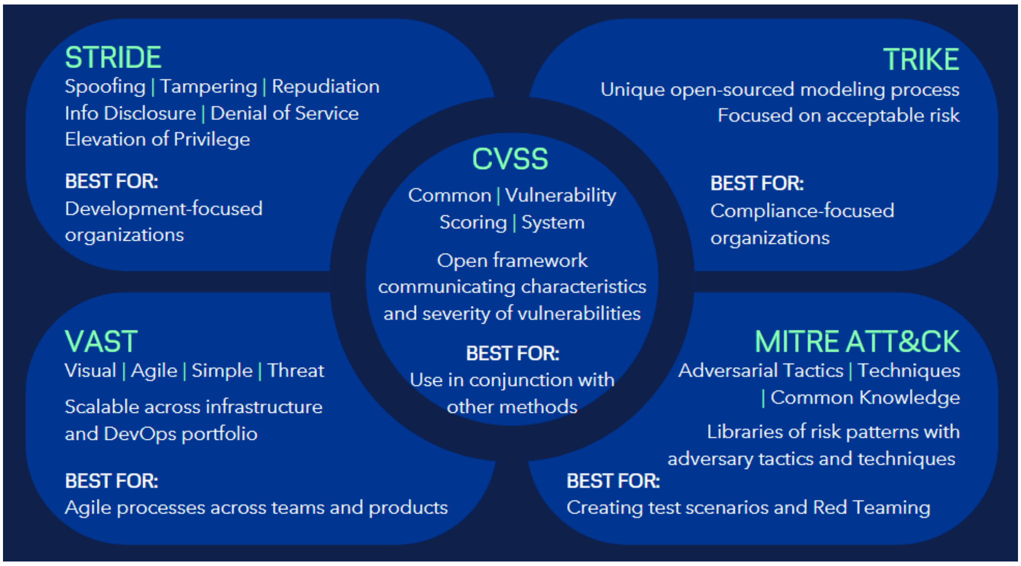
Unit 3: Introduction to Threat Modelling and Management

1. Describe a number of threat modelling techniques.

Threat modelling is crucial for building a robust cybersecurity culture. It involves identifying potential security risks before development begins. This process can and should be scaled for projects of any size involving experts and non-experts alike. Different techniques are used to answer the four fundamental questions. However, threat modelling is at its core about keeping things simple, focusing on people and collaboration, and continuously refining the process to ensure that your systems and data remain as secure as possible (Veracity, N.D.).



STRIDE
Spoofing | Tampering | Repudiation
Info Disclosure | Denial of Service
Elevation of Privilege

BEST FOR:
Development-focused organizations

TRIKE
Unique open-sourced modeling process
Focused on acceptable risk

BEST FOR:
Compliance-focused organizations

CVSS
Common | Vulnerability Scoring | System

Open framework communicating characteristics and severity of vulnerabilities

BEST FOR:
Use in conjunction with other methods

VAST
Visual | Agile | Simple | Threat

Scalable across infrastructure and DevOps portfolio

BEST FOR:
Agile processes across teams and products

MITRE ATT&CK
Adversarial Tactics | Techniques | Common Knowledge

Libraries of risk patterns with adversary tactics and techniques

BEST FOR:
Creating test scenarios and Red Teaming

(Veracity, N.D.).

According to Tatam et al. (2021), Threat Modelling (TM) is a crucial process that systematically identifies potential security vulnerabilities and risks so that they can be addressed in a targeted and effective manner. By modelling threats, we can proactively identify, classify, and describe them, empowering us to take proactive measures to mitigate them. TM is a non-negotiable aspect of effective security management and should be a top priority for any organisation serious about protecting its assets and reputation.

Furthermore, OWASP (N.D.) highlights that threat modeling is a security process used to identify applicable threats on a particular system and determine responses to these threats. It should be performed early in the SDLC and maintained alongside the system. It should be integrated into the team's normal SDLC process. For instance, here are some popular methods and techniques:

1.1. **The STRIDE** technique is a reliable security framework that uses six core concepts to identify potential threats in a system. These concepts are Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. The flexible framework helps prioritise risks, shows potential attack vectors, and reduces breaches. However, it can be resource-intensive, provides a static analysis, and needs constant maintenance. It should not be considered a replacement for security testing, as it demands expertise and may not address non-technical threats (Allen-Addy (2023).

1.2. **VAST** is the ultimate automated threat modelling method for large enterprises to identify and eliminate infrastructural and operational concerns. It requires the creation of two types of threat models: an application threat model and an operational threat model. VAST is a powerful solution that supports exponential growth by enabling self-service threat modelling through automation, integration, and collaboration (SmartState.tech, 2022).

1.3. **Trike** is a robust security audit framework that uses cutting-edge threat modelling techniques to manage risk and defence. The framework empowers analysts to build a comprehensive requirement model that generates a step matrix with columns representing assets and rows representing actors. With Trike, the analysts can assess attack risks using a five-point probability scale for each CRUD action and actor and evaluate actors based on their permission level for each action. Trike's powerful data-flow diagramming capabilities map each element to the appropriate assets and actors, enabling analysts to quickly identify and mitigate potential denial of service and privilege escalation threats (Gonzalez, 2020).

1.4. **The MITRE ATT&CK** framework is a comprehensive library of attack methods threat actors use. By mapping an organisation's potential attack surface against it, organisations can identify possible gaps in their defences and prioritise the development of countermeasures. Organisations should identify potential threats and attack vectors to use the framework effectively, map them to the MITRE ATT&CK framework, develop countermeasures, and continuously monitor and refine defences (CyberGeek, 2023).

1.5. **The Common Vulnerability Scoring System (CVSS)** is a highly effective method that captures a vulnerability's essential characteristics and assigns a numerical score, ranging from 0-10, with ten being the worst, to indicate its severity. This score is then translated into a qualitative representation such as Low, Medium, High, and Critical. Such representation helps organisations assess vulnerabilities more efficiently and prioritise their vulnerability management processes for optimal results (Simplilearn, 2024).

2. Advise which technique should be used in specific situations.

Threat modelling is an essential responsibility for every cybersecurity team. It involves proactively identifying potential risks and threats, working through various scenarios, response models, and other forms of threat detection to safeguard an organisation and its assets (Ledesma, 2023). However, choosing the proper framework or method is crucial. Factors like industry, security department size, available resources, and the organisation's makeup should be considered.

For beginners, data flow diagrams, STRIDE, and kill chains are the three most common threat modelling techniques and methodologies, according to Shostack (N.D.). These structured processes are fast, cost-effective, and an excellent starting point. As you gain more experience, you should adjust your techniques to suit your needs. Combining security and privacy threats can save time and improve the value of your investment.

According to Shevchenko (2018), Attack trees help assess the security of complex systems by building them for each component instead of the entire system. This approach can assist administrators in making informed security decisions, evaluating system vulnerability to attacks, and examining specific types of attacks. Attack trees are often used with other techniques in frameworks such as STRIDE, CVSS, and PASTA.

Allen-Addy (2023) underscores that TRIKE is not just another threat modelling process but an efficient one that ensures effective risk management and defence. The process involves assigning likelihood and impact scores to each asset, which empowers users to prioritise mitigation efforts. TRIKE ensures that the risk associated with each asset is acceptable to stakeholders and facilitates coordination and collaboration. With TRIKE, users can easily enumerate and assign a risk value, create security controls or preventive measures to address threats and use visual models to represent threat scenarios, providing a robust framework for comprehensive risk management.

Threat modelling is crucial in identifying and prioritising mobile app security risks (Halder, 2023). To do this, build a cross-functional team and use Microsoft's threat identification models. Perform a code and configuration review to ensure controls are in place. Use DREAD or STRIDE methods to prioritise risks. When mobile app threat modelling, decompose the app, identify and rank threats, and determine countermeasures. Define the scope clearly, create a visual understanding, model attack possibilities, ask the right questions, track weak controls, and update the threat model.

3. Discuss when techniques should be combined in a hybrid model.

Modern software systems are vulnerable to attacks that impair functioning or expose confidential information. Such security breaches frequently appear in the news, affecting cyber-physical systems, transportation systems, self-driving cars, and more. Therefore, it is essential to adopt a systematic approach to developing any public-facing system that analyses security needs and documents mitigating requirements (Mead & Shull, 2018).

The Hybrid Threat Modeling Method (hTMM) is a security methodology that combines two other methodologies, Security Quality Requirements Engineering (SQUARE) and Persona non grata (PnG). hTMM identifies all possible threats, eliminates false positives, maintains consistent results, and is cost-effective. It uses Security Cards to identify potential threats, eliminates unlikely PnGs, summarises results, and assesses risk using SQUARE. By combining these methodologies, hTMM provides an efficient way to identify and prioritise security requirements, uncover vulnerabilities, and evaluate risk (Gonzalez, 2020).

Krishnan (2017) notes that adopting a hybrid model that combines the strengths of different techniques is essential when performing threat modelling. This approach leads to a more comprehensive and effective threat modelling exercise. To achieve this, it is important to prioritise a structured approach, optimum detail, and readability. A structured approach involves adopting a suitable software development lifecycle model, which provides a solid foundation for the exercise. Optimum detail ensures that software developers, architects, and testers can easily understand and interpret the information presented. On the other hand, readability involves presenting data in the most effective way possible to simplify the exercise.

Thus, the threat modelling process includes design analysis, threat identification, establishing trust boundaries, identifying threat actors, and identifying the attack surface. It is crucial to categorise threats and use the STRIDE technique. Categorising threats helps determine the appropriate countermeasures for a given scenario, even if threats overlap multiple categories. The STRIDE technique is a widely used threat identification and categorisation method valuable in your threat modelling arsenal. Lastly, the exercise should be documented using an appropriate template to ensure its effectiveness and reproducibility.

References:

- Veracity (N.D.). *The importance of threat modeling*. [online] Available at: https://www.veracity.com/article/cyber-security-importance-of-threat-modeling.
- Tatam, M., Shanmugam, B., Azam, S. and Kannoorpatti, K. (2021). A review of threat modelling approaches for APT-style attacks. *Heliyon*, 7(1), p.e05969. doi:https://doi.org/10.1016/j.heliyon.2021.e05969.
- OWASP (N.D.). *Threat Modeling*. [online] cheatsheetseries.owasp.org. Available at: https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html.
- Allen-Addy, C. (2023). *Threat Modeling Methodology: STRIDE*. [online] Available at: https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride.
- SmartState.tech (2022). *Threat Modeling Methodology: VAST*. [online] Medium. Available at: https://smartstatetech.medium.com/threat-modeling-methodology-vast-5c7de64cd924.
- Gonzalez, C. (2020). 6 Threat Modeling Methodologies: Prioritize & Mitigate Threats. [online] Exabeam. Available at: https://www.exabeam.com/information-security/threat-modeling/.
- CyberGeek (2023). *CMS Information Security & Privacy Group*. [online] Available at: https://security.cms.gov/posts/how-use-mitre-attck-conjunction-threat-modeling.
- SImplilearn (2024). *What is Threat Modeling: Process and Methodologies*. [online] Simplilearn.com. Available at: https://www.simplilearn.com/what-is-threat-modeling-article.
- Ledesma, J. (2023). *What is Threat Modeling and How To Choose the Right Framework*. [online] Available at: https://www.varonis.com/blog/threat-modeling.
- Shostack (N.D.). *The Ultimate Beginner's Guide to Threat Modeling*. [online] Available at: https://shostack.org/resources/threat-modeling.
- Shevchenko, N. (2018). *Threat Modeling: 12 Available Methods*. [online] SEI Blog. Available at: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/.
- Halder, S. (2023). *Mobile App Threat Modeling and Security Testing*. [online] www.appknox.com. Available at: https://www.appknox.com/blog/mobile-app-threat-modeling-and-security-testing.
- Mead, N. R. & Shull, F, (2018). *The Hybrid Threat Modeling Method*. [online] Available at: https://insights.sei.cmu.edu/blog/the-hybrid-threat-modeling-method/.
- Krishnan, S (2017). *A Hybrid Approach to Threat Modelling A Hybrid Approach to Threat Modelling.* [online] www.appknox.com. Available at: https://www.researchgate.net/publication/320183133_A_Hybrid_Approach_to_Threat_Modelling_A_Hybrid_Approach_to_Threat_Modelling/citations.