**Unit 8 Seminar – Quantitative Risk Modelling: Case Study**

**Title:** Quantitative Risk Modelling – Case Study  
**Reading:** Aijaz, M. and Nazir, M. (2024) *Modelling and Evaluating Social Engineering Threats in Cyber Systems.* *Journal of Information Security and Applications,* 75, pp. 102–119.

**1. Main Challenges in Modelling and Evaluating Social Engineering Threats (SETs)**

The study highlights several key challenges in **modelling and quantifying Social Engineering Threats (SETs)**:

* **Human factors and unpredictability:** Human behaviour cannot be easily parameterised; emotions, trust, and situational awareness vary across individuals.
* **Lack of structured models:** Traditional risk assessment frameworks often overlook the psychological and contextual aspects of manipulation.
* **Dynamic and evolving attack patterns:** Attackers adapt techniques quickly, making static models ineffective.

Aijaz and Nazir (2024) address these issues by introducing a **hybrid quantitative framework** combining **Attack Tree Modelling** and **Markov Chain Modelling** to simulate attack progressions and outcomes probabilistically.

**2. Persuasion Principles and Modalities in SETs**

The study draws on **Cialdini’s persuasion principles** (e.g., authority, scarcity, reciprocity, and social proof) to explain how attackers exploit cognitive biases.  
By categorising social engineering modalities — such as **phishing, baiting, and pretexting** — the authors show how these techniques manipulate trust and perception.

Analysing persuasion principles systematically is vital because it allows security teams to:

* Identify behavioural vulnerabilities.
* Design targeted awareness training.
* Quantify how different psychological levers increase attack success rates.

This approach links **psychological theory** with **quantitative modelling**, improving prediction accuracy for SET-related incidents.

**3. Role of Attack Tree and Markov Chain Models**

* **Attack Tree Model:**  
  Decomposes complex attacks into smaller, logical sub-events (e.g., initial contact → data request → credential theft). Each branch is assigned a probability based on prior evidence or expert judgment.
* **Markov Chain Model:**  
  Represents the **transition probabilities** between attack states — such as moving from initial deception to exploitation.  
  This dynamic modelling captures the evolving nature of human interaction in social engineering scenarios.

Together, these models enable the calculation of:

* **Attack Occurrence Probability (AOP)** – the likelihood that an attack will be attempted.
* **Attack Success Probability (ASP)** – the likelihood that it will succeed given specific contextual and behavioural conditions.

This dual modelling approach bridges qualitative human aspects with quantitative statistical reasoning, providing measurable outputs for decision-making.

**4. Policy and Framework Implications**

The study’s findings provide actionable insights for policy development and governance frameworks:

* Support for **evidence-based training programmes** that focus on real-world persuasion tactics.
* Establishment of **risk thresholds** for social engineering incidents using quantified ASP and AOP metrics.
* Integration of **behavioural analytics** into security monitoring tools to detect early signs of manipulation or insider compromise.
* Adoption of **adaptive awareness frameworks** that evolve with emerging attack trends.

By integrating quantitative risk models into institutional cybersecurity policies, organisations can move from reactive awareness to **proactive, data-driven prevention strategies**.

**5. Reflection**

This seminar expanded my understanding of how **quantitative models can represent human-centric security risks**. Previously, I viewed social engineering mainly as a qualitative challenge. Through Aijaz and Nazir’s framework, I learned how statistical modelling — particularly Markov Chains and Attack Trees — can quantify attacker behaviour and success probability.  
The focus on persuasion principles also reinforced that human factors are measurable and should be treated as key risk variables. I now appreciate that combining behavioural science with data analytics enables more accurate risk prediction and policy design.  
This learning directly supports my professional goal of implementing **data-driven awareness and risk governance frameworks** that blend psychology, statistics, and cybersecurity practice.

**References**

* Aijaz, M. and Nazir, M. (2024) *Modelling and Evaluating Social Engineering Threats in Cyber Systems.* *Journal of Information Security and Applications,* 75, pp. 102–119.
* Cialdini, R. (2007) *Influence: The Psychology of Persuasion.* New York: HarperCollins.
* ISO (2018) *ISO 31000:2018 – Risk Management — Guidelines.* Geneva: ISO.