Name: Maria Riaz

Hard Problem Area: Security Metrics and Models

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).

The objective of this research is to facilitate analysts in security requirements engineering by providing a framework that supports a systematic and thorough analysis of security goals of a software system.

Specifically, we want to improve the identification of an initial set of security goals. We also want to explicitly capture assumptions and relations that lead to identification of additional and implied security goals.

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.

Software systems manage information that is important not only for individuals and institutions but also for economy as well as national security. Early identification and specification of security requirements of a software systems is important for secure software development. Errors and omissions in requirements can lead to serious security concerns. Software security goals provide a foundation for security requirements engineering while capturing the rationales behind these requirements and providing a measure of completeness of requirements.

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

To achieve the goal of supporting security requirements analysis we outline the following steps:
- Identify a set of security goal patterns that capture the various dimensions of security for assets in software systems.
- Explicitly capture relations among security goals and assumptions underlying security goals.
- Provide a framework that leverages knowledge of security goal patterns and relations to support systematic and thorough analysis of security goals.
- Provide considerations for operationalizing security goals by mapping goals to candidate security requirements and controls.
- Evaluate the process through controlled experiments.

**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.

For identifying security goals patterns and relations, we synthesize data from:
- Security taxonomies and standards
- Security requirements of existing systems
- Existing security patterns

For empirical evaluation of our framework, we performed a controlled experiment involving 28 students enrolled in a computer and network security course. To ensure that no group was inherently better at identifying security goals prior to the experiment, a pre-experimental exam was given to assess each student’s ability to identify security goals. Students were then randomly assigned to either the control or treatment groups in such a way that the pre-experimental scores were balanced across the two groups.

Each student was then asked to identify security goals for two systems (iHRIS and Cyclos), performing each in a randomized order. We selected these systems as they manage diverse set of assets, operations on assets cover all action types and require consideration for different security goals thus allowing for a detailed analysis of DIGS framework.

Following the experiment, students were given a survey asking about their previous academic and work experiment, as well as a self-assessment on whether the tasks and methodology to complete the tasks were clear. The purpose of the latter is to determine whether students in the treatment group were able to understand the instructions given to them. This information could potentially explain the evidence or lack of statistical differences between the two task groups.

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

Our success criteria is based on how well our framework supports identification of security goals to support security requirements engineering. We have the following null hypotheses:
**H01**: The relevance of security goals identified is unrelated to the use of our framework.

**H02**: The quantity of security goals identified is unrelated to the use of our framework.

**H03**: The ease of identifying security goals is unrelated to the use of our framework.

For relevance of identified goals, we use precision and recall metrics computed based on security goals identified by participants in the treatment and control groups against an oracle.

For quantity of identified goals, we look at the % of security goals correctly categorized out of total possible goals in the oracle.

For ease of identifying goals, we look at qualitative feedback from participants to see if participants using our framework had a positive opinion about the process versus the control group.

We further categorize the goals as follows and see if differences exist between treatment and control groups in identification of particular types of security goals:

- Based on operational context
  - Prevention goals
  - Detection goals
  - Response goals

- Based on relations among goals
  - Initial goals
  - Implied goals

**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?

In a controlled setting, teaching a specific methodology to participants in a short amount of time is a challenge. If the participants don't understand the methodology, we might not see significant differences. Moreover, under time pressure, participants may not apply the methodology and default to prior knowledge. At the end of the experiment, we asked participants if they were clear about the task and the methodology for performing the task. We also asked participants to briefly summarize the methodology they used for identifying security goals. Based on this feedback, we can assess if participants adequately understood and applied the methodology or not.

Finding sufficient number of participants to create multiple groups is another challenge. The experimental design we followed is that of an analysis of variance (ANOVA) of a split-plot design where the whole-plot factor was the task group (control or treatment) and the split-plot factor was the system (iHRIS and System). This allowed to collect more data points with same number of participants. However, it left less time to spend on each system which might result in low recall of security goals.