COINS - Norwegian Information Security Conference

Yi-Ching Liao
Norwegian Information Security laboratory
Norwegian University of Science and Technology
yi-ching.liao@ntnu.no

1 Feasibility Analysis of Simulating Cybercrime Scenarios

Norwegian Information Security Conference (NISK) emphasizes on the theoretical and practical issues of information security. Since my Ph.D. project is about cybercrime investigation, I found one of the publications: "Visualising the Impact of Network Attacks on Business Processes using the DEViSE Framework" (by Huw Read, Konstantinos Xynos, Iain Sutherland, and Mikhaila Burgess) to be beneficial for my research. Using recently discovered attacks as input knowledge, integrating with current business process, and customizing the network traffic for attack simulation, it is feasible to simulate cybercrime (even combined with other types of crimes) for preparing investigators or first responders for different crime scenarios. Through comparing different tactics employed by trainees, we can easily figure out more effective strategies for combating cybercrime than existing guidelines.

2 Cost-Benefit Analysis of Simulating Cybercrime Scenarios

Additionally, I found the other publication: "Improving Computer Network Defense Analysis Training with Adversary Replication Techniques" (by Juan J. Güelfo and Ingrid C. Bentzen) to be valuable for my Ph.D. project. Several factors affect the effectiveness of simulating cybercrime scenarios for forensic readiness, such as the feasibility of implementation, the amount of resources required, the usability of production environment, and the simulation levels of detail. Therefore, it is essential to consider these factors for cost-benefit analysis to prepare investigators or first responders for different crime scenarios.

3 Realism Enhancement of Simulating Cybercrime Scenarios

Moreover, after visiting the simulation and training of marine operations in Ålesund, it will be interesting to implement virtual environment techniques to enhance the simulation levels of detail for cybercrime scenario simulations. Similar to every marine operations are essential for safe and efficient offshore working environments, each operation of

incident investigation is important for future root cause analysis and the admissibility of evidence. Integrating virtual environment techniques and real case scenarios can provide investigators or first responders more realistic cybercrime scenario simulations.