Chapter 24

Threat Modeling in Agile Software Development

Martin Gilje Jaatun
https://orcid.org/0000-0001-7127-6694
SINTEF Digital, Norway

Karin Bernsmed
SINTEF Digital, Norway

Daniela Soares Cruzes
SINTEF Digital, Norway

Inger Anne Tøndel
https://orcid.org/0000-0001-7599-0342
SINTEF Digital, Norway

ABSTRACT

Threat modeling is a way to get an overview of possible attacks against your systems. The advantages of threat modeling include tackling security problems early, improved risk assessments, and more effective security testing. There will always be limited resources available for security, and threat modeling will allow you to focus on the most important areas first. There is no one single "correct" way of doing threat modeling, and "agile" is no excuse for not doing it. This chapter describes the authors' experiences with doing threat modeling with agile development organizations, outlining challenges to be faced and pitfalls to be avoided.

1. INTRODUCTION

Threat modeling has been identified as one of the most important activities in the Security Development Lifecycle (SDL) (Howard & Lipner, 2006). According to Jeffries (Jeffries, 2012), Microsoft SDL author Michael Howard states: "If you're only going to do one activity from the SDL, it should be threat modeling". The main idea behind threat modeling is to *think like an attacker*. A well-defined threat model

DOI: 10.4018/978-1-6684-3702-5.ch024

helps to identify threats to the different assets of a system by utilizing well-grounded assumptions on the capabilities of any attacker interested in attacking such a system. It enables the teams to identify critical areas of design, which need to be protected. Over time, various threat modeling approaches and methodologies have been developed, and are being used in the process of designing secure applications (Cruzes, Jaatun, Bernsmed, & Tøndel, 2018). The approaches vary from conceptual frameworks to practical methodologies. To speed up software delivery, many organizations have adopted an agile software development approach, in which development teams produce code in shorter iterations with frequent feedback loops. In agile software development, however, threat modeling is not widespread, and the practitioners have few sources of recommendations on how to proceed to adopt the practice in their process. In addition, in agile software development, it is often challenging in itself to adopt security practices, either because security practices are not prioritized, or because the practitioners are not able to see the relevance and importance of the activities to the improvement of the security in the project (Cruzes et al., 2018). Studies in software security usually focus on software security activities in general, and there are few empirical studies focusing on specific practices in agile software development. The threat modeling activity is particularly important in software security, since many security vulnerabilities are caused due to architectural design flaws (McGraw, 2004). Furthermore, fixing such vulnerabilities after implementation may be very costly, requiring workarounds which sometimes increase the attack surface. A well-defined threat model helps to identify threats to different assets of a system by utilizing well-grounded assumptions on the capabilities of any attacker interested in exploiting such a system. It also enables the development teams to identify critical areas of the design which need to be protected, as well as mitigation strategies. However, threat modeling can also be challenging to perform for developers, and even more so in agile software development.

This chapter is based on results from the ongoing *SoS-Agile - Science of Security for Agile Software Development* research project (https://www.sintef.no/en/digital/sos-agile/) which investigates how to meaningfully integrate software security into agile software development activities. The project started in October 2015 and will end in October 2020, and involves many software development companies in Norway. The method of choice for the project is Action Research, which is an appropriate research methodology for this investigation because of the combination of scientific and practical objectives that aligns with the basic tenet of action research, which is to merge theory and practice in a way such that real-world problems are solved by theoretically informed actions in collaboration between researchers and practitioners (Greenwood & Levin, 1998), (Davison, Martinsons, & Kock, 2004).

The remainder of this chapter is structured as follows: Section 2 outlines our approach to threat modeling in broad strokes. In Section 3 we explore some particular challenges associated with agile software development, which influence how we think about threat modeling. Section 4 offers additional recommendations on how to successfully perform threat modeling in agile software development. We conclude in Section 5.

2. FUNDAMENTAL THREAT MODELING ACTIVITIES

Threat modeling is a wide concept that encompasses a broad range of techniques that can be utilized to make a system more secure. Threat modeling usually employs two types of models; one that represents the system that is to be built and another one that represents the actual threats to the system (Shostack, 2014b). In the context of software development, what is being built can be almost anything that will use