Unit 4 Seminar Preparation - Threat Modelling Exercises:

The threat model based on a large international bank based in the UK:

“Threat modelling is the key to a focused defense. Without threat modelling, you can never stop playing whack-a-mole.” — (Adam Shostack 2014)

Teams that evaluate platforms and applications for threats employ methods akin to pen testers. Typically, internal AppDev, DevOps, and SecOps teams handle threat modelling. Pen testers, on the other hand, are often an external third party with experience in engaging in ethical hacking.

OWASP A method for gathering, compiling, and evaluating all of this data is called threat modelling. This applied to risk assessment software. A prioritised list of security enhancements to the idea, specifications, design, or implementation of an application is also typically produced by threat modelling activities. (Adam Shostack 2014)

Collaboration between the threat modelling team and the pen testers that is accomplished during the same agile sprints could be part of the first level of engagement. A third-party white-hat pen tester could be a member of this team when choosing the team for the threat modelling, establishing the scope, and documenting the predicted threats. In white-hat pen engagements, the AppDev and pen tester frequently collaborate to establish the engagement's full extent. Usernames and passwords, IP addresses of the targeted hosts, and the expected testing criteria are typically made available to the white-pen tester. A more thorough 360-degree picture would result from forming a partnership between a white-hat third-party tester and the

internal threat modelling team. The results of threat modelling without collaboration would be based only on internal resource knowledge. The results of the threat modelling will be much more valuable with both parties' involvement and experience if there is an independent third-party pen tester. (Nataliya Shevchenko, Timothy A. Chick, Paige O'Riordan, Thomas Patrick Scanlon, & Carol Woody, 2018)

Collaboration between a threat modelling team and a black-hat pen tester would constitute the second level of engagement. The black-hat tester wouldn't have any prior knowledge of the platform or application during this collaboration engagement. Instead of AppDev, DevOps, and NetOps, SecOps would be the internal sponsor of this engagement.

Threat modelling, white-hat, and black-hat pen testers will compare notes if the black-hat pen team finds vulnerabilities to determine whether either party found the same security issue or a different one. The results from the white-hat, black-hat, and threat modelling teams should all be combined into the MITRE attack portal for full sprint engagement. This portal functions as a combined platform for threat modelling and analysis of actual attacks from both pen-testing operations. In addition to providing direction on how to reduce the potential risk using a combination of detection and mitigation techniques, this consolidation can help to ensure that a prospective and real danger are correctly identified during threat modelling. (J. Spring, E. Hatleback, A. Householder, A. Manion and D. Shick, 2021)

References:

Adam Shostack, "Threat Modeling: Designing for Security" Wiley Publication; February 2014

Nataliya Shevchenko, Timothy A. Chick, Paige O'Riordan, Thomas Patrick Scanlon, PhD, & Carol Woody, PhD, "THREAT MODELING: A SUMMARY OF AVAILABLE METHODS" Carnegie Mellon University; July 2018

J. Spring, E. Hatleback, A. Householder, A. Manion and D. Shick, "Time to Change the CVSS?," in IEEE Security & Privacy, vol. 19, no. 2, pp. 74-78, March-April 2021, doi: 10.1109/MSEC.2020.3044475.