**Hey Alexa, is this Skill Safe?**

Taking a Closer Look at the Alexa Skill Ecosystem

Christopher Lentzsch¹, Sheel Jayesh Shah², Benjamin Andow³,⁴, Martin Degeling¹, Anupam Das², William Enck²

---

Skills can impersonate known developers, bypass permission APIs, run unapproved code and don't provide adequate privacy policies

### Our Approach

- Large-scale analysis of Alexa skills
- Collected meta-data for 90,194 unique skills
- Invoked existing skills semi-automated via TTS
- Enhanced PoliCheck to analyze skills' privacy policy
- Published our own skills to confirm findings
- Found limitations in the vetting process
- Analyzed use of Skill squatting techniques
- Evaluated the use of mandatory privacy policies

### Future Work

- Understanding people’s mental model of how skills operate and process personal data
- Distinguishing native vs. 3rd party skills
- Dynamic analysis of skills to detect further violations of policies

---

Our research was presented at the Network and Distributed System Security Symposium (NDSS) in February 2021.


---

**Dormant Intents – Back-end Code Changes after Approval**

- An attacker can alter responses without being detected
- These changes can direct the user to trigger dormant intents
- These intents are not triggered and not checked during certification
- Dormant intents can collect sensitive data (e.g., phone number)

### Publish skills using well-known Developer Names

- Developers can register themselves with any company
- Skills appear to be developed by an authentic source
- This can help an adversary launch phishing attacks
- We registered as several well-known companies

### Bypassing Permissions – Access without the APIs

- Permissions allow accessing personal information
- Users must grant permission upon activation
- Several Skills directly request or ask such information from end-users
- We found 358 skills requesting information protected by a permission API

### Privacy Policies – Data practices aren't fully disclosed

- Skills requesting permissions must provide a privacy policy
- Do privacy policies properly address the permissions requested? i.e., explicitly state the data collection and share practices
- 23.3% do not fully disclose the data types associated with permissions requested

---

**Workflow diagram for making backend code changes to trigger a dormant intent which will contain sensitive information like phone number.**

**Detailed breakdown of skills potentially bypassing the Alexa permission model.**

---

This material is based upon work supported in parts by the National Science Foundation under grant number CNS-1849997 and by the state of North Rhine-Westphalia.

https://alexa-skill-analysis.org