DOI: https://doi.org/10.30837/csitic52021232185

# Measuring Vulnerability in Threat Modeling With Risk Matrix

Andrii Hapon[1],
Volodimir Fedorchenko[2]

[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: gapon.andrei@gmail.com
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: volodymyr.fedorchenko@nure.ua

***Abstract.*** *Threat modeling is one of the most important parts when it comes to security in development of programing product. The main challenges for that are time and prioritization of the scope of work. Risk matrix is effective tool for making clear what should be done first and which consequences can be. There are few levels of consequences which are ranged by the influence on business. With help of vulnerability assessment threats can be measured by impact on confidentiality, integrity, and availability. The Common Vulnerability Scoring System is appropriate tool for catching the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.*

***Keywords:*** *Threat modeling; CVSS; Likelihood; Attack Vector; Metrics.*

## I. THREATS MODELING

Threat modeling deployed across the customer journey and user experience flows typically uses an informal, creative process that leads to "misuse" and "attacker stories" - business risks.

Threat modeling for a technical project and its data flows leads to a more mechanical approach, which leads to specific design changes and technical security measures [1].

Estimated Barriers to Threat Modeling:

- Time. Threat modeling is a time-consuming process and is the most expensive product in a software development team.
- Prioritization. Security and privacy are two aspects that developers should consider. It also needs to address issues of architectural and technical debt management, performance, operational cost optimization, service design, and bug fixing.

Fortunately, there is an elegant way to solve both problems.

Software teams manage their work through tickets (or backlog items). If the task is framed in the form of a ticket, then its implementation has become an obvious and obvious necessity. This need can then be balanced and prioritized over all other paid work.

Security work is traditionally not included in separate tickets. Rather, it remains a set of safety requirements and guides, general acceptance criteria, or, indeed, a set of vague non-functional constraints. This became a problem when teams were faced with tight deadlines and functional pressures because - although there were rules - there was no clear allocation of time.

By making threat modeling (and all other manual security actions) visible as development tickets, you can track the distribution of time. The analysis and suggested remedial actions also become tickets in and of themselves. Consequently, safety is prioritized by taking a seat at the table when discussing business priorities.

Probabilities and Consequences for Business

Risk is defined as the possibility of loss, damage, or destruction something of value (information, reputation, finances, etc). Risk is expressed as multiplication of an attack likelihood on possible business impact. Risk assessment is a process of identification of risks for valuable business and functional assets and determining their severity. Results of risk assessment are business security requirements that mitigate identified business risks [2].

| | | Consequence | | |
|---|---|---|---|---|
| | | *Minor Business Impact* | *Moderate Business Impact* | *Major Business Impact* |
| Likelihood | *Very Likely* | MEDIUM | HIGH | HIGH |
| | *Likely* | MEDIUM | MEDIUM | HIGH |
| | *Possible* | LOW | MEDIUM | HIGH |
| | *Unlikely* | LOW | LOW | LOW |

Figure 1. Business priorities

The likelihood can be expressed as the level of motivation of the malicious user (anonymous user, authenticated user, administrator, employee, etc.) and the abilities that he possesses. Motivating a threat agent to attack company assets

Potential business consequences should be considered: impact on reputation, loss of business due to loss of customer confidence, business interruption, financial losses - cost of recovery, forensic investigation, lost income, possible fines / penalties [3].

Table 1. Consequence's level

| Consequence | Description |
|---|---|
| **Minor** | Slight loss of assets, no change in the way of doing business. |
| **Moderate** | Moderate changes in the way we do business. Serious adverse impact on the organization's operations, the assets of the organization, or individuals. |
| **Major** | Going out of business if countermeasures are not immediately taken. Serious or catastrophic adverse impact on the organization's operations, the organization's assets, or individuals. |

## II. VULNERABILITY ASSESSMENT

The impact metrics capture the effects of a successfully exploited vulnerability on the component that suffers the worst

outcome that is most directly and predictably associated with the attack. Analysts should constrain impacts to a reasonable, final outcome which they are confident an attacker is able to achieve.

Only the increase in access, privileges gained, or other negative outcome as a result of successful exploitation should be considered when scoring the Impact metrics of a vulnerability [4].

Table 2. Impact indicators

| | |
|---|---|
| **Impact on confidentiality (C)** | This metric measures the confidentiality impact of information resources managed by a software component due to a successfully exploited vulnerability. |
| **Impact on integrity (I)** | This metric measures the integrity impact of a successfully exploited vulnerability. Honesty refers to the reliability and accuracy of information. |
| **Impact on availability (A)** | This metric measures the impact on the availability of an affected component as a result of a successfully exploited vulnerability. |

The Common Vulnerability Scoring System (CVSS) is an open schema that allows the exchange of information about vulnerabilities. Each metric is a number (score) in the range from 0 to 10, and a vector is a short textual description with values that are used to derive the score [5].

Table 3. Baseline assessment indicators

| | |
|---|---|
| **Attack vector (AV)** | This metric reflects the context in which a vulnerability can be exploited. This metric value (and therefore the baseline score) will be the greater the more remote (logically and physically) an attacker can be to exploit the vulnerable component. |
| **Attack Difficulty (AC)** | The Attack Severity metric describes the attacker-independent conditions that must exist to exploit a vulnerability. As described below, such conditions may require the collection of additional target information, the presence of certain system configuration parameters, or computational exceptions. " |
| **Required Privileges (PR)** | This metric describes the level of privilege that an attacker must have to successfully exploit the vulnerability. " |
| **User interaction (UI)** | This metric reflects a requirement for a non-attacker user to participate in the successful compromise of a vulnerable component. This metric determines whether a vulnerability can be exploited solely at the request of an attacker, or whether an individual user (or a process initiated by a user) must be involved in some way. |
| **Volume (S)** | The ability of a vulnerability in one software component to affect resources beyond its capabilities or privileges. |

c

CVSS is accepted as the primary method for quantifying the severity of vulnerabilities across a wide range of organizations and companies.

REFERENCES


[1] OWASP [Electronic resource]. – https://owasp.org/www-community/Application_Threat_Modeling

[2] Hubbard, Douglas W.; Seiersen, Richard (2016). How to Measure Anything in Cybersecurity Risk. Wiley. pp.

[3] Science direct [Electronic resource]. – https://www.sciencedirect.com/topics/engineering/consequence-category

[4] Balbix [Electronic resource]. – https://www.balbix.com/insights/base-cvss-scores/

[5] First [Electronic resource]. – https://www.first.com