# Automated Social Engineering Tools

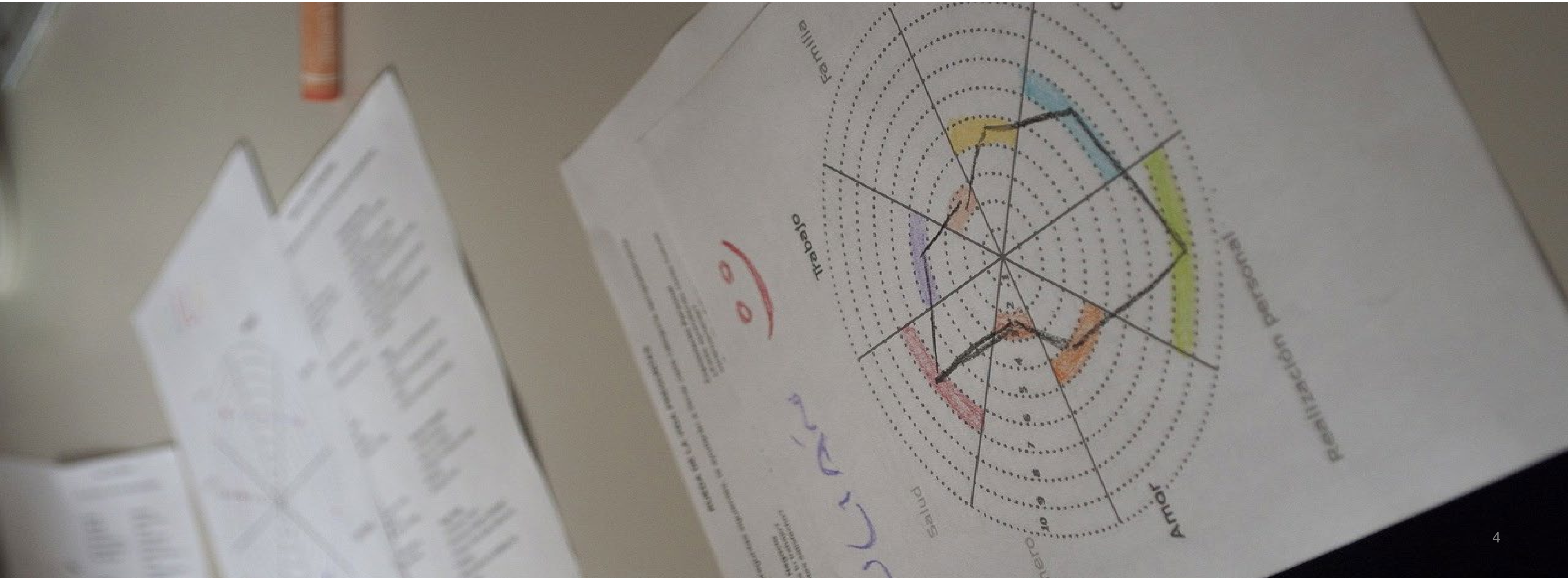
Dominik Dana, Sebastian Schrittwieser, Peter Kieseberg

# What?

# Research Questions

- RQ1: To what extent are freely available Social Engineering supporting tools already automated and what does this mean in terms of Social Engineering?
- RQ2: Which phases of Social Engineering can be handled with the tools?
- RQ3: How do the different tools interact with each other, are there tool suites that start and accompany a complete Social Engineering process?
- RQ4: How reliable are the results of the tools?

# Methodology

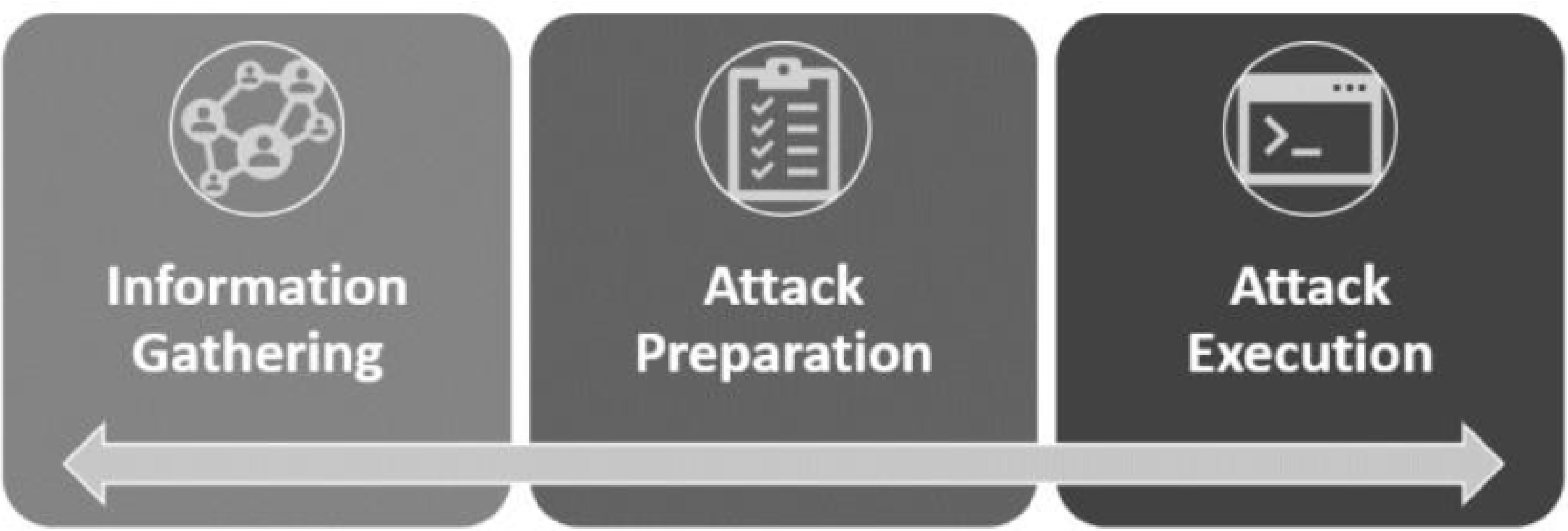


# Legal and ethical aspects

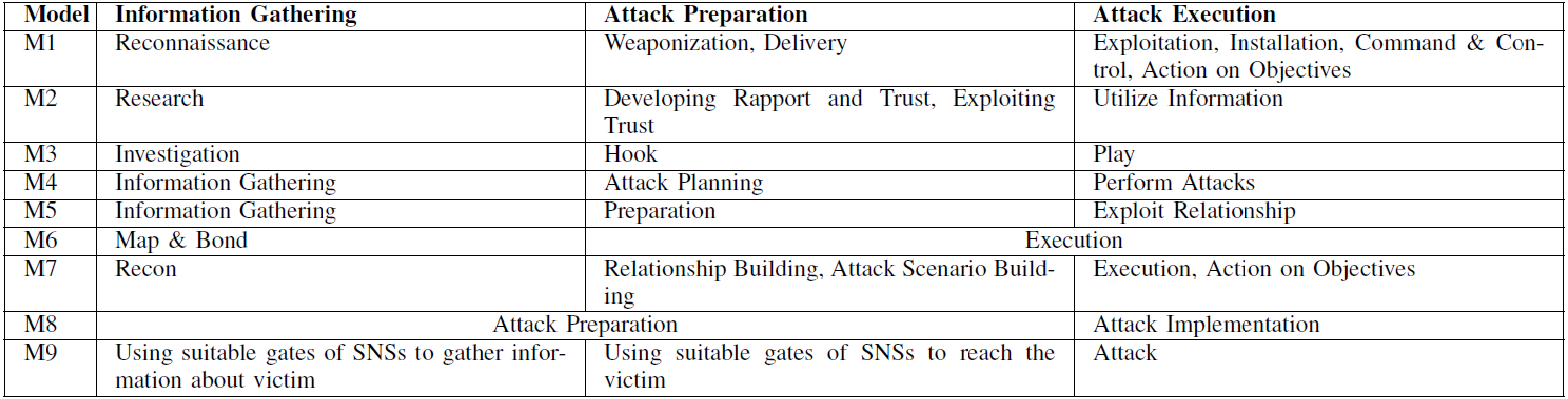
# SE Models and Frameworks - Selection

- The Cyber Kill Chain (M1)
- Social Engineering Cycle (M2)
- Social Engineering Lifecycle (M3)
- Social Engineering Pyramid (M4)
- Social Engineering Attack Framework (M5)
- Cycle of Deception (M6)
- Social Engineering Attack Spiral (M7)
- Session and Dialogue Based Framework (M8)
- Phase based and Source based Model (M9)

# The technical Social Engineering model (TSE)



# Phase Assignment



| Model | Information Gathering | Attack Preparation | Attack Execution |
|---|---|---|---|
| M1 | Reconnaissance | Weaponization, Delivery | Exploitation, Installation, Command & Control, Action on Objectives |
| M2 | Research | Developing Rapport and Trust, Exploiting Trust | Utilize Information |
| M3 | Investigation | Hook | Play |
| M4 | Information Gathering | Attack Planning | Perform Attacks |
| M5 | Information Gathering | Preparation | Exploit Relationship |
| M6 | Map & Bond | Execution | |
| M7 | Recon | Relationship Building, Attack Scenario Building | Execution, Action on Objectives |
| M8 | Attack Preparation | | Attack Implementation |
| M9 | Using suitable gates of SNSs to gather information about victim | Using suitable gates of SNSs to reach the victim | Attack |

# Tool Comparison

Information Gathering

- User Data
- Technology checks
- Email formats
- Data breaches and leaks
- Online times
- Personal information

Attack Preparation & Execution

- Preparing Payloads
- Tone & Emotions in Text
- Bot preparation
- Phishing with website cloning
- Mass Mailer
- Bot utilization

# Conclusion & Outlook

Contact: Peter Kieseberg

Institute of IT Security Research
St. Pölten University of Applied Sciences
Campusplatz 1, 3100 St. Pölten
peter.kieseberg@fhstp.ac.at