Unit 2: Threat Modelling Exercises

1. **Describe where to find the essential tools and resources used for threat modelling.**

A threat modelling tool proactively identifies and resolves possible security threats to your software, data, or device. It is crucial in today's online world, as hackers always look for vulnerabilities. Threat modelling involves asking critical questions about business goals, potential threats, rectification plans, and prevention in the future. It can be resource-intensive, so using a threat modelling tool makes sense (Mohanakrishnan, 2021). For instance, here are the top 10 threat modelling tools according to Kirvan (2023):

- **CAIRIS**: an open-source tool that creates attacker personas and identifies attack patterns.
- **Cisco Vulnerability Management**: a SaaS tool that generates real-time threat intelligence and recommended risk-based actions.
- **IriusRisk**: a tool that analyses and models software application risks during the design phase.
- **Microsoft Threat Modeling Tool**: free, open-source software that uses the STRIDE methodology to create threat models for Windows-based applications and systems running on Microsoft Azure cloud services.
- **OWASP Threat Dragon** is a free, cross-platform tool for creating DFDs and delivering threat lists, recommendations, and reports.
- **SD Elements**: a tool that automates the identification of threats and vulnerabilities through surveys and extensive reporting and testing capabilities.
- **Splunk Enterprise Security**: a tool that uses AI and machine learning to assess an organisation's technology architecture and identify potential threats.
- **Threagile**: an open-source, code-based tool for Agile environments that produces DFDs and detailed reports.
- **ThreatModeler**: an automated tool for large organisations with complex technology infrastructures.
- **Tutamen Threat Model Automator**: a cloud-based tool for security development that supports inputs from Visio and Excel and delivers flexible reports.

According to Drake (2022), threat modelling is a process that identifies, communicates, and understands threats and mitigations to protect something of value. It can be applied to software, applications, systems, networks, and business processes. The

process involves capturing, organising, and analysing information to make informed decisions about application security risks. A prioritised list of security improvements is also produced. The Threat Modeling Manifesto contains values, principles, patterns, and anti-patterns to facilitate the adoption of threat modeling.

As per Kopriva's (2019) notes on methodologies and best practices for Threat Modeling, below are some of the resources used:

- **Attack trees** are charts showing the path of attacks in a system. They display attack goals as a root with possible paths as branches. This threat modeling technique is widely used and often included in internal data flow and system interoperability reviews. It's usually combined with other methodologies like PASTA, CVSS, and STRIDE (Gonzalez, 2020).

- **The DREAD** threat modelling approach is used to detect and prioritise threats. It was developed by Microsoft and published in 2002. DREAD stands for Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability. These factors are ranked on a scale of 0-10, and the sum of these values determines the risk of a potential attack. The higher the value, the greater the risk and mitigation strategies must be employed immediately (Manikandan, 2023).

- **LINDDUN** is the ultimate privacy threat modelling framework developed by top privacy experts at KU Leuven. It provides a robust and reliable support system to swiftly identify and mitigate privacy threats at the earliest stages of the development lifecycle. Adopting LINDDUN is necessary for building a privacy-driven system core (Linddun, N.D.).

- **OCTAVE** is a risk-based assessment and planning technique for security that helps organisations understand their information security needs. It is self-directed and flexible, allowing organisations to prioritise areas of improvement and set their security strategy based on risks to the most critical assets. OCTAVE is targeted at organisational risk and focused on strategic, practice-related issues. It enables an organisation to make information-protection decisions based on risks to confidentiality, integrity, and availability of critical information-related assets (Alberts et al. 2003).

- **Process for Attack Simulation and Threat Analysis (PASTA)** is an attacker-centric methodology with seven steps that guide teams in identifying, counting, and prioritising threats. It correlates business objectives with technical requirements, including defining business objectives and scope, identifying application controls, vulnerability detection, attack modelling, and risk analysis (Gonzalez, 2020).

- **STRIDE** is a threat model created by Microsoft to identify system threats. It covers Spoofing, Tampering, Repudiation, Information Disclosure, and Denial of the system's model and is effective for evaluating individual systems (Gonzalez, 2020).

- **CARVER** is a methodology that assesses the probability of an attack on infrastructure assets or critical resources. It was developed for the US military and uses a numerical ranking matrix to identify vulnerable components.

- **Trike** is a security audit framework that uses threat modeling techniques to manage risk and defence. Analysts enumerate a system's assets, actors, rules, and actions to build a requirement model. Trike generates a step matrix with columns representing the assets and rows representing the actors. It also assesses attack risks using a five-point probability scale for each CRUD action and actor (Gonzalez, 2020).

- **Visual, Agile, and Simple Threat (VAST**) is an automated threat modelling method built on the ThreatModeler platform. It can help large enterprises generate reliable, actionable results, maintain scalability and integrate into the DevOps lifecycle. Two threat models are created: the application and operational threats (Gonzalez, 2020).

- **The NIST Guide to Data–Centric System Threat Modeling (SP 800-154)** offers essential data-centric system threat modelling guidance. This effective risk assessment technique models the attack and defence aspects of data within a system. This guide is a must-have for organisations that seek to incorporate this methodology into their risk management processes. The publication clearly outlines the core principles that must be a part of any reliable data-centric system threat modelling methodology (Souppaya & Scarfone, 2016).

- **MITRE ATT&CK** is a framework that lists tactics, techniques, and procedures used by threat actors in attacks. By aligning an organisation's potential attack surface with the framework, possible gaps in their defences can be identified, and countermeasures can be prioritised accordingly (MITRE, 2023).

References:

- Mohanakrishnan, R. (2021). *Top 10 Threat Modeling Tools in 2021*. [online] Available at: https://www.spiceworks.com/it-security/vulnerability-management/articles/top-threat-modeling-tools/.
- Kirvan, P. (n.d.). *Top 10 threat modeling tools, plus features to look for | TechTarget*. [online] Available at: https://www.techtarget.com/searchsecurity/tip/Top-threat-modeling-tools-plus-features-to-look-for.
- Drake, V. (2022). *Threat Modeling | OWASP*. [online] owasp.org. Available at: https://owasp.org/www-community/Threat_Modeling.
- Kopriva, J. (2019). *Resources and Tools*. [online] Untrusted Network. Available at: https://untrustednetwork.net/en/csirt/ [Accessed 11 Mar. 2024].
- Gonzalez, C. (2020). *6 Threat Modeling Methodologies: Prioritize & Mitigate Threats*. [online] Exabeam. Available at: https://www.exabeam.com/information-security/threat-modeling/.
- Manikandan, J. (2023). *DREAD Threat Modeling Methodology*. [online] Practical DevSecOps. Available at: https://www.practical-devsecops.com/dread-threat-modeling/.
- Linddun (N.D.). *PRIVACY THREAT MODELING*. [online] Available at: https://linddun.org/.
- Alberts, C., Dorofee, A., Stevens, J. & Woody, C. (2003). *Introduction to the OCTAVE ® Approach*. [online] Available at: https://www.itgovernance.co.uk/files/Octave.pdf.
- Deming, W. E. (N.D.). *The Counter-Espionage for Business Travellers Online Training Course*. [online] Available at: https://www.smiconsultancy.com/carver-target-analysis [Accessed 11 Mar. 2024].
- Souppaya, M. & Scarfone, K. (2016). *Guide to Data-Centric System Threat Modeling*. [online] csrc.nist.gov. Available at: https://csrc.nist.gov/pubs/sp/800/154/ipd.
- MITRE (2023). *MITRE ATT&CK™*. [online] Mitre.org. Available at: https://attack.mitre.org/.