Conducting Ethical yet Realistic Usable Security Studies

Amir Herzberg and Ronen Margulies
Dept. of Computer Science
Bar Ilan University

Agenda

- Conflicts in usable security studies
- Introducing the Experiment, or: “how to balance the risk level”
- Ethical Attacks Simulations

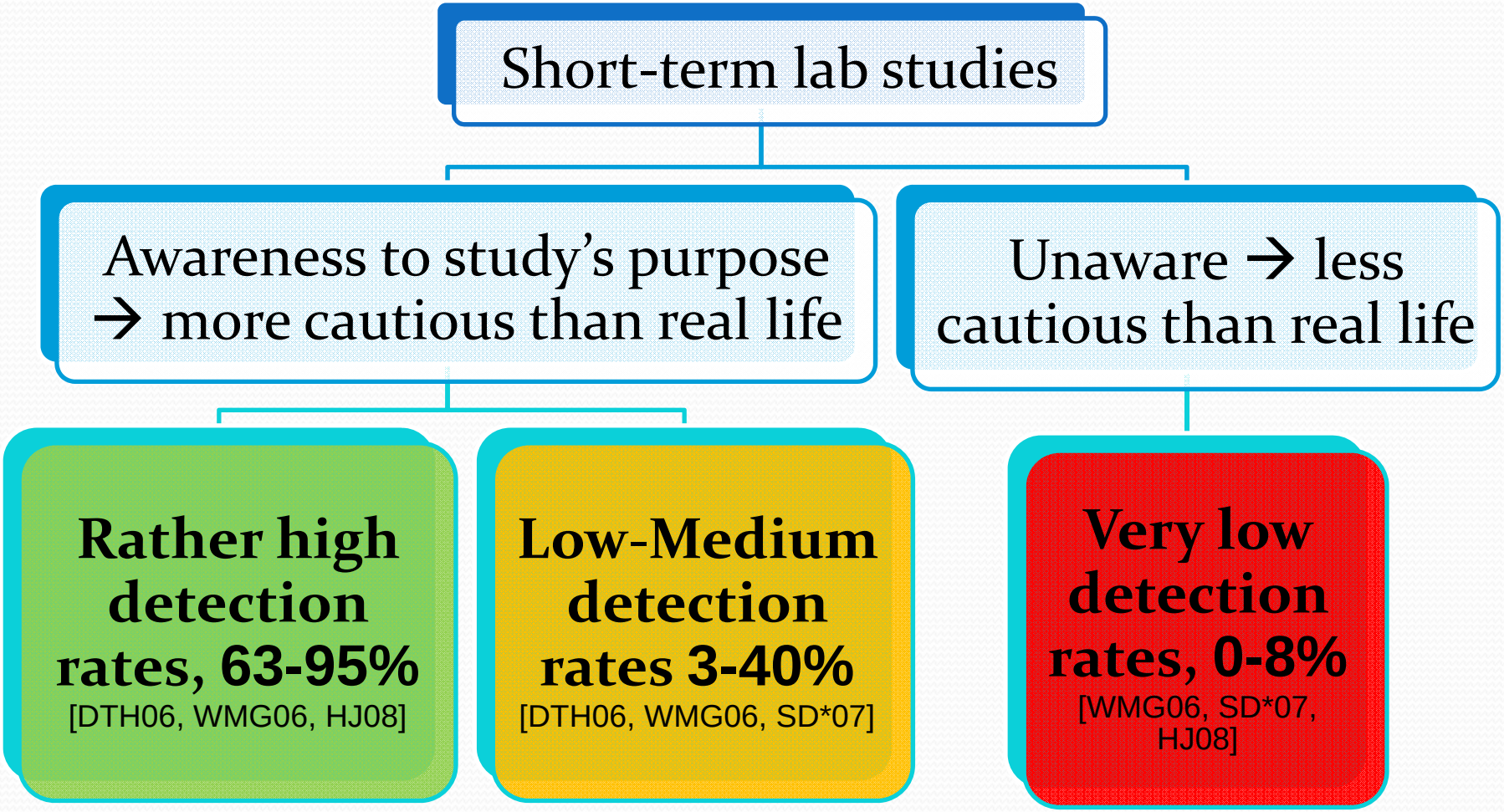
Conflicts in Usable Security Studies

- Two (conflicting) requirements for a user study
  - **Ethics**: Users should know they might be attacked
  - **Realism**: Users should act as in real-life

What affects users' behavior?

- **Presenting the study's (true) purpose**
  - Yes: users may be over cautious
  - No: unethical(?), irrelevant for testing new defenses
- **User account and risk**: fake/real, site sensitivity
- **Study's environment**
  - Lab environment: @ University, w/ or w/o experimenter
  - Home environment: personal device, favorite browser

Previous Anti-Phishing User Studies



Solution: Long-Term Real-Use Studies

- Long-term experiment, real-purpose system
  - **Realistic**
    - Awareness is not a problem (less focus on security)
    - New mechanisms can be taught
    - Familiar environment
  - **Ethical**: users know they will be attacked
- What else is missing?
  - Use of real sensitive user accounts is unacceptable

➔ Need to provide motivation to detect attacks as in sensitive sites

Agenda

- Conflicts in usable security studies
- Introducing the Experiment, or: “how to balance the risk level”
- Ethical Attacks Simulations

Balancing Attack Detection Motivation

- **Our system**: Online exercise submission system
  - ~400 students, used regularly for 2 years
  - Dozens – hundreds logins per user
- `Only' an exercise submission system, not so sensitive..
- Sensitive Site: **negative** results upon credentials theft
  - Rare but significant
- Our study: **positive** reward for detecting attacks
  - Certain but not so significant
- Challenge to fine-tune the reward to best match real-life motivation

Introducing the Study

- First year, attempt #1: Weak Motivation
  - Did not mention the study, only "test for mechanisms"
  - Up to 5 points bonus for detecting attacks
  - 26% did not cooperate
- Second year, attempt #2: Extra Motivation
  - Explained about phishing, ourselves and the experiment
  - Asked to participate and promised our gratitude
  - 5 points bonus for participation, reduced if not detecting attacks
  - 18% did not cooperate

Fairness

- Reward is based on performance, performance is based on the defense mechanisms (some better than others)
  - Is this fair? Is it Ethical?
  - Division to groups of defense mechanisms is a must
  - No harm done if not detecting attacks
  - Compare with medical studies (weak medicine, placebo)

Agenda

- Conflicts in usable security studies
- Introducing the Experiment, or: “how to balance the risk level”
- Ethical Attacks Simulations

Ethical Attacks Simulations

- Deciding on simulated attacks
  - Real-life popularity & feasibility
  - How hard it is to implement on a user-study
  - Legal & ethical issues, user-consent
- Some attacks are problematic to simulate
  - Pharming – requires DNS spoofing
  - Browser interference (e.g., bookmark replacement)
- Partial implementation (**as if** 1st phase occurred)
  - Redirect to spoofed site **as if** DNS poisoned
  - Redirect to spoofed site **as if** bookmark replaced

Measuring Attacks Results

- What is the expected user behavior upon detecting a spoofed login page?
- How would users be sure their detection was noticed?
- Disconnecting is not enough, need to report detection
  - We used a “Report Phishing Page” button
  - Is there some bias here?
- Long-term usage causes users to ignore the button unless feeling under attack

Conclusions

- **Challenge #1**: Realistic & Ethical studies
  - Awareness + Long-Term ➔ A solution to both issues
- **Challenge #2**: Sense of risk on non-sensitive sites?
  - Positive reward instead of using real sensitive accounts
- **Challenge #3**: Simulating Problematic Attacks
  - Partial implementation of attacks **as if** 1st phase occurred

Thank you!

Questions?