The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game

Sylvain Frey
University of Southampton, UK
frey.sylvain@gmail.com

Awais Rashid
University of Bristol, UK
awais.rashid@bristol.ac.uk

Pauline Anthonysamy
Google, Switzerland
Lancaster University, UK
anthonysp@google.com

Maria Pinto-Albuquerque
Instituto Universitario de Lisboa
(ISCTE-IUL), Portugal
maria.albuquerque@iscte-iul.pt

Syed Asad Naqvi
Lancaster University, UK
s.naqvi@lancaster.ac.uk

ABSTRACT

Motivation: The security of any system is a direct consequence of stakeholders' decisions regarding security requirements. Such decisions are taken with varying degrees of expertise, and little is currently understood about how various demographics – security experts, general computer scientists, managers – approach security decisions and the strategies that underpin those decisions. What are the typical decision patterns, the consequences of such patterns and their impact on the security of the system in question? Nor is there any substantial understanding of how the strategies and decision patterns of these different groups contrast. Is security expertise necessarily an advantage when making security decisions in a given context? Answers to these questions are key to understanding the "how" and "why" behind security decision processes.

The Game: In this talk[1], we present a tabletop game: Decisions and Disruptions (D-D)[2] that tasks a group of players with managing the security of a small utility company while facing a variety of threats. The game is kept short – 2 hours – and simple enough to be played without prior training. A cyber-physical infrastructure, depicted through a Lego® board, makes the game easy to understand and accessible to players from varying backgrounds and security expertise, without being too trivial a setting for security experts.

Key insights: We played D-D with 43 players divided into homogeneous groups: 4 groups of security experts, 4 groups of non-technical managers and 4 groups of general computer scientists.

- ***Strategies:*** Security experts had a strong interest in advanced technological solutions and tended to neglect intelligence gathering, to their own detriment. Managers, too, were technology-driven and focused on data protection while neglecting human factors more than other groups. Computer scientists tended to balance human factors and intelligence gathering with technical solutions, and achieved the best results of the three demographics.
- ***Decision Processes:*** Technical experience significantly changes the way players think. Teams with little technical experience had shallow, intuition-driven discussions with few concrete arguments. Technical teams, and the most experienced in particular, had much richer debates, driven by concrete scenarios, anecdotes from experience, and procedural thinking. Security experts showed a high confidence in their decisions – despite some of them having bad consequences – while the other groups tended to doubt their own skills – even when they were playing good games.
- ***Patterns:*** A number of characteristic plays were identified, some good (balance between priorities, open-mindedness, and adapting strategies based on inputs that challenge one's pre-conceptions), some bad (excessive focus on particular issues, confidence in charismatic leaders), some ugly ("tunnel vision" syndrome by over-confident players). These patterns are documented in the full paper – showing the virtue of the positive ones, discouraging the negative ones, and inviting the readers to do their own introspection.

Conclusion: Beyond the analysis of the security decisions of the three demographics, there is a definite educational and awareness-raising aspect to D-D (as noted consistently by players in all our subject groups). Game boxes will be brought to the conference for demonstration purposes, and the audience will be invited to experiment with D-D themselves, make their own decisions, and reflect on their own perception of security.

CCS CONCEPTS

• **Security and privacy** → *Human and societal aspects of security and privacy*; • **Software and its engineering** → *Risk management*;

KEYWORDS

Security decisions, security requirements, games, decision patterns

ACM Reference Format:
Sylvain Frey, Awais Rashid, Pauline Anthonysamy, Maria Pinto-Albuquerque, and Syed Asad Naqvi. 2018. The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. In *ICSE '18: ICSE '18: 40th International Conference on Software Engineering , May 27-June 3, 2018, Gothenburg, Sweden.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3180155.3182549

[1]Original journal paper: S. Frey, A. Rashid, P. Anthonysamy, M. Pinto-Albuquerque, and S. A. Naqvi. The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. IEEE TSE, 2017.
[2]Game rules available at: http://decisions-disruptions.org.

ICSE '18, May 27-June 3, 2018, Gothenburg, Sweden

ACM ISBN 978-1-4503-5638-1/18/05.
https://doi.org/10.1145/3180155.3182549