A threat-focused approach in cyber risk management

Maria Brempou | November 2020

Overview

Incorporating a threat mindset in cyber risk management

Step 1: Threat Modeling

Identifying threats that are prevalent to the system/application under review

Step 2: Cyber Risk Assessment

Connecting identified threats with the resulting cyber risks to the environment

Step 3: Risk Scoring Methodology

Utilizing a quantitative threat-driven methodology for defining the risk scoring

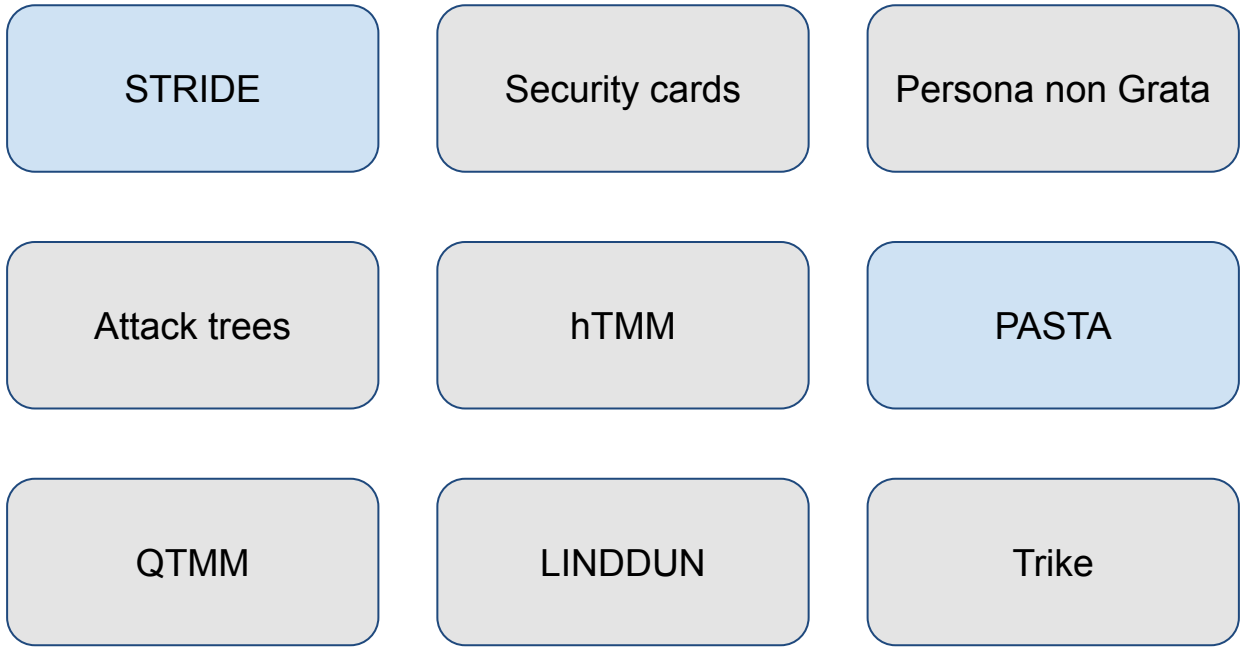
Threat Modeling

What is threat modeling?

> “Threat modeling works to identify, communicate, and understand threats and mitigations within the context of protecting something of value.”

- Threat modeling can help make your technical setup more secure and trustworthy.
- Can be applied to a wide range of things, including systems, applications, networks, business processes, etc.
- Can be done at any stage of development, preferably early - so that the findings can inform the design.
- Using threat modeling to think about security requirements can lead to proactive architectural decisions that help reduce threats from the start.

Threat modeling frameworks



= To be analyzed in further detail

Threat modeling - STRIDE

Spoofing
Tampering
Repudiation
Information Disclosure
Denial of Service
Elevation of Privilege

Currently the most mature threat-modeling method.

Has evolved over time to include new threat-specific tables and the variants STRIDE-per-Element and STRIDE-per-Interaction.

	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 do

Threat modeling - PASTA

***P**rocess for*
***A**ttack*
***S**imulation and*
***T**hreat*
***A**nalysis*

The framework consists of **seven** stages

Risk-centric framework which employs an attacker-centric perspective.

It elevates the threat-modeling process to a strategic level by involving key decision makers.

Cyber Risk Assessment

Connecting the threats with the risks

The output of the threat modeling exercise becomes a baseline for the cyber risk assessment

Defining the risks that could result from each identified threat scenario

Defining the controls that address each identified risk

The outcome

Identifying the threat surface and risk profile of the specific setup
The threat modeling and risk assessment exercises for each setup or defined scope lead to a unique output.

Creating a repeatable framework
By performing multiple models and assessments, a repeatable framework of threats, risks and controls can be created.
BUT: This framework cannot be “blindly” applied to new setups, as each setup is different and has a unique profile. However, it can assist with automating part of future assessments.

Example: API integration with a 3rd party

Step 1: Identifying the threat scenarios that are applicable to this specific use case.

Step 2a: Translate each threat scenario to the related risks that could materialize in your environment.

Step 2b: Identify the controls that can (partially or fully) mitigate the identified risks.

1 Threat scenario	2a Description of Risk and impact	2b Recommendation/Control
Information Disclosure	Sensitive data leakage, which could result to reputational damage and/or immaterial financial penalties	Follow the guidelines on best practices from security to avoid introducing vulnerabilities in the code.
Information Disclosure	Sensitive data leakage, which could result to reputational damage and/or immaterial financial penalties	Performance of a technical vulnerability assessment and remediation of all critical- and high-risk vulnerabilities identified according to the defined SLAs.
Information Disclosure	Lack of security monitoring of the web application might result in sensitive data leakage that is not timely detected.	Route traffic through a Web Application Firewall (WAF).
Spoofing	Improper secret safeguarding could lead to secret leakage and spoofing attacks.	Store the API keys following the relevant security guidelines.
Denial of Service	Loss of availability due to denial of service attacks.	Implement a throttling or rate limiting solution to the API endpoints.

* The STRIDE methodology has been applied to this example.
** This is a generic, indicative example. The list of threats and risks is not complete and the list of controls is not as specific as it needs to be.

Risk Scoring Methodology

Adopting a quantitative risk scoring approach

Why?

- **Granularity** of risk assessment results
- **RIsk scoring consistency** due to concrete guidance
- **Clarity** for the prioritization of workload

The threat-focused risk scoring methodologies that will be reviewed are ***DREAD***, ***CVSS*** *and* ***OWASP's risk rating methodology***.

Threat-focused risk scoring: DREAD

Damage
Reproducibility
Exploitability
Affected users
Discoverability

Rating is based on answering 5 questions:

1. *How bad would an attack be?*
2. *How easy is it to reproduce the attack?*
3. *How much work is it to launch the attack?*
4. *How many people will be impacted?*
5. *How easy is it to discover the threat?*

Example - How?

- For each identified risk, assign a **score per category** considering the respective question.
  - *Indicative scoring example: 3 - high risk, 2 - medium risk, 1 - low risk*
- The **total score of the identified risk** is obtained by adding the values for all categories and concluding in which bucket does the risk belong.
  - *Indicative total scoring buckets: 12-15 - high risk, 8-11 - medium risk, 5-7 - low risk*
- The **overarching system/application risk score** may inherit the highest calculated risk score associated with it, depending on the risk appetite

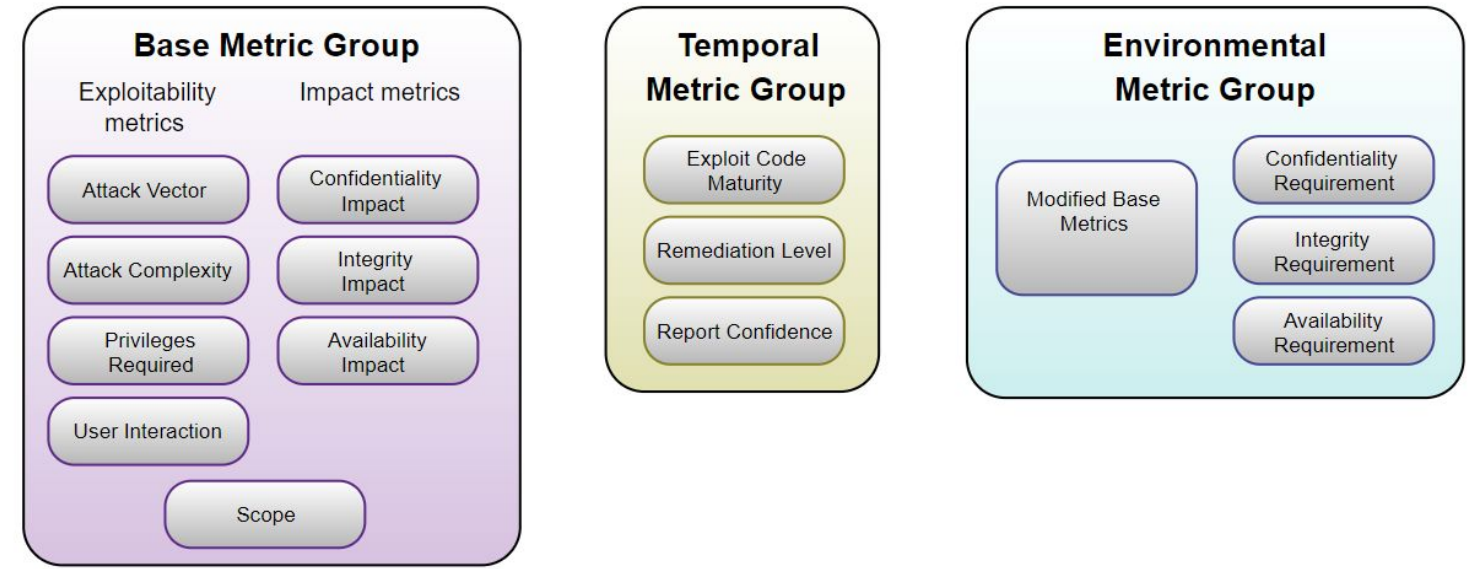
Threat-focused risk scoring: CVSS

***C**ommon*
***V**ulnerability*
***S**coring*
***S**ystem*

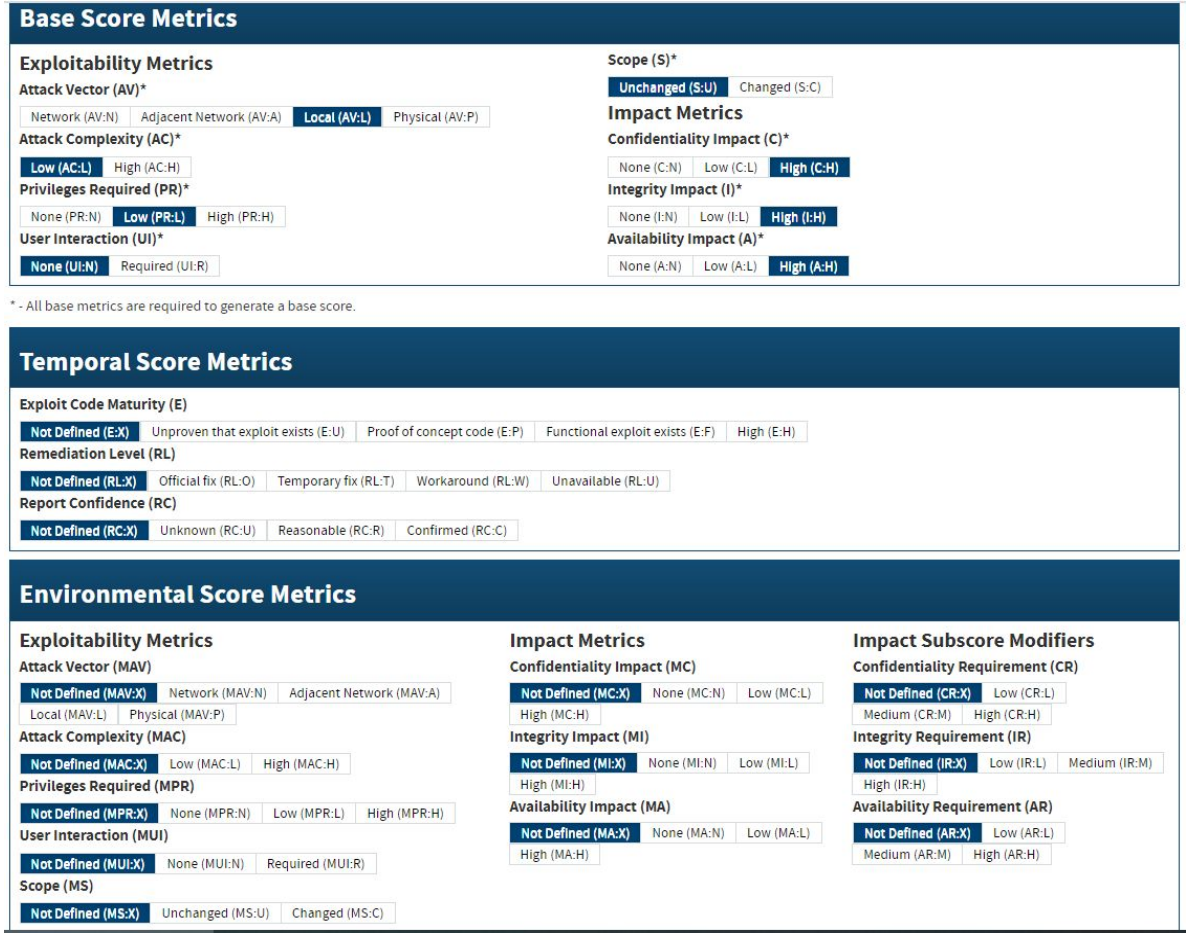
Provides a standardized scoring system within different platforms.

A CVSS score can be computed by a calculator that is available online.

Consists of **three** metric groups



Threat-focused risk scoring: CVSS example



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) | Adjacent Network (AV:A) | **Local (AV:L)** | Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) | High (AC:H)

Privileges Required (PR)*

None (PR:N) | **Low (PR:L)** | High (PR:H)

User Interaction (UI)*

None (UI:N) | Required (UI:R)

Scope (S)*

Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | Low (C:L) | **High (C:H)**

Integrity Impact (I)*

None (I:N) | Low (I:L) | **High (I:H)**

Availability Impact (A)*

None (A:N) | Low (A:L) | **High (A:H)**

* - All base metrics are required to generate a base score.

Temporal Score Metrics

Exploit Code Maturity (E)

Not Defined (E:X) | Unproven that exploit exists (E:U) | Proof of concept code (E:P) | Functional exploit exists (E:F) | High (E:H)

Remediation Level (RL)

Not Defined (RL:X) | Official fix (RL:O) | Temporary fix (RL:T) | Workaround (RL:W) | Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:X) | Unknown (RC:U) | Reasonable (RC:R) | Confirmed (RC:C)

Environmental Score Metrics

Exploitability Metrics

Attack Vector (MAV)

Not Defined (MAV:X) | Network (MAV:N) | Adjacent Network (MAV:A) | Local (MAV:L) | Physical (MAV:P)

Attack Complexity (MAC)

Not Defined (MAC:X) | Low (MAC:L) | High (MAC:H)

Privileges Required (MPR)

Not Defined (MPR:X) | None (MPR:N) | Low (MPR:L) | High (MPR:H)

User Interaction (MUI)

Not Defined (MUI:X) | None (MUI:N) | Required (MUI:R)

Scope (MS)

Not Defined (MS:X) | Unchanged (MS:U) | Changed (MS:C)

Impact Metrics

Confidentiality Impact (MC)

Not Defined (MC:X) | None (MC:N) | Low (MC:L) | High (MC:H)

Integrity Impact (MI)

Not Defined (MI:X) | None (MI:N) | Low (MI:L) | High (MI:H)

Availability Impact (MA)

Not Defined (MA:X) | None (MA:N) | Low (MA:L) | High (MA:H)

Impact Subscore Modifiers

Confidentiality Requirement (CR)

Not Defined (CR:X) | Low (CR:L) | Medium (CR:M) | High (CR:H)

Integrity Requirement (IR)

Not Defined (IR:X) | Low (IR:L) | Medium (IR:M) | High (IR:H)

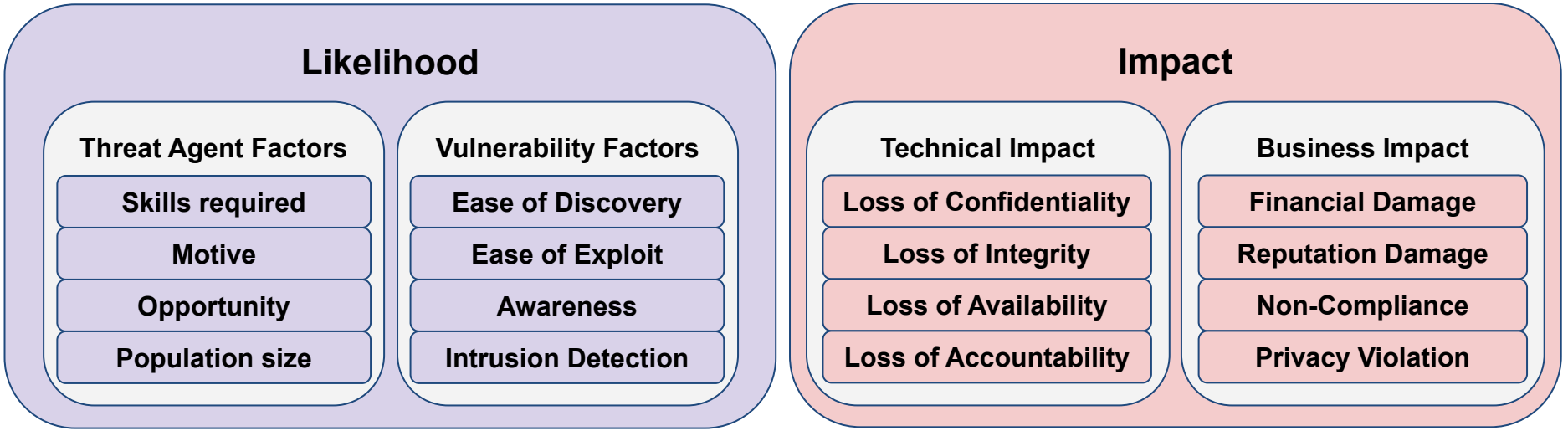
Availability Requirement (AR)

Not Defined (AR:X) | Low (AR:L) | Medium (AR:M) | High (AR:H)

Threat-focused risk scoring: OWASP Risk Rating Methodology

How?

- For each identified risk, assign a **score per factor**.
- Calculating the **average score of impact and likelihood** per risk as the **risk score**,
- The **overarching system/application risk score** may inherit the highest calculated risk score associated with it, depending on the risk appetite.



Threat-focused risk scoring: OWASP example

Likelihood factors

Threat Agent Factors

Skills required	Security penetration skills [1]
Motive	Possible reward [4]
Opportunity	Some access or resources required [7]
Population Size	Anonymous Internet users [9]

Vulnerability Factors

Easy of Discovery	Difficult [3]
Ease of Exploit	Difficult [3]
Awareness	Hidden [4]
Intrusion Detection	Logged without review [8]

Score

Impact factors

Technical Impact Factors

Loss of confidentiality	Extensive non-sensitive data disclosed [6]
Loss of Integrity	Minimal seriously corrupt data [3]
Loss of Availability	Extensive primary services interrupted [7]
Loss of Accountability	Attack fully traceable to individual [1]

Business Impact Factors

Financial damage	Significant effect on annual profit [7]
Reputation damage	Minimal damage [1]
Non-Compliance	Clear violation [5]
Privacy violation	Hundreds of people [5]

Score

Overall Risk Severity = Likelihood x Impact

	Impact		
Likelihood	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	Critical

Q&A

Thanks

Appendix

Resources

Threat modeling

- Definition of threat modeling
- Threat Modeling: 12 Available Methods
- STRIDE
  - The STRIDE per Element Chart
  - STRIDE-per-Interaction
- Security Cards: A Security Threat Brainstorming Kit
- How Well Do You Know Your Personae Non Gratae?
- Attack Trees
- hTMM: A Hybrid Threat Modeling Method
- PASTA Risk-centric Threat Modeling
- QTMM: Software and attack centric integrated threat modeling for quantitative risk assessment
- LINDDUN
- Trike

Additional threat modeling resources:

- VAST modeling
- Cybersecurity Threat Modeling with OCTAVE

Resources

Threat-focused risk scoring

- DREAD (risk assessment model)
- Application Threat Modeling using DREAD and STRIDE
- CVSS (v3.1 Specification Document)
- CVSS calculator - Vulnerability Metrics
- CVSS Calculator example
- Introduction and implementation OWASP Risk Rating Management
- OWASP risk calculator