

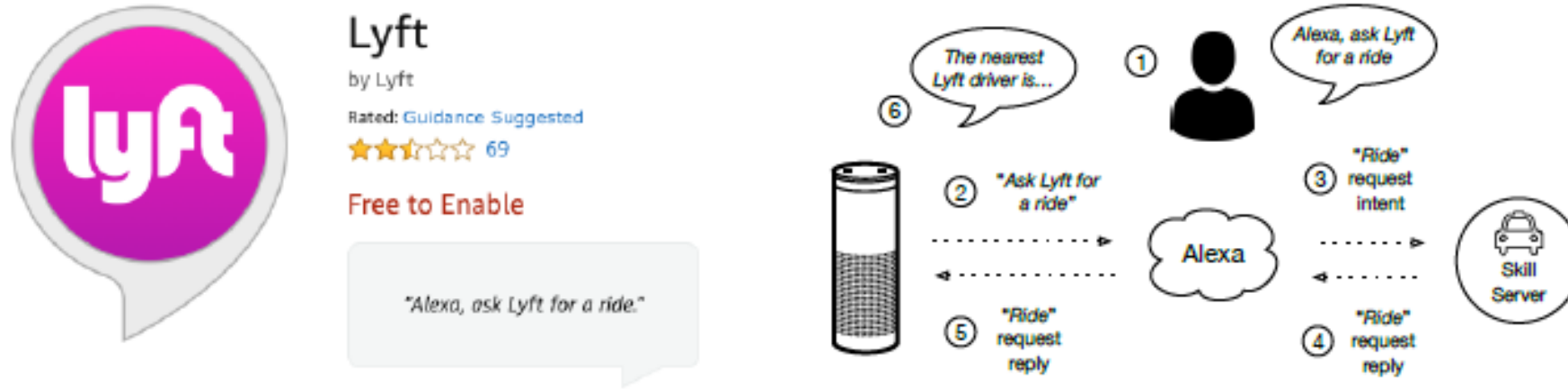
CPSC 8570 -Security in Advanced Networking technologies

Skill Squatting Techniques on Amazon Alexa – A Demonstration

Nandini Krupa Krishnamurthy

Recap

1. Objective – To demonstrate skill squatting attack on Amazon Alexa.
2. Skills – The third party applications that leverage Alexa voice services.
3. Alexa Skill Invocation



4. Types of errors :
 - a. Homophones – same pronunciation. Sail-Sale, boil-Boyle
 - b. Compound words – super-highway-superhighway, outdoors-out doors
 - c. Phonetic Confusions – wet (W EH T)- what (W AH T)
 - d. Other errors – no specificity
5. Skill Squatting Attack – Confusion in the systematic error from one word to another creates a possibility of invocation of a malicious skill instead of the target skill.

Method

1. Build pairs of skills (27) that are frequently confused by Alexa .

Skill 1	Skill 2
How much is the Time?	How much is the Dime?
Spell Sweden	Spell Sweeten
Wet Cloth	What Cloth
Adventures Out Doors	Adventures Outdoors
Lock Test	Luck Test
Sail Directions	Sale Directions
Cell Size	Sell size

2. Test these.
3. Squat existing Skills.



Cat Fats
FREE
Available instantly on your connected Alexa device.

Skill 1	Skill 2
Cat Fats	Cat Facts
Phish Geek	Fish Geek



Cat Facts
★★★★☆ ~ 306
FREE
Available instantly on your connected Alexa device.

“How much is the time” vs “How much is the dime”

The screenshot displays the Alexa Developer Console interface. At the top, the navigation bar includes links for 'Your Skills', 'Spell Sweden', 'Build', 'Code', 'Test' (which is the active tab), 'Distribution', 'Certification', and 'Analytics'. On the right side of the navigation bar, there are icons for search, user profile (NK), and a 'Feedback forum' link.

Below the navigation bar, a section indicates 'Skill testing is enabled in:' with a dropdown menu set to 'Development'. To the right of this, there are three checkboxes: 'Skill I/O' (checked), 'Device Display' (checked), and 'Device Log' (unchecked).

The main content area is divided into three tabs: 'Alexa Simulator' (selected), 'Manual JSON', and 'Voice & Tone'. Under the 'Alexa Simulator' tab, there is a language selector set to 'English (US)' and a text input field with a microphone icon and the placeholder text 'Type or click and hold the mic'.


Below the input field, a chat log shows the interaction history:

- A user input bubble: "alexa open how much is the time"
- An Alexa response bubble: "It's 11:40 AM."
- A user input bubble: "alexa can you please open how much is the time"
- An Alexa response bubble: "It's 11:40 AM."

On the right side of the console, there is a large blue speech bubble with the text "It's 11:40 AM." and a play button icon.

Below the speech bubble, there is a section titled 'Skill I/O' with two columns: 'JSON Input' and 'JSON Output'. Both columns are currently empty. A message at the bottom of this section states: "Skill I/O is available only for speech requests to skills you have created."

“Sweden” vs “Sweeten”

 alexa developer console

< Your Skills

Spell Sweden

Build




Code

Test

Distribution

Certification

Analytics

Feedback forum

Skill testing is enabled in:

Development

☒ Skill I/O

☒ Device Display

☐ Device Log

Alexa Simulator

Manual JSON

Voice & Tone

English (US)


Type or click and hold the mic

alexaspeakertest


Here's your spelling: Sweeten is spelled as S W E E T E N. Congratulations, you are not under a possible attack.

alexaspeakertest

'Sweden' is spelled: SWEDEN.



'Sweden' is spelled: SWEDEN.



Skill I/O

JSON Input


1

JSON Output

1

Skill I/O is available only for speech requests to skills you have created.

“Wet” vs “What”

 alexa developer console

[Your Skills](#) [Spell Sweden](#) [Build](#) [Code](#) [Test](#) [Distribution](#) [Certification](#) [Analytics](#)

Feedback forum

Skill testing is enabled in:

Development

☒ Skill I/O ☒ Device Display ☐ Device Log

Alexa Simulator

Manual JSON

Voice & Tone

English (US)

Type or click and hold the mic

alexasimulatorecho

Here's your spelling: So, this is actually the correct skill you were searching for. Congratulations, you are not under a possible attack. Wet cloth means a piece of cloth covered or saturated with water or another liquid.

alexa open wetcloth

alexaopenwetcloth

Here's your spelling: Wet cloth means a piece of cloth covered or saturated with water or another liquid. Congratulations, you are not under a possible attack.

Skill I/O


JSON Input

```
1 {
2   "version": "1.0",
3   "session": {
4     "new": true,
5     "sessionId": "amzn1.echo-api.session.0e977ab",
6     "application": {
7       "applicationId": "amzn1.ask.skill.dc837f",
8     },
9     "user": {
10      "userId": "amzn1.ask.account.AGG2QV6BN66",
11    },
12  },
13  "context": {
14    "System": {
15      "application": {
16        "applicationId": "amzn1.ask.skill.dc",
17      },
18      "user": {
19        "userId": "amzn1.ask.account.AGG2QV6",
```

JSON Output

```
1 {
2   "body": {
3     "version": "1.0",
4     "response": {
5       "outputSpeech": {
6         "type": "SSML",
7         "ssml": "<speak> Here's your spelling:",
8       },
9       "card": {
10        "type": "Simple",
11        "title": "Wet Cloth",
12        "content": "Wet cloth means a piece of",
13      },
14      "shouldEndSession": true,
15      "type": "_DEFAULT_RESPONSE"
16    },
17    "sessionAttributes": {},
18    "userAgent": "ask-nodejs/1.0.25 Node/v6.10.3"
19  }
```

“Phish” vs “Fish”

 alexa developer console

[Your Skills](#) [Spell Sweden](#) [Build](#) [Code](#) [Test](#) [Distribution](#) [Certification](#) [Analytics](#)

Feedback forum

Search

NK

Menu

Skill testing is enabled in: Development

☒ Skill I/O ☒ Device Display ☐ Device Log

Alexa Simulator

Manual JSON

Voice & Tone

English (US)

Type or click and hold the mic


alexla open fish geek

Here's your fun fish fact: Lungfish can live out of water for several years. It secretes a mucus cocoon and burrows itself under the unbaked earth. It takes in air with its lung through a built-in breathing tube that leads to the surface. A lungfish has both gills and a lung.

alexla can you please open fish geek

Here's your fun fish fact: The mud skipper is a fish that spends most of its time out of water and can “walk” on its fins. It carries a portable water supply in its gill chambers when it leaves the water. It can also breathe through the pores of its wet skin.

Skill I/O




Phish Geek

★★★★☆ 2

FREE

Available instantly on your connected Alexa device.



Fish Geek


★★★★★ 4

FREE




Available instantly on your connected Alexa device.

Skill I/O is available only for speech requests to skills you have created.

“Fats” vs “Facts”

 alexa developer console

[Your Skills](#)[Spell Sweden](#)[Build](#)[Code](#)[Test](#)[Distribution](#)[Certification](#)[Analytics](#)

[Feedback forum](#)

Skill testing is enabled in:

Development

☒ Skill I/O☒ Device Display☐ Device Log

[Alexa Simulator](#)[Manual JSON](#)[Voice & Tone](#)

English (US)

Type or click and hold the mic

alexaspeakertest

alexaspeakertest

alexaspeakertest

alexaspeakertest

alexaspeakertest

alexaspeakertest

alexaspeakertest


alexaspeakertest

alexaspeakertest


alexaspeakertest

alexaspeakertest

alexaspeakertest

 Here's your Cat Fact! Cats respond better to women than to men, probably due to the fact that women's voices, have a higher pitch.


Skill I/O



Cat Fats

FREE

Available instantly on your connected Alexa device.



Cat Facts

★★★★★ ~ 306

FREE

Available instantly on your connected Alexa device.

Skill I/O is available only for speech requests to skills you have created.

- Attacks in this project are tested only in a controlled, developer environment.
- Care is taken not to produce any malicious skill to the public skill store.

Drawback

- Unavailability of NSP dataset.
- Until now testing is based on a single user.

Drawback

1. Testing with different user inputs for the same skills.
2. Extending skill squatting attacks to Spear Skill squatting attacks which is based on interpretation of words based on demography and gender.
3. Extend the project to Word Squatting attacks on the currently available Skills.

Next Steps



Thank You!