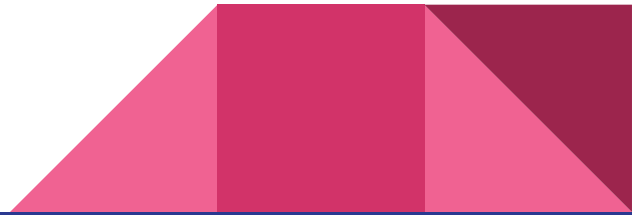
Skill Squatting Attacks on Virtual Personal Assistants (VPAs)

Group #9

Introduction

- VPAs - **Amazon Alexa**, Apple's Siri, **Google Now,** Microsoft's Cortana, etc.
- Voice Squatting Attack (VSA) - the adversary exploits how a skill is invoked and the variations in the ways the command is spoken to cause a VPA system to trigger a malicious skill instead of the one the user intends.
- Voice Masquerading Attack (VMA) - aims at the interactions between the user and the VPA system



Threats

- Both skills are susceptible to threats that include disclosure of one's home address, financial data, and other sensitive information.
- Information stealing
- Phishing

Defense Against VSAs and VMAs

- *Skill-name Scanner* - a web crawler that will be built to collect metadata from Alexa's skill market to scan for skills that are susceptible to VSAs.
- Defense against VMA - take a skill's and/or user's response as input to determine whether an impersonation risk is present, and alert the user once detected.
  - *Skill Response Checker (SRC)* - capture suspicious responses from a malicious skill
  - *User Intention Classifier (UIC)* - check voice commands issued by the user to find out whether he/she attempted to switch to a different skill in a wrong way, which can lead them right into the trap set by the malicious skill.

Tentative Schedule