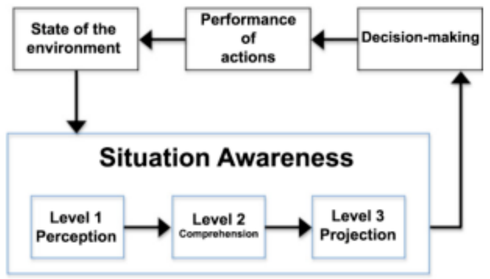
Defining the Expert: Using Situation Awareness to Identify Security Expertise

Hanan Hibshi & Travis Breaux
Institute for Software Research, Carnegie Mellon University
Maria Riaz & Laurie Williams
North Carolina State University

Background

- We rely on experts to evaluate systems' security requirements.
- Better expertise should lead to better security.
- What makes a better expert? How can we identify the expert?
- We need to understand the cognitive process of experts to be able to identify what distinguishes them.
- We use concepts from Situation Awareness (Endsley, 1988) to model expertise.

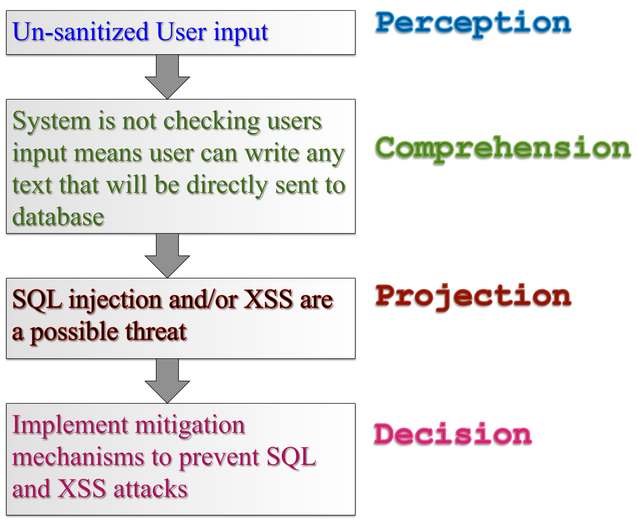
Situation Awareness



Endsley's Situation Awareness (Source: NIST.gov)

Experts **perceive** cues in the environment, which they **comprehend** to interpret the meaning and be able to **project** future consequences.

Uncertainty could occur at any SA level.



Approach

Interviewing Security Experts

We conducted 9 experts interviews (and additional two pilots) where we asked security experts to analyze three artifacts: Source code, Dataflow Diagrams and Network Diagrams.

Conducting grounded analysis

We used coding theory to code the interview transcripts. The codes are driven from SA:

- **P, C, J, D** for Perception, Comprehension, Perception, Decision.
- We added the Prefix U for uncertainty: **UP, UC, UJ, UD**.
- **Q** if participant asks a question., **A** if participant makes an assumption.

Extracting patterns

Find patterns in the data to distinguish experts and novices.

Experts vs. Novices

Novices and experts could many paths to decision making that does not literally follow the P→C→J→D path.

Example: P3 and P5 looked at a network diagram with a firewall on it. They were asked if the following security requirement could be met based on the diagram:
Company X's network, with the exception of the publically available services which will reside in a (DMZ), will be unavailable for connections initiated from the Internet to Company X's network.

P3's response followed the pattern: P→C→D , while P5's response was: P→UC→Q
P3 made more decisions than P5 (41 vs. 14) and had less uncertainties (23 vs. 67)

Patterns Found

Classic SA Patterns following the path: P→C→J→D or with some simple variation like skipping a level. Examples of such patterns include : P→C→J, P→C→D, J→D, C→D

Reverse SA Patterns following the reverse path of classic SA: D→J→C→P. We saw more of those patterns from experts from non-western cultures (probably following an inductive reasoning style). Examples of such patterns include : D→J→C→P, J→C→P, D→C→P, J→C, D→C

Uncertainty and Assumption Patterns where participants face uncertainty in any of SA levels. We saw experts more likely to transition from uncertainty to assumptions, and novices more likely to ask clarifying questions. Examples of such patterns include : UP→UC, UC→UJ, UC→A, UC→A→D, UC→Q

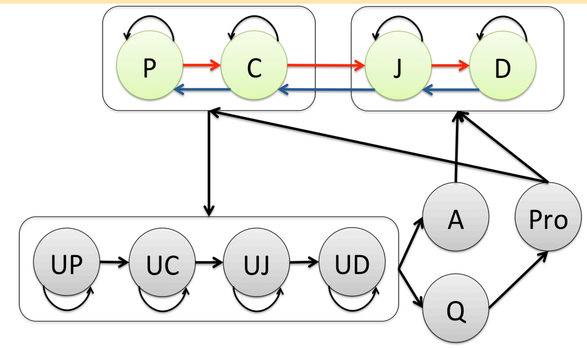
Our Proposed Model

From Interfaces to State machines

From our patterns and qualitative insights, we extended Endsley's SA model to account for uncertainty, the role of assumptions and inquiry.

We hypothesize that transition between the SA levels could occur at many different patterns other then P→C→J→D.

Experts should exhibit patterns different then novices. Novices would have lower confidence to make risky decisions.



Tracing Expert Analysis through Perception, Comprehension, Projection and Decision

Conclusions & Future Work

- We introduce a new approach to model security expertise and help understand experts' decision-making.
- While the original SA framework aims to model the decision-making process with respect to design better user interfaces, we are more interested in discovering how analysts comprehend problem descriptions and notations, and how this comprehension leads to changes in design.
- We plan to conduct more user experiments to test the patterns that we found in our qualitative results.

References

(Ensley, 1988) M. R. Endsley, "Design and evaluation for situation awareness enhancement," *HFES Annual Mtg.*, 1988, 32: 97–101 Second reference