Human-Centered Cybersecurity Strategies and Behavioral Incentives for Secure Smart Homes

Student's name: N'guessan Yves-Roland DOUHA

Laboratory's name: Laboratory for Cyber Resilience (サイバーレジリエンス構成学研究室)

Supervisor's name: Professor Youki KADOBAYASHI (門林 雄基)

Abstract

The proliferation of the Internet of Things (IoT) and smart homes has blurred the boundary between human and computer security, leading to an increase in cybersecurity threats. While previous research has primarily focused on technological vulnerabilities, the risks posed by context-based attacks that exploit user-related factors have been overlooked. This thesis adopts a human-centered approach to secure smart homes by investigating cybersecurity awareness among users and exploring the effectiveness of behavioral incentives. The research objectives include analyzing the costs and benefits of cybersecurity initiatives using game-theoretic models to identify the conditions favoring investment in cybersecurity education, and investigating users' opinions on cybersecurity education and non-financial incentives. The theoretical investigation analyzes the costs and benefits of cybersecurity investment using static and evolutionary game-theoretic approaches. The empirical investigation collects and analyzes the perspectives of smart-home users on cybersecurity education and explores the influence of national cultures on their interests and motivations. The research contributes by providing insights into the costs, benefits, and implications of cybersecurity practices in smart homes. It identifies conditions for achieving Nash equilibria, emphasizes the importance of behavioral incentives and low-cost training, and highlights the need to consider cultural factors. The findings of this study underscore the crucial importance of investing in cybersecurity education and recognizing non-financial incentives to promote responsible cybersecurity behaviors among smart-home users. These actions would play a pivotal role in empowering individuals to prevent and respond effectively to cyberattacks targeting smart homes. However, the study has limitations, including the assumption of rational actors in the theoretical investigation and the focus on a specific group of participants in the empirical investigation. Future research should explore more sophisticated game models that can capture the complexities of cybersecurity decision-making. Additionally, delving deeper into the underlying motivations of the participants in the empirical study would provide valuable insights. This dissertation highlights the significance of human-centric approaches to address cybersecurity challenges in the realm of smart homes. It lays the foundation for further initiatives and policy development in securing smart homes, which is of utmost importance in our interconnected world.