

Threat Modelling

An objectives-based primer

Why this talk?

<rant>

Threat modelling isn't a religious ceremony or magical ritual.

Millions of threat modelling talks, few talk about :

- Not how to do threat modelling but *why we do it*
- Not *what activities do we do*, but *what those activities do for us*.

</rant>

This talk tries to address ^. To do this: get a basic understanding of:

- Key terms & concepts
- A general sense of Threat Modelling, Threat Assessments, Threat Assessments in Risk Management

Who am I?

In this capacity: Co-Lead of OWASP Toronto Chapter

Day Job: Director of Advisory at Security Compass

Both: Security brain for hire with speciality in appsec interpretive dance.

Find me at opheliar.chan@owasp.org or <https://www.linkedin.com/in/opheliar-chan/>

Disclaimer: I express my own views and don't represent anyone else in speaking.

My company is nice enough to let me speak without a gag order, and I'd like to keep it that way. Blame goes to me, Praise to people and companies who influence/allow me to interact with community members like you! Also: none of these attributions are necessarily recommendations.

A scene from the movie Toy Story featuring Woody and Buzz Lightyear. Woody, on the left, is a cowboy with brown hair, wearing a yellow and black plaid shirt over a red bandana and blue jeans. He has a concerned expression. Buzz Lightyear, on the right, is in his iconic green and white space suit with purple accents. He is holding Woody's shoulder with his right hand, which is raised in a 'V' for victory sign. Buzz has a confident, slightly mischievous smile. The background is a simple indoor setting with a white door and a blue wall. The text 'HACKERS!' is overlaid in large, white, bold, sans-serif font with a black outline at the top. The text 'HACKERS EVERYWHERE!' is overlaid in the same font at the bottom.

HACKERS!

HACKERS EVERYWHERE!

**Infosec is about evaluating and managing information
system risk to a business or entity**

“

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

”

- Sun Tzu

The Art of War

<http://classics.mit.edu/Tzu/artwar.html>

“

If you know the enemy and know yourself, you
need not fear the result of a hundred battles.

- Sun Tzu ”
The Art of War
<http://classics.mit.edu/Tzu/artwar.html>

Class ThreatModelling extends SystemModelling {}

Class SystemModelling extends ScientificModelling{}

```
/**create an abstraction of the world or system via  
* conceptual models for understanding  
* operational models to simulate and test operations  
* graphical models to visualize the subject  
* mathematical models to quantify  
*/
```


Risk Aggregation

Aggregate related risk into a single/small superset of risk(s) meant to:

- Contextualize risk at higher level of scope to support decision making at that level
- Group tightly related risks for handling as a unit
- Allow for higher organizational tiers to effectively monitor groups of related risks relative to an objective/baseline

Risk aggregation examples



The Aggregation of Threat Modelling information is where we got:

- Baseline security controls and configurations
- Patch and vulnerability management practices
- Start of security frameworks (e.g. authentication/authorization -> SSO)
- Invention of perimeter defense (e.g. firewalls) and host-defense (e.g. anti-virus)
- “Best practices” and much more...

TL;DR

Early Computing



PRACTICAL JOKES

It's all fun and games until Grandpa has a heart attack while eating his salad.

VERY DEMOTIVATIONAL.com

Early Internet



#316372732

Today



Infosec

#403081330

+

YOU

Act 3: Trying to resolve the Big Problem...

Threat Modelling and You

Security Champions

SME's - not just infosec

MILITARY SERVICE ACT, 1916

Every man to whom the Act applies will on Thursday, March 2nd, be deemed to have enlisted for the period of the War unless he is excepted or exempt.

Any man who has adequate grounds for applying to a Local Tribunal for a

CERTIFICATE OF EXEMPTION

UNDER THIS ACT

Must do so BEFORE

THURSDAY, MARCH 2

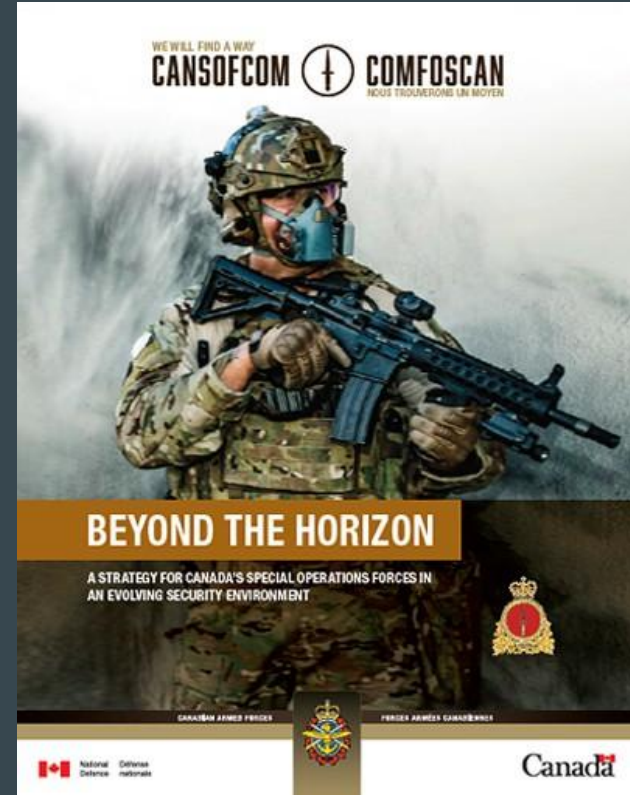
Why wait for the Act to apply to you?

Come now and join of your own free will.

You can at once put your claim before a Local Tribunal for exemption from being called up for Military Service if you wish.

ATTEST NOW

Published by the PARLIAMENTARY AND JOINT LAYERS RESERVING COMMITTEE, LONDON. POSTER No. 150. W. W. 17107701.



Scale Threat Modelling?



Uh... no?

Continuous Improvement



Photo via 5th Canadian Division - DND Canada

How to Reduce Risk in a System

Direct Means

- Implement the mitigations, fix the vulnerabilities

Indirect Means

- Have good security hygiene and baselines
- Change the design (threat landscape)
- Education
 - Learn from your mistakes
 - Challenge/Verify your assumptions
- Make recovery/continuity/response plans

Changing the Threat Landscape

Before



<https://www.reviewjournal.com/local/local-las-vegas/wisconsin-man-wins-1-23m-jackpot-at-downtown-las-vegas-casino/>

After



Clark County Nevada

@ClarkCountyNV



The newest pedestrian bridge over the Las #Vegas Strip will open on Monday morning. Construction on the bridge between @parkmgm, @TMobileArena and Showcase Mall has taken 14 months. This is the 17th pedestrian bridge on #LasVegas Blvd.



5:17 PM · Dec 20, 2019



182



42



Copy link to Tweet

Outputs to Reduce Risk in a System (and keep it gone)

Outputs

- Improved Security Baselines
- Design and architecture changes
- Educational material
- Experimental models and plans
- Process changes/updates/creation
- Response plans
- New defenses & tests

Indirect Means

- Have good security hygiene and baselines
- Change the design (threat landscape)
- Education
 - Learn from your mistakes
 - Challenge/Verify your assumptions
- Make recovery/continuity/response plans

Where should your experts be spending their time?

The important things to focus experts on (in threat modelling & elsewhere):

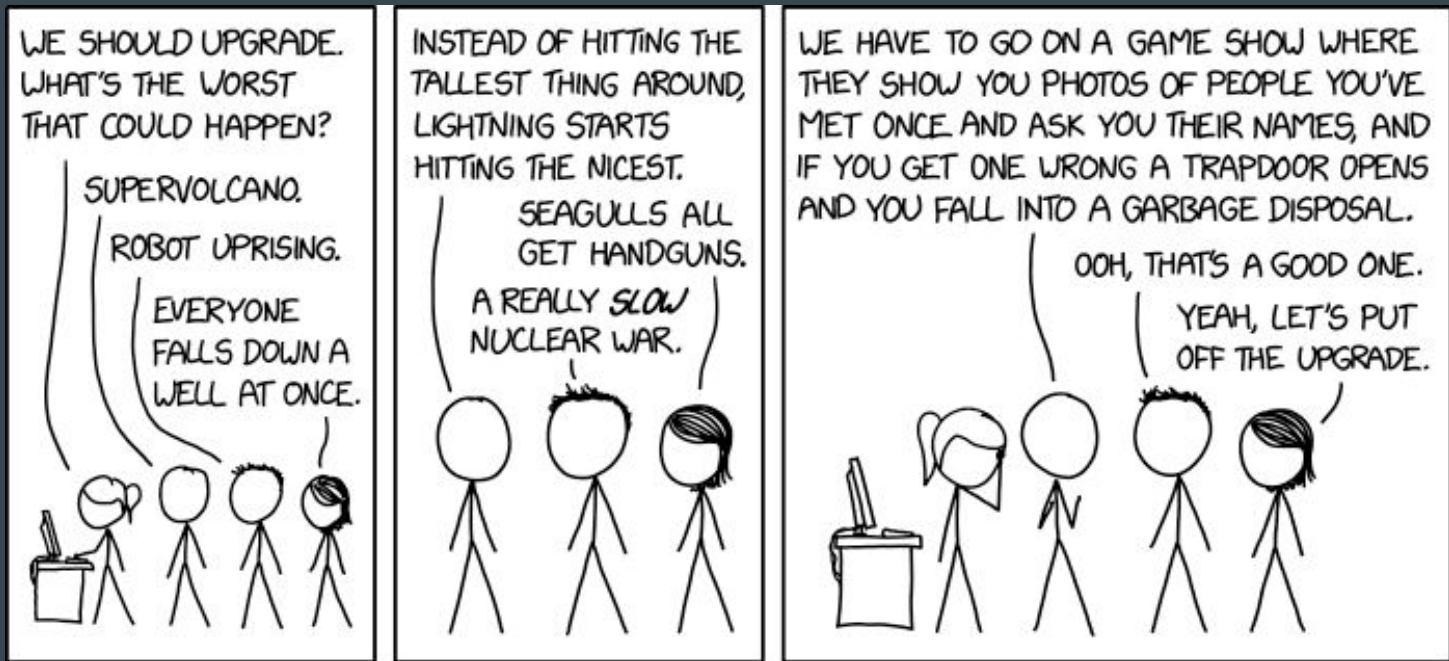
- Design decisions
- Access control (trust zones)
- Data security (dfd's)
- Incident response
- Determining what '(ab)normal behaviour' looks like for behavioural analysis
- Control baseline adequacy & improvement

The rest, use vuln scanning tooling, other devsecops process, education, and procedure to get baseline security/ops controls handled, vulns managed as a separate issue. Focus on the stuff that NEEDS SMEs

Threat Modelling

Basic Concepts

Master-Class Style



Please Participate!

**“Risk of physical harm/injury if I get
hit by a vehicle while crossing the
street.”**

Grammatical Analysis of Risk Statements

Subject(s)

The person, place, or thing that is performing the action

“Risk of physical harm/injury
if I get hit by a vehicle while
crossing the street.”

Grammatical Analysis of Risk Statements

Subject(s)

The person, place, or thing that is performing the action

Predicate(s)

The action or being

“Risk of physical harm/injury
if I get hit by a vehicle while
crossing the street.”

Grammatical Analysis of Risk Statements

Subject(s)

The person, place, or thing that is performing the action

Predicate(s)

The action or being

Direct/Indirect Object(s)

The recipient of the action or the being the action is being done for/to.

**“Risk of physical harm/injury
if I get hit by a vehicle while
crossing the street.”**

Basics of a Threat

Subject(s)

The person, place, or thing that is performing the action

Predicate(s)

The action or being

Direct/Indirect Object(s)

The recipient of the action or the being the action is being done for/to.

Threat Actor

An individual, group, or phenomenon posing a threat, usually with some motivation to act.

Threat Event

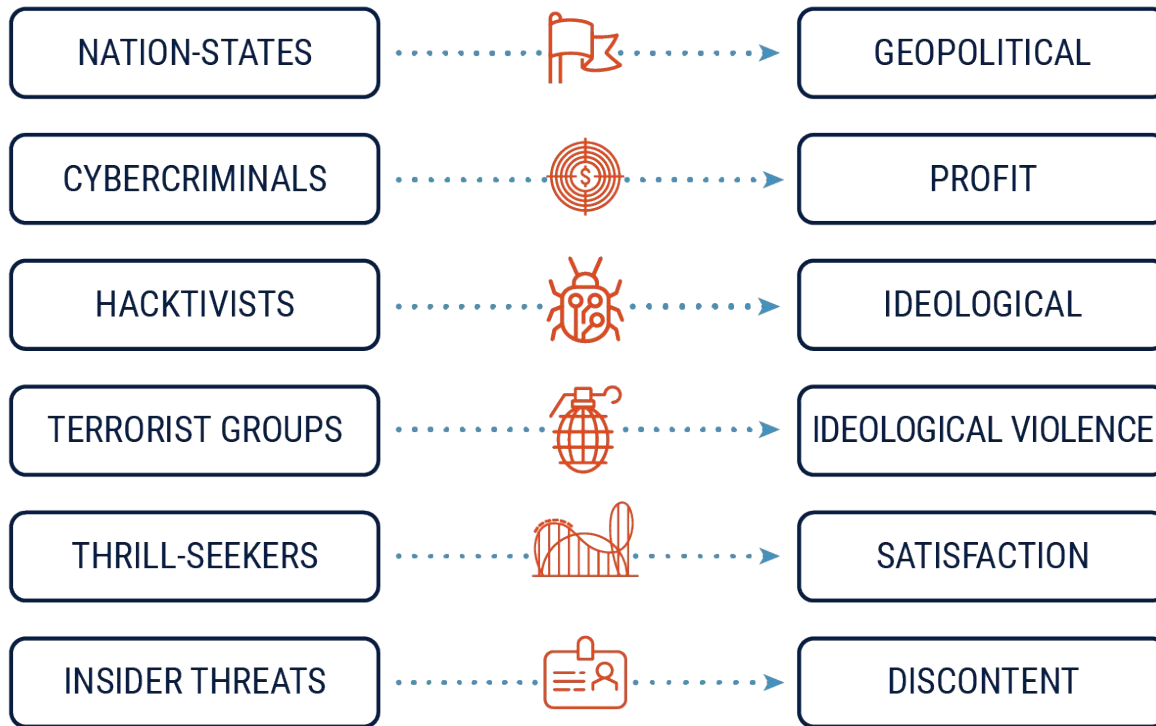
Something happening at a point in time that has the potential to cause an unauthorized/unexpected result.

Asset(s)

Anything that contributes to a business function and therefore has value.

CYBER THREAT ACTOR

MOTIVATION



Threat Event Types



Accidents



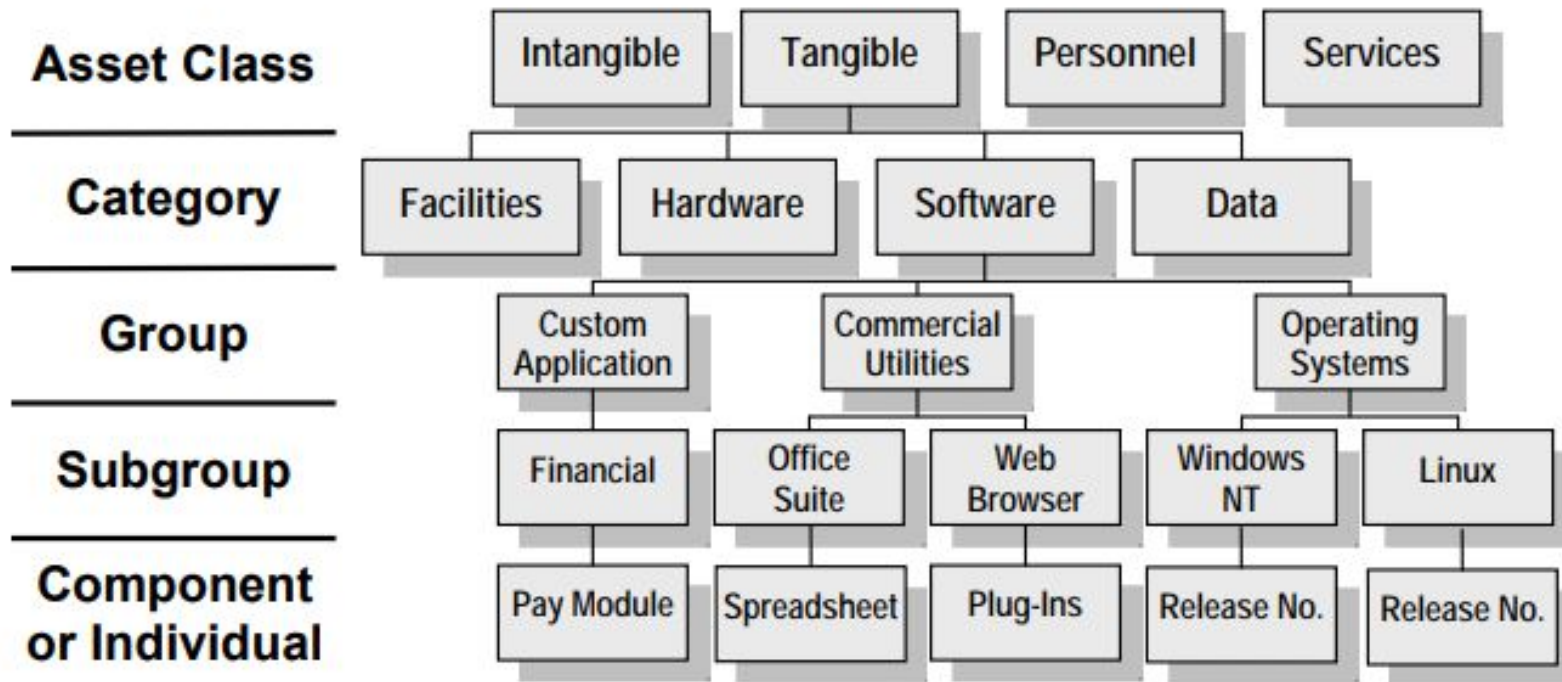
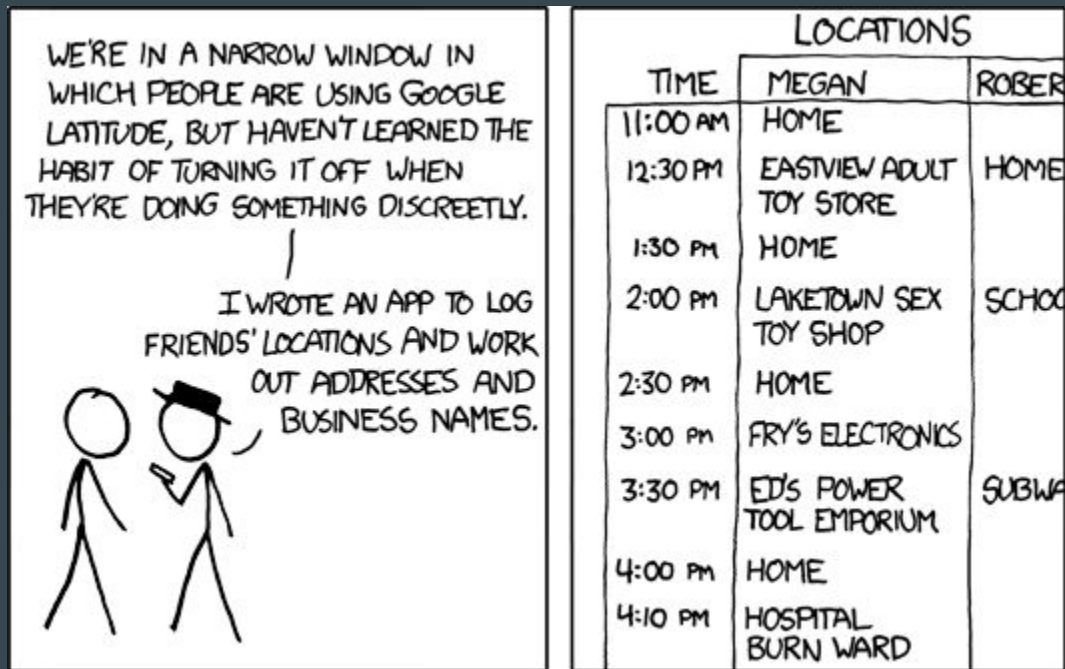


Figure B-2: Sample Segment of the Asset Listing Hierarchical Structure

Privacy (asset) & the law of unintended consequences



Statement

“Risk of physical harm/injury if I get hit by a vehicle while crossing the street.”

Threat

- **Threat Actor:** driver of car (implied)
- **Threat Event:** hit by car
- **Asset:** whoever “I” is.

**You've just done the brainstorming/enumerating threats
part of an informal threat modelling process.**

(Oh, and received informal training.)

What turns a Threat into a Risk?

“Risk of physical harm/injury if I get hit by a vehicle while crossing the street”

- **Threat Actor:** driver of car (implied)
- **Threat Event:** hit by car
- **Asset:** whoever “I” is. Your life, specifically.
- ?

What turns a Threat into a Risk?

“Risk of death if I get hit by a vehicle while crossing the street”

“Risk of losing a leg if I get hit by a vehicle while crossing the street”

Risk Characteristics

- **Impact:** Why do I care?
- **Likelihood:** How often, what recurrence, % chance of success

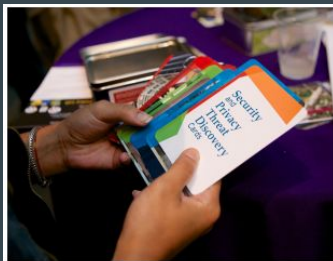
given a threat event, prevalence of weaknesses/opportunities, attacker motivation & skill, etc

Threat Modelling

The How

Can be

“Threat Modelling ~~is~~ a 7 step process that has these 6 diagrams and this mnemonic and this rating sheet”



securitycards.cs.washington.edu



OWASP Cornucopia



Microsoft Elevation of Privilege



Owasp Snakes & Ladders



Control+ALT Hack

training and tools you could start threat modelling with

Mnemonics

Possible impacts

- STRIDE <- Microsoft
- CIA
- BIA results

Rating & Prioritization

- CARVER + Shock - US Army Special Forces, FDA
- DREAD - Microsoft
- CVSS - FIRST

Lists of:

- Vulnerabilities
- Threats & threat actors
- Assets
- Tactics, Techniques, Procedures
- Defenses
- Common Controls

Ask not *what activities do we do*,
but *what do those activities do for*
us?

Threat Modelling

Ask four key questions:

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good (enough) job?

Key Activities:

- Describe System
- Enumerate Threats
- Decide if threats are relevant/important
- Find the best mitigation strategies/countermeasures for the important threats
- Define 'good (enough)'
- Compare job to 'good (enough)'

**Describe System to communicate and come to
a common, unambiguous understanding**

To who?



Describe System to **communicate** and come to
a common, unambiguous understanding

Describe System to communicate and come to
a **common, unambiguous understanding**



Of what? At what level of detail?
For what reason?

By building models



Describe System to communicate and come to
a common, unambiguous understanding

Class ThreatModelling extends SystemModelling {}

Class SystemModelling extends ScientificModelling{}

```
/**create an abstraction of the world or system via  
* conceptual models for understanding  
* operational models to simulate and test operations  
* graphical models to visualize the subject  
* mathematical models to quantify  
*/
```

Diagrams



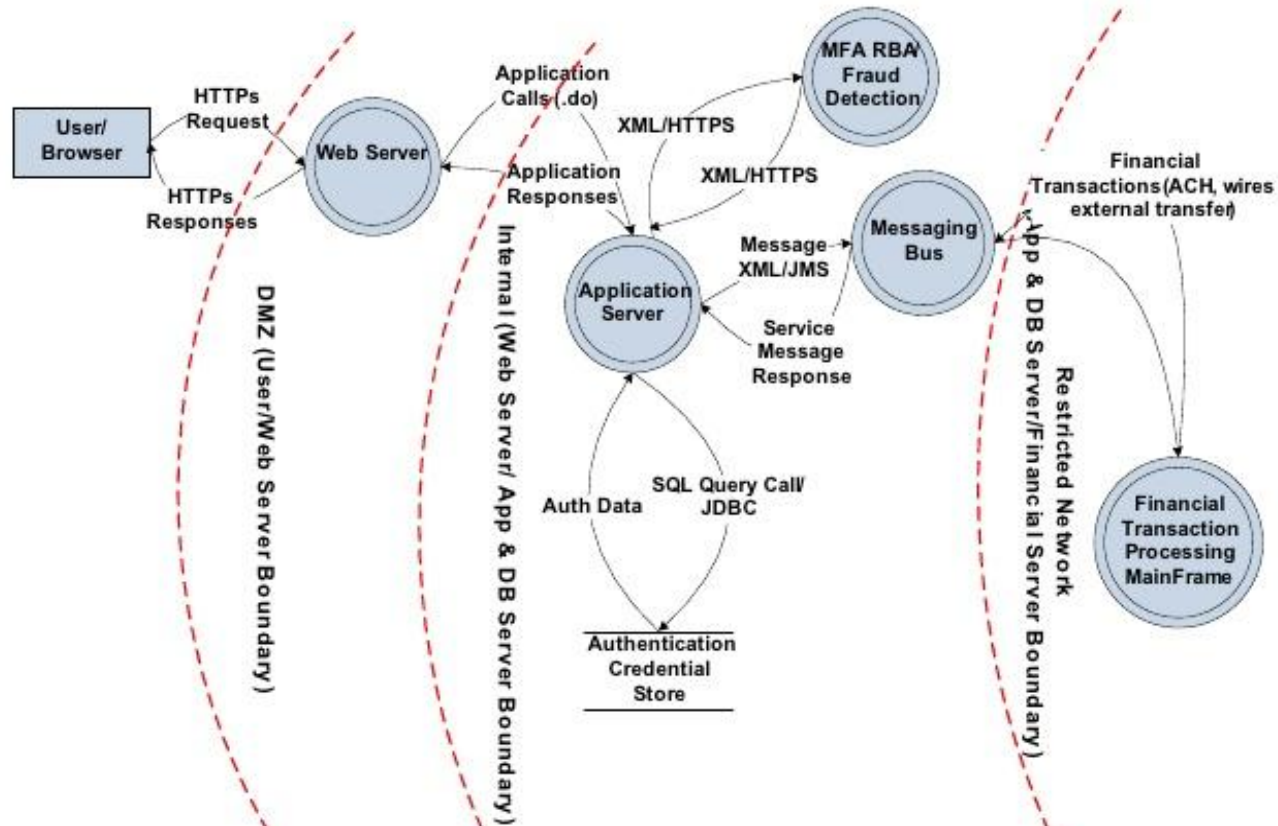
Typical Conceptual and Graphical Models

Diagrams & related docs, in practice

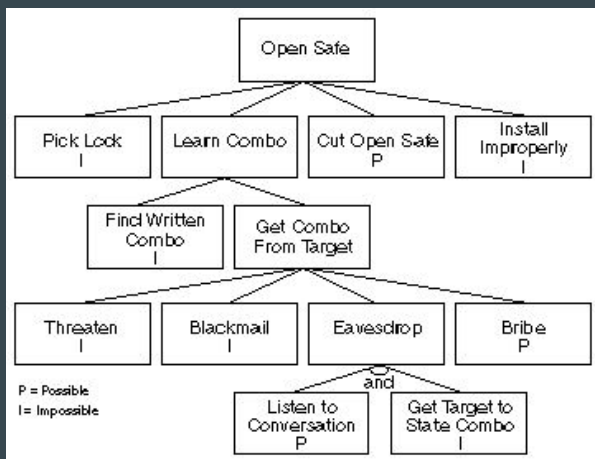
(Tech: architecture diagrams, design docs, activity/sequence diagrams, wireframes, db schemas, interface definition files, etc)

(Security: data flow, attack/threat/rule trees, abuse cases, etc)

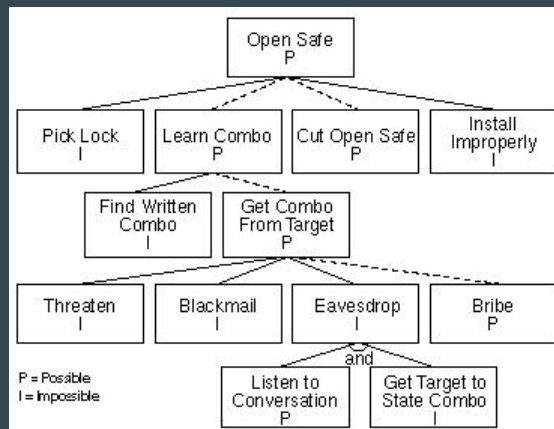
Data flow diagram-Online Banking Application



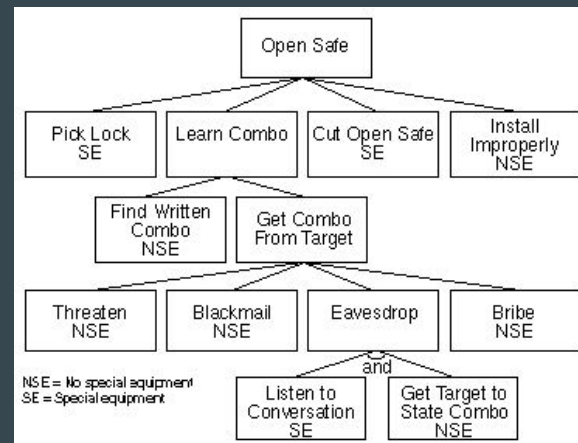
Attack Trees



Attack Nodes

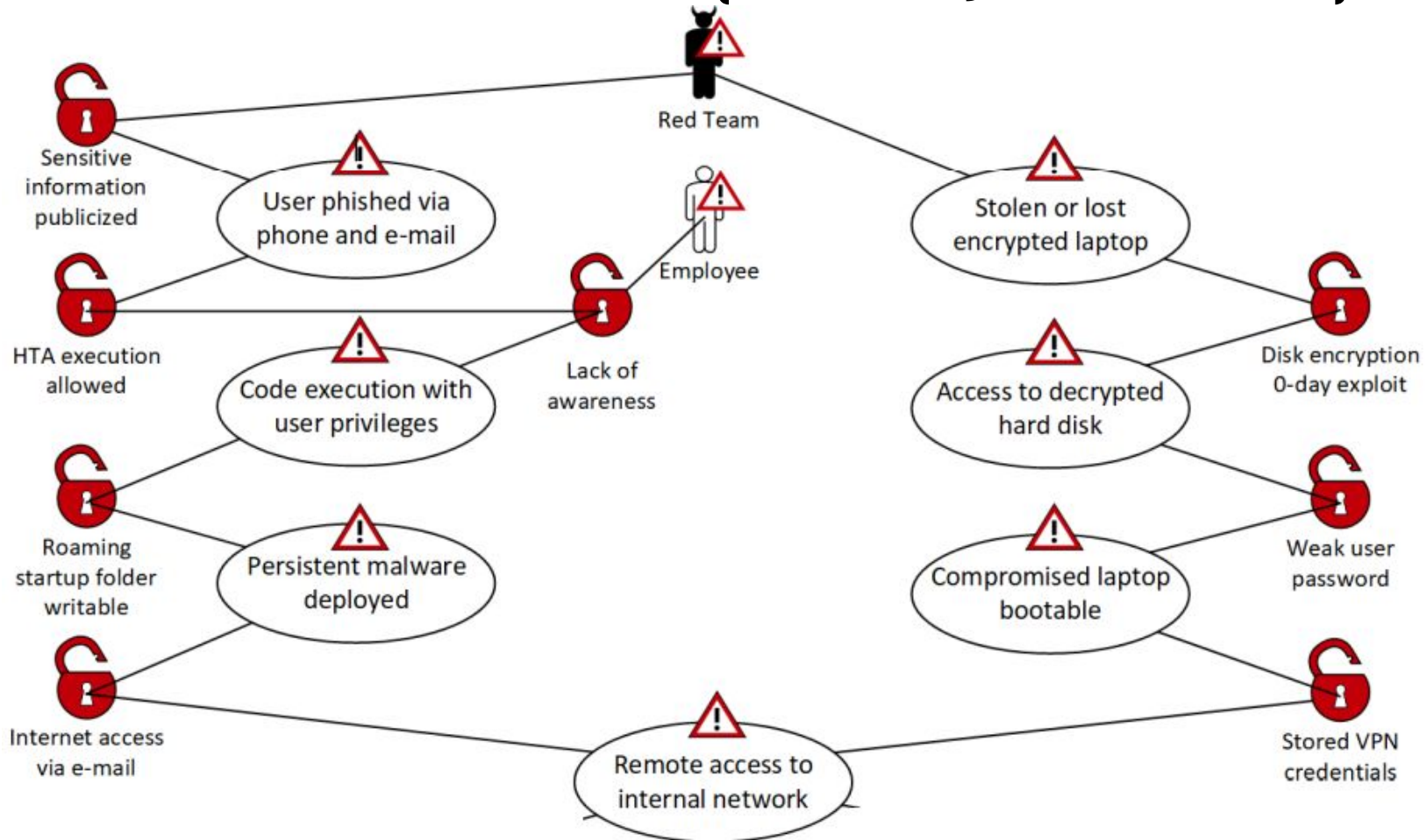


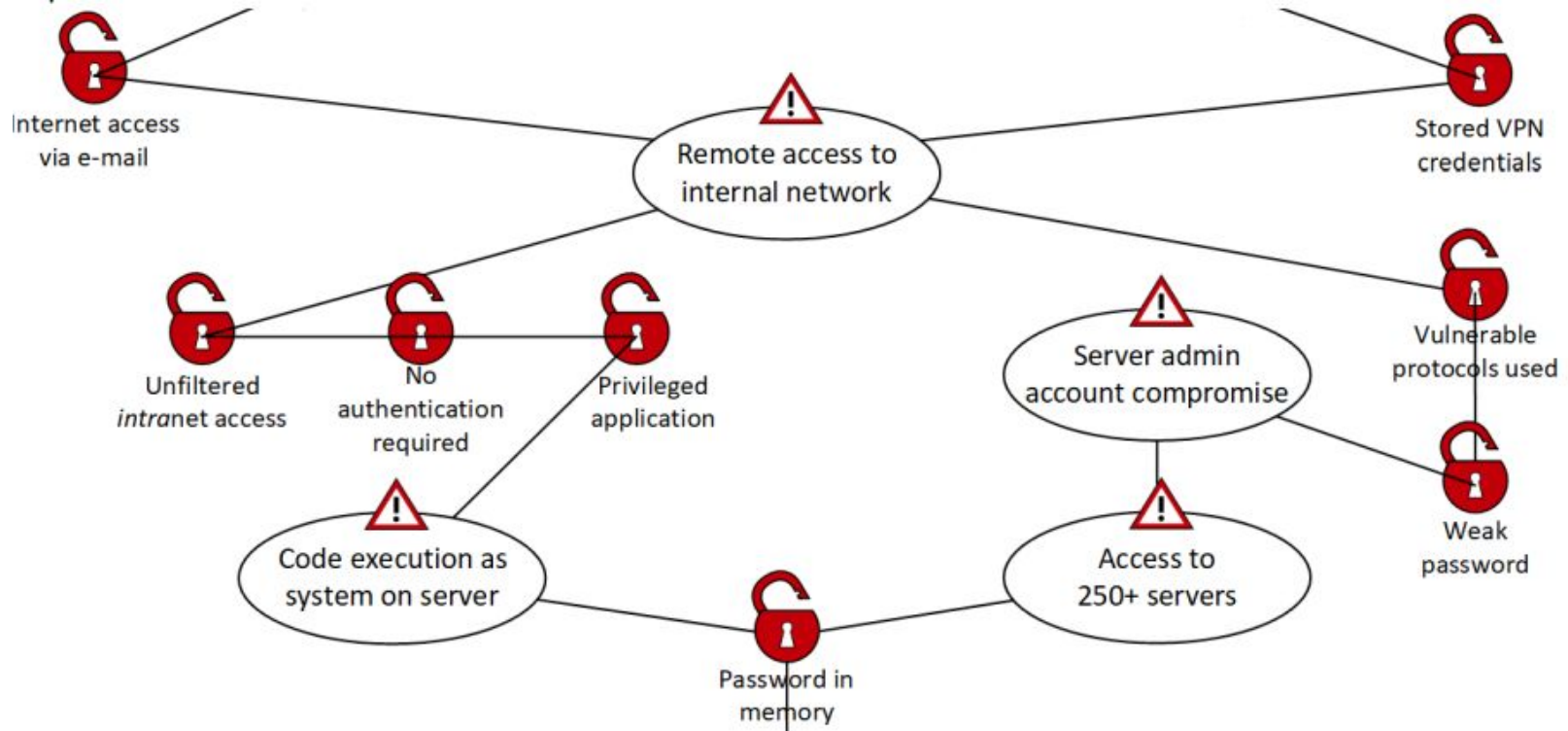
Possible Attacks



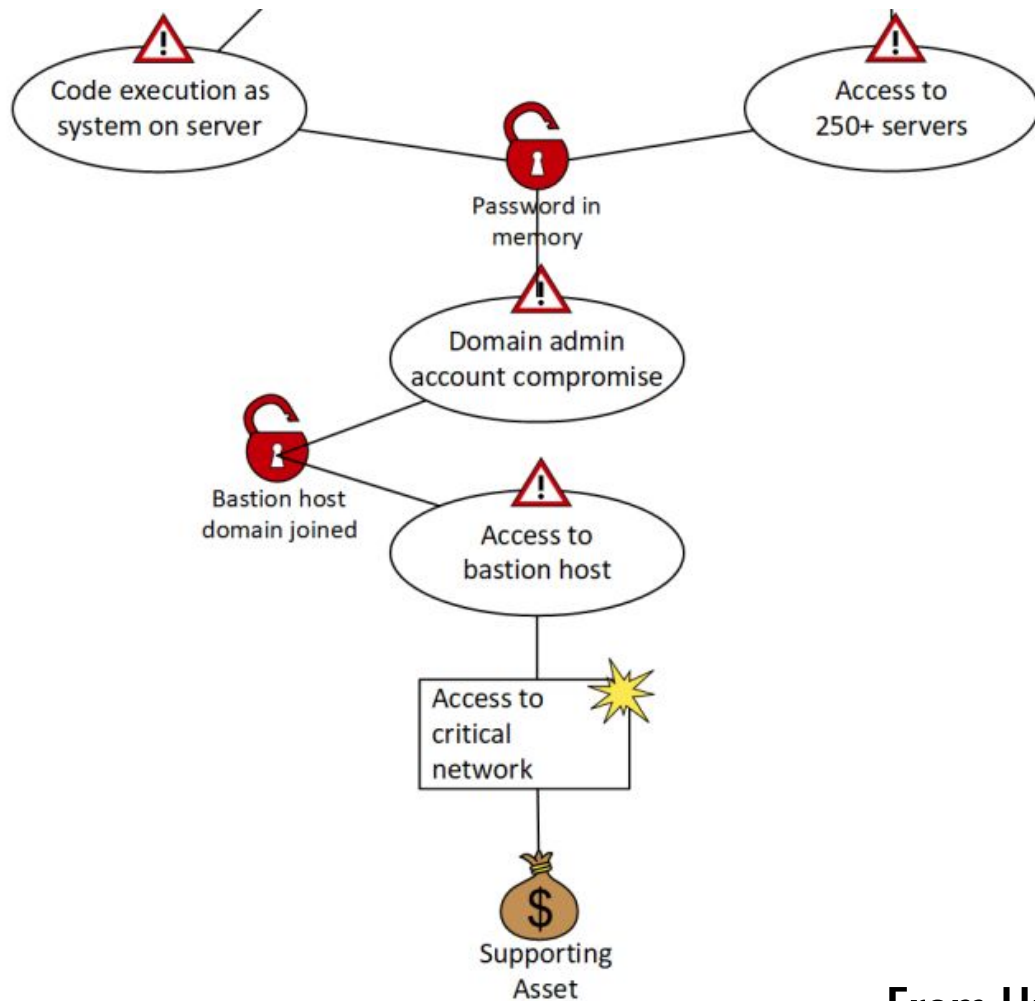
Special Equipment Required

Attack Visualizations (Unified Cyber Kill Chain)





From Unified Cyber Kill Chain



From Unified Cyber Kill Chain

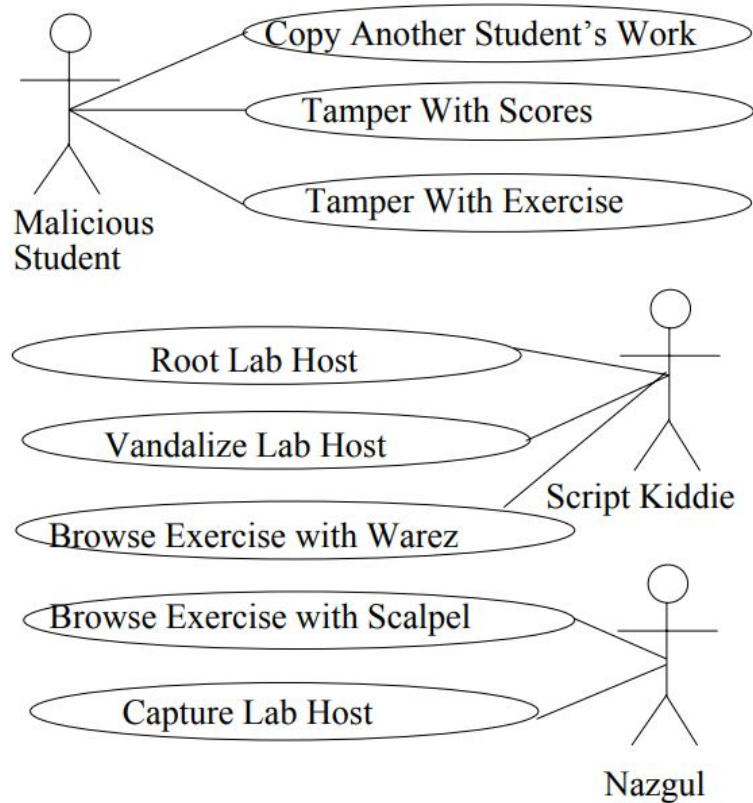


Figure 3. Abuse Case Diagram for an Internet-Based Information Security Laboratory

Browse Server Exercises With Warez

Harm: The users of the lab will be legally, ethically, and morally responsible for increasing the abilities of the Script Kiddie. The users may also be responsible for allowing information about previously unknown exploits to be released.

Privilege Range: The Script Kiddie might carry out this abuse using privileges in the following range:


1. Installation of modified system utilities with root/administrator privileges on a source or target host
2. One-time control of a root/administrator account on a source or target host
3. One-time control of a root/administrator session on a source or target host
4. Installation of modified utilities with user privileges on a source or target host
5. One-time control of a single instructor session on a server host
6. One-time control of a single student session on a server host

Abusive Interaction: Using the TCP/IP protocol suite and a hypothetical attack tool called Warez 1, the Script Kiddie requests or attempts to initiate a session on some lab host. The initial session could be on a...

Class ThreatModelling extends SystemModelling {}

Class SystemModelling extends ScientificModelling{}

```
/**create an abstraction of the world or system via  
* conceptual models for understanding  
* operational models to simulate and test operations  
* graphical models to visualize the subject  
* mathematical models to quantify  
*/
```


- 
- Chaos engineering
 - Resiliency
 - Machine Learning/Formal Systems

“Chaos Engineering is the discipline of experimenting on a distributed system in order to build confidence in the system’s capability to withstand **turbulent conditions** in production.”

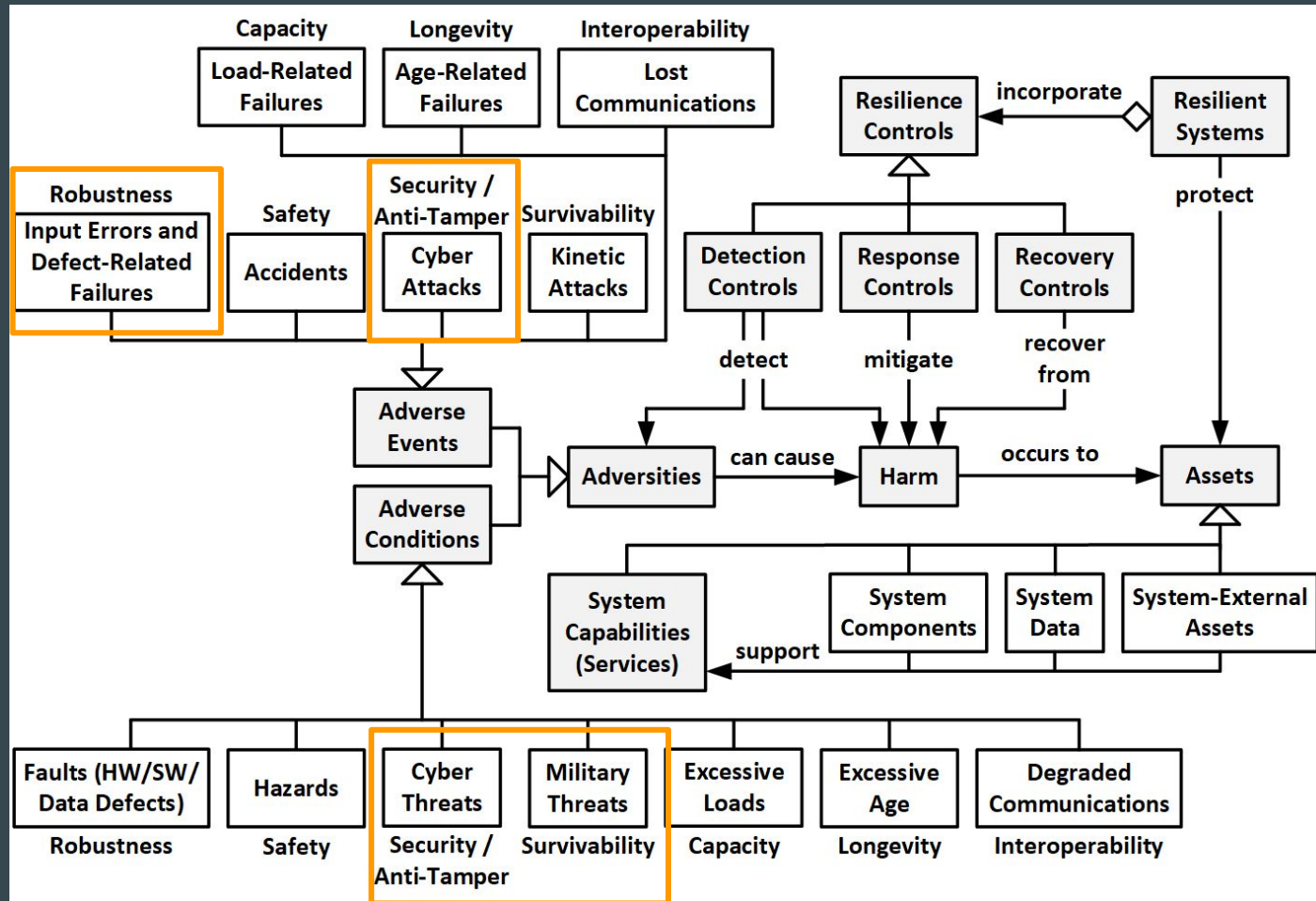
Attacks? Accidents? => Threats?

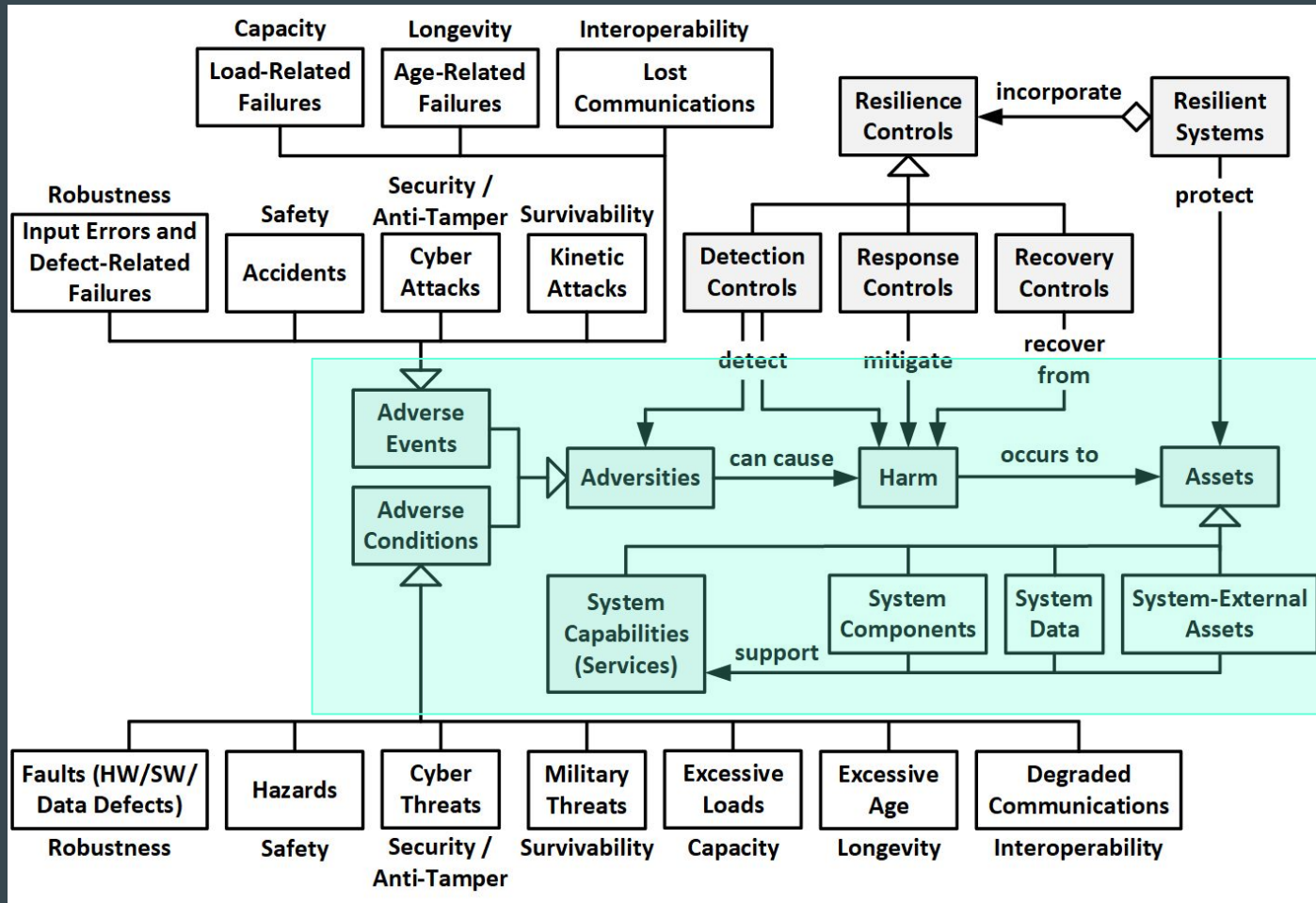
<https://www.oreilly.com/content/chaos-engineering/>

“The system is resilient if it continues to carry out its mission in the face of **adversity**.”

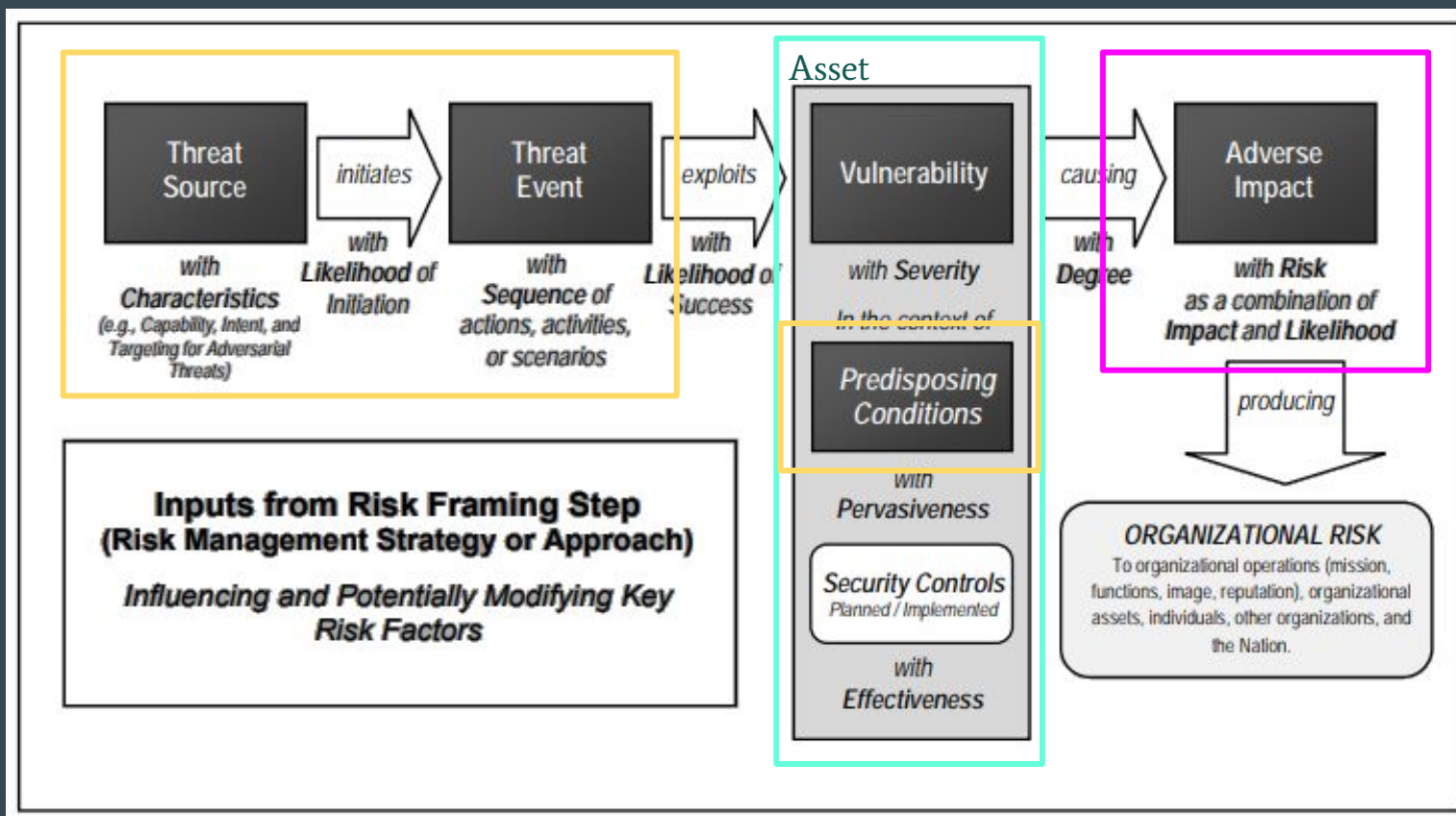


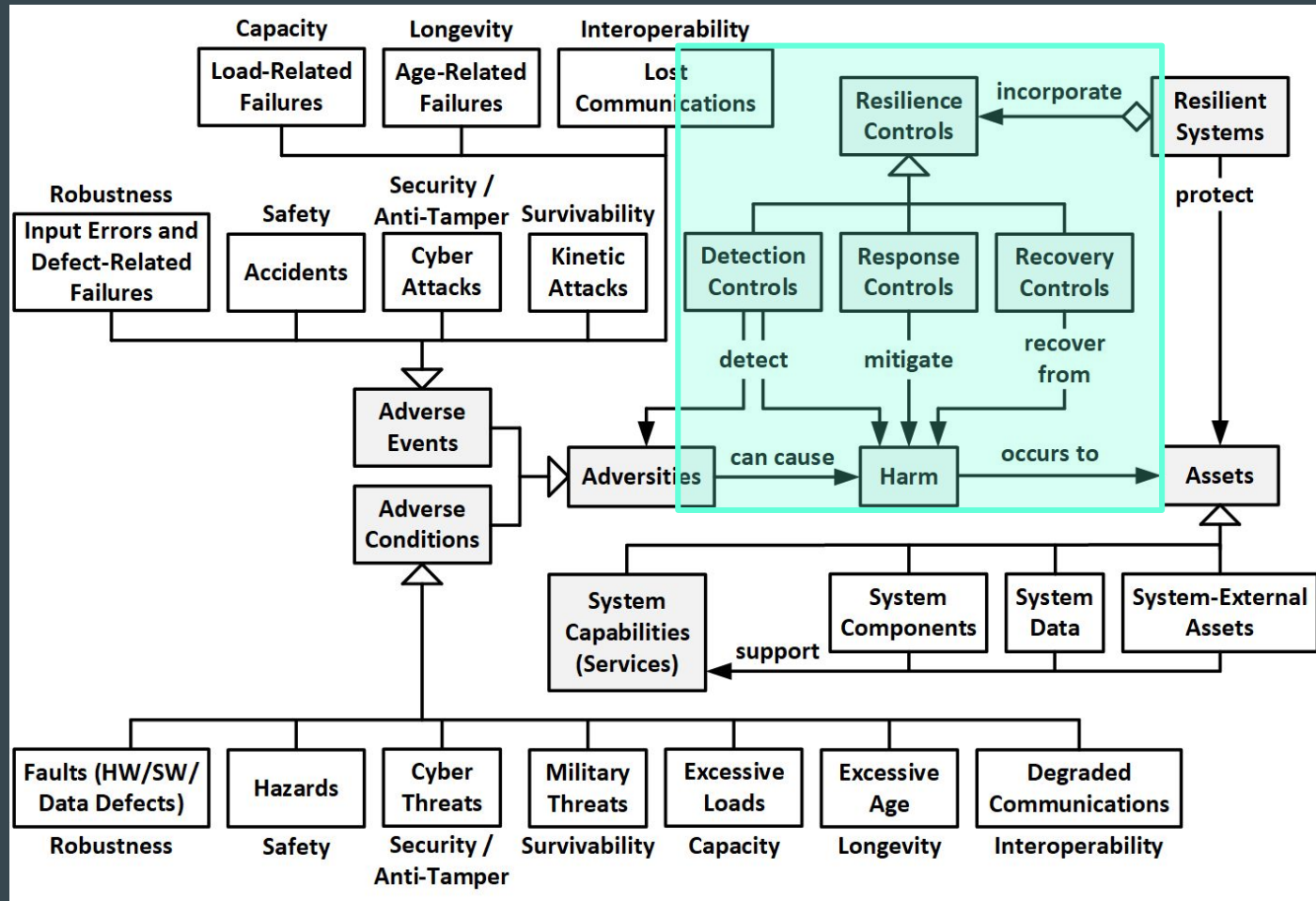
Attacks? Accidents? Abuse? => Threats?





NIST Risk Model





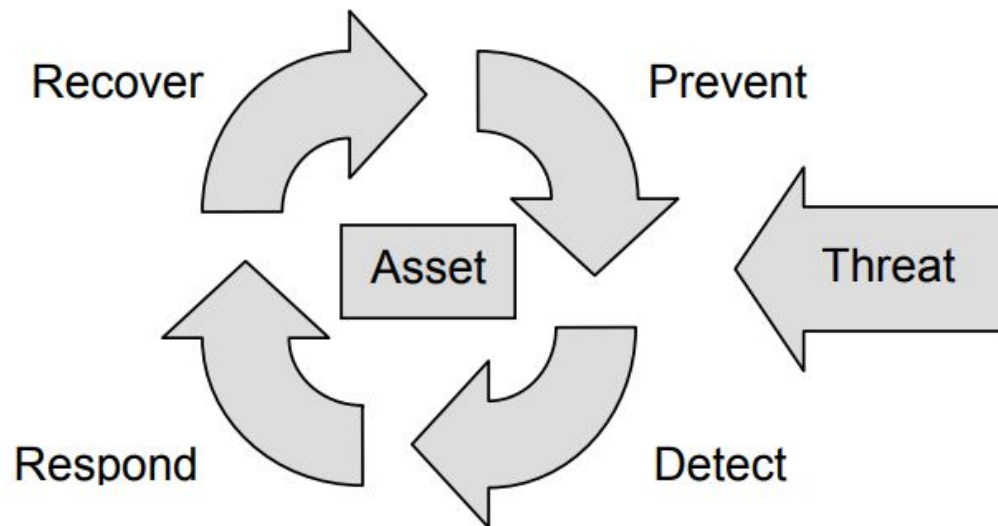


Figure F-1: Active Security Strategy

Enumerating Threats

High Level Approaches (risk mgmt & threat mgmt)

- **Threat Oriented** - identify threat sources & events. Develop threat scenarios. Evaluate vulnerabilities in context of threat events. Evaluate impact based on adversary intent
- **Vulnerability Oriented** - starting with a set of predisposing conditions or vulnerabilities, weaknesses, or deficiencies, identify threat events that could exercise those vulnerabilities along with possible consequences
- **Asset/Impact Oriented** - starting with a list of critical assets (possibly using the results of a mission or business impact analysis), identify impacts or consequences of concern that could affect the critical assets, and then the threat sources that could seek those impacts or consequences.

Threat Oriented

- **Description** - identify threat sources & events. Develop threat scenarios. Evaluate vulnerabilities in context of threat events. Evaluate impact based on adversary intent and likelihood based on the adversary capabilities, etc.
- **Examples** - PASTA, MITRE ATT&CK Framework, Attack Visualizations from Unified Cyber Kill Chain, etc

Vulnerability Oriented

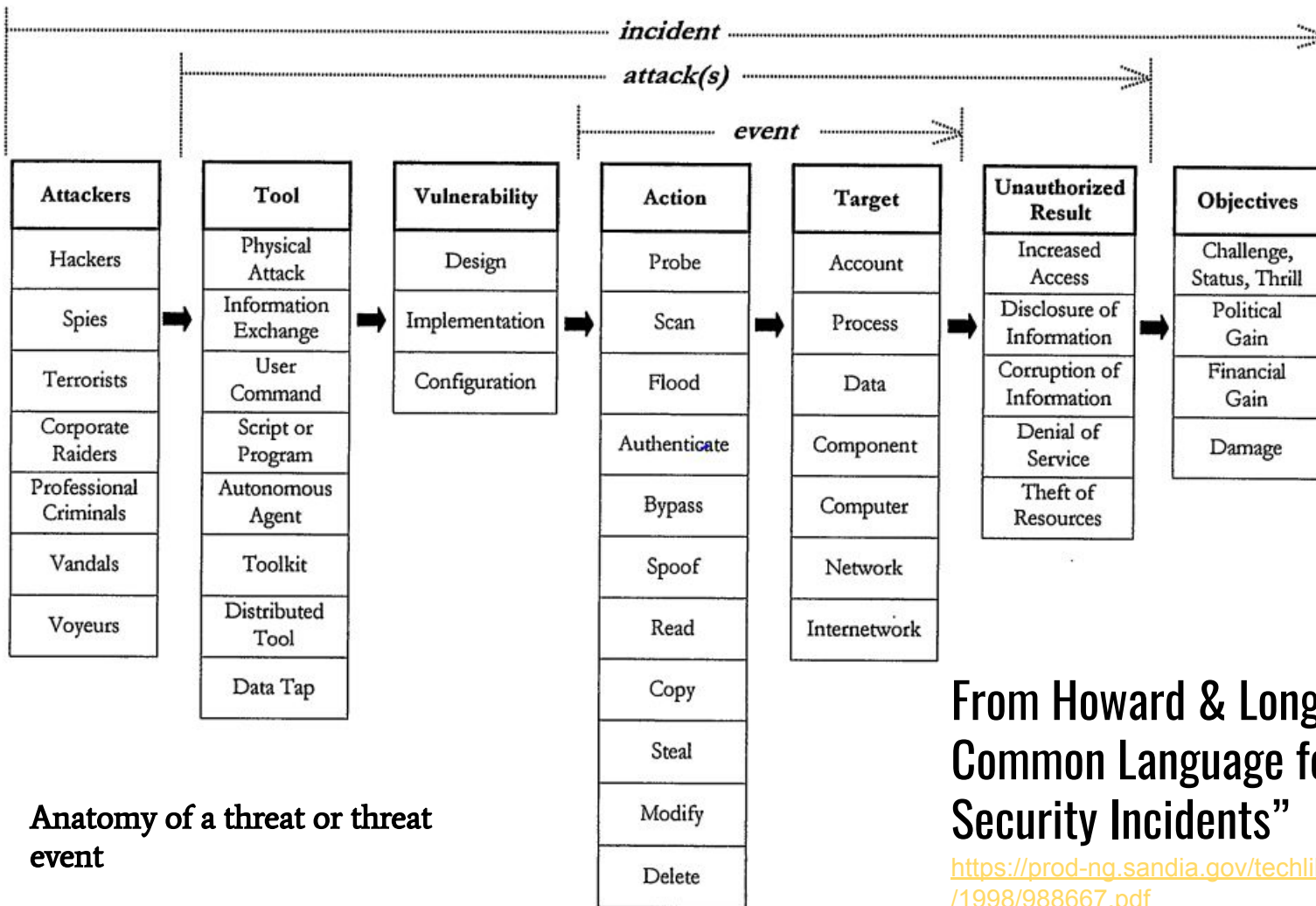
- **Vulnerability Oriented** - starting with a set of predisposing conditions or vulnerabilities, weaknesses, or deficiencies, identify threat events that could exercise those vulnerabilities along with possible consequences
- **Examples**
 - reading a pentesting report and asking “is this relevant to me?”
 - anything involving CVSS or CWE listings (e.g most threat intel sources)

Asset/Impact Oriented

- **Asset/Impact Oriented** - starting with a list of critical assets (possibly using the results of a mission or business impact analysis), identify impacts or consequences of concern that could affect the critical assets, and then the threat sources that could seek those impacts or consequences.
- **Examples:**
 - OCTAVE, STRIDE
 - Anything using Data Flow Diagrams (DFD), most things using attack trees
 - Anything where looking at Confidentiality, Availability, and Integrity is a key part of analysis framework

Enumerating Information Sources

Attackers & Objectives	Tool	Vulnerability	Action	Target	Unauthorized Result
FAIR Threat Agents	Kali Tools L1st	CWE	CAPEC Mechanisms	CAPEC Domains	CIA
Canadian Center for Cyber Security Threat Actors	ATT&CK Software	CVSS	ATT&CK Tactics	VERIS Asset	STRIDE
NIST SP 800-30		CVE	ATT&CK Techniques		ATT&CK Impacts
MITRE Groups					



Decide if threats are relevant/important

Impact

The magnitude of harm expected to result from a successful threat event (a.k.a expected loss)

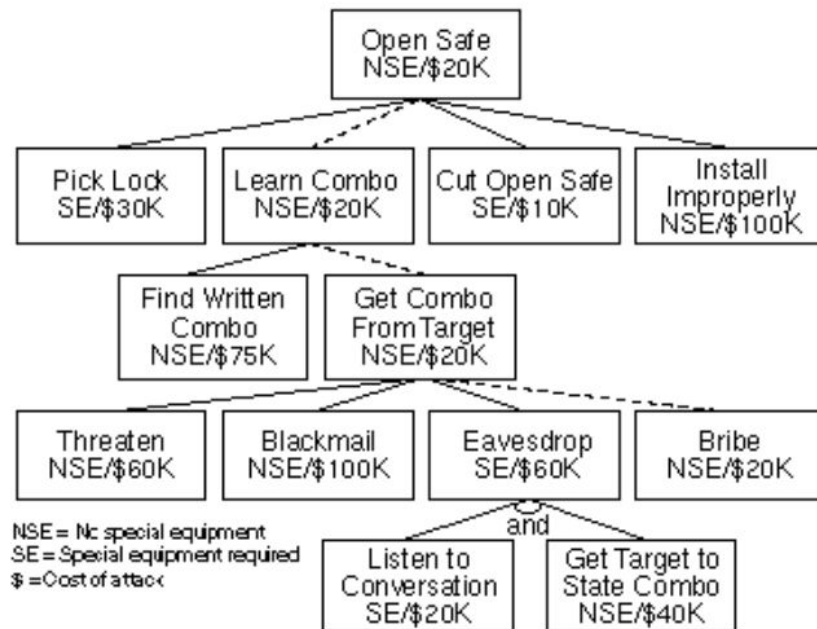


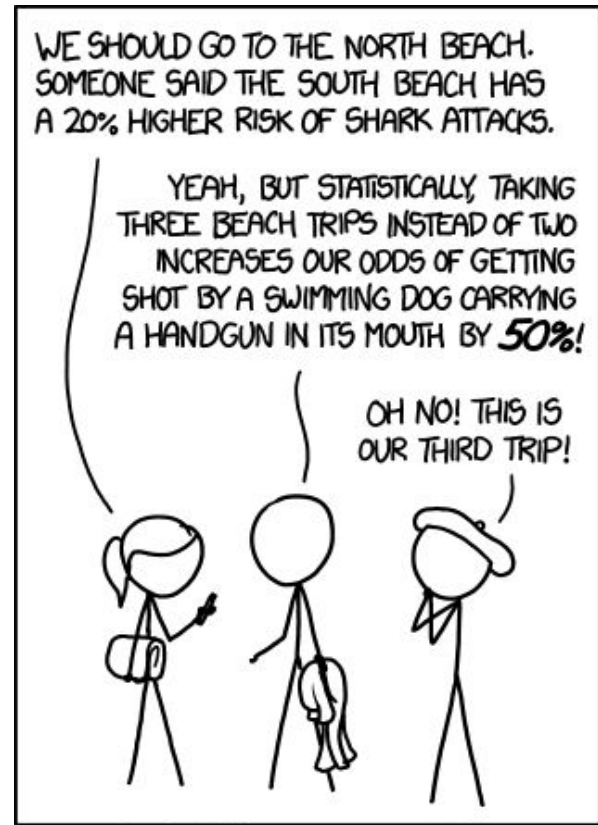
Figure 6: Cheapest Attack Requiring No Special Equipment

From Bruce Schneier on Attack Trees

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

Likelihood

Often framed as: the expected rate of occurrence in a standard unit of time, usually a year

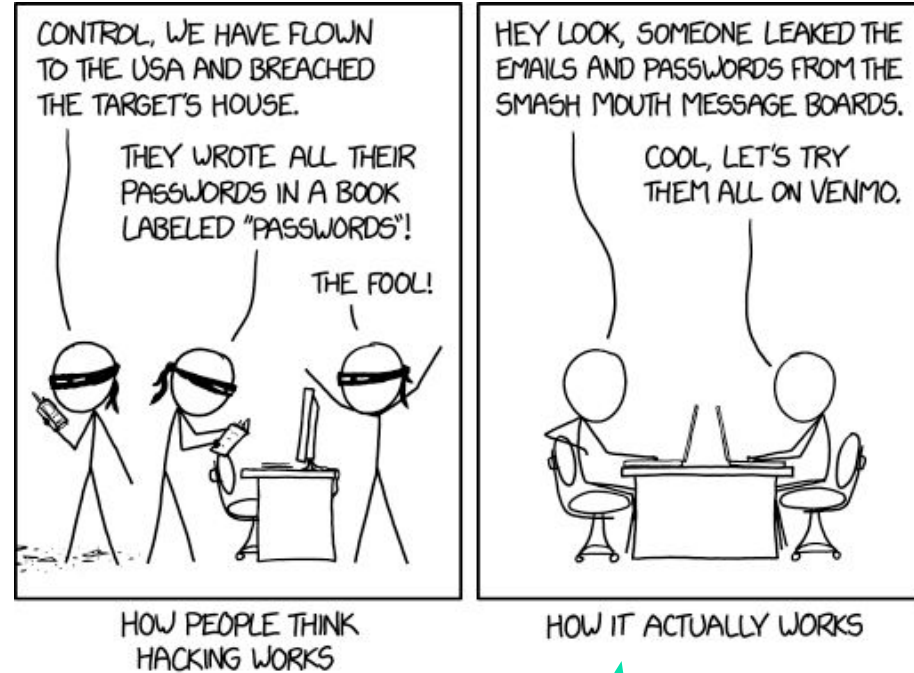


REMINDER: A 50% INCREASE
IN A TINY RISK IS *STILL TINY.*

Prioritization

The action or process of deciding the relative importance or urgency of a thing or things.

- Oxford Languages Online



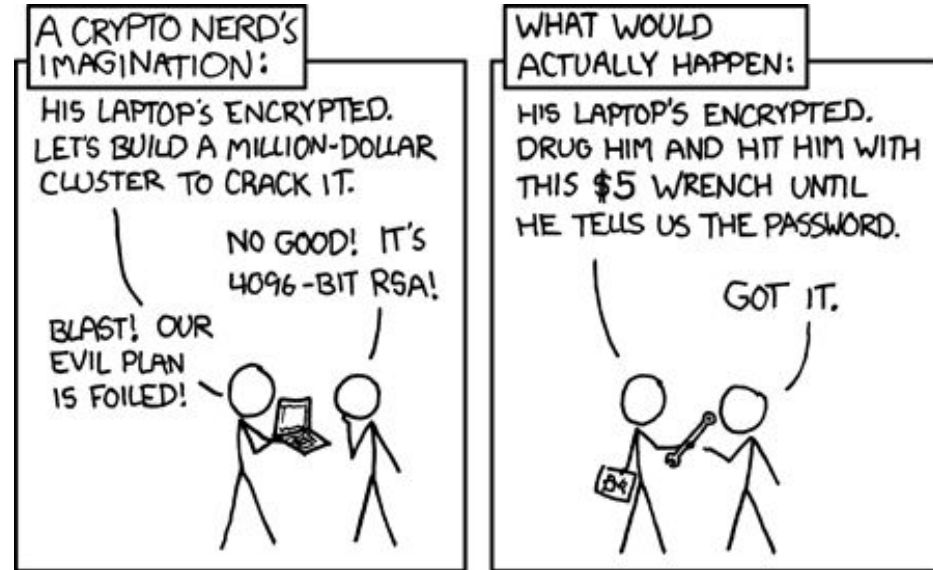
———— Description of [Credential Stuffing](#) attack

XKCD - Randall Munroe <https://xkcd.com/2176/>

Sanity Check

Is this sane, realistic, rational?
See also: Reality Check

(i.e. apply Occams Razor)



Doable? Cost effective? Easiest to implement?
Handles your worse case scenario? Easiest to
use? Can be purchased from someone?



Find the **best** mitigation
strategies/countermeasures

Courses of Defensive Action

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Recon	Web Analytics	Firewalls ACLs				
Weaponization	NIDS	NIPS				
Delivery	Security Awareness	Proxy Filter	Antivirus	Queuing		
Exploitation	HIDS	Patching	Data execution prevention			
Installation	HIDS	Chroot/ Virtualization	Antivirus			
C2	NIDS	Firewall/ACL	network intrusion prevention system	Tarpit	DNS Redirect	
Actions on Objectives	Logging/ Monitoring			Quality of service	Honeypot	

Cyber Kill Chain from Lockheed Martin

Defensive Tooling

ON-PREMISES	AWS	AZURE	GOOGLE	ORACLE	IBM	ALIBABA
Firewall & ACLs	Security Groups AWS Network ACLs	Network Security Groups Azure Firewall	Cloud Armor VPC Firewall	VCN Security Lists	Cloud Security Groups	NAT Gateway
IPS/IDS	3rd Party Only	3rd Party Only	3rd Party Only	3rd Party Only	3rd Party Only	Anti-Bot Service Website Threat Inspector
Web Application Firewall (WAF)	AWS WAF AWS Firewall Manager	Application Gateway	Cloud Armor	Oracle Dyn WAF	Cloud Internet Services	Web Application Firewall
SIEM & Log Analytics	AWS Security Hub Amazon GuardDuty	Azure Sentinel Azure Monitor	Stackdriver Monitoring Stackdriver Logging	Oracle Security Monitoring and Analytics	IBM Log Analysis Cloud Activity Tracker	ActionTrail
Antimalware	3rd Party Only	Microsoft Antimalware / Azure Security Center	3rd Party Only	3rd Party Only	3rd Party Only	Server Guard
Data Loss Prevention (DLP)	Amazon Macie	Information Protection (AIP)	Cloud Data Loss Prevention API	3rd Party Only	3rd Party Only	Web Application Firewall
Key Management	Key Management Service (KMS)	Key Vault	Cloud Key Management Service	Cloud Infrastructure Key Management	Key Protect Cloud Security	Key Management Service
Encryption At Rest	EBS/EFS Volume Encryption, S3 SSE	Storage Encryption for Data at Rest	Part of Google Cloud Platform	Cloud Infrastructure Block Volume	Hyper Protect Crypto Services	Object Storage Service
DDoS Protection	AWS Shield	Built-in DDoS defense	Cloud Armor	Built-in DDoS defense	Cloud Internet Services	Anti-DDoS
Email Protection	3rd Party Only	Office Advanced Threat Protection	Various controls embedded in G-Suite	3rd Party Only	3rd Party Only	3rd Party Only

Marius Mocanu & Adrian Grigorof

Enterprise Mitigations

Mitigations: 40

ID	Name	Description
M1036	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.
M1015	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.
M1049	Antivirus/Antimalware	Use signatures or heuristics to detect malicious software.
M1048	Application Isolation and Sandboxing	Restrict execution of code to a virtual environment on or in transit to an endpoint system.

Define “Good enough”

Compare threat model to “good enough”

Characteristics of Threat Modelling/Assessments as a 'Practice'

- Improve or maintain security posture
 - Implied: Supports decision making about security posture
 - Implied: Supports reduction of risk by improving security posture
- Thorough(-ish), repeatable, communicable, defensible (in an audit)

Threat Modelling Outputs

Outputs

- System Description/Models/Diagrams
- Prioritized/classified list of threats
- Prioritized List of potential mitigations for each threat
 - Bugs
 - Technical requirements/decisions
 - Architectural requirements/decisions
 - new/modified user stories
 - vulnerabilities
- Documentation of above

Key Activities

- Describe System
- Enumerate Threats
- Decide if threats are relevant/important and, if so, find the best mitigation strategies/countermeasures
- Define 'good enough' -> compare job to desired level of rigour



No process or diagrams or
documentation

PROGRESS
NOT
PERFECTION

Process, diagrams & documentation
that meet your objectives.

Threat Modelling

RECAP

Threat Modelling

(as a practice)
(Ophe's Definition)

A set of modelling & analysis techniques for finding out what threats are relevant to a system, prioritizing them, and then seeing what we *could* do about them.

(hopefully, post threat model, you *actually* do something about them)

Threat Modelling

Ask four key questions:

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good (enough) job?

Key Activities:

- Describe System
- Enumerate Threats
- Decide if threats are relevant/important
- Find the best mitigation strategies/countermeasures for the important threats
- Define 'good (enough)'
- Compare job to 'good (enough)'

Thank you Wealthsimple Team

`</rant>` Questions?

There will be a video and slides available later at

OWASP Toronto Chapter web page: <https://owasp.org/www-chapter-toronto/>

OWASP Toronto Chapter Youtube: https://www.youtube.com/channel/UCqmBl-u_4cOEiH3OXWE3sPg

Bonus Material

Threat Modelling

ORIGIN STORY!



Act 1: The seeds of conflict are sown...

1969
unics/
unix
started

1983 -
modern
internet
born

1991 v1
Linux
released

- 1960's Authentication born (passwords and other knowledge-based mechanisms) at MIT
- 1971 - birth of Phreaking - John Draper (aka Cap'n Crunch) hacks phone systems using a toy whistle from a cereal box and CREEPER (self replicating program) spreads on ARPANET.
- 1983 - Kevin Poulsen (aka Dark Dante) is arrested for breaking into the Arpanet
- and 'Computer Virus' demoed by Fred Cohen at a security seminar at Lehigh University (incidentally, Rich Skrenta beat him to it by releasing Elk Cloner for Apple II gaming systems in 1982)
- 1984 - Credit Reporting Agency TRW Information Systems (now Experian)'s database breached. Password posted to an electronic bulletin board.
- 1986 - Hacker's Manifesto published by Loyd Blakeship (Legion of Doom member) after arrest
- 1988 - Morris Worm released onto the Internet



Act 2: Trying to resolve the Big Problem...

- 1986 - [Computer Fraud and Abuse Act](#)
- 1988 CERT/CC (later CERT SEI) created at DARPA's direction in response to Morris Worm
- 1993 - [Bugtraq](#) created by Scott Chasin - one of the first security mailing lists, dedicated to publicly disclosing security flaws.
- 1995 - all 'limitations' on commercial use of Internet end when [National Science Foundation ends sponsorship of Internet backbone \(NSFNet\)](#) and all traffic relies on commercial networks.
- 2002 - Microsoft starts Trustworthy Computing initiative
- 2003 - DHS partners with CMU to create [US-CERT](#) & [CSIRT](#)



Act 2: Trying to resolve the Big Problem via Threat Modelling...

- 1977 - architectural patterns threat modelling methodology published by Christopher Alexander
- 1988 - 'first' IT-system attacker profile developed by Robert Bernard
- 1994 - Threat Trees (based on decision tree diagrams) mentioned in Edward Amoroso's "[Fundamentals of Computer Security Technology](#)" book
- 1998 - Attack trees described by Bruce Schneier in his paper "[Towards a secure system engineering methodology](#)"
- 1999 - Microsoft publishes STRIDE threat modelling methodology
And CMU introduces Operationally Critical Threat, Asset, and Vulnerability Evaluation ([OCTAVE](#)) to manage organizational IT Risk
- 2004 - Frank Swiderski and Window Snyder release [first book on Threat Modelling](#) published by Microsoft Press
And [Threat Analysis & Modelling tool](#) released by Microsoft - uses DFDs and Attack Trees

TL;DR



PRACTICAL JOKES

It's all fun and games until Grandpa has a heart attack while eating his salad.

VERY DEMOTIVATIONAL .com

Early Computing

Early Internet



Today

Act 3: Trying to resolve the Big Problem...



Some more references:

- [A Brief History of Hacking](https://encyclopedia.kaspersky.com/a-brief-history-of-hacking) (Encyclopedia.kaspersky.com)
- [evolution of IT-based threat modelling](https://en.wikipedia.org/wiki/evolution_of_IT-based_threat_modelling) (wikipedia)
- [Evolution of Threat Modelling](https://threatmodeller.com/evolution-of-threat-modelling) (ThreatModeller.com)
- [The World's First Computer Password? It Was Useless Too](https://www.wired.com/2013/01/the-worlds-first-computer-password-it-was-useless-too/) (Wired)
- [Android evolution image](https://nettantra.com/android-evolution-image/) used on these pages (Nettantra.com)
- European Union Agency for Cybersecurity (ENISA) [Threat Taxonomy](#) and [Threat Landscape materials](#)