Designing Forensic Analysis Techniques through Anthropology

Sathya Chandran Sundaramurthy
Kansas State University
sathya@ksu.edu

ABSTRACT

Current tools and solutions to handle incident response and forensics focus only on one piece of evidence, doing very little towards presenting the big picture. My PhD dissertation will focus on developing analytical tools that can automate repeated tasks whenever possible and also be able to connect the dots among multiple data sources. The tools of my research will focus more on reducing the time incident responders spend on mundane tasks through automation also by providing data in a more abstract and context specific manner. Such presentation will be more useful in constructing the intrusion scenario than when it is presented raw. Another challenge security researchers face today is validating their research ideas on real-world data.

The traditional approach taken by the security research community for innovation is to read the current literature on a problem, identify areas for improvement, and then develop tools and methodologies that address those problems. While this process may result in theoretically sound solutions there has always been a issue of how usable these solutions are in the real-world. The main reason, I believe, for this problem is the discrepancy between what the security practitioners actually want and what the researchers perceive as what they want.

Few years back I worked on validating our previous work SnIPS [4] a correlation engine that works on top of Snort alerts and host logs to identify high-confidence attacks in an enterprise network. In addition to manual analysis we also worked with the Kansas State University (K-State) Computer Science Department System Administrator to identify the value he sees in such a tool as ours. We did this by spending some time asking questions for an hour or so every semester. Since he was already overwhelmed with other departmental duties we were not able to continue our interview process further on.

Anthropologists study a community by spending significant amount of time with the people of that community [2]. The reason being that one cannot understand the internal thinking or "tacit knowledge" of the people by just observing from outside as pointed out by Michael Polanyi [5]. Polanyi also found out that "We can know more than we can tell." Cybersecurity practitioners work based on "intuition" or "hunch feeling" which is primarily due to their years of experience in looking at data. Through the study of Jeane Lave and Etienne Wenger it is found that knowledge in a community is (1) not always explicit, (2) often embodied in practice, and (3) the knowledge may not even be "in" an individual but emobodied in the community of practice [3]. Also this tacit knowledge can only be acquired not just by being part of the community but also doing what they do on a daily basis [1].

My PhD work will focus on applying anthropological methods to identify the "tacit knowledge" of incident responders and make them explicit through tools, processes, and publications.

Categories and Subject Descriptors

C.2.3 [**Computer-Communication Networks**]: Network Operations—*Network management, Network monitoring*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

Keywords

Anthropology in Security, Forensic Analysis, Security Operation Centers.

1. REFERENCES

[1] J. S. Brown and P. Duguid. Knowledge and organization: A social-practice perspective. *Organization science*, 12(2):198–213, 2001.

[2] J. Elyachar. Before (and after) neoliberalism: Tacit knowledge, secrets of the trade, and the public sector in egypt. *Cultural Anthropology*, 27(1):76–96, 2012.

[3] J. Lave and E. Wenger. *Situated learning: Legitimate peripheral participation*. Cambridge university press, 1991.

[4] X. Ou, S. R. Rajagopalan, and S. Sakthivelmurugan. An empirical approach to modeling uncertainty in intrusion analysis. In *Computer Security Applications Conference, 2009. ACSAC'09. Annual*, pages 494–503. IEEE, 2009.

[5] M. Polanyi and A. Sen. *The tacit dimension*. Peter Smith Gloucester, MA, 1983.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage, and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s). Copyright is held by the author/owner(s).
NSPW'13, September 9–12, 2013, Banff, AB, Canada.
ACM 978-1-4503-2582-0/13/09.
http://dx.doi.org/10.1145/2535813.2535826.