Tutorial: Threat Modeling of Cloud-based Solutions

Lotfi ben Othmane[1], Heinrich Gantenbein[2] Hasan Yasar[3], Simone Curzi[4], Altaz Valani[5], Arun Prabhakar[6], Robert Cuddy[7]
[1]University of North Texas, Denton, TX, USA
[2]Microsoft Industry Solutions (Consulting), St. Paul, MN, USA
[3] Carnegie Mellon University, Pittsburgh, PA, USA
[4] Microsoft Industry Solutions (Consulting), Perugia, Italy
[5]Security Compass, Toronto, ON, Canada
[6] Boston Consulting Group, Toronto, ON, Canada
[7] HCL Technologies, Aliso Viejo, CA, USA
e-mails: lotfi.benothmane@unt.edu, heinrich.gantenbein@microsoft.com, hyasar@cmu.edu, simone.curzi@microsoft.com, avalani@securitycompass.com, prabhakar.arun@bcg.com, robert.cuddy@hcl.com

I. The topic

The tutorial aims to train the participants to apply a threat modeling process to identify potential threats to given cloud-based systems and prioritize countermeasures.

II. Expected audience

Empirical studies showed that cybersecurity professionals are often familiar with common security activities, including network security, code analysis, vulnerability analysis, and penetration testing, but not familiar with threat modeling. The tutorial targets software security students, technical cybersecurity professionals, solution architects, and IT management professionals. The tutorial aims to train novices to threat modeling and to discuss advances to threat modeling with experts.

III. Learning outcomes

The main learning outcomes are:

1) Understand the value and importance of threat modeling,
2) Apply the threat modeling process and use the interviewing techniques,
3) Use Threats Manager Studio to create threat models to identify threats, define and prioritize mitigations, define residual risks and roadmaps,
4) Become familiar with threats applicable to systems based on cloud computing,
5) Become familiar with integrating threat modeling into DevOps.

IV. Tutorial format

The tutorial lasts for 180 minutes and includes four parts. It includes informative short lectures, a role-play session, and a practice exercise. The description of the parts are:

Prerequisites The participants shall download and install the tutorial Docker image containing Threats Manager Studio from DockerHub.

Introduction (30 min) Ben Othmane will start the tutorial. They will outline the threat modeling scenario for the tutorial including the components and various personas common to threat modeling.

Threat modeling process (45 min) Curzi and Gantenbein will talk about the Threat modeling process, depicted by Figure 1, which uses an expanded view that includes threat modeling (collect information, diagram, identify threats, select mitigations) and extends it with quantitative risk analysis, tracking of implementations to mitigations with DevOps, continuous learning and risk management [1].

Gantenbein and Curzi will take the discovery content from the role play to demonstrate the use of Threats Manager Studio (TMS) [2] to develop a sample threat model and generate the reports. Threats Manager Studio is an open-source threat modeling tool developed mainly

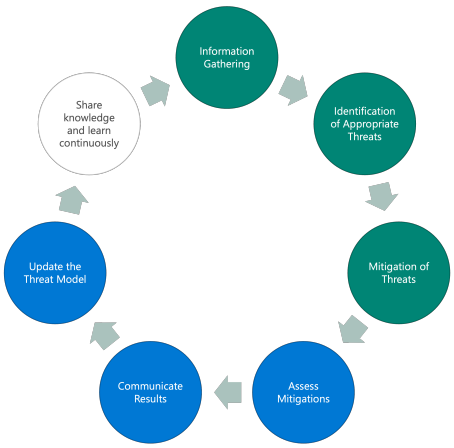

Fig. 1: Expendable threat modeling process.

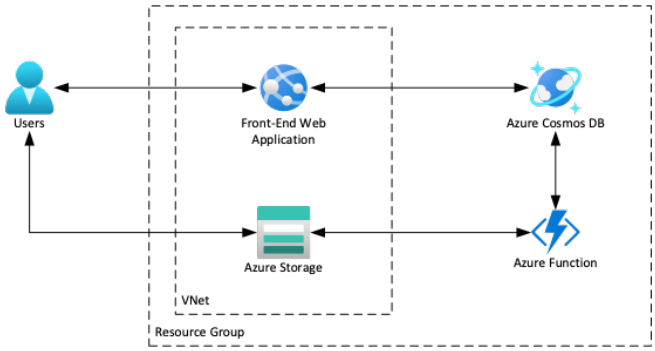

Fig. 2: Example system to be used to demonstrate threat modeling.

by co-author Simone Curzi. Figure 2 shows the diagram of the example of the system that will be used in the threat modeling role play.

Practice exercise (75 min). The participants will be asked to form groups and download and use windows virtual machine to experiment with threat modeling using the Threats Manager Studio (TMS). They will be given a scenario with diagrams and discovery content. Groups will be asked to use TMS to create a Threat Model through realistic role playing of various scenarios. The presenters will act as tutors and circulate through the classroom to help the attendees.

The participants will be invited to discuss their experience in performing threat modeling and the challenges that they may have in their scenarios. The participants will be given a slack channel to post questions about their threat modeling practices, and presenters will offer two-hour free mentoring sessions to help the participants practice threat modeling on their systems.

Discussion (30 min). Valani will moderate a panel discussion on the state of threat modeling including perspectives on DevSecOps, AI, Cyber Physical Systems, and soft skills. This will also be an opportunity for attendees to ask questions.

Ben Othmane will conclude the training session with a summary of the lessons learned.

V. Prior tutorials or talks on similar topics

Heinrich and Curzi teach threat modeling to Microsoft's customers and internally to their colleagues. They deliver consulting services offering Threat Modeling for Security Risk. Ben Othmane teaches software security at University of North Texas (UNT) and taught the subject at Iowa State University and Technical University Darmstadt, Germany [3].

Talks by the presenters include:

1) L. Ben Othmane. On Continuous Threat Modeling of Cyber-physical Systems, SecDevOps days, Washington DC, 2021
2) L.Ben Othmane. Threat Modeling in Practice, The 7th International Workshop on Secure Software Engineering (SSE 2021), Digital, 2021 (keynote)
3) Integrate Threat Modeling into your DevOps Pipeline, Security Compass, Linkedin event, 2022.
4) Hasan Yasar, Simone Curzi, Arun Prabhakar, Altaz Valani, and Lotfi Ben Othmane. Evolving Threat Modeling for Agility and Business Value with DevSecOps, SecDevOps days, Washington DC, 2021
5) Hasan Yasar, Simone Curzi, Arun Prabhakar, Altaz Valani, and Lotfi Ben Othmane. Hackathon on Effective Threat Modeling, Microsoft, Online, 2021.

References

[1] S. Curzi, J. Freund, A. Prabhakar, A. Valani, H. Yasar, "Evolving Threat Modeling for Agility and Business Value", , 2022, URL: https://simoneonsecurity.files.wordpress.com/2021/03/evolving-threat-modeling.pdf.

[2] "Threat Manager Studio", , 2022, URL: https://threatsmanager.com/.

[3] L. ben Othmane, "CprE 562x – Secure Software Engineering", , 2021, URL: https://www.engineering.iastate.edu/~othmanel/CPRE562.html.