WIP: Guidelines for Improving Scientific Reporting in Cyber Security

THE UNIVERSITY OF ALABAMA® | College of Engineering

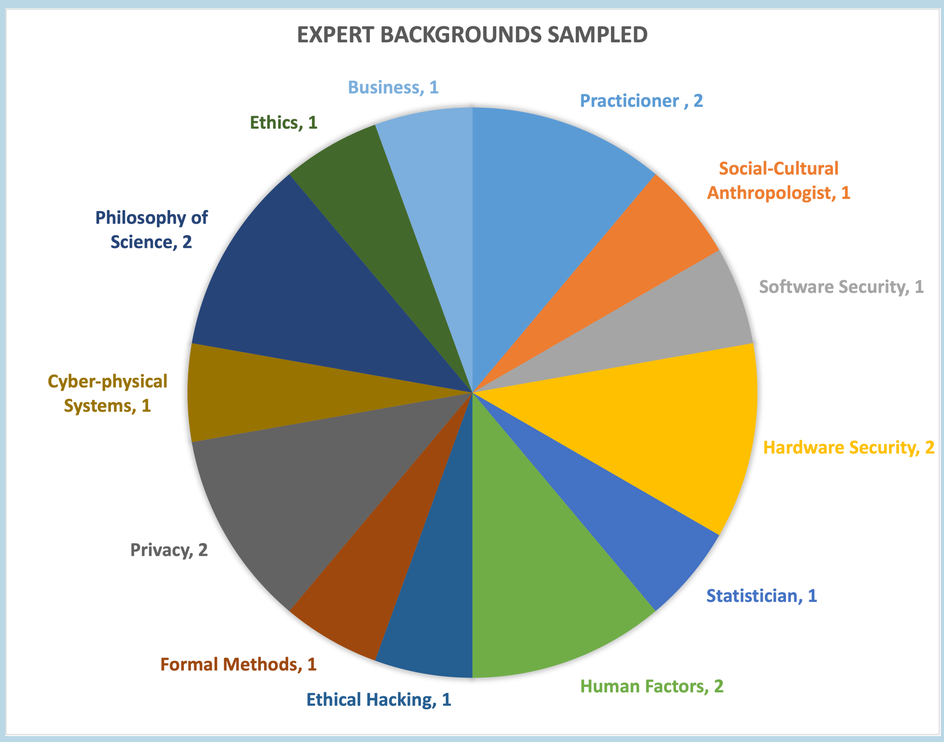
Matthew Armstrong, Jeffrey Carver
maarmstrong3@crimson.ua.edu, carver@cs.ua.edu

Problem

In order to build the Science of Security, cyber security research must be reported in a scientifically rigorous and valid manner. We interviewed cyber security experts with the goal of developing a set of guidelines for reporting scientifically rigorous cyber security research.

Expert Sampling

- 12 Experts Interviewed
- 9 different backgrounds
- Members of or associated with the Science of Security Lablet community



Interview Script

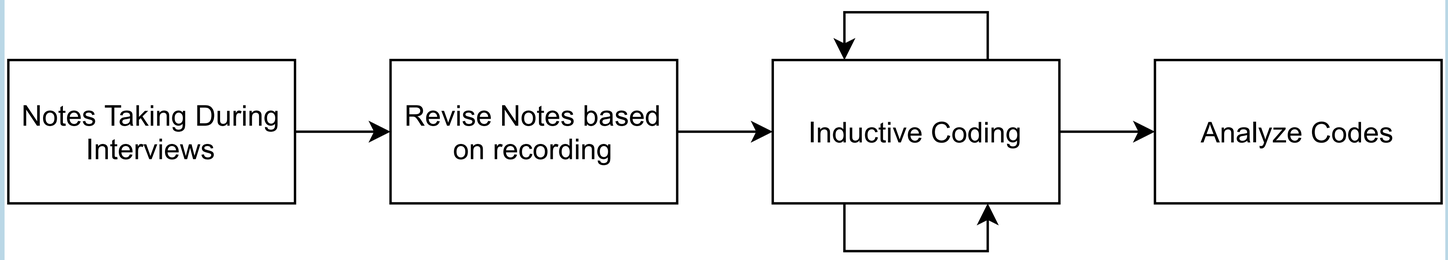
- What aspect(s) of cyber security are your primary focus?
- In the context of the cyber security area(s) with which you are most familiar, how do you define scientific validity and scientific rigor? What specific concepts do they include?
- From the answer above, what information do you consider to be critical (i.e. you would reject the paper without it) and what information is optional, but nice to have?
- What types of cyber security papers have you read and written?
- For different types of cyber security papers, are there any specific factors that are required for scientific rigor or validity, which may differ from other types of cyber security papers?
- Who else should we talk with about this idea?

Acknowledgements

We thank the experts who participated in the interviews, especially during COVID-19.
Sponsorship This research is sponsored by the U.S. Department of Defense. DoD representatives are authorized to review research records.

Analysis

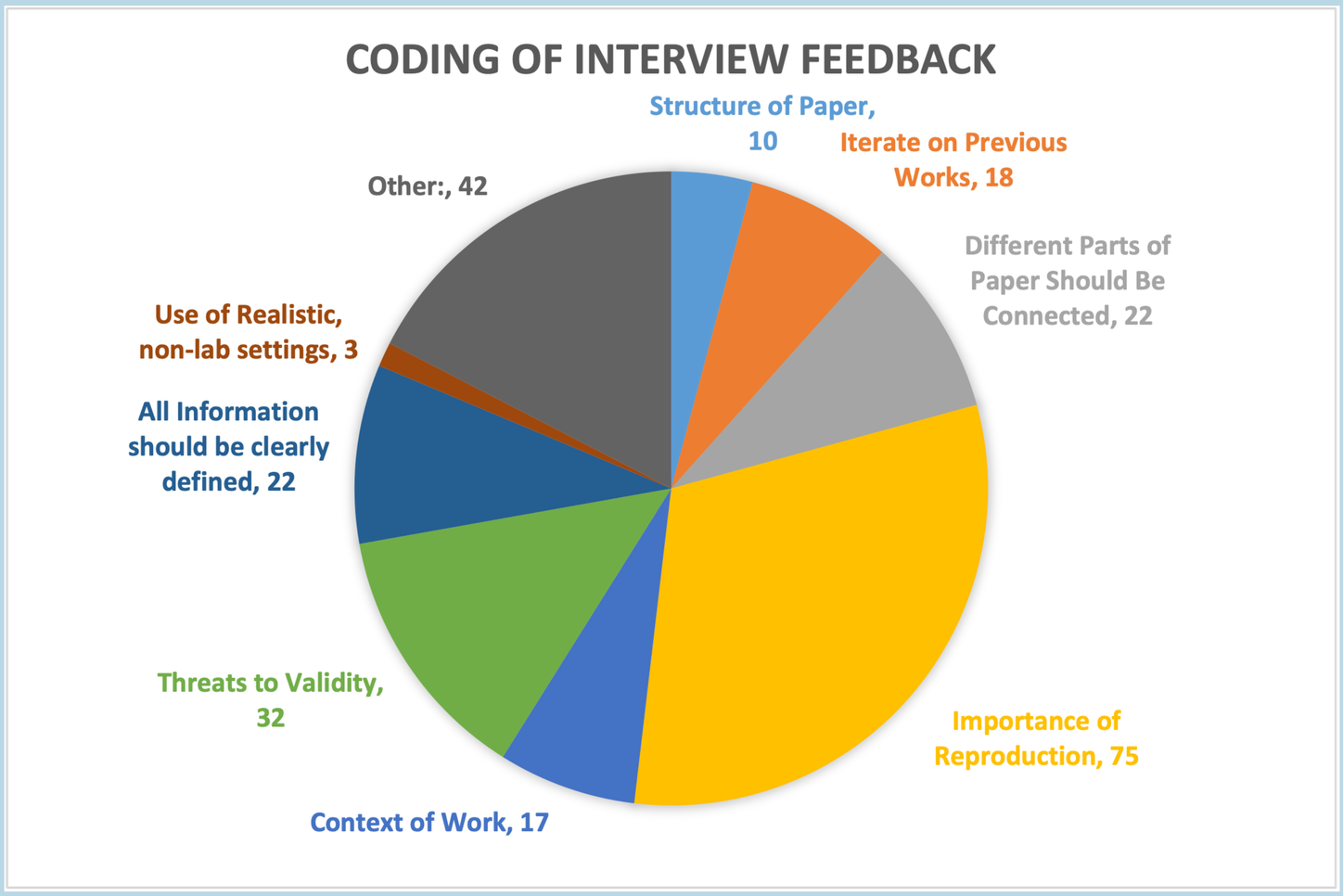
- One researcher conducted the interview while the other took notes
- Audio recordings to ensure completeness of notes
- Inductive Coding Analysis



Initial Findings

We have completed the coding process of the qualitative interview data, and are now moving to analysis. So far, we have determined several emerging themes and concepts that would fit well into a set of guidelines.

- A comprehensive set of guidelines would have to be complex to cover the unique requirements of different types of and different sub-domains of cyber security.
- Not all papers have to be scientifically rigorous or valid to provide valuable contributions to the overall science.
- Authors should consider ethical impacts of work when possible.
- Information needed for reproduction efforts is greatly desired.
- Threats to validity, both external and internal, should be considered in literature.



Future Works

After the analysis of the interview data is complete and an initial set of guidelines are created, we plan to expand the project to cyber security experts outside of the SoS community. Including the input of the wider cyber security community would validate any guidelines that are produced as a result and increases the chances of the guidelines being adopted outside of the SoSL community. This increase in adoption would, in turn, increase the scientific validity, rigor, and ultimately contribution of compliant cyber security literature.

Conference

HOTSOS 2021

Hot Topics in the Science of Security Symposium
April 13-15, 2021 | Hosted by the National Security Agency