

Based on Aijaz & Nazir (2024)

CHALLENGES OF MODELLING SETS

- Human behavior is subjective and variable
- Multiple persuasion principles and modalities
- Scarcity of empirical data
- Evolving attacker strategies

STUDY'S APPROACH

- Attack Tree Model → maps possible attack paths
- Markov Chain Model → quantifies probabilities
- Together estimate: AOP and ASP

PERSUASION & MODALITIES

- Principles: authority, trust, urgency, social proof
- Modalities: email, vishing, social media impersonation
- Systematic analysis → improves defense

ROLE OF MODELS

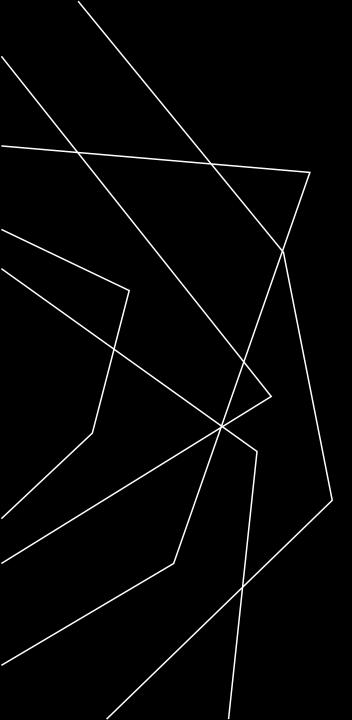
- Attack Tree → structure of attack scenarios
- Markov Chain → probabilistic transitions
- Integration → numerical risk estimation

POLICY IMPLICATIONS

- Evidence-based frameworks
- Training on persuasion principles
- Controls for high-risk modalities
- Continuous monitoring

CONCLUSION

- SETs are difficult to model but critical to address
- Attack Trees + Markov Chains = actionable insights
- Supports stronger policy and risk management



REFERENCES

- 1. 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. https://doi.org/10.1007/s41870-023-01573-3
- 2. Almohri, H.M.J. and Yao, D.D. (2021) 'On the (in)effectiveness of the Common Vulnerability Scoring System', International Journal of Information Security, 20(5), pp. 649–666. https://doi.org/10.1007/s10207-020-00530-0
- 3. Cialdini, R.B. (2021) Influence: The psychology of persuasion. Revised edn. New York: Harper Business.
- 4. Sarker, I.H. (2022) 'Cybersecurity risk management in the era of digital transformation', Journal of Cybersecurity and Privacy, 2(3), pp. 435–456. https://doi.org/10.3390/jcp2030023