Unit 8 Seminar preparation

Title: Quantitative Risk Modelling - Case Study

Workshop Questions based on Aijaz and Nazir (2024)

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

- Social Engineering Threats (SETs) exploit human psychology (Aijaz and Nazir, 2024). Each individual responds uniquely based on personality, experience and awareness, making victim responses variable, difficult to predict and to model (Albladi and Weir, 2020; Kumarage et al., 2025).

  Aijaz and Nazir (2024) attempts to address this by

  - **Attack tree modelling** – Uses static attack trees to calculate Attack Occurrence Probability (AOP) by breaking SETs into communication modalities (e.g., email, phone, face-to-face) and persuasion principles (e.g., authority, reciprocity, commitment) (Aijaz and Nazir, 2024, pp. 1232–1233).
  - **Markov chain modelling** – Applies a Markov chain to compute Attack Success Probability (ASP) by modelling sequential attacker states (Disconnect, Connect, Persuade, Success) and the probabilistic transitions between them (Aijaz and Nazir, 2024, pp. 1234–1235).
  - **Scenario validation** – Tests the framework on ten realistic SET cases, showing how modalities and persuasion strategies shape both AOP and ASP (Aijaz and Nazir, 2024, pp. 1235–1236).

- **Limited formal modelling** – Few studies have systematically represented persuasion principles and communication modalities (Aijaz and Nazir, 2024, p. 1232). Aijaz and Nazir (2024) attempts do address this by developing their own model.

- **Scarcity of empirical data** – Aijaz and Nazir (2024) similarly note that their probability values are based on limited statistical evidence, and they propose generating further empirical data in future work to validate their model (p. 1232).

- **SETs are adaptive and evolving in nature** – static models struggle to capture how attacker strategies change over time (Gadyatskaya and Mauw, 2019). In their study, Aijaz and Nazir employ static attack trees, but acknowledge this limitation and highlight the potential of dynamic attack trees to better represent evolving social engineering threats in future research (2024, p. 1233).

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

Persuasion principles and modalities contribute to the success of SETs by enabling attackers to exploit psychological vulnerabilities (e.g., authority, reciprocity) and deliver them through strategically chosen channels. Attackers adapt their approach to align the persuasion technique with the communication medium, thereby maximising impact and increasing the likelihood of victim compliance.
For instance, email allows for wide dissemination and scalability but typically exerts weaker influence, whereas face-to-face interactions generate stronger trust, urgency, and social pressure.

At is important to analyse persuasion principles and modalities systematically because they are the fundamental drivers of SETs. By incorporating them into structured models, the study can move beyond descriptive accounts and produce quantitative measures of attack occurrence and success. This provides clearer insights into how SETs operate and supports more targeted and effective defensive strategies.

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:** quantifies how likely an attack is to occur. The AOP (Attack Occurrence Probability) reflects the likelihood of an SET taking place, based on observed frequencies of modalities and persuasion strategies.
- **Markov Chain Model:** estimates how likely an attack is to succeed. The ASP (Attack Success Probability) represents the chance that an SET reaches its objective once initiated**,** by simulating attacker progression through stages based on effectiveness data.

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?**

The quantification of SETs via the modeled probabilities of occurrence and success enables a systematic ranking of social engineering threats by both prevalence and effectiveness, thereby guiding policymakers in allocating resources toward technical safeguards, targeted training, and awareness initiatives.

However, by focusing exclusively on human behaviour, this approach reflects the same limitation found in models that address only technical vulnerabilities: both risk neglecting the socio-technical interaction exposing organisations to a higher level of cybersecurity risk than is necessary (McEvoy and Kowalski, 2019), Similarly, Khadka

and Ullah (2025) emphasise that isolating either human or technical dimensions leads to incomplete assessments.

Additionally, Aijaz and Nazir's model is built on the assumption that humans are inherently the weakest link—an idea frequently cited but not always sufficiently scrutinised:

- **Misinterpretation of industry reports**: Figures from Verizon's DBIR (2023; 2025) are often simplified into claims that human error causes most breaches, even though Verizon refers to human involvement rather than causation (Peters, 2023; Keepnet Labs, 2025).
- **Academic echo chamber**: Claims are repeated uncritically in scholarly work, such as Aijaz and Nazir's reference to Siddiqi et al., even though that paper does not explicitly make the "weakest link" claim.
- **Involvement ≠ breach**: Human actions do not automatically cause compromise; for example, clicking a phishing link does not necessarily result in a breach, as intent, context, and follow-up actions are decisive.
- **Problematic reliance on simulations**: Phishing simulation results are frequently presented as proof of human fallibility, yet clicks in simulations do not reliably correspond to real breaches and may even be triggered by automated systems (Mimecast, 2023).

Moreover, all breaches involve humans to some extent—whether directly, through errors or misuse, or indirectly, through system design and coding flaws (Verizon, 2025, p. 19). By uncritically adopting the weakest-link narrative, models such as that of Aijaz and Nazir risk misdirecting organisational priorities, placing disproportionate emphasis on user blame at the expense of socio-technical defences.

References

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. Available at: https://doi.org/10.1007/s41870-023-01540-z (Accessed: 11 August 2025).

Albladi, S., Weir, G. (2020) 'Predicting individuals' vulnerability to social engineering in social networks', *Cybersecur,* 3, Article 7. Available at: https://doi.org/10.1186/s42400-020-00047-5 (Accessed: 10 September 2025).

Akkaya, O. and Keleştemur, S. A. (2024) 'Quantifying Social Engineering Impact: Development and Application of the SEIS Model,' *International Journal of Scientific Research and Engineering Development,* 7(5), pp. 523-532. Available at:

https://www.academia.edu/125062204/Quantifying_Social_Engineering_Impact_Development_and_Application_of_the_SEIS_Model (Accessed: 10 September 2025).

Gadyatskaya, O. and Mauw, S. (2019) 'Attack-Tree Series: A Case for Dynamic Attack Tree Analysis', in *Graphical Models for Security: 6th International Workshop, GraMSec 2019, Held in Conjunction with CSF 2019, Barcelona, Spain, July 12, 2019. Proceedings*, Lecture Notes in Computer Science, vol. 11720, pp. 7–19. Cham: Springer. Available at: https://doi.org/10.1007/978-3-030-36537-0_2 (Accessed: 10 September 2025).

Keepnet Labs (2025) *The Hidden Psychology Behind Phishing Simulations: Why Employees Still Click*. Available at: https://keepnetlabs.com/blog/the-hidden-psychology-behind-phishing-simulations-why-employees-still-click (Accessed: 10 September 2025).

Khadka, K. and Ullah, A. (2025) 'Human factors in cybersecurity: an interdisciplinary review and framework proposal', *International Journal of Information Security*, 24. Available at: https://doi.org/10.1007/s10207-025-01032-0 (Accessed: 01 July 2025).

Kumarage, T., Johnson, C., Adams, J., Ai, L., Kirchner, M., Hoogs, A., Garland, J., Hirschberg, J., Basharat, A. and Liu, H. (2025) *Personalized Attacks of Social Engineering in Multi-turn Conversations -- LLM Agents for Simulation and Detection*. Available at: https://arxiv.org/abs/2503.15552 (Accessed: 10 September 2025).

McEvoy, T. and Kowalski, S. (2019) 'Cassandra's Calling Card: Socio-technical Risk Analysis and Management in Cyber Security Systems', Conference: CEUR Workshop Proceedings. vol. 2398. Available at: https://www.researchgate.net/publication/338502878_Cassandra (Accessed: 10 September 2025).

Mimecast (2024) *Introducing Human Risk: The Next Generation of Security Awareness*. Mimecast Blog. Available at: https://www.mimecast.com/blog/introducing-human-risk-the-next-generation-of-security-awareness/ (Accessed: 10 September 2025).

Peters, J. (2023) *74% Data Breaches Are Due to Human Error.* Available at: https://www.infosecinstitute.com/resources/security-awareness/human-error-responsible-data-breaches/ (Accessed: 10 September 2025).

Verizon (2023) *Data Breach Investigations Report 2025*. Verizon Business Resources. Available at: https://www.verizon.com/business/resources/Tbd7/reports/2023-data-breach-investigations-report-dbir.pdf (Accessed: 20 June 2025).

Verizon (2025) *Data Breach Investigations Report 2025*. Verizon Business Resources. Available at: https://www.verizon.com/business/resources/reports/dbir/ (Accessed: 20 June 2025).