Threat Modeling

A summary of available methods

Adopted from CEI (https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf)

Dr. Panayotis Kikiras
INFS133

Intro to threat modeling

“Threat modeling is the key to a focused defense. Without threat modeling, you can never stop playing whack-a-mole.”

– Adam Shostack : *Threat Modeling: Designing for Security.* Wiley, 2014. ISBN 978-1118809990

What is thread modeling

- **Threat modeling** is a process by which potential threats, such as structural vulnerabilities can be (from a hypothetical attacker's point of view):
  - identified,
  - enumerated,
  - and prioritized

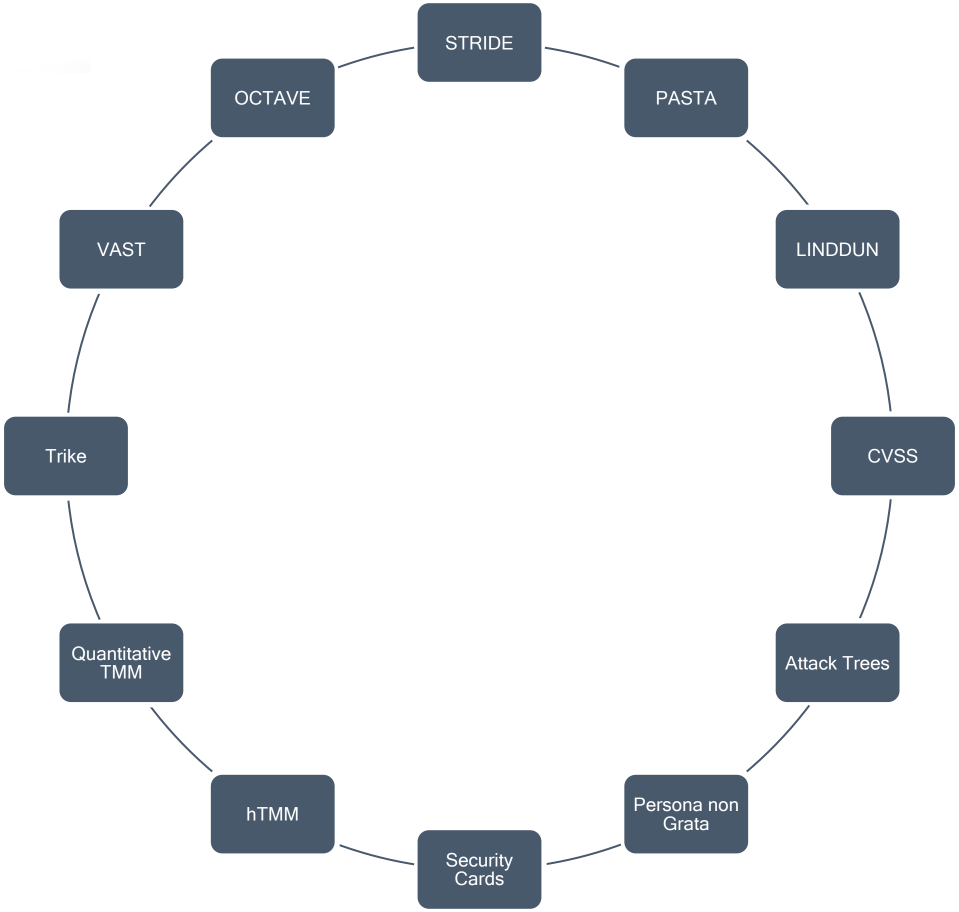
- The purpose of threat modeling is to provide defenders with a systematic analysis of the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker.

- Threat modeling answers questions like:
  - *"Where are the high-value assets?"*,
  - *"Where am I most vulnerable to attack?"*,
  - *"What are the most relevant threats?"*, and
  - *"Is there an attack vector that might go unnoticed?"*.

How threat models are used?

- Threat modeling methods are used
  - to create an abstraction of the system;
  - profiles of potential attackers, including their goals and methods;
  - Catalog(s) of potential threats that may arise
- There are many threat modeling methods that have been developed.
- Not all of them are comprehensive;
  - some focus on the abstraction and encourage granularity while others are more people-centric.
  - Some meth-ods focus specifically on risk or privacy concerns.
- Threat modeling methods can be combined to cre-ate a more robust and well-rounded view of potential threats.

Methodologies to be discussed



STRIDE

PASTA

LINDDUN

CVSS

Attack Trees

Persona non Grata

Security Cards

hTMM

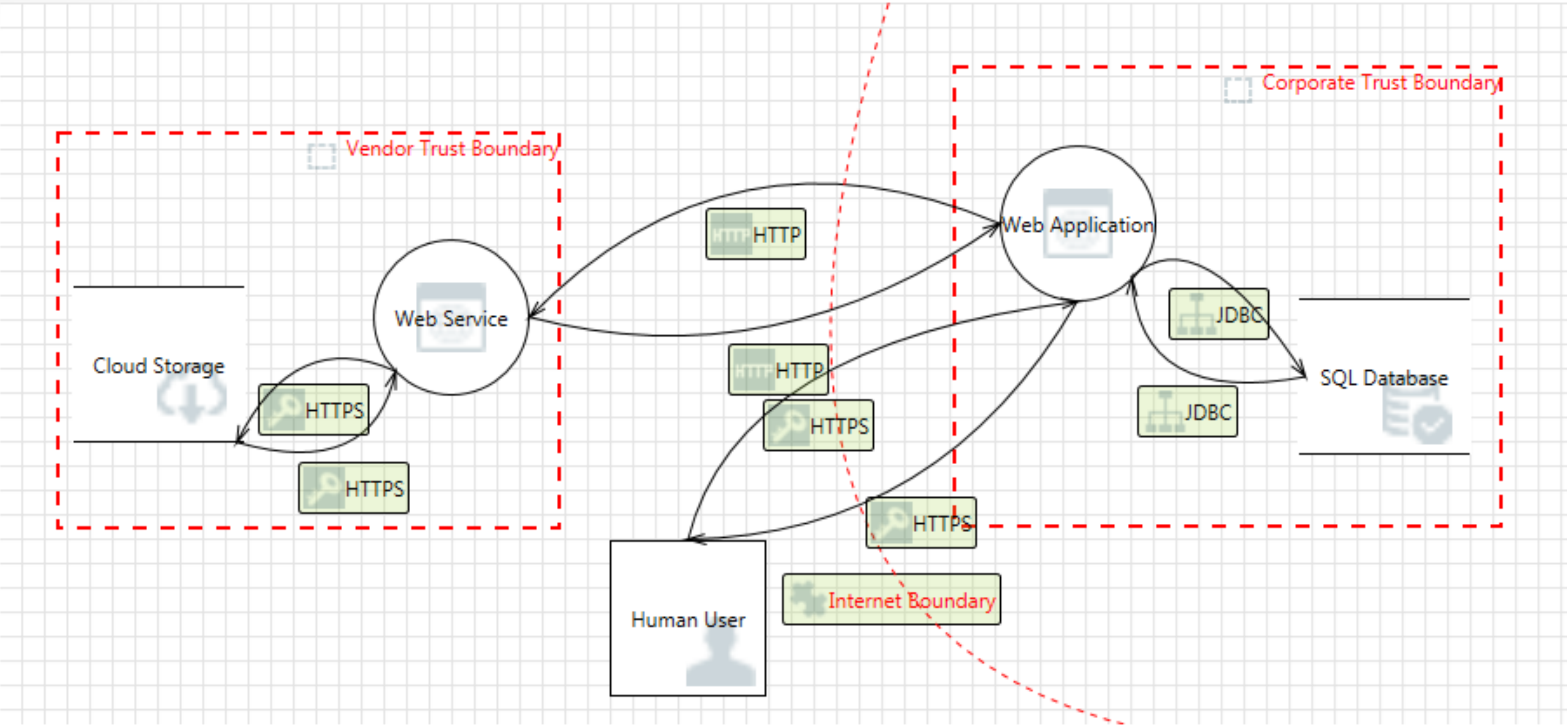
Quantitative TMM

Trike

VAST

OCTAVE

STRIDE


Vendor Trust Boundary
Corporate Trust Boundary
Web Application
HTTP
Cloud Storage
Web Service
JDBC
SQL Database
HTTP
HTTPS
HTTPS
JDBC
HTTPS
HTTPS
Human User
Internet Boundary

STRIDE

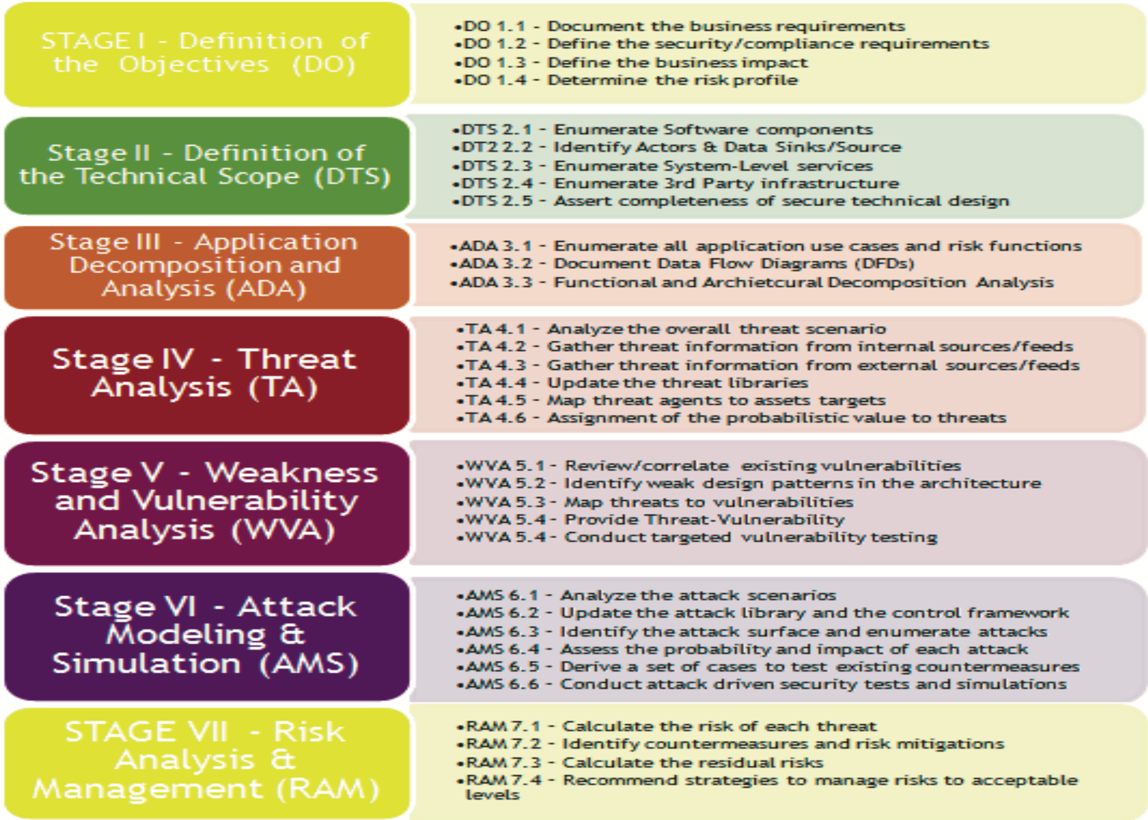
	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn’t do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to

STRIDE

- This method is easy to adopt but can be time consuming
- STRIDE's main issue is that the number of threats can grow rapidly as a system increases in complexity.
- STRIDE has been successfully applied to cyber-only and cyber-physical systems.
- Microsoft no longer maintains STRIDE, it is implemented as part of the Microsoft Se- cure Development Lifecycle (SDL) with the Threat Modeling Tool, which is still available
- Microsoft developed another similar method called DREAD, which is also a mnemonic (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability) with a different approach for assessing threats.
  - It assigns one of three values (0, 5, 10) to the first four categories and one of four values (0, 5, 9, 10) to the last category, which "allows for an average value to be calculated to represent the risk of the entire system.

PASTA

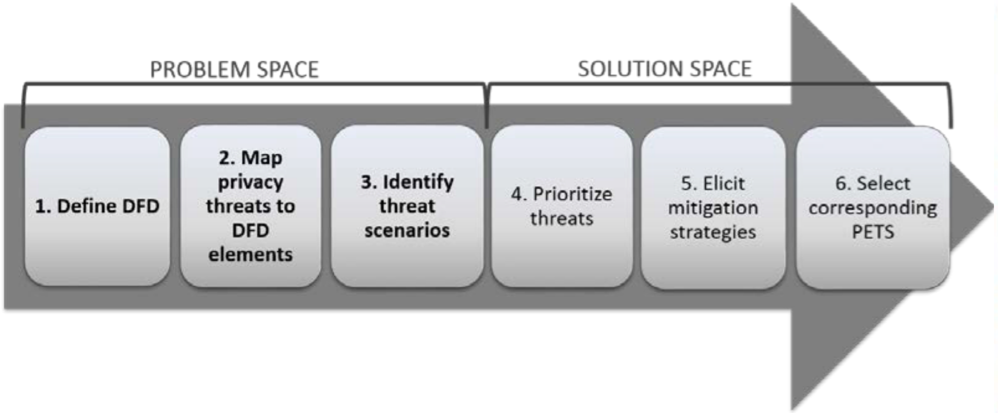
- The Process for Attack Simulation and Threat Analysis (P.A.S.T.A) is a risk-centric threat modeling framework developed in 2012 by Tony Uceda Vélez. It contains seven stages, each with multiple activities.



STAGE I - Definition of the Objectives (DO)	•DO 1.1 - Document the business requirements •DO 1.2 - Define the security/compliance requirements •DO 1.3 - Define the business impact •DO 1.4 - Determine the risk profile
Stage II - Definition of the Technical Scope (DTS)	•DTS 2.1 - Enumerate Software components •DT2 2.2 - Identify Actors & Data Sinks/Source •DTS 2.3 - Enumerate System-Level services •DTS 2.4 - Enumerate 3rd Party infrastructure •DTS 2.5 - Assert completeness of secure technical design
Stage III - Application Decomposition and Analysis (ADA)	•ADA 3.1 - Enumerate all application use cases and risk functions •ADA 3.2 - Document Data Flow Diagrams (DFDs) •ADA 3.3 - Functional and Archietcural Decomposition Analysis
Stage IV - Threat Analysis (TA)	•TA 4.1 - Analyze the overall threat scenario •TA 4.2 - Gather threat information from internal sources/feeds •TA 4.3 - Gather threat information from external sources/feeds •TA 4.4 - Update the threat libraries •TA 4.5 - Map threat agents to assets targets •TA 4.6 - Assignment of the probabilistic value to threats
Stage V - Weakness and Vulnerability Analysis (WVA)	•WVA 5.1 - Review/correlate existing vulnerabilities •WVA 5.2 - Identify weak design patterns in the architecture •WVA 5.3 - Map threats to vulnerabilities •WVA 5.4 - Provide Threat-Vulnerability •WVA 5.4 - Conduct targeted vulnerability testing
Stage VI - Attack Modeling & Simulation (AMS)	•AMS 6.1 - Analyze the attack scenarios •AMS 6.2 - Update the attack library and the control framework •AMS 6.3 - Identify the attack surface and enumerate attacks •AMS 6.4 - Assess the probability and impact of each attack •AMS 6.5 - Derive a set of cases to test existing countermeasures •AMS 6.6 - Conduct attack driven security tests and simulations
STAGE VII - Risk Analysis & Management (RAM)	•RAM 7.1 - Calculate the risk of each threat •RAM 7.2 - Identify countermeasures and risk mitigations •RAM 7.3 - Calculate the residual risks •RAM 7.4 - Recommend strategies to manage risks to acceptable levels

LINDDUN

- LINDDUN (Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance) is a threat modeling method that focuses on privacy concerns and can be used for data security
- One of the strong features of the LINDDUN method is its extensive privacy knowledgebase and documentation. The LINDDUN method is labor intensive and time consuming. It suffers from the same issues as STRIDE—the number of threats can grow rapidly as a system increases in complexity.



PROBLEM SPACE

SOLUTION SPACE

1. Define DFD

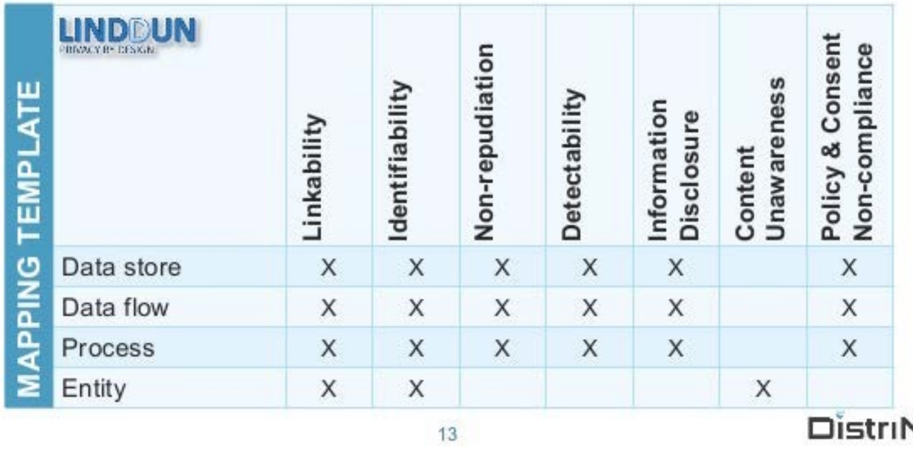
2. Map privacy threats to DFD elements

3. Identify threat scenarios

4. Prioritize threats

5. Elicit mitigation strategies

6. Select corresponding PETS



MAPPING TEMPLATE

LINDDUN PRIVACY BY DESIGN	Linkability	Identifiability	Non-repudiation	Detectability	Information Disclosure	Content Unawareness	Policy & Consent Non-compliance
Data store	X	X	X	X	X		X
Data flow	X	X	X	X	X		X
Process	X	X	X	X	X		X
Entity	X	X				X	

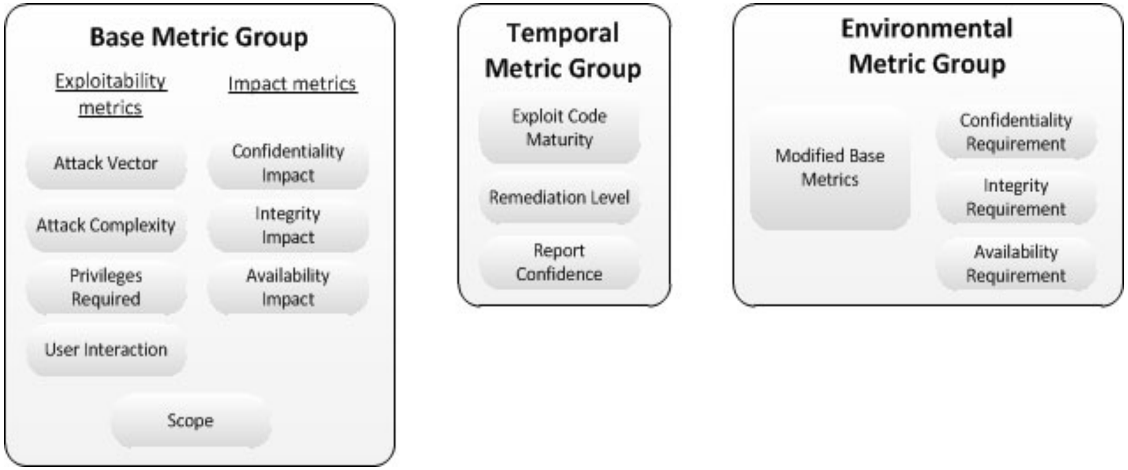
13

DistriN

CVSS

- The Common Vulnerability Scoring System (CVSS) is a method that “capture[s] the principal characteristics of a vulnerability, and produce[s] a numerical score reflecting its severity”

- A CVSS score is computed based on values assigned by an analyst for each metric.
- The equations used for this process are not clear, but all metrics are explained in the documentation quite extensively.
- The method is widely used, despite some concerns related to the non-transparent score calculations and possible inconsistencies produced by different judging “experts” .



Base Metric Group

Exploitability metrics

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction

Impact metrics

- Confidentiality Impact
- Integrity Impact
- Availability Impact

Scope

Temporal Metric Group

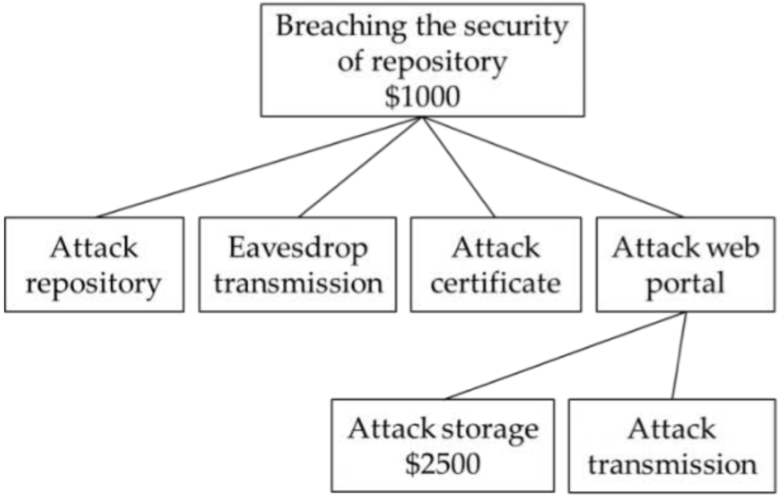
- Exploit Code Maturity
- Remediation Level
- Report Confidence

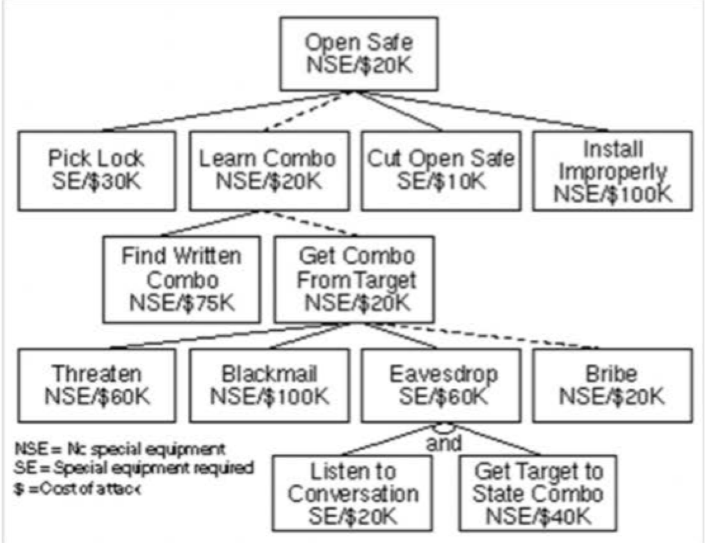
Environmental Metric Group

- Modified Base Metrics
- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement

Attack Trees

- Using attack trees to model threats is one of the oldest and most widely applied techniques on cyber- only systems as well as cyber-physical and physical systems

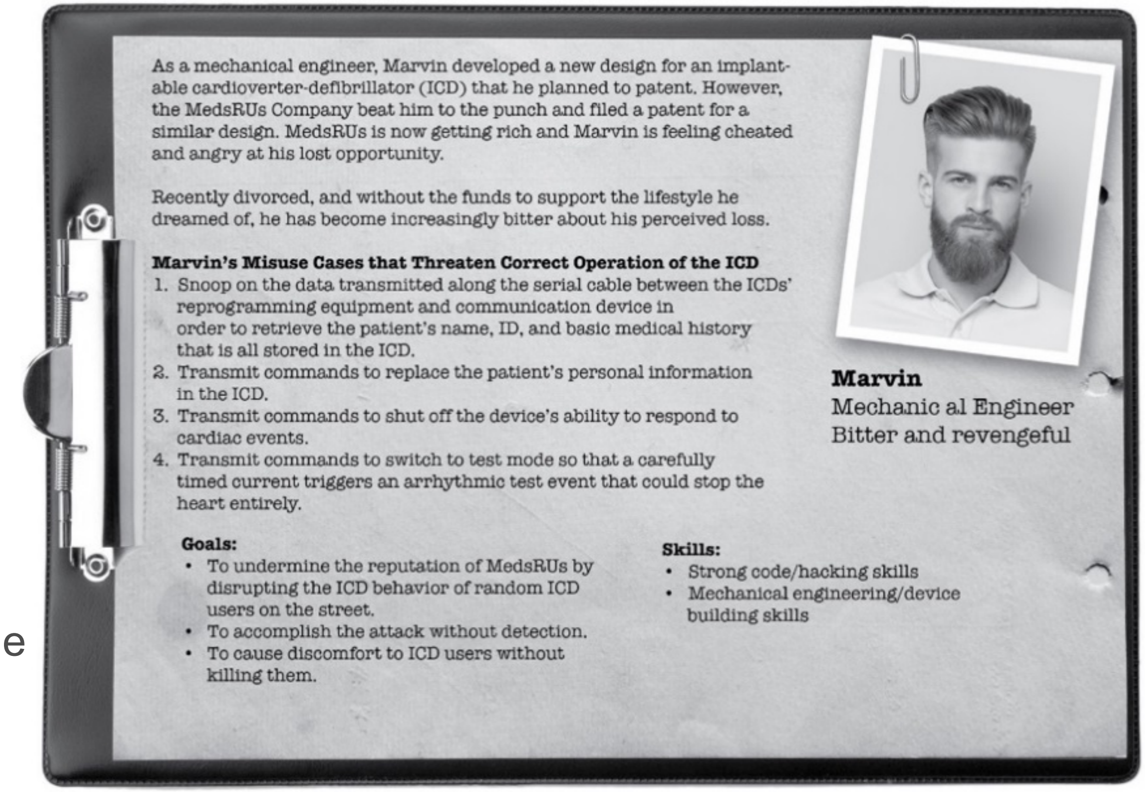



Open Safe NSE/$20K
Pick Lock SE/$30K
Learn Combo NSE/$20K
Cut Open Safe SE/$10K
Install Improperly NSE/$100K
Find Written Combo NSE/$75K
Get Combo From Target NSE/$20K
Threaten NSE/$60K
Blackmail NSE/$100K
Eavesdrop SE/$60K
Bribe NSE/$20K
and
Listen to Conversation SE/$20K
Get Target to State Combo NSE/$40K
NSE = No special equipment
SE = Special equipment required
$ = Cost of attack

Persona non Grata

- As a threat modeling method, Persona non Grata (PnG) focuses on the motivations and skills of hu- man attackers. It characterizes users as archetypes that can misuse the system and forces analysts to view the system from an unintended use point of view

- When used, PnG can help visualize threats from the counterpart side, which can be helpful in the early stages of the threat modeling.
- The idea is to "introduce" a technical expert to a potential attacker of the system and their skills, motivations, and goals that help the expert to see the system's vulnera- bilities and points of compromise from the other side.
- PnG is easy to adopt but is rarely used or researched. This technique fits well into the agile approach, which incorporates personas



As a mechanical engineer, Marvin developed a new design for an implantable cardioverter-defibrillator (ICD) that he planned to patent. However, the MedsRUs Company beat him to the punch and filed a patent for a similar design. MedsRUs is now getting rich and Marvin is feeling cheated and angry at his lost opportunity.

Recently divorced, and without the funds to support the lifestyle he dreamed of, he has become increasingly bitter about his perceived loss.

Marvin's Misuse Cases that Threaten Correct Operation of the ICD

1. Snoop on the data transmitted along the serial cable between the ICDs' reprogramming equipment and communication device in order to retrieve the patient's name, ID, and basic medical history that is all stored in the ICD.
2. Transmit commands to replace the patient's personal information in the ICD.
3. Transmit commands to shut off the device's ability to respond to cardiac events.
4. Transmit commands to switch to test mode so that a carefully timed current triggers an arrhythmic test event that could stop the heart entirely.

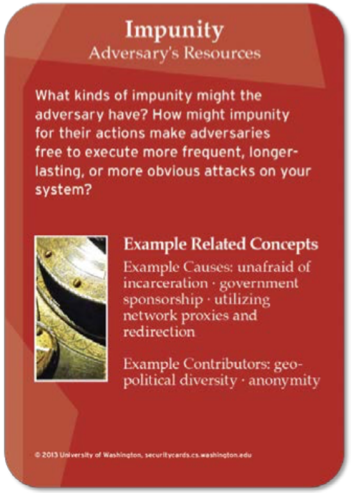
Marvin
Mechanic al Engineer
Bitter and revengeful

Goals:
- To undermine the reputation of MedsRUs by disrupting the ICD behavior of random ICD users on the street.
- To accomplish the attack without detection.
- To cause discomfort to ICD users without killing them.

Skills:
- Strong code/hacking skills
- Mechanical engineering/device building skills

Security Cards

- Security Cards is a technique that centers on identifying unusual and complex attacks. It is not a formal method but more of a brainstorming technique.
- This method uses a deck of 42 cards to facilitate threat discovery activities: Human Impact (9 cards), Adversary's Motivations (13 cards), Adversary Resources (11 cards), and Adversary's Methods (9 cards).



Impunity
Adversary's Resources

What kinds of impunity might the adversary have? How might impunity for their actions make adversaries free to execute more frequent, longer-lasting, or more obvious attacks on your system?

Example Related Concepts

Example Causes: unafraid of incarceration · government sponsorship · utilizing network proxies and redirection

Example Contributors: geo-political diversity · anonymity

Human Impact

- the biosphere
- emotional well-being
- financial well-being
- personal data
- physical well-being
- relationships
- societal well-being
- unusual impacts

Adversary's Motivations

- access or convenience
- curiosity or boredom
- desire or obsession
- diplomacy or warfare
- malice or revenge
- money
- politics
- protection
- religion
- self-promotion
- world view
- unusual motivations

Adversary's Resources

- expertise
- a future world
- impunity
- inside capabilities
- inside knowledge
- money
- power and influence
- time
- tools
- unusual resources

Adversary's Methods

- attack cover-up
- indirect attack
- manipulation or coercion
- multi-phase attack
- physical attack
- processes
- technological attack
- unusual methods

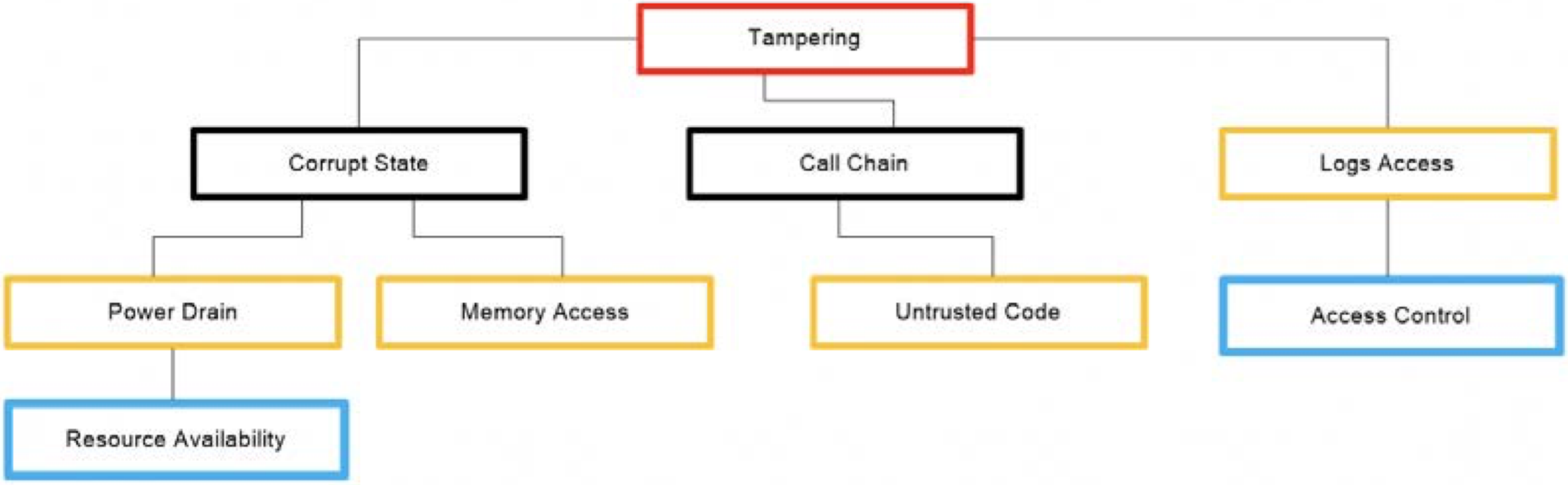
hTMM

- The Hybrid Threat Modeling Method (hTMM) was developed by the Software Engineering Institute in 2018. It consists of a combination of SQUARE (Security Quality Requirements Engineering Method), Security Cards, and PnG activities.

- The following are the main steps of the method:
  - Identify the system to be threat-modeled.
  - Apply Security Cards based on developer suggestions.
  - Remove unlikely PnGs (i.e., there are no realistic attack vectors).
  - Summarize the results using tool support.
  - Continue with a formal risk assessment method.

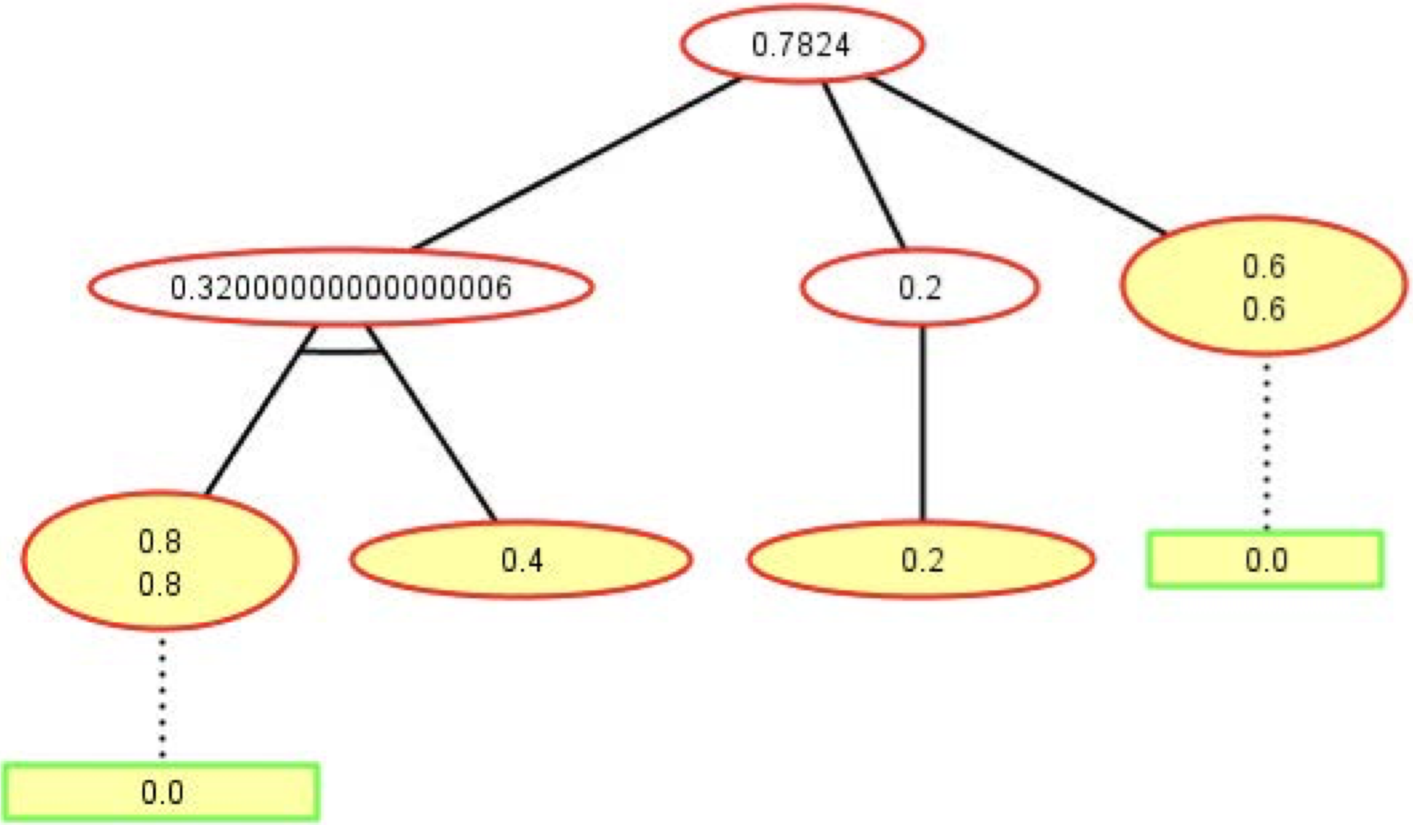
Quantitative Threat Modeling Method

- This hybrid method consists of Attack Trees, STRIDE, and CVSS methods applied in synergy.
- The first step of the Quantitative Threat Modeling Method (Quantitative TMM) is to build component attack trees for the five threat categories of STRIDE.



Quantitative Threat Modeling Method

- After that, the CVSS method is applied and scores are calculated for the components in the tree.

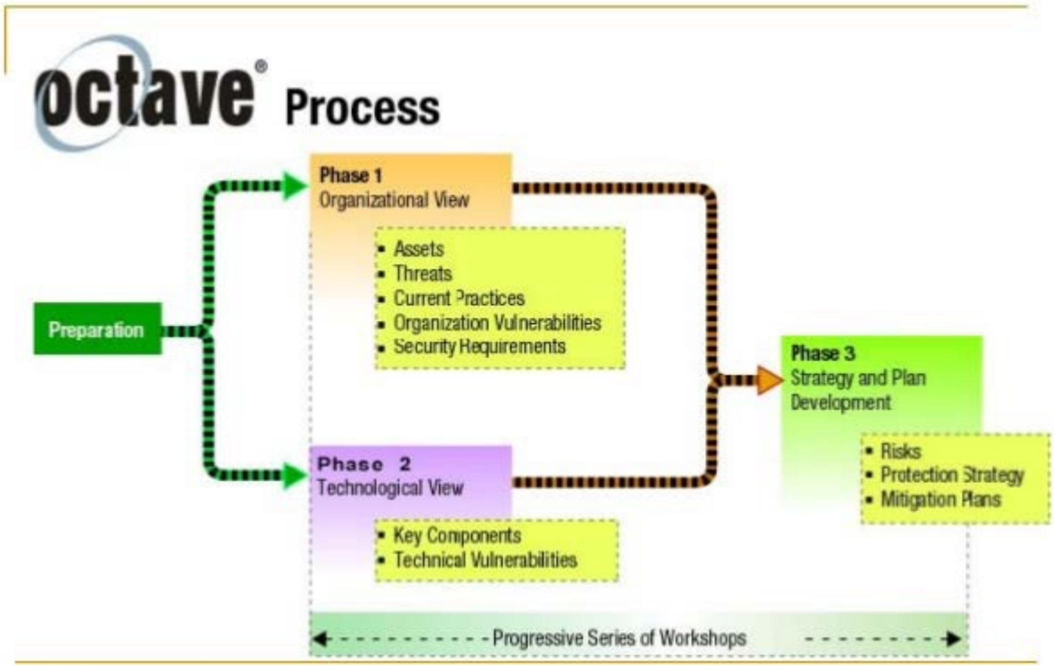


OCTAVE

- The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method is a risk- based strategic assessment and planning method for cybersecurity
- OCTAVE has three phases:
  - Build asset-based threat profiles. (This is an organizational evaluation.)
  - Identify infrastructure vulnerability. (This is an evaluation of the information infrastructure.)
  - Develop a security strategy and plans. (This is an identification of risks to the organization’s critical assets and decision making.)

OCTAVE

- OCTAVE evaluates activities, not continuous processes. It is primarily designed for large organizations.
- The downsides of OCTAVE are that the process requires a significant time commitment, and the documentation is large and vague



Conclusions

- Threat modeling can help make your product more secure and trustworthy.
- Choosing what method is best for a project requires thinking about:
  - if there are any specific areas you want to target (risk, security, privacy),
  - how long you have to perform threat modeling,
  - how much experience you have with threat modeling,
  - how involved stakeholders want to be,
  - and …more.

Discussion