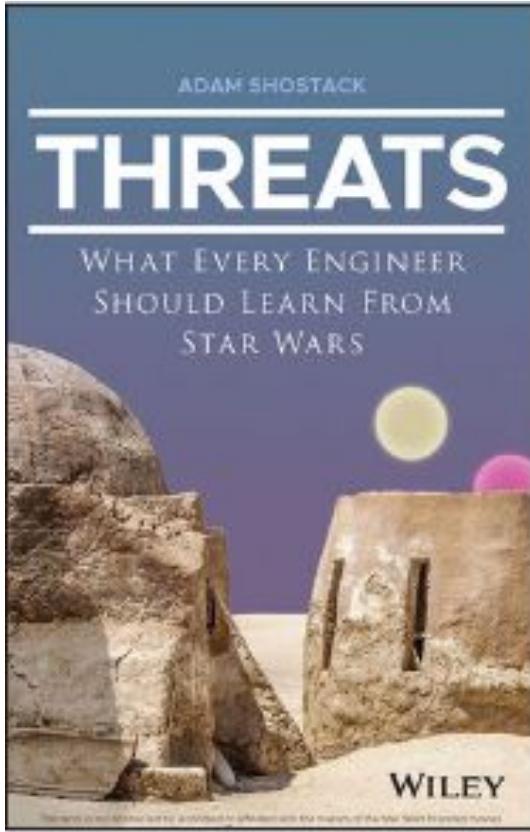
<https://www.flickr.com/photos/38478466@N06/3700355684>

@jkuemerle@infosec.exchange





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



<http://bit.ly/3W4ofx8>

@jkuemerle@infosec.exchange

I HAVE A QUESTION.

WELL, LESS OF A QUESTION
AND MORE OF A COMMENT.

I GUESS IT'S LESS OF A COMMENT
AND MORE OF AN UTTERANCE

REALLY IT'S LESS AN UTTERANCE,
MORE AN AIR PRESSURE WAVE.

IT'S LESS AN AIR PRESSURE WAVE
AND MORE A FRIENDLY HAND WAVE.

I GUESS IT'S LESS A FRIENDLY
WAVE THAN IT IS A FRIENDLY BUG.

I FOUND THIS BUG AND NOW WE'RE
FRIENDS. DO YOU WANT TO MEET IT?



<https://xkcd.com/2191/>

@jkuemerle@infosec.exchange

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/>