Name: Özgür Kafali


Overall Research Goal(s):
*What do you ultimately hope to show with your research? This section can involve some jargon, but try to relate these goals to your broad impact section. Start with the larger goal(s) and narrow the scope towards your specific study (and specific goals, below).*

Recent data breaches in domains such as healthcare, where confidentiality of data is crucial, indicate that misuse cases often originate from user errors rather than vulnerabilities in the technical (software or hardware) architecture. Current approaches can control users’ access to sensitive system resources, e.g., how a physician accesses patients’ records. However, these approaches fail to characterize how a user is expected to interact with others with regards to the resources, e.g., how a physician keeps patient’s information private when consulting a colleague.

Our goal is to incorporate social aspects of security, and help security analysts identify the associated misuse cases so as to assess a system’s vulnerabilities.

Broad Impact:
*Why is your research important? This section should avoid any technical jargon and should be meaningful to the general public. Try to keep this down to five sentences. This should be hierarchical: the broad impact decomposed into more specific impacts that connect your overall research goals to your more specific goals.*

Understanding the vulnerabilities of a software system is crucial to prevent security breaches. There are existing methods to find such vulnerabilities at the software level. However, misuse cases often originate from a user’s social interactions with others rather than software-level vulnerabilities. Therefore, being able to identify such malicious actions is important to prevent data breaches.

Specific Research Goals:
*Lay out the steps you are going to take to achieve your overall research goal. You can get technical here.*

Previous work proposed visual representations for misuse cases such as system architecture diagrams (SAD) and misuse case maps (MUCM). While these methods are intuitive, they do not have formal representations and do not support multiple actor scenarios to capture the interactions among various actors.

We propose to use social norms to regulate users’ social interactions. Our research goal is to help security analysts identify misuse cases by systematically generating potential enactments that violate formally stated social norms. Our research will help the security requirements engineering effort for designing more secure systems as well as the digital forensics effort for diagnosing such misuse cases.
Proposed Data Collection (if applicable):
What data will you collect to answer your research goals? How will you collect it? Will it be an observational study, randomized comparative experiment, or simulation study? Include potential biases and be prepared to explain how the data will achieve your specific research goals.

There are studies on the helpfulness of previous approaches (such as MUCM) for identifying malicious behavior. We will design similar user studies to evaluate the performance of our approach with regards to previous approaches for the representation and identification of misuse cases.

We will also start experimentation on the open source medical records system iTrust (http://agile.csc.ncsu.edu/iTrust/wiki/doku.php). Previous work has identified malicious user scenarios for iTrust by manually going through its functional requirements and use case diagrams. We will investigate how our generation results compare to those scenarios.

Success Criteria:
How will you determine whether you satisfied your specific and overall research goals?

We will define formal metrics to compare our approach to the relevant literature. Previous work lacks such concrete measures to assess how much a method is helpful in identifying the vulnerabilities associated with a software system. Through our metrics, we will show that our method is helpful in identifying misuse cases. In particular, we aim to show that (i) our approach is superior to other approaches for some scenarios, in particular for identifying social misuse cases, and (ii) it is complementary to other approaches for some other scenarios.

One metric is coverage: we will measure whether our approach is able to identify more misuse cases. Another metric is consistency: we will verify whether our approach is consistent in identifying similar cases as misuse. Humans are often inconsistent in identification tasks. We believe that having a priority relation among the stated norms would help classify similar misuse cases.

We will also achieve theoretical basis for our methods, and prove that our misuse generation method is sound and complete with respect to the stated norms.

Anticipated Difficulties, Limitations, and Criticisms:
What will make the above specific research goals difficult to achieve? How do you plan on dealing with these difficulties if they arise?

Designing a user study and recruiting participants to reflect a real-world security requirements engineering task is not trivial. We will carefully design the scope of our user study, select real-world scenarios from the literature, and include participants with the right demographics to demonstrate the advantages our method over previous approaches.