**Problem Definition**

- Traditional security attacks exploit vulnerabilities in software, systems and network infrastructures that supported information services.
- New attack models pollute input data to online personalization algorithms and effectively control the output.
- Users make informed decisions based on the information presented to them via online systems.
- By controlling the information presented to the user, an attacker can influence user’s decisions, attitude, behavior, or compromise the integrity of e-commerce.

**Goals and Objectives**

- Conduct a qualitative study to understand what users know about personalization in the online search domain, and/or pollution attacks.
- Evaluate a user facing browser extension named Bobble that shows how search results are personalized by location to gather feedback about user’s experience and awareness of personalization in search and pollution attacks.
- Use the findings to derive design implications for tools to alert users regarding anomalous personalization inputs or outputs and enable them to repair their profiles as a defense mechanism against pollution attacks.

**Methodology**

- Conducted a qualitative study of 20 users in spring 2015 to inquire about their search habits, awareness of personalization and knowledge of manipulation of search results.
- Users installed Bobble and performed a series of weekly tasks to search for key phrases provided to them over a one month period.
- In these tasks, search results were manipulated for 10 users to check if users were able to discern the manipulated results.

**Preliminary Findings**

- Users were unaware about the functioning of personalization algorithms and the extent to which pollution attacks could influence their preferences and behaviors.
- Most users did not detect that search results were manipulated.
- Bobble was deemed to be useful but difficult to interpret.

**Future Work**

- Complete data analysis and write up.
- Design and implement a user-facing tool to support users in detecting and undoing the effects of a pollution attack.