Threat modelling for hackers

— a hands-on workshop —

Arne Padmos

Systems created by humans may – no *will* – contain flaws. In order to shine a light on these flaws, you can use a technique called threat modelling. We will take a look at different threat modelling methods that empower hackers (and others) to study the architecture of a system.

There are hundreds if not thousands of different threat modelling methods that can be used to tease apart the structure of a system in the search for security issues. In this workshop, we will cover the key principles behind these methods and we will provide prototypical worked examples. In order to give you hands-on experience with threat modelling, we will go through an archetypical threat modelling exercise together. We will close the workshop by having you apply these methods to one of your own systems. You will be provided with relevant background material to allow you to integrate threat modelling into your daily activities going forward.

Duration: 90 minutes

1 Learning objectives

The overarching goal of the workshop is to provide participants a head-start with integrating security-by-design principles into their projects. They should be able to start asking themselves and others the question 'what could possibly go wrong?'. During the workshop, we will study the history and foundations of threat modelling, looking into a few common methodologies, and covering general facets that can be applied widely. The emphasis of the hands-on parts of the workshop will be how to run a threat modelling session focused on analysing a system's architecture from a security perspective. How such sessions relate to earlier and later activities will also be discussed. Concretely, as a result of following the workshop, participants should be able to:

- explain the role that threat modelling plays in developing secure systems
- describe the key differences between the major threat modelling flavours
- name some common methods for threat modelling and their main properties
- provide examples of fundamental concepts and explain how they are related
- plan a threat modelling session around a generic high-level framework
- execute the facets of a threat modelling engagement on a simple system
- check their own threat models – and the work of others – using checklists
- consider the pitfalls of relying on models and take mitigating measures
- plan how to learn more, including how to optimise and monitor learning

2 Lesson planning

The general structure will be 'tell', 'show', 'do', 'apply' (although to some extent these will be interleaved). Participants are reminded of the power of note taking. The workshop will start with a general overview as an introduction. This will be followed by a discussion of several fundamental concepts. Building on this foundation, a generic framework for threat modelling is presented that will be used in the rest of the workshop. Various examples will be given, after which participants will work on exercises. Background material is shared at the end. The workshop will provide:

- a general overview of what threat modelling is and why it is useful
- coverage of some fundamental concepts on which threat modelling is built
- a generic framework for threat modelling made up of six central facets
- worked examples structured around subgoals, to be walked through and narrated
- in-class exercises that increase in complexity, with some self-assessment
- pointers for further exploration, including homework questions and reading