The Human Capital Model for Security Research New Insights into Technology Transition

S. Raj Rajagopalan
Honeywell
Phoenix, AZ, U.S.A.
Siva.Rajagopalan@Honeywell.com

ABSTRACT

As a security researcher, have you ever wondered how much of security research that is done and presented at research conferences is ever used by practitioners or is incorporated into products? Four years ago we formed a team with diverse backgrounds and embarked on a systematic study on the question of which technological solutions would security practitioners actually use if we built them. To carry this out program, we embedded our students who worked inside several Security Operation Centers (SOCs) both in universities and corporations, to learn how security solutions get used in reality. Previous efforts at improving the efficiency of SOCs have emphasized building tools for analysts or understanding the human and organizational factors involved, but they have not significantly changed the status quo – solutions are built or bought but seldom used. This was because these efforts did not view these solutions from multiple contextual perspectives of the local participants, the analysts and their managers. After some initial failures, we realized that this kind of study is beyond the reach of conventional Computer Science approaches, so we worked with a Professor in Socio-cultural Anthropology to get a fresh look at the problem and get a new set of tools to use in our research. In our 4-year project we have used Anthropological fieldwork methods to study SOCs and in the process uncovered inherent contradictions between the multiple objectives a SOC has to meet as an organization and the conflicts between the goals of the human participants. This discovery was guided by Activity Theory, a theory proposed by the famous social scientist Y. Engestrom [1], which provides a framework for analyzing such kinds of fieldwork data. We discovered that successful SOC innovations must continually resolve the extant conflicts to be effective in improving operational efficiency. Our analysis provides evidence of the importance of conflict resolution as a prerequisite for operations improvement, both process and technological. It also enabled us to understand the fundamental challenge in security research, namely, why some innovations work well in SOCs while others fail. It also helped us devise a potentially successful and repeatable mechanism for introducing new technologies to future SOCs.

In this talk, we will detail the important insights we gained in the course of this project so that the security research community may benefit from them and even incorporate these new tools. We will also present examples of the challenges faced by commercial manufacturers in designing security into their products and our ongoing work on using these insights to address these challenges in innovative ways that seem to fare better than previous attempts.

This is based partially on joint work with Professors Xinming Ou (Southern Florida University Computer Science Department), Michael Wesch (Kansas State University Department of Anthropology), and John McHugh (Dalhousie University and RedJack, Inc, Retired) as well as their graduate students, Sathya Chandran Sundaramurthy and Alexandru Bardas. •

CCS Concepts

•Security and privacy ~ Human and societal aspects of security and privacy • Security and privacy ~ Social aspects of security and privacy • Human-centered computing ~ Ethnographic studies • Applied computing ~ Ethnography •Applied computing ~ Psychology • General and reference ~ Metrics •Social and professional topics ~ Management of computing and information systems

Author Keywords

Security; SOC; practitioners; Anthropology; Activity Theory; field study

CODASPY'17, March 22–24, 2017, Scottsdale, AZ, USA.
ACM ISBN 978-1-4503-4523-1/17/03.
DOI: http://dx.doi.org/10.1145/3029806.3044200

BIOGRAPHY

S. Raj Rajagopalan is a Senior Principal Research Scientist at Honeywell Labs where he leads the Product cyber security research effort aimed at designed-in security for Honeywell's vast control system product portfolio. His research interests include all aspects of Computer Security, including Software Engineering techniques for training software development teams in security practices, especially in the context of product manufacture. In collaboration with Computer Science Prof. Simon Ou (University of South Florida) and Anthropology Professor Mike Wesch of Kansas State University, he has been involved in a five-year study of several Security Operations Centers across universities and corporations on why it is so hard to make security tools that actually get used. He also leads an initiative to enable more academic research to the areas of cyber security and personal privacy for modern buildings management systems. Dr. Rajagopalan has a PhD in Computer Science from Boston University, and a B.Tech. in Computer Science and Engineering from the Indian Institute of Technology at Mumbai.

REFERENCES

1. Y. Engestrom. Learning by Expanding: An Activity-Theoretical Approach to Developmental Research. Orienta-Konsultit Oy, 1987.