Comparing Misuse Case and Mal-Activity Diagrams for Modelling Social Engineering Attacks

Peter Karpati, Norwegian University of Science and Technology, Norway
Guttorm Sindre, Norwegian University of Science and Technology, Norway
Raimundas Matulevičius, Institute of Computer Science, University of Tartu, Estonia

ABSTRACT

Understanding the social engineering threat is important in requirements engineering for security-critical information systems. Mal-activity diagrams have been proposed as being better than misuse cases for this purpose, but without any empirical testing. The research question in this study is whether mal-activity diagrams would be more efficient than misuse cases for understanding social engineering attacks and finding prevention measures. After a conceptual comparison of the modelling techniques, a controlled experiment is presented, comparing the efficiency of using the two techniques together with textual descriptions of social engineering attacks. The results were fairly equal, the only significant difference being a slight advantage for mal-activity diagrams concerning perceived ease of use. The study gives new insights into the relative merits of the two techniques, and suggests that the advantage of mal-activity diagrams is smaller than previously assumed. However, more empirical investigations are needed to make detailed conclusions.

Keywords: Conceptual Comparison, Controlled Experiment, Mal-Activity Diagrams, Misuse Cases, Security, Social Engineering, Threat Modelling

1. INTRODUCTION

The term ‘social engineering’ (Townsend, 2010) comes from the hacker community and is a widely accepted jargon for conning people into helping an attacker to compromise a target system. Social engineering is often considered the easiest way to get illegitimate access to confidential information or perform other security-related attacks on information systems (Mitnick & Simon, 2002). Yet the information security efforts of many organizations tend to be focused on technical solutions. In a survey (Gallagher & Gallagher, 2010) where organizations were asked about their effectiveness in mitigating ten different security issues, social engineering came tenth, so organizations considered that they were least effective in dealing with this. Yet
there is comparatively little research related to social engineering, meaning that it remains one of the most under-researched topics in information security (Taylor & Garrett, 2007). Security professionals predict that it will continue being a dominant threat (Northcutt, 2011).

One important step in addressing social engineering is to understand the threats (Power & Forte, 2006). Techniques for this must be easy to understand and not presuppose advanced technical knowledge, since victims of social engineering are not only computer workers but also front desk clerks, personnel officers, janitors or anyone in an organization who might have access to offices, infrastructure, people or sensitive information. Misuse cases (Sindre & Opdahl, 2005), henceforth abbreviated MUC, is one technique for threat modelling, often argued to be simple to understand even for people without technical expertise. However, in Sindre (2007) it was argued that misuse cases might not give a good representation of social engineering, since such attacks are often comprised of many different episodes, e.g., the attacker first talks to person A, posing as X, achieving some partial result. Then he talks to person B, posing as Y (e.g., Y = A, using insights from the former conversation), etc., until the confidential information is finally obtained. Motivated by this, Sindre (2007) proposed another notation, mal-activity diagrams, henceforth abbreviated MAD, which was assumed to be better than misuse case diagrams for depicting social engineering attacks.

An example of a mal-activity diagram is shown in Figure 1, the attacker’s (malicious) activities shown with inverted icons, together with normal icons similar to a UML activity diagram. The attacker is a con man hired by a competitor to perform industrial espionage on a robotics company to obtain the design plans for a new product they are working on. The attacker first calls in as a potential investor interested in setting up a meeting with the boss of a robotics company. After juggling with the dates he manages to find out that the boss will be away for a week in the near future, on a long awaited golf vacation. Then he collects more information from the PR consultant of the target posing as a potential costumer over a pricy lunch and one more drink than she really wanted. After preparing well, the social engineer pays a visit to the company when the boss is away, posing as a business partner and persuades the receptionist to gather the key people and take them out for a lunch, where he befriends them and creates optimism that the collaboration with the partner company that he represents will really boost the market potential of the new product. In particular, he takes care to befriend the chief designer who has access to the plans, and a couple days later he calls this person, claiming he is with the boss at the resort where the boss is on a golf vacation, working out some final details of the collaboration. He tells the designer that the boss needs to have the last version of the product design emailed to him, but that he is unable to access his job email address from the resort and therefore instead needs it sent to a private email address that the boss has (e.g., hotmail or similar) - an email address which has of course really been set up by the attacker. After receiving the email with the design plans, he passes it to his clients. The corresponding MUC representation of the case consisted of two separate diagrams one presented in Figure 2. In addition to normal use cases and normal actors, the MUC diagram shows malicious actors performing misuse cases using inverted graphics for both. On the other hand, unlike MADs, MUCs do not show the order of the various actions. Misuse cases threaten use cases when the use cases are exploited or hindered by the misuse cases.

The above attack is just one example, and other examples will be different. In most cases, attackers will prefer to avoid face-to-face communication unless strictly necessary, since this entails a greater risk of being caught if something goes wrong. Instead they typically rely on phone calls and email. Today there is also an increasing trend towards hybrid attacks which are partly social and partly technical, for instance using phishing and various types of malware (Abraham & Chengalur-Smith, 2010). In the above case, face-to-face communication was
Threatening the Cloud: Securing Services and Data by Continuous, Model-Driven Negative Security Testing
www.igi-global.com/chapter/threatening-cloud-securing-services-data/72236?camid=4v1a

Secure Key Generation for Static Visual Watermarking by Machine Learning in Intelligent Systems and Services
www.igi-global.com/article/secure-key-generation-static-visual/39098?camid=4v1a