A Human Vulnerability Assessment Methodology

Dr. Andrea Cullen
Ms. Lorna Armitage

Outline

- Research overview:
  - The integration of personality types and social traits into a targeted attack scenario
  - Used as a method to make training and awareness raising more effective against social engineering attacks
- Social engineering background
- Personality preference models
- Social engineering tactics
- The developed human vulnerability assessment methodology
- Summary & future work

Social Engineering

- Social engineering attacks exploit vulnerabilities in individuals for access to confidential information
- Trick users into doing something that goes against the interest of security: using influence and persuasion
- Social engineering attacks continue as a significant issue
- Training and awareness raising remain key to any social engineering security strategy
  - It is important to ensure that any training or awareness raising is as affective as possible

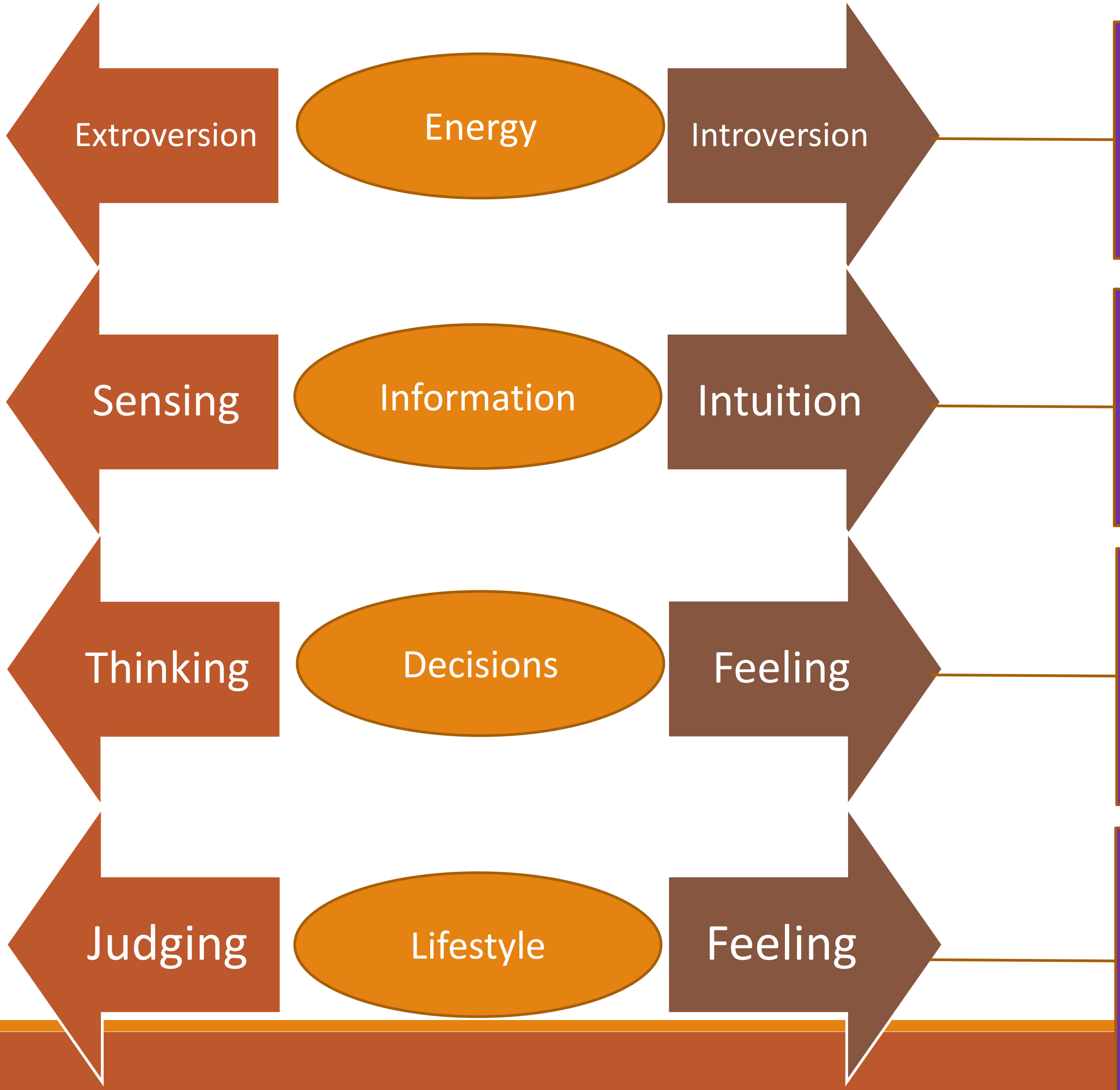
Social Engineering & Decisions

- Personality traits have an impact on preferences and therefore significantly influence decisions made
- Social engineers target individuals to negatively influence these decisions
- Within a social engineering attack, individual targets make multiple decisions, with limited information, in an environment where the attacker is attempting to trick them
- Different personalities are susceptible to different types of social engineering attacker tactics
  - It is important to understand this difference

Personality Preference Models

- A number of personality preference models have been developed to help understand difference in general (e.g. FFM, MBTI)
- Myers-Briggs Type Indicator (MBTI)
  - Has 16 personality types, derived from four dimensions, each of which is a dichotomy, that is an either-or choice
  - Individuals have four pairs of preferences where one is prominent from each pair: extroversion-introversion; sensing-intuition; thinking-feeling; and judging perceiving
- MBTI is useful for understanding yourself and others; solving problems; and training and development
- Relevant for understanding people in the context of security; their different vulnerabilities; how to develop more effective training and awareness raising

MBTI Preference Pairs



Extroversion Energy Introversion

Sensing Information Intuition

Thinking Decisions Feeling

Judging Lifestyle Feeling

The way we prefer to focus attention. The (E)extrovert is interested in the external environment, i.e. people and objects that are outside the individual. Talk through problems. The (I)ntrovert - interested in the world of concepts and ideas, the inner world. Reflects before acting.

The way we gather information. (S)ensing - rely on their senses to gather information from the outside world. Trust experience, focus on what is real and factual. i(N)tuition - rely on hunches and own thought processes to gather information. Like ambiguity, enjoy thinking about the future.

The way we make judgments and decisions. (T)hinking - analyses facts objectively and makes decisions based on cause and effect. Objective logic. (F)eeling – subjective decision making drawing conclusions based on empathy with the views of others (their heart to rule their head). Common ground and harmony with others.

The way people like to Live their lives, either by gathering information or drawing conclusions. (J)udging - prefer to live in a structured, systematic, planned and organised way. Enjoy decision making and planning. (P)erceiving - prefer to gather information, usually easily side-tracked by things that looks more interesting. Keeps options open. Enjoys last minute time pressure.

Social Engineering Tactics

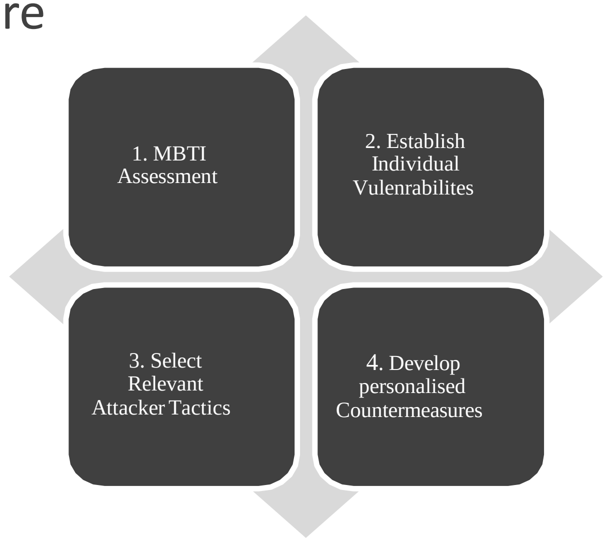
- The Principles of Persuasion in Social Engineering (PPSE) are tactics used in social engineering attacks:
  - authority; social proof; liking; commitment; reciprocation and consistency; and distraction
  - Individuals are susceptible to persuasion in different ways based on their traits
- The success of persuasion techniques is based on an individuals' social traits as well as perpetrator tactics
- Our research indicates that:
  - Tactics are designed to attack specific vulnerabilities in individuals in the same way as technical attacks target technical vulnerabilities *[E.g. the Extrovert may be more likely to succumb to liking/Similarity as a social engineering tactic than those who prefer working and thinking alone (the Introvert)]*
  - vulnerabilities in an individual can be "patched"

Research & the Developed Methodology

- Primary data was collected
  - Ten individuals completed MBTI assessments
  - Four were selected as they represented discrete profiles.
  - Different phishing emails were then presented to the four individuals
  - Individuals were asked which they felt to be the most compelling and appealing: they were able to select as many as they wanted from 0 to 6
- Mapping between the tactics used and MBTI profiles showed the tactics most likely to be successful in each case

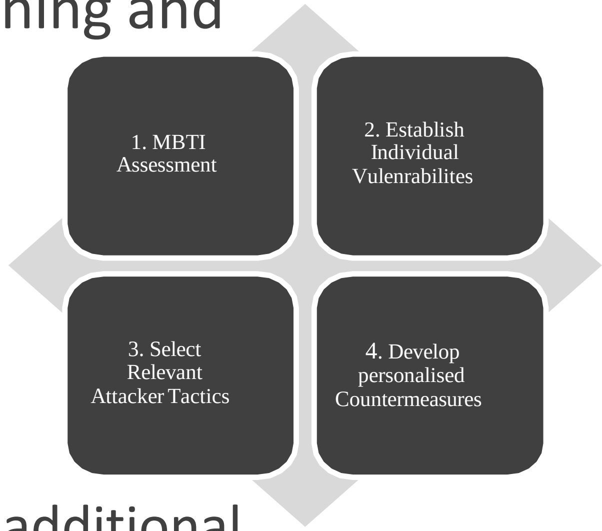
Assessment Methodology

- Vulnerability Assessment Methodology model includes four discrete phases:
  - **MBTI assessment:** helps an individual to understand their personality preferences.
  - **Vulnerability ID:** profiles analysed and individual vulnerabilities established
  - **Select relevant tactics:** examine social engineering tactics and map each personality
  - **Develop personalised countermeasures:** establishing a personalised countermeasure plan; namely targeted training and awareness raising
- This methodology follows a similar patter to a technical vulnerability assessment [e.g. understand the context, detect vulnerabilities, identify attacks that are able to exploit the vulnerabilities and finally apply an appropriate countermeasure]
- **NB.** MBTI is useful for establishing a learning model that can determine the most effective implementation and design for learning


1. MBTI Assessment
2. Establish Individual Vulenrabilites
3. Select Relevant Attacker Tactics
4. Develop personalised Countermeasures

Summary & Future Work

- Developed a methodology for assessing the vulnerabilities in individuals to social engineering attacks
- Involved four key stages. The final step considers personalised training and awareness raising


1. MBTI Assessment
2. Establish Individual Vulenrabilites
3. Select Relevant Attacker Tactics
4. Develop personalised Countermeasures

- Next steps:
  - Test the model using a social engineering pen testing methodology
  - Test the effectiveness of personalising training and awareness raising
  - We will consider how this model can be further developed to include additional countermeasures

Questions