Workshop Questions and Answers

1. What are the main challenges in modelling and evaluating the outcomes of Social Engineering Threats (SETs), and how does this study attempt to address them?

The key complexities of the Social Engineering Threats (SETs) modelling are due to being human centered. In comparison to technical vulnerabilities which may be measured by using system metrics, SETs take advantage of psychological manipulation, trust and behaviour, which are unpredictable by their nature. The subjective uncertainty in factors of cultural context, awareness of the users and emotional state is hard to model quantitatively(Wang, Zhu and Sun,2021).

The combination of attack tree modeling with the Markov chain model is the solution to these challenges. The attack tree is a hierarchical and structured expression of the possible attack paths, whereas Markov model measures state changes and chances of successes with time(Syafitri et al.,2024). This is a model that gives the possibility to estimate the Attack Occurrence Probability (AOP) and Attack Success Probability (ASP) and develops a quantifiable model of evaluating SET risks.

2. How do persuasion principles and modalities contribute to the success of SETs, and why is it important to analyse them systematically?

Persuasion principles: Some persuasion principles, including authority, reciprocity, commitment, liking, and social proof are very important in the effectiveness of SETs since they capitalize on inherent cognitive biases in human behaviour (Naruoei et al.,2024). To illustrate, pretending to be in authority role raises the level of compliance whereas social proof can be used to enforce the validity of fraudulent messages. It is imperative to analyze these principles systematically to measure their impact on the level of attack success and create the specialized awareness training.

3. What role do the Attack Tree Model and Markov Chain Model play in estimating the Attack Occurrence Probability (AOP) and Attack Success Probability (ASP) of SETs?

Attack tree model is a hierarchical conceptualization of the potential attack scenarios into small manageable events. Every node is a possible step of a social engineering attack, and the probability of success is attached to it(Aijaz and Nazir,2024). This break down aids in determining key points of weakness and the best courses of attack.

Markov Chain Model, conversely, describes the changing dynamic attack states with time. It represents the way in which an attacker moves through one phase (reconnaissance) to another (exploitation) using predetermined transition probabilities(Al-Karaki et al.,2024).

These models combined allow one to create a quantitative estimate of the AOP (probability of an attack happening) as well as the ASP (probability of an attack being successful). This integrated modelling system enhances the predictive accuracy and assists the security managers to distribute resources efficiently.

4. In what ways can the findings of this study support the development of effective policy frameworks for mitigating social engineering threats in information systems?

(i) Prioritise **training programs** focusing on the most exploited psychological weaknesses.
(ii) Design **risk-based access controls** and **incident response strategies**.
(iii) Develop **data-driven awareness campaigns** that reflect real-world threat probabilities.
(iv) Enhance compliance with standards such as ISO 27001 and NIST SP 800-53 through measurable risk assessment.

References

Wang, Z., Zhu, H. and Sun, L., 2021. Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *Ieee Access*, *9*, pp.11895-11910.

Syafitri, W., Shukur, Z., Asma'Mokhtar, U., Sulaiman, R. and Ibrahim, M.A., 2022. Social engineering attacks prevention: A systematic literature review. *IEEE access*, *10*, pp.39325-39343.

Naruoei, B., Hakimpour, H., Mahmoodzadeh Vashshan, M. and Mohammadi, M., 2024. The effectiveness of Cialdini's principles on persuasion in digital marketing (A case study of Iran's furniture industry). *International Journal of Nonlinear Analysis and Applications*, *15*(4), pp.135-148.

Aijaz, M. and Nazir, M., 2024. Modelling and analysis of social engineering threats using the attack tree and the Markov model. *International Journal of Information Technology*, *16*(2), pp.1231-1238.

Al-Karaki, J.N., Gawanmeh, A., Almalkawi, I.T. and Alfandi, O., 2022. Probabilistic analysis of security attacks in cloud environment using hidden Markov models. *Transactions on Emerging Telecommunications Technologies*, *33*(4), p.e3915.