Unit 3: Introduction to Threat Modelling and Management.

The terms vulnerability and threat are often used in information security and the difference between the terms are important to allow the organisation to correctly implement, document and assess information security activities and controls.

Different between vulnerability and threat

A vulnerability is a weakness in a system, system security procedures, internal controls, or implementation that could triggered by a threat source as explained by NIST SP 1800-17b. Other sources, defines vulnerability in Information technology as a flaw in code or design that creates a potential point of security compromise for an end or network, meaning that vulnerabilities create possible attack vectors (Tech Target contributor) and it also be defined as the weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system and after exploiting a vulnerability, a cyberattack can run malicious code, install malware and even steal sensitive data(Tunggal .A,2023). All vulnerabilities are managed based on a threat assessment.

A threat is defined as: "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability." FIPS 200 under THREAT from CNSSI 4009 - Adapted NIST SP 1800-15B under Threat from FIPS 200 (NIST, 2022). Threat is risk-based and measured by a risk management process - i.e., it is evaluated and classified as accept, avoid, control, transfer, or monitor.

Threat Management Models:

Threat modelling should be performed early in the development cycle, and it means that potential challenges can be caught early and remedied, preventing a much costlier fix down the line (Shevchenko et al, 2018). An early application of the principles allows architectural decisions that can reduce both vulnerabilities and the threat attack surface. The Threat Modelling is a structured representation of all information that affects the security of an application, and it can be applied to range of things like software, applications, systems, networks, internet of Things (IoT) devices and business process (Drake.V).

The Microsoft Threat Modelling requires six step process that:

1. Asset identification (Web-site, IT Applications, Datacenters, data base, employées).
2. Create an architecture overview of the system (dataflow, external factors &Boundaries etc).
3. Decompose the application (identify the vulnerabilities points).
4. Identification of Threat (using risk assessment frameworks like STRIDE).
5. Documentation of identified vulnerabilities and threats
6. Rate the Threats (Using DREAD assessment framework).

Threat modelling Techniques include STRIDE and DREAD, Attack Trees, PASTA, OWASP, CVSS, Octave, Open FAIR, Kill Chain and Mitre Attack. Few of the modelling will be explained.

- **Explanations of STRIDE:**

  Spoofing: This is where the attackers pretend to be someone else (impersonation).

  Tampering: The attacker modifies the targeted asset from its original state.

  Repudiation: The ability of a user or system to deny having performed a particular action (false identity, manipulation of log or deletion of evidence).

  Information Disclosure: Attacker gets access to unauthorised information i.e., confidential, and sensitive data.

  Denial of Service: Attacker prevents authorised users to have access to a system (making a system unavailable).

  Elevation of Privileges involves an increased privileged access beyond a certain level by an attacker i.e., higher level of privileged access.

Match of threats with the tenet it affects:

S/N	Threats	Violated Property
	Spoofing	Authentication
	Tampering	Integrity
	Repudiation	Non-Repudiation
	Information Disclosure	Confidentiality
	Denial of Service	Availability
	Elevation of Privilege	Authorization

- **Dread** is a framework associating with evaluation and threat rating and the meaning of the acronym is:

  Damage potential measures the amount of damage an attack will have on a system.

  Reproducibility: This the ability to simply replicate an attack

  Exploitability: how easy is a successful attack on vulnerabilities points

  Affected user: How many people will be affected by the threat.

  Discoverability: This factor rates the discoverability of the vulnerabilities

The risk effects are ranked on scale of 0-10 and summed up. The higher the risk of a potential attack on the enterprises, the urgent a mitigation is required to be deployed.

CVSS (Common Vulnerability Scoring System) is referred as a key metric for cybersecurity according to NIST and it is an open framework for communicating the characteristics and severity of software vulnerabilities. The two common uses of CVSS are in calculating the severity of vulnerabilities discovered in a system and as a factor in prioritization of vulnerability remediation activities and the National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

Attack tree: is structure built to analyse different security threats using different paths to achieve the attack goal, as well as enumerating the threat and the malicious users' methods for achieving their goal. Elementary attacks are placed at the leaf level, and primary attacks are placed at the root. The non-leaf part of the trees are the internal nodes representing a combined attack of the elementary nodes in the next higher level. These can be combined by either conjunctive aggregation (AND nodes) or disjunctive (OR nodes). (Mauw & Oostdijk, 2005).

OCTAVA FORTE: This leverages on Enterprise Risk Management (ERM) principles to identify security risk and the business formulate strategic objective.It is a risk assessment method that focus on speed, efficiency of a business.

PASTA (**P**rocess for **A**ttack **S**imulation and **T**hreat **A**nalysis) is a risk-centric threat modelling framework, proposed by Tony UcedaVélez in 2012 *(Wolf et al, 2020).* Wolf et al (2020) use the model to perform a threat and risk analysis on an IOT system. PASTA recommends the use of other frameworks alongside and integrated with its own methodology e, g use of attack trees and the STRIDE/DREAD methodology alongside PASTA and it encourages use hybrid methodology to assess a threat.

Reference:

Drake.v, (ND), OWASP. Threat Modelling, Available from: https://owasp.org/www-community/Threat_Modeling [Accessed 27 August 2023].

NIST Information Technology Laboratory COMPUTER SECURITY RESOURCE CENTER, Vulnerability, Available from: https://csrc.nist.gov/glossary/term/vulnerability[Accessed 29 August 2023].

Shostack.A. (2014) Threat Modelling : Designing for Security. Available from:https://ebookcentral.proquest.com/lib/universityofessex-ebooks/detail.action?docID=1629177&pq-origsite=primo[Accessed 26 August 2023],

TechTarget Contributor, vulnerability (information technology),Available from: https://www.techtarget.com/whatis/definition/vulnerability#:~:text=A%20vulnerability%2C%20in%20information%20technology,access%20a%20target%20system's%20memory [Accessed 28 August 2023].

Tunggal. A, (2023), UpGuard, what is a Vulnerability? Definition + Examples. Available from:https://www.upguard.com/blog/vulnerability [Accessed 25 August 2023].

University Essex Lecture Cast unit 3. Introduction to Threat Modelling and

Management, Available from: https://www.my-

course.co.uk/Computing/Cyber%20Security/SRM/SRM%20Lecturecast%202/conten

t/index.html#/ [Accessed 25 August 2023].