Tempest

ACADEMY

Conference

2023

Mapeamento de vulnerabilidades no Amazon Echo

Através do uso de Alexa Skills

Classificação da Informação: PÚBLICA
Autor da apresentação: Renato Alpes

01 Introdução

02 Conceitos básicos

03 Superfície de ataque

04 Ataques

05 Conclusão

Introdução

whoami

Tempest

[ACADEMY]

Conference

Conceitos básicos

Echo Dot 3

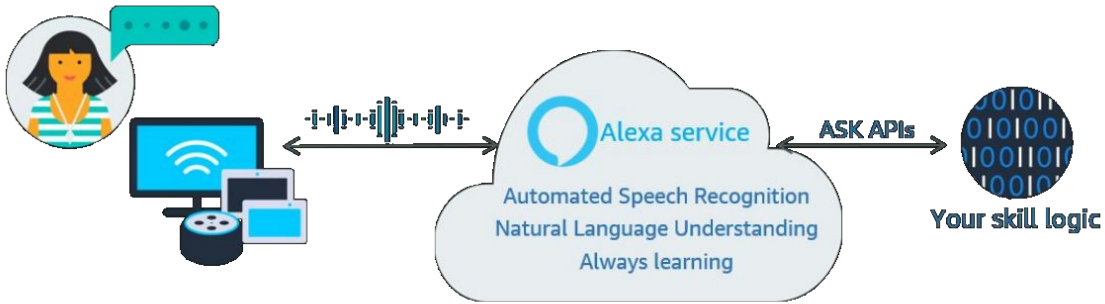
Tempest

:ACADEMY:

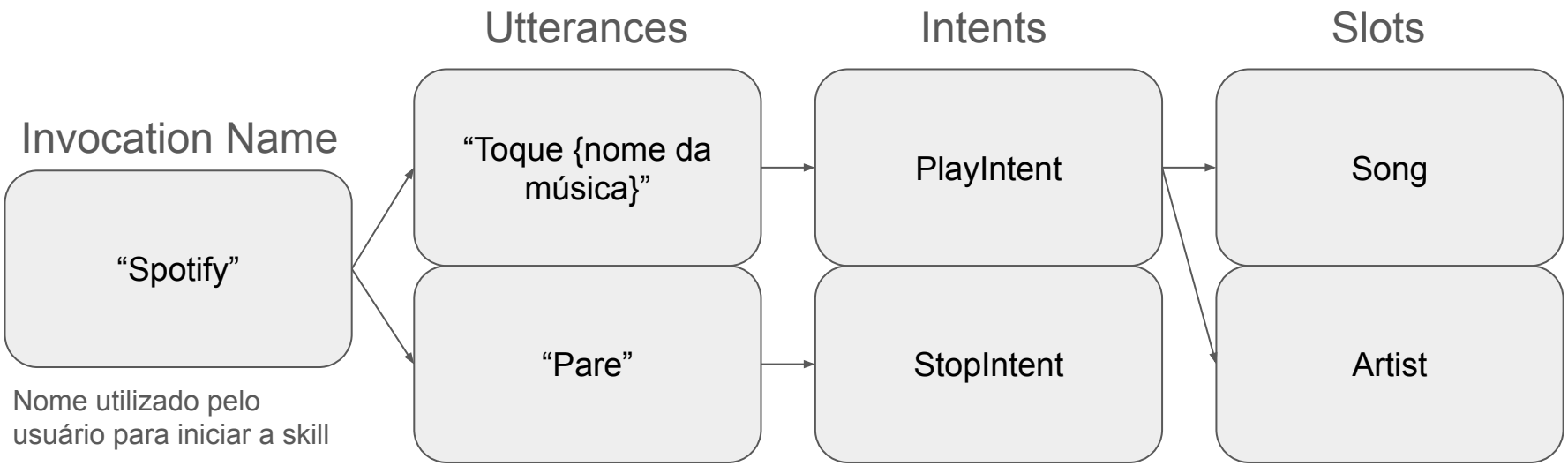
Conference

Alexa Skills

- Permitem que terceiros criem funcionalidades para a Alexa
- Podem ser utilizadas para a integração de um serviço com a Alexa



Voice Model


Utterances
Intents
Slots
Invocation Name
“Spotify”
“Toque {nome da música}”
“Pare”
PlayIntent
StopIntent
Song
Artist
Nome utilizado pelo usuário para iniciar a skill
Uma ou mais frases que são mapeadas para um Intent
Objeto que define uma intenção do usuário
Zero ou mais informações extras associadas a um Intent

Ativação de skills

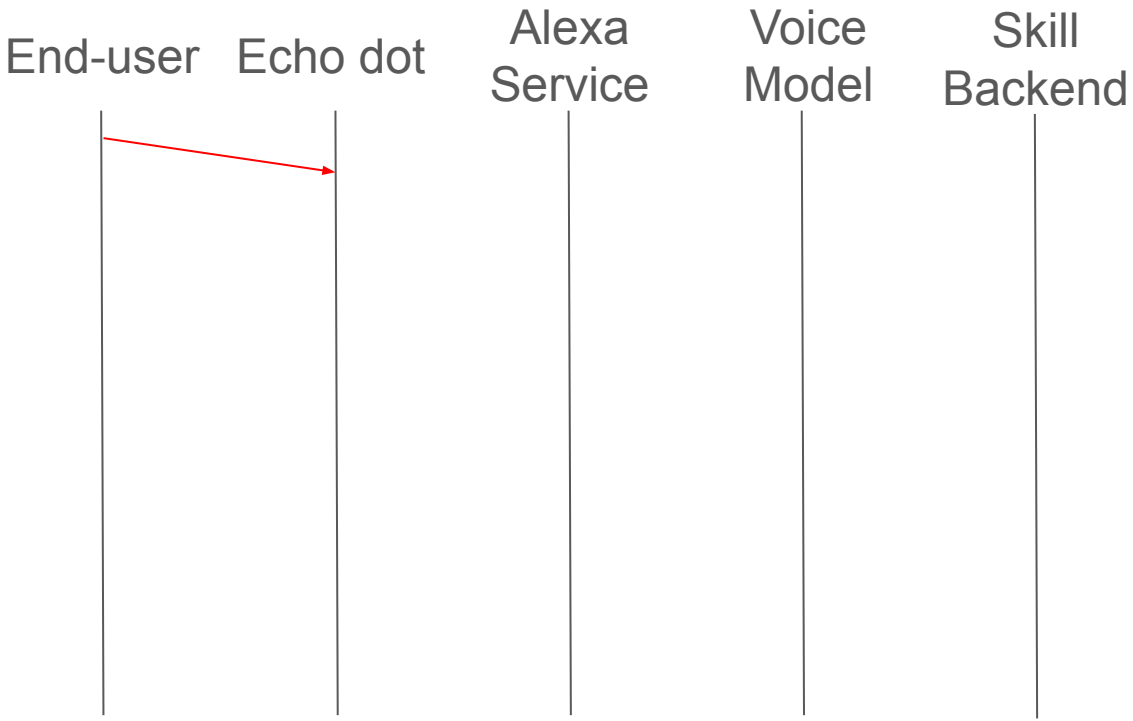
Manual:

- O usuário ativa a skill manualmente pelo *companion app*

Por voz:

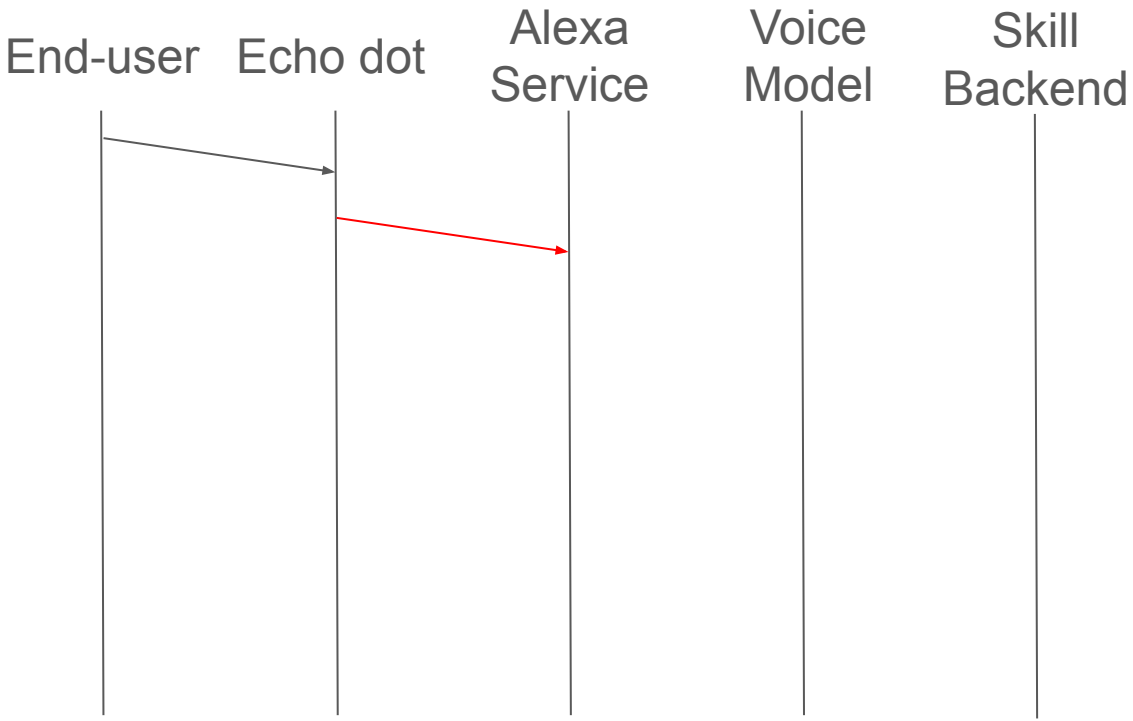
- Intencionalmente: O usuário solicita o uso da skill utilizando a frase de ativação específica
- Ativação inferida: O usuário faz um pedido que pode ser atendido por uma ou mais skills da loja, sem solicitar alguma skill em particular

Interação com uma skill



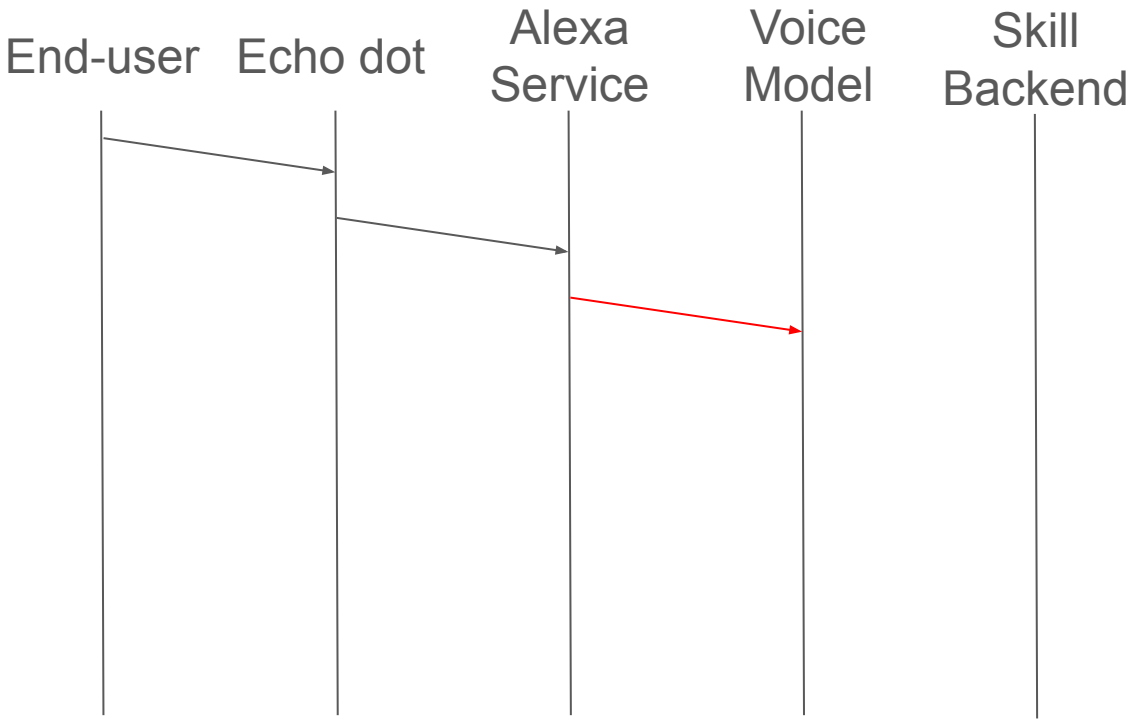
“Alexa, abra o Spotify e toque Idol por Yoasobi”

Interação com uma skill



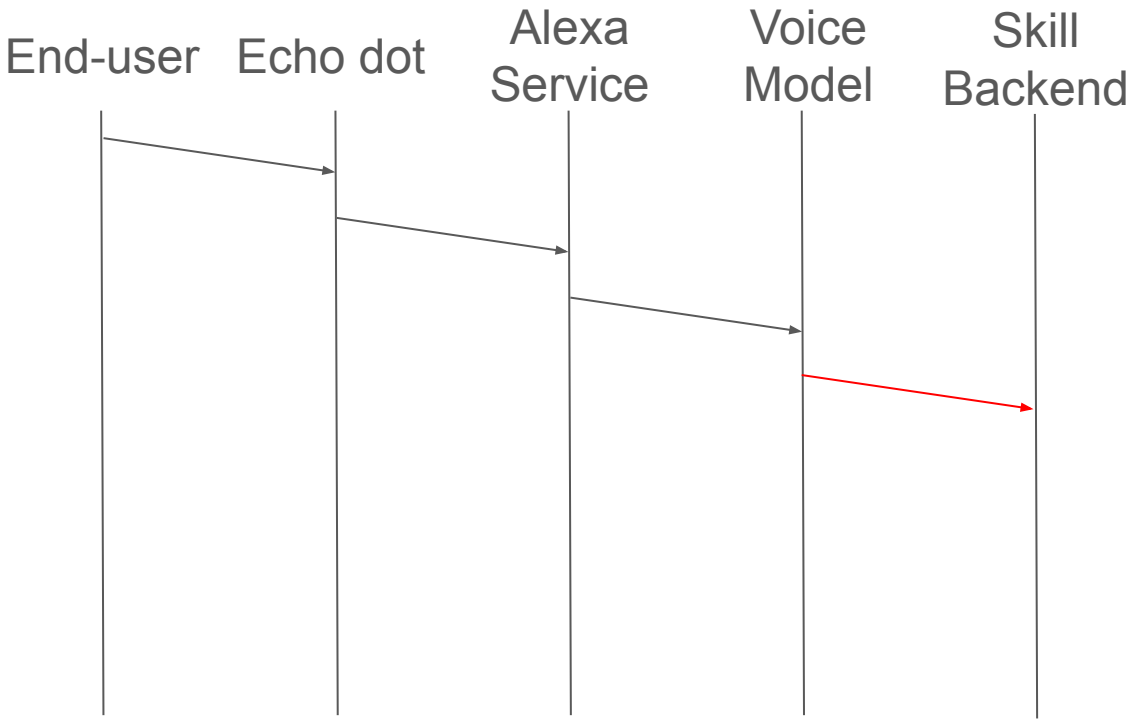
“Abra o Spotify e toque Idol por Yoasobi”

Interação com uma skill



Skill: Spotify
Utterance: Toque
Intent: PlayIntent
Slots: Idol, Yoasobi

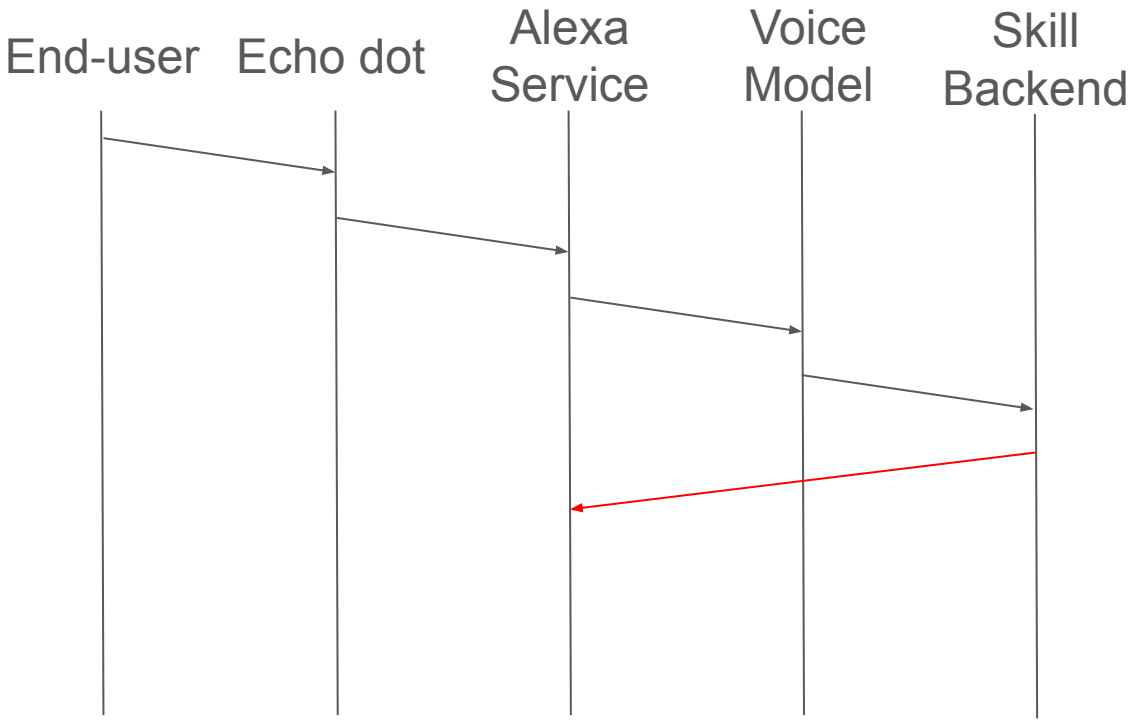
Interação com uma skill



POST /api HTTP 1.1
Host: spotify.com
[...]
Content-Type: application/json
[...]

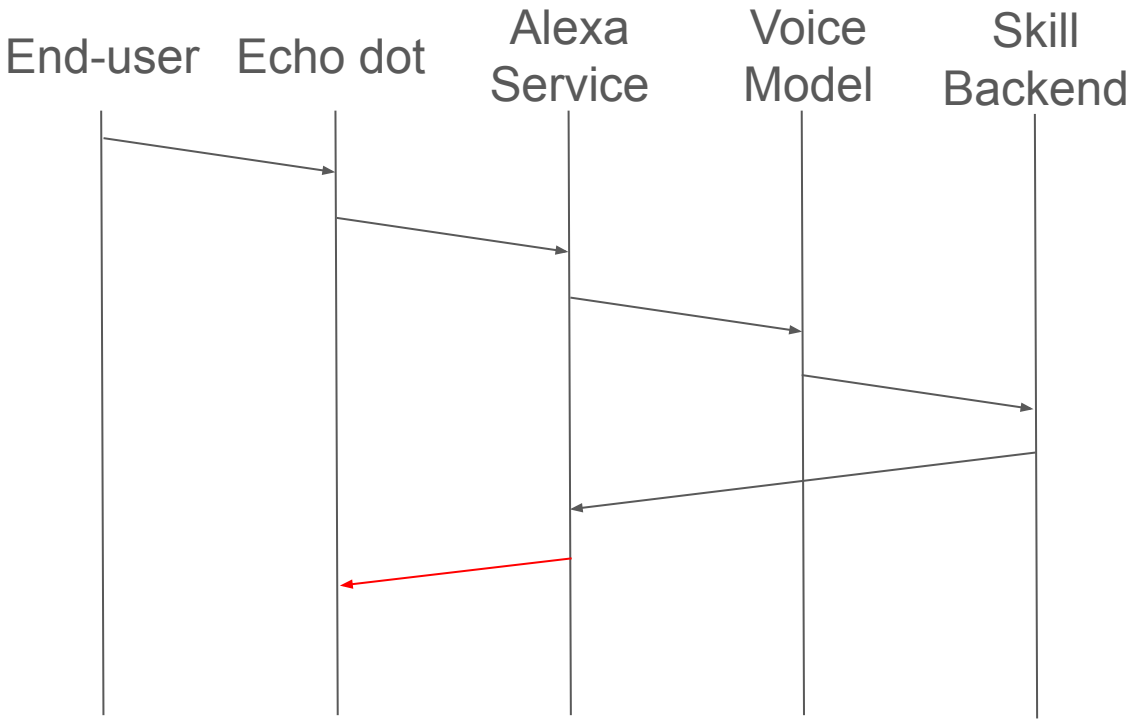
{[...],
“request”:{“intent”:
“PlayIntent”,
“Song”:”Idol”,
“Artist”:”Yoasobi”}
}

Interação com uma skill



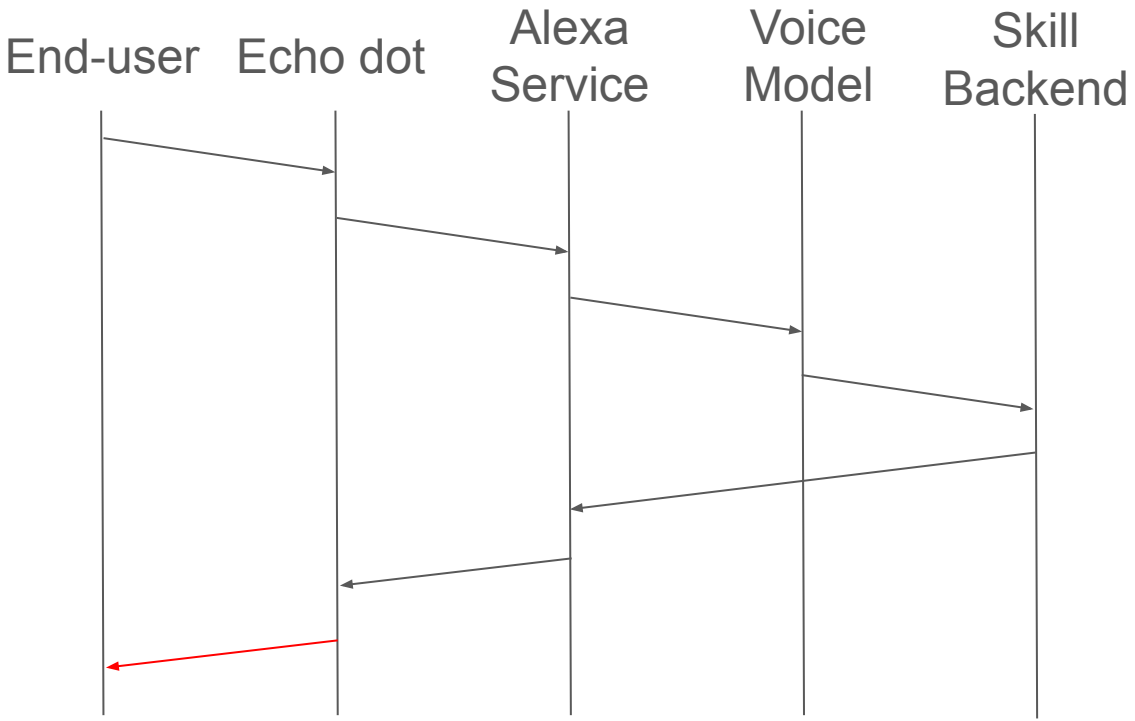

```
HTTP/1.1 200 OK
Content-Type:
application/json
[...]
{[...],
“response”:{
   “outputSpeech”:{
      “type”:”PlainText”,
      “text”:”Tocando idol”,
      [...]},
   [...]},
[...]}
```

Interação com uma skill



Reply: Tocando Idol

Interação com uma skill



“Tocando Idol”

Superfície de ataque

Conexão Bluetooth

- Modo de pareamento ativado por voz
- Nenhuma confirmação necessária para parear
- Speaker é controlado remotamente após pareado

Tempest

:ACADEMY:

Conference

Reconhecimento de comandos de voz

- Aceita comandos de terceiros
- Aceita comandos enviados através do speaker
- Arquivos de áudio gerados adversariamente podem ser entendidos como comandos

Ativação da skill

- Realiza a ativação de skills cuja frase de ativação foi enunciada sem confirmar com o usuário
- Permite a ativação automática de skills que dizem ser capazes de atender ao pedido do usuário
- Permite a criação de skills com frases de ativação com pronúncias idênticas
- Falhas na API da amazon podem permitir ativação arbitrária de skills

Tempest

:ACADEMY:

Conference

Execução da skill

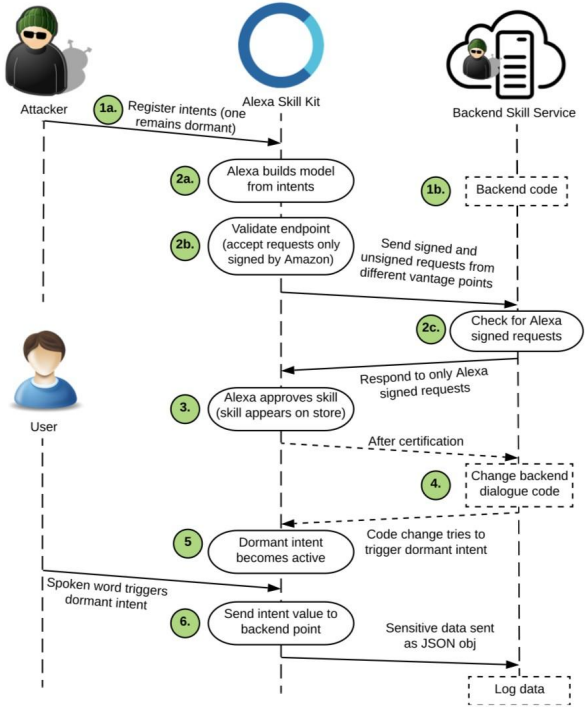
- Não garante que o comportamento da skill não foi modificado após sua publicação
- Permite que desenvolvedores contornem facilmente o uso das APIs da Amazon para lidar com informações sensíveis
- Não informa ao usuário quando a execução continua por um período muito longo de tempo

Resposta ao usuário

- Permite que skills enviem arquivos de áudio arbitrários
- Permite que skills enviem respostas arbitrárias
- Permite o envio de respostas vazias
- Permite a modificação de respostas para intents comuns como ajuda, parar e cancelar

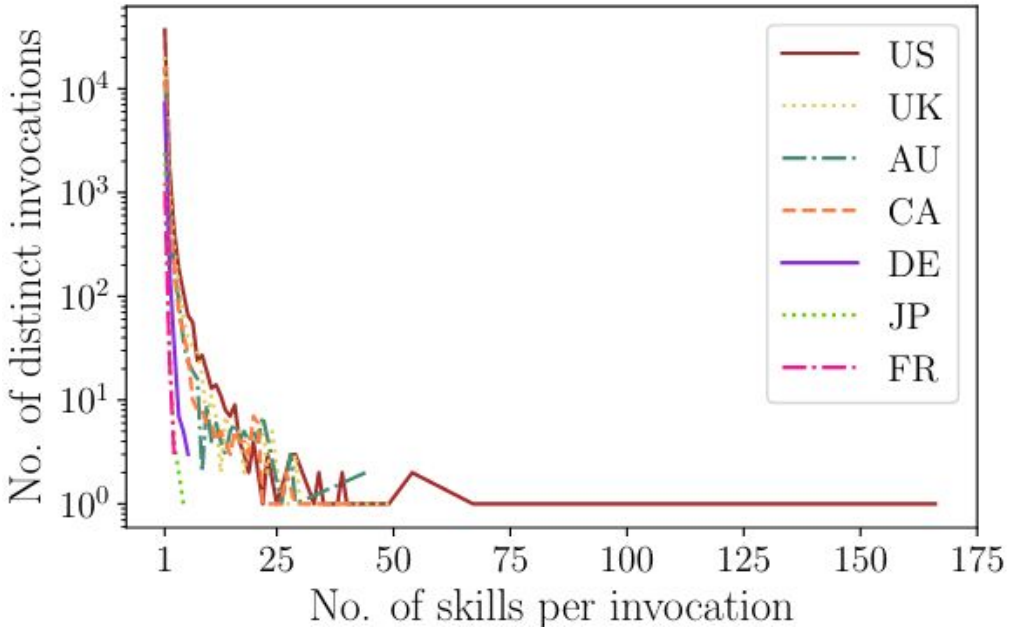
Ataques

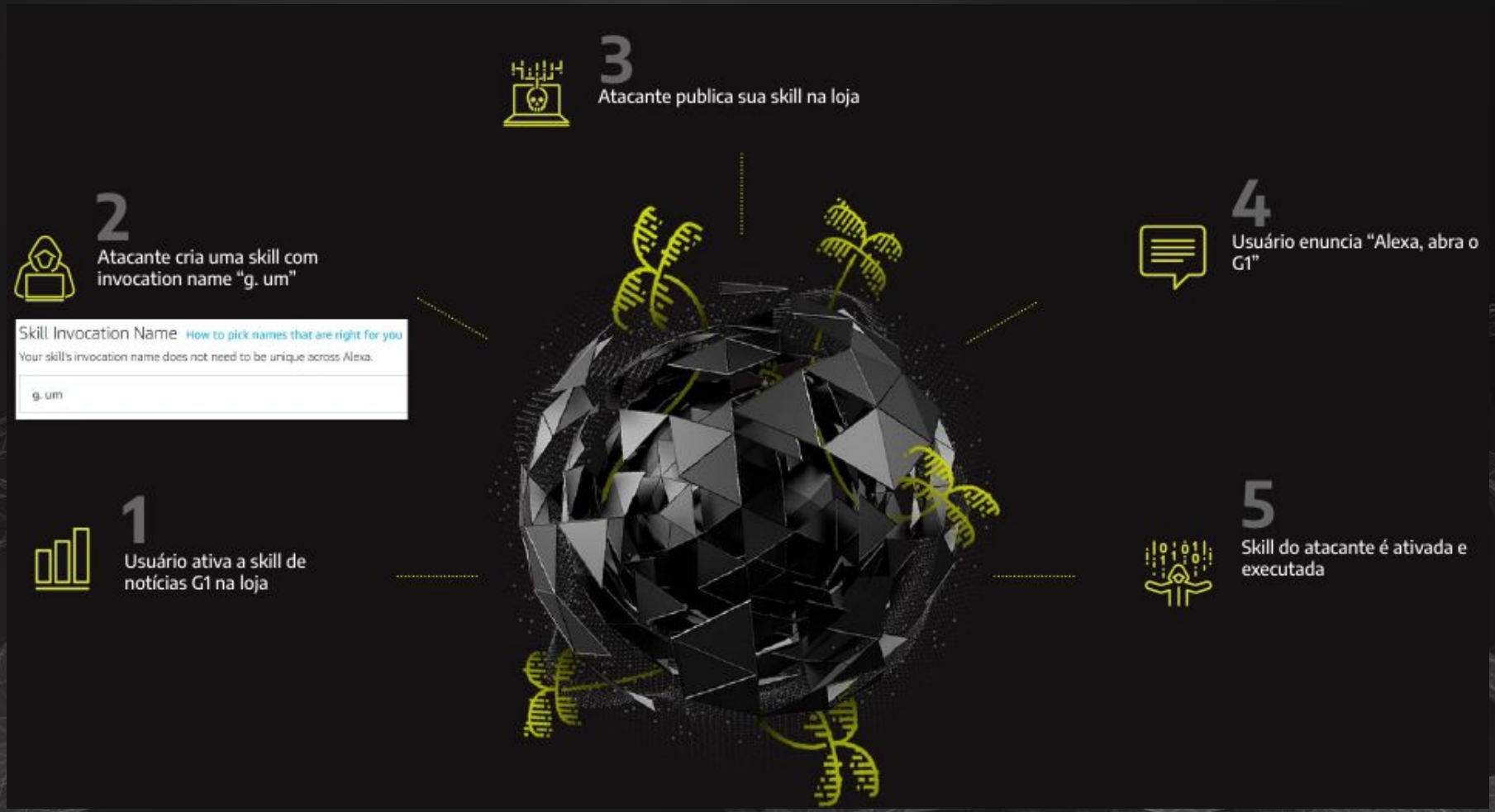
Bypass da certificação



Tempest
:ACADEMY:
Conference

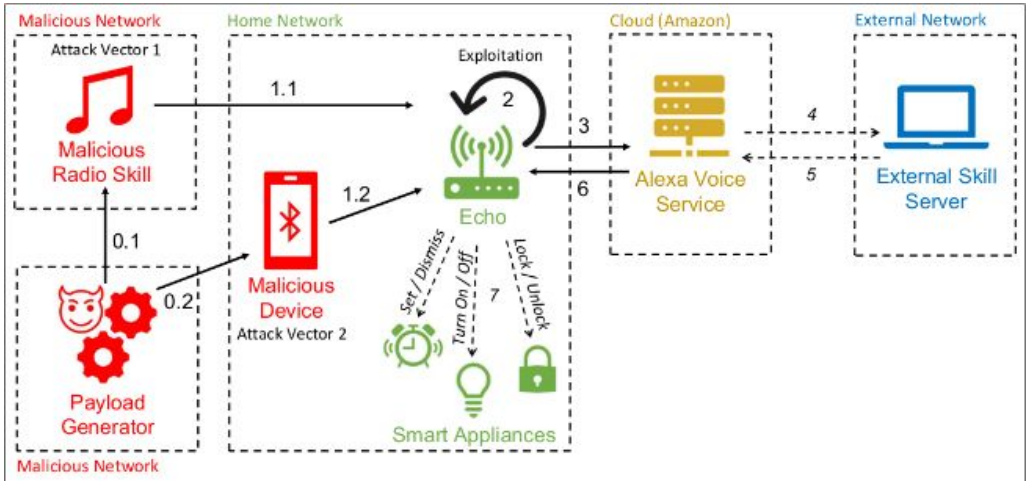
Skill Squatting




3
Atacante publica sua skill na loja
2
Atacante cria uma skill com invocation name "g. um"
Skill Invocation Name
How to pick names that are right for you
Your skill's invocation name does not need to be unique across Alexa.
g. um
4
Usuário enuncia "Alexa, abra o G1"
1
Usuário ativa a skill de notícias G1 na loja
5
Skill do atacante é ativada e executada

Tempest
:ACADEMY:
Conference

Alexa vs Alexa



3
Atacante toca o áudio no echo dot

2
Atacante conecta no echo vulnerável através do bluetooth

4
"Alexa, turn off [pausa] Alexa, what time is it?"

1
Atacante prepara um áudio malicioso com TTS

5
Echo reconhece e executa um comando arbitrário

Alexa vs Alexa

Tempest
[ACADEMY]
Conference

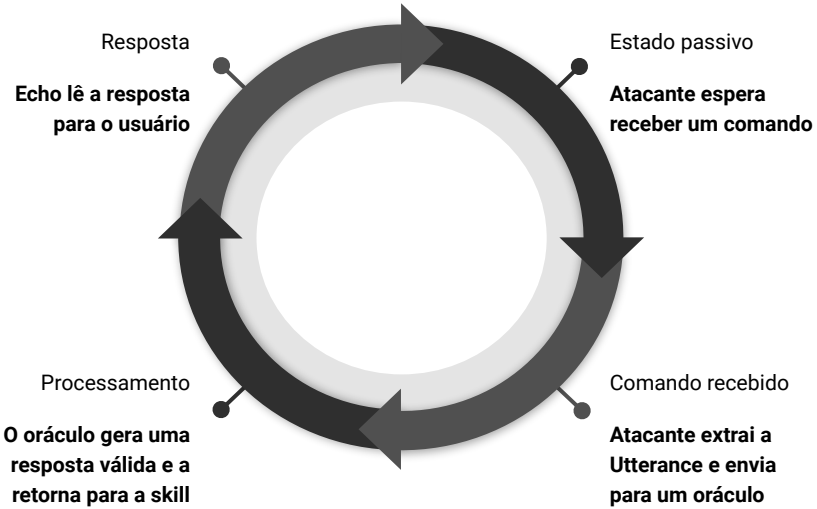
Vetor	Remoto	Múltiplo	FVV	Global	Engenharia social	Pode reiniciar
Skill de rádio	S	S	N	N	S	N
Bluetooth	N	N	S	S	N	S

- Permite controlar aplicações de smart home
- Permite editar calendários da conta
- Permite responder e deletar e-mails
- Permite fazer chamadas telefônicas
- Permite comprar itens na Amazon
- Permite invocar qualquer skill

Tempest
:ACADEMY:
Conference

Mask Attack

- Permite capturar comandos de voz
- Permite capturar dados pessoais
- Permite capturar senhas e PINs
- Permite modificar respostas
- Permite inferir hábitos do usuário



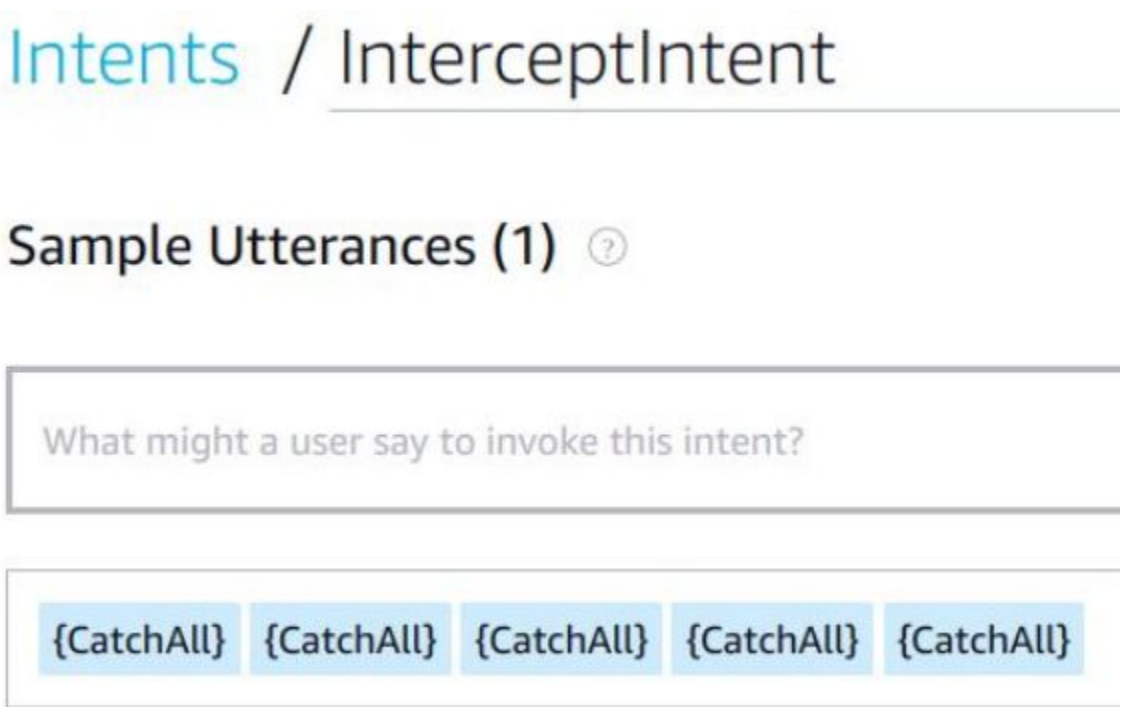
Mask Attack - setup

Tempest
[ACADEMY]
Conference

```
class LaunchRequestHandler(AbstractRequestHandler):
    """Handler for Skill Launch."""
    def can_handle(self, handler_input):
        # type: (HandlerInput) -> bool

        return ask_utils.is_request_type("LaunchRequest")(handler_input)

    def handle(self, handler_input):
        # type: (HandlerInput) -> Response
        speak_output = '<break/><break/><break/><break/><break/><break/><break/><break/>

        return (
            handler_input.response_builder
                .speak(speak_output)
                .ask(speak_output)
                .response
        )
```

Mask Attack - setup

Tempest
[ACADEMY]
Conference



Mask Attack - setup

Tempest
[ACADEMY]
Conference

Slot Types / Everything

Custom slot types with values define a representative list of possible values, IDs and synonyms.

Slot Values (5)

Bulk Edit

Enter a new value for this slot type

VALUE	ID (OPTIONAL)	SYNONYMS (OPTIONAL)
kij192eu912e9	Enter ID	Add synonym
28ue891h2	Enter ID	Add synonym

Mask Attack - execução

Tempest
[ACADEMY]
Conference

Passo 1	Passo 2	Passo 3	Passo 4
Skill maliciosa é executada	Backend malicioso recebe o LaunchIntent	Backend responde o LaunchIntent com “<break/><break/>...”	Skill permanece escutando por toda a duração da resposta

Mask Attack - execução

Tempest
[ACADEMY]
Conference

Passo 5	Passo 6	Passo 7	Passo 8
Usuário realiza uma interação ("Alexa, como está o clima em Recife?")	Skill recebe cada palavra como um slot preenchido de InterceptIntent	Backend encaminha o pedido para a API da Amazon e retorna a resposta	Informação sensível fica armazenada no backend

Bypass da API de informações sensíveis

Técnica de *bypass*	Dado obtido
Redireciona o usuário para uma página web onde ele deve cadastrar seu nome e ID do jogo	Nome
Redireciona o usuário para uma página web que pede seu e-mail para enviar um código utilizado para criar uma sessão do jogo	E-mail
Skill pede para o usuário adicionar seu endereço a uma lista Alexa criada pela skill	Endereço
Skill pede o telefone do usuário como parte do cadastro por voz	Telefone

Conclusão

Tempest
[ACADEMY]
Conference

Ataques contra o hardware

- Não foram encontrados com os métodos utilizados

Ataques contra o usuário

- O echo dot é capaz de espionar usuários através de diversas técnicas que estão em constante evolução
- Ataques de *phishing* são facilitados pelo grau de confiança implícita que usuários tem na Alexa

Ataques contra Skills

- Dependem da implementação da Skill alvo

Sidechannel

https://www.sidechannel.blog/mapeamento-de-vulnerabilidades-no-amazon-echo-atraves-do-uso-de-alexa-skills/

Tempest

ACADEMY

Conference

Contato

Linkedin: rhas

rhas@cin.ufpe.br

Tempest
ACADEMY
Conference

Referências

- Attackers can force Amazon Echos to hack themselves with self-issued commands | Ars Technica
- Alexa, Google Home Eavesdropping Hack Not Yet Fixed | Threatpost
- Researchers Hacked Amazon’s Alexa to Spy On Users, Again | Threatpost
- How to Improve Alexa Skill Discovery with Name-Free Interaction and More | Amazon Developer
- The Scalable Neural Architecture behind Alexa’s Ability to Select Skills - Amazon Science
- HypRank: How Alexa determines what skill can best meet a customer’s need - Amazon Science
- Amazon Fixes Alexa Glitch That Could Have Divulged Personal Data | Threatpost
- Keeping the gate locked on your IoT devices: Vulnerabilities found on Amazon's Alexa - Check Point Research
- Documentation Home | Alexa Voice Service

Tempest

ACADEMY

Conference

Referências

- K. M. Malik, H. Malik, R. Baumann (2019). "Towards Vulnerability Analysis of Voice-Driven Interfaces and Countermeasures for Replay Attacks”
- D. Su, J. Liu, S. Zhu, X. Wang, W. Wang (2020). ""“Are you home alone?” “Yes” Disclosing Security and Privacy Vulnerabilities in Alexa Skills”
- S. Esposito, D. Sgandurra, G. Bella (2022). "Alexa versus Alexa: Controlling Smart Speakers by Self-Issuing Voice Commands”
- Y. Kim, D. Kim, A. Kumar, R. Sarikaya (2018). "Efficient Large-Scale Neural Domain Classification with Personalized Attention”
- A. Sabir, E. Lafontaine, A. Das (2022). "Hey Alexa, Who Am I Talking to?: Analyzing Users’ Perception and Awareness Regarding Third-party Alexa Skills”
- C. Lentzsch, S. Shah, B. Andow, M. Degeling, A. Das, W. Enck (2021). "Hey Alexa, is this Skill Safe?: Taking a Closer Look at the Alexa Skill Ecosystem”

Dúvidas?

Tempest

:ACADEMY:

Conference

2023