A INTERNET DAS COISAS: uma análise de segurança do dispositivo ECHO DOT

THE INTERNET OF THINGS: a security analysis of the ECHO DOT device

Tiago dos Santos Lisboa
Graduando em Redes de Computadores pela Fatec Bauru
E-mail: tiago.lisboa@fatec.sp.gov.br

João Victor Lopes Machado
Graduando em Redes de Computadores pela Fatec Bauru
E-mail: Joao.machado12@fatec.sp.gov.br

Henrique Pachioni Martins
Docente na Fatec Bauru
E-mail: henrique.martins01@fatec.sp.gov.br

RESUMO

Atualmente, está se tornando cada vez mais comum utilizar dispositivos de Internet das Coisas (IoT), como assistentes virtuais inteligentes, aparatos smart e demais outras possibilidades que tornam nosso cotidiano cada vez mais automatizado e simples. Além de tornar mais prático nosso dia a dia, o crescente número de dispositivos de IoT ergueram a questão considerável a respeito da privacidade e integridade dos usuários. Este artigo tem como proposta de fazer uma análise de segurança no dispositivo Amazon Echo dot, uma caixa de som inteligente desenvolvido pela Amazon e sem dúvida um dos dispositivos de IoT mais utilizados na atualidade. Para isso primeiro demonstramos a funcionalidade do Echo, e depois realizamos testes para encontrar vulnerabilidades possíveis, baseando-se em 3 critérios: ataque por som, por rede e por aplicativos de terceiros. Os resultados obtidos pelos nossos testes atendem as expectativas, expondo uma política de segurança da Amazon bem consolidada e regida. Constata-se, portanto, que as medidas implementadas pela Amazon em seus dispositivos Echo e no seu serviço em nuvem da Alexa, são ideias para o uso íntegro dos usuários.

Palavras-chave: Echo dot. IoT. Amazon.

ABSTRACT

Nowadays, it is becoming increasingly common to use Internet of Things (IoT) devices such as intelligent virtual assistants, smart appliances, and other possibilities that make our daily lives increasingly automated and simple. In addition to making our daily lives more practical, the growing number of IoT devices has raised the considerable question of user privacy and integrity. This article aims to conduct a security analysis of the Amazon Echo dot device, a smart speaker developed by Amazon and undoubtedly one of the most used IoT devices today. To do this we first

demonstrate the functionality of the Echo, and then perform tests to find possible vulnerabilities, based on 3 criteria: attack by sound, by network and by third-party applications. The results obtained by our tests meet expectations, exposing a well consolidated and regulated Amazon security policy. It can therefore be seen that the measures implemented by Amazon on its Echo devices and its Alexa cloud service are ideal for users to use with integrity.

Keywords: **:** *Echo dot. IoT. Amazon.*

1 INTRODUÇÃO

Muito se fala atualmente dos aparelhos da internet das coisas (IOT) para automatizar tarefas do cotidiano. Um desses dispositivos que surgiu e logo ficou bem famoso é o Echo dot, uma caixa de som com uma assistente pessoal integrada ao serviço da Amazon que possui uma inteligência artificial, denominada Alexa, que pode responder solicitações como definir lembretes, lembrar compromissos diários, fazer pedidos ou compras, realizar perguntas gerais e controlar aparelhos inteligentes com comandos de voz, como iluminação, câmeras, sensores para quase tudo, além de outras possibilidades.

Por essa prática de automatizar objetos e realizar tarefas através de uma central está se tornando cada vez mais comum, isso levanta a dúvida sobre como solucionar os riscos de segurança colocados pelos dispositivos de IoT. Para ampliar ainda mais os riscos, muitos dispositivos têm um nível baixo de computação, memória e capacidades de armazenamento como o Echo Dot, o que limita as oportunidades de implementar segurança neles. Mesmo se você implementar as melhores práticas securitárias, novos vetores de ataque surgem constantemente.

Além disso, o serviço da Alexa integrado ao Echo Dot necessita de rede para poder dar respostas mais dinâmicas e precisas, podendo também controlar dispositivos conectados a essa rede. Com tudo sabemos que qualquer coisa que se utiliza de uma rede não está imune de sofrer ameaças de ataques. A Amazon não divulga a quantidade de Echos vendidos, mas é interessante analisar que somente na loja da Amazon Brasil há uma estimativa de 100 mil de Echo dot vendidos, considerando que possui 80 mil avaliações de compradores. Ou seja, 100 mil ou mais de usuários brasileiros que se utilizam do serviço da Alexa, onde, por exemplo, pode estar vinculado dados pessoas de usuários para pagamentos ou para acesso de aplicativos de terceiros. Sendo que, uma pequena brecha no sistema de segurança da Amazon pode acabar gerando consequências muito negativas.

Por isto julgamos importante rever e analisar a segurança nos dispositivos Echo dot, para poder identificar e detectar possíveis falhas ou brechas no Echo e híbridos conectado a ele.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Assistentes Pessoais Inteligentes (IPAs)

Antes de abordarmos as vulnerabilidades é importante intendermos como funciona as tecnologias de assistentes pessoais inteligentes. Conforme demonstrado

por Hauswald et al. (2015, p.223), uma IPA é um aplicativo que usa entradas (comandos) como voz do usuário, gestos, imagens e informações contextuais para fornecer apoio respondendo a perguntas em linguagem natural (união de aprendizagem humana e o raciocínio mecânico), fazendo recomendações e realizando ações. As aplicações de IPAs são projetadas para executar as tarefas solicitadas dos usuários através de fontes online disponíveis na Internet.

Já a Alexa é um software considerada uma IPA que é projetada especificamente para executar nos dispositivos Echo, realizando funções solicitadas por voz enquanto se comunica através de uma conexão de Internet WiFi local com servidores em nuvem AWS da Amazon. Como é possível ver na figura 1, a mais de um Echo com características únicas. Um exemplo é o Echo show que continua sendo uma caixa de som inteligente, entretanto com uma tela integrada, porém todos usam a mesma IPA Alexa. Dentre todos esses Echo o mais popular e acessível deles é o dot, por isso a nossa escolha por ele.

Figura 1 – Dispositivos Echo

Fonte: Os autores (2021)

De acordo com a página de suporte da Amazon (2020), responsável pela criação do Echo dot, diz que a comunicação do Echo com os seus servidores, é dada quando o software de reconhecimento de fala da Alexa recebe uma palavra ou frase de gatilho do usuário; por exemplo a palavra “Alexa”, utilizada para acordar o Echo. Mas esse gatilho pode ser alterado pelo usuário.

Após acordar (ativar) o Echo é possível fazer solicitações a ele. Essas solicitações se tornam gravações e são enviadas para a nuvem da Amazon, onde serão filtradas e processadas pela Alexa, e retornaram ao usuário com a resposta adequada ao que foi pedido, além de gerar um registro dos resultados ao usuário que ficam disponíveis no aplicativo da Alexa, como é ilustrado na figura 1. Essas gravações e outras informações incluindo serviços de terceiros são usadas para responder as perguntas dos usuarios de forma a melhorar a experiencia mais personalizada nos serviços da Amazon, ou seja, quanto mais usam, mas o sistema da Alexa se adapta as rotina, padrões de fala, vocabulários e as preferências de quem a utiliza.

Figura 2 - Arquitetura do sistema amazon echo

Fonte: Imagem modificada de Amazon Web Services (2020)

3 MATERIAIS E MÉTODOS

3.1 Vulnerabilidades

Entendido como funciona o sistema da Alexa e baseando-se na política de privacidade da Amazon, faremos uma análise de segurança nos dispositivos Echo dot e estimaremos se a diretrizes implementadas por ela são ideais. Seguiremos 3 critérios: Vulnerabilidade por som, por rede e por API (Aplicativos de terceiros).

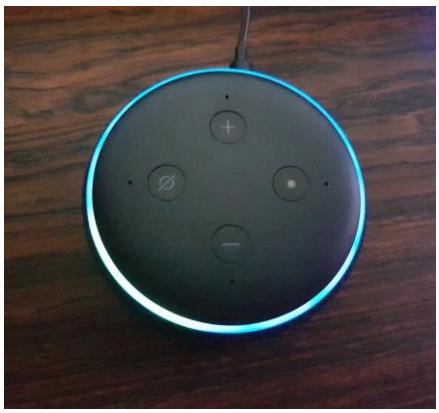
Para realizar nossos testes de segurança utilizaremos pelo menos os seguintes itens: um Echo dot, no nosso caso de 3 geração, um computador com sistema operacional kali Linux e acesso à internet. Os testes de segurança serão feitos através do uso das ferramentas disponíveis no sistema operacional kali Linux em um ambiente controlado, iremos utilizar o Echo dot como um usuário comum fazendo solicitações enquanto rodamos aplicações que de teste de vulnerabilidade para analisar os pontos fortes e fracos da segurança do dispositivo.

3.1.1 Vulnerabilidade por Som

a) Adquirir informações apenas com a fala

Como foi visto anteriormente nenhuma gravação e feita e enviada para a nuvem sem a palavra-chave de ativação. Quando é solicitada essa palavra é mostrado pelo dispositivo Echo um som de ativação e uma luz azul que fica circundando o dispositivo, como é visto na figura 3. Por esse motivo ficamos limitados em tentar solicitar ah Alexa algo, sem que pessoas por perto saibam. Com isso usamos o cenário hipotético ao qual o dono do Echo e demais pessoas não estivesse perto do dispositivo.

Figura 3 – Quando é feito uma solicitação a Alexa



Fonte: Os autores (2021)

Montado esse cenário, começamos a fazer alguns testes de solicitações a Alexa para ver como ela reagiria e se ela daria alguma informação sobre o usuário, como por exemplo Informações pessoais do dono do Echo.

De início fizemos algumas perguntas básicas como: qual meu RG, meu CPF, meu endereço, meu e-mail, meu cartão de credito e demais outras. Todas essas solicitações são interpretadas pela Alexa como se fosse uma pesquisa no Google ou ela diz “que não entende” ou “não tem certeza” e para de escutar, abandonando o pedido feito. A única informação que a Alexa deu foi o primeiro nome do usuário e o endereço, dizendo a rua e o número da casa de acordo com o que foi registrado na conta da Amazon do usuário. Descartamos essa informação como um ponto de vulnerabilidade pelo fato de que nesse cenário provavelmente o invasor estaria na mesma localidade do Echo, por necessitar estar perto do dispositivo para fazer as solicitações por voz.

Tentamos também alterar os dados da conta da amazona, pedido a Alexa por exemplo para trocar o endereço para que pudéssemos solicitar uma compra para o endereço que desejássemos. Com tudo a Alexa apenas diz que “não sabe nada sobre isso” ou “não conheço essa”.

Chegamos à conclusão que apenas solicitando a Alexa alguns dados, ela n consegue dizer, pois os dados como por exemplo o número de cartão de credito, identidade do usuário e demais outros tipos de dados não estão armazenados no dispositivo Echo dot e sim nos servidores da Amazon. Para que pudéssemos acesso a esses dados, seria necessária uma vulnerabilidade no sistema da Amazon ou man-in-the-middle (Homem no meio) que interceptaria os dados quando um usuário solicitasse uma compra, ou algo parecido pelo Echo Dot, mas essa possibilidade abordaremos melhor na próxima sessão [3.1.2] que aborda melhor a possibililidade de vulnerabilidade por rede.

É interesante dizaer que todos nossas solicitaçoes que fizemos ao echo ficam gravadas como um historico de pedidos. Esses historicos ficam disponilvel tanto no APP da alexa nos dispositivos moveis, quanto na conta da amazon do usuario, Então mesmo que possiveis invasores tentem pedir algo para a alexa, logo o dono vera no historico que foi feito um pedido ao qual ele não fez.

Nesse ponto é importante citar o que a Amazon (2020) chama de "falsas vigílias" que pode ser considerado uma falha, Essa falha se trata da assistente do Echo dot interpretar palavras parecidas com a palavra de ativação e uma vez ativada

a Alexa, ela começa a gravar e pode acabar gravando conversas privadas, como é abordado pelo Spencer Soper (maio de 2018) redator da revista Bloomberg, no artigo This Is How Alexa Can Record Private Conversations, onde cita sobre um casal que estava conversando, e acidentalmente foi mandado a gravação da conversa deles para o funcionário do marido. Isso aconteceu pelo dispositivo ter interpretado a frase de ativação e posteriormente ter ouvido a palavra “enviar mensagem” durante a conversa do casal.

Como foi dito é possível acessar essas gravações tanto de solicitação ao dispositivo e as que ocorreram através das “falsas vigílias” tendo de alguma forma acesso a conta da Amazon do usuário. Porem de acordo com Williams (setembro de 2018),, ex-analista de segurança da NSA, que comenta no artigo da revista CNBC, da autora Ali Montag, denominado ”Make It denominado “Former NSA privacy expert: Here’s how likely it is that your Amazon Echo will be hacked”, que é muito trabalho para invadir Uma caixa de som inteligente, os provável invasores não se preocupam em saber o que e dito nas suas casas ou estabelecimentos, eles estão preocupados em monetizar dados, ou seja a complexidade que eles tem para poder escutar as suas gravações ou conversas na maioria das vezes não compensa pela informação que eles vão adquirir. Assim restam apenas duas alternativas para os hackers adquirirem seus dados: Infiltre-se no tráfego de dados nos servidores Amazon ou na comunicação de voz no dispositivo Echo Dot.

b) Controlar dispositivos apenas com a fala

A assistente do Echo pode se conectar com dispositivos inteligentes através da rede para poder controla-los, como lâmpadas, interruptores, fechaduras eletrônicas e demais outros gadgets. Com isso abordamos também a possibilidade de um invasor controlar por voz esses dispositivos.

Nos nossos testes conseguimos gritar para Alexa do lado de fora da casa, para que ela acendesse a luz, e deu certo, com isso podemos ver que Alexa pode ser influenciada por pessoas fora do local em que está. Logo os possíveis invasores conseguiriam gritar facilmente através de uma parede, janela ou porta. Para os pedidos que não são restritos, como no exemplo que demos de acender a luz, descartamos como uma possível vulnerabilidade visto que no máximo os invasores conseguiriam é incomodar os moradores da residência, ligando os aparelhos conectados à rede. No entanto, a Amazon para alguns dispositivos, disponibiliza a autenticação do usuário para pedidos restritos, requerendo um PIN de 4 dígitos. Um exemplo é solicitar a Alexa para abrir uma fechadura eletrônica.

Sabendo dessa autenticação, tentamos burlar ela com um ataque de força bruta ao PIN de 4 dígitos, ou seja, tentar todos os números possíveis. Como seria 10000 possibilidades de 0000 a 9999 decidimos fazer uma lista por qual numero começaria e terminaria. Seguindo o blog Lifehacker que publicou The Most (and Least) Common PIN Numbers and Numeric Passwords. Is Yours One of Them? onde aborda os PINs mais e menos utilizados como é demostrado pela figura 4. Começaríamos a nossa lista com os números frequentes. Após colocar os PINs previsíveis, em seguida colocaríamos os demais números de 20 a 9980 sendo que os últimos 20 PINs seria os números menos utilizados seguindo também a lista do blog Lifehacker,

Figura 4 – PINs previsíveis

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

	PIN	Freq
#9980	8557	0.001191%
#9981	9047	0.001161%
#9982	8438	0.001161%
#9983	0439	0.001161%
#9984	9539	0.001161%
#9985	8196	0.001131%
#9986	7063	0.001131%
#9987	6093	0.001131%
#9988	6827	0.001101%
#9989	7394	0.001101%
#9990	0859	0.001072%
#9991	8957	0.001042%
#9992	9480	0.001042%
#9993	6793	0.001012%
#9994	8398	0.000982%
#9995	0738	0.000982%
#9996	7637	0.000953%
#9997	6835	0.000953%
#9998	9629	0.000953%
#9999	8093	0.000893%
#10000	8068	0.000744%

Fonte: https://lifehacker.com/the-most-and-least-common-pin-numbers-and-numeric-pas-5944567 (2021)

Vimos que quando é pedido o PIN para a autenticação do usuário, a Alexa oferece 3 chances antes de resetar o serviço. Com o reset a Alexa força um delay de 20 segundos antes que o usuário possa solicitar um novo PIN. Nos nossos calculamos que para cada 3 tentativas leva cerca de 50 segundos, por tanto para nos tentar gerar todas as alternativas da nossa lista através de um script levara aproximadamente 46 horas, supondo que o PIN correto seria a última opção da lista. Vimos então que é possível burlar o sistema de autenticação da Alexa e dependendo do PIN escolhido pelo usuário o tempo pode ser reduzido significativamente. Entretanto se torna inviável os ataques de força bruta, que seira testar senha por senha, visto que pode levar um bom tempo para que esse ataque de certo, um risco muito grande para um possível invasor.

3.1.2 Vulnerabilidade por Rede

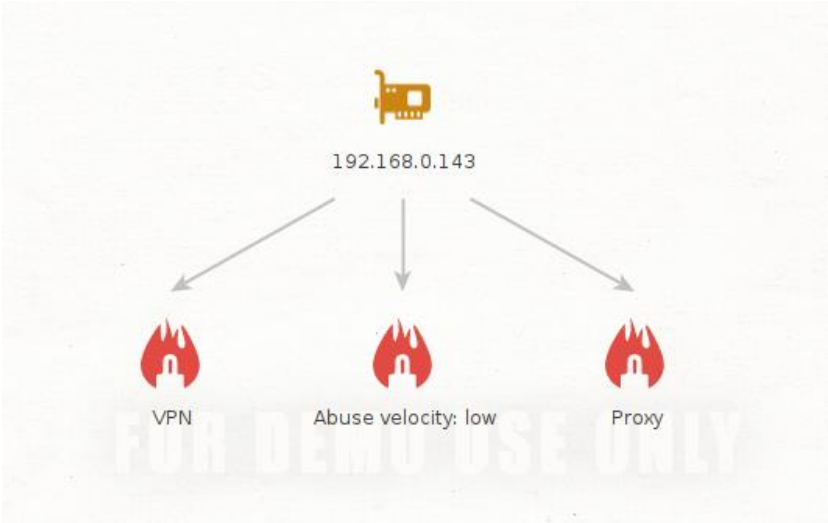
A vulnerabilidade pela rede refere-se a possíveis ataques que possam ocorrer quando o atacante tem acesso a rede em que o dispositivo se encontra, há vários tipos de ataques que podem ser feitos de diversas formas como por exemplo o man in the midle que consistem em interceptar pacotes antes dele ir para seu destino, onde esses pacotes são analisados ou até mesmo modificados e para isso há várias ferramentas disponíveis na internet como por exemplo o ettercap. O objetivo de nossos testes de vulnerabilidade por rede, é verificar se a Amazon criou todos os

cenários possíveis e preparou as medidas de segurança necessárias afim de evitar os mais diversos tipos de ataque por rede, garantindo os 5 pilares da segurança da informação.

Iniciamos pela etapa de tentar mapear a comunicação entre o dispositivo Echo e os servidores da Amazon. Para o primeiro teste foi utilizado Maltego Comunity Edition uma versão gratuita, porém limitada do Maltego. Segundo o site dos desenvolvedores o Maltego retorna indicadores visuais sobre um endereço IP e o serviços utilizados por esse endereço. Com isso pegamos o endereço ipv4 do Echo dot pelo aplicativo do roteador da rede local e colocamos no Maltego, selecionando para fazer uma análise em quanto solicitávamos algo para a Alexa.

Com o resultado vimos que o serviço amazona Alexa integrados aos dispositivos Echos, possuem 3 serviços em execução. O Velocity controlando a quantidade de requisições feitas ao Echo Dot, o serviço de proxy atuando como um intermediário que é responsável pelo roteamento de pacotes entre cliente servidor e pôr fim a VPN, que segundo Tanenbaum (2011) é uma rede sobreposta a rede pública, mas com a maioria das propriedades das redes privadas, ou seja, gera uma conexão direta e segura com os servidores em nuvem da amazona, criando um túnel de transmissão de dados criptografado com regras estipuladas pelo firewall da Amazon, com o objetivo de manter a integridade dos pacotes de dados e de que eles não sejam interceptados no caminho.

Figura 5 – Analise no Maltego



Fonte: Os autores (2021)

Os serviços integrados da Amazon demostrados pela figura, inviabiliza a possibilidade de tentar executar determinados processos por meio de acesso não autorizado a invadir os servidores da amazona através do rastreio da comunicação do Echo com os servidores. Mas podíamos ainda tentar interceptar os dados da comunicação logo após as solicitações saírem do cliente (solicitação feitas pelo usuário). Tentamos então capturara algum pacote usando um sniffer como por exemplo o **Wireshark,** mas vimos que a comunicação do Echo dot com os servidores em nuvem da Amazon é projetado com uma criptografia TLSv1.2 de ponta a ponta e não há uma maneire simples de descriptografar os dados sem a chave. Essa criptografia descarta a possibilidade de qualquer software de sniffer

conseguir interceptar algum pacote e mesmo que um possível invasor o consiga, n teria a chave necessária para que possa ver os dados.

Seguimos os testes com objetivo de conseguir mais informações sobre o dispositivo, agora usamos o **nmap** que de acordo com Moreno (2019) é um port scanner com vários plugins que nos permite: descoberta de máquinas online, detecção de: serviços e suas versões, sistema operacional, rotas e várias outras funcionalidades.

Para levantar mais informações gerais sobre o Echo dot foi utilizado o seguinte comando: **nmap -sV - O - A 192.168.0.144**, onde o **nmap** escaneia o dispositivo buscando parâmetro citados anteriormente. O resultado do scan no endereço IPv4 é demostrado pela figura 6.

Figura 6 – Analise no Maltego

Fonte: Os autores (2021)

O **nmap** descobriu 2 portas abertas a 1080 usando protocolo TCP e o serviço Socks que é um acrônimo para Secured Over Credential-based Kerberos Services (em português Serviços Kerberos com base em credenciais garantidos) é um protocolo da Internet para transferência de dados de um cliente para um servidor. O proxy SOCKS não transmite para o servidor remoto variáveis de si mesmo em resposta à solicitação HEAD (em contraste com o servidor proxy HTTP). É por isso que, se for para falar sobre um nível de anonimato, um proxy SOCKS é totalmente anônimo (Premproxy, 2021), ou seja, refere-se à porta utilizada pelo proxy. Através do nmap conseguimos uma informação adicional sobre o proxy que não tínhamos conseguido no teste anterior.

Em seguida temos a porta 8888 também utiliza o protocolo TCP o serviço listado está com tcpwrapped, que é referência ao tcpwrapper é uma ferramenta tem sido usada com sucesso para sistemas de blindagem e para detecção de atividade de cracker (Venema, 1990), mais em baixo o **nmap** conseguiu pegar as informação do Sistema Operacional, no caso o Echo tem um sistema modificado baseado em Linux e em seguida a versão do kernel, de longe a melhor informação obtida até o

momento, por abrir um leque de opções as quais podemos verificar com metasploit framework se há algum exploit com base na versão do Linux ou do kernel.

Após levantar as informações sobre o dispositivo, vamos iniciar a procura de alguma possível vulnerabilidade. Dentro da ferramenta msfconsole fizemos uma busca de exploits para o socks5, tcpwrapper, e não localizamos nenhum exploit. Seguimos a procura pela versão do Linux, porém não achamos nada para a versão especificada pelo nmap. Fizemos também busca de exploits para Echo dot e não houve resultados, ou seja, sem sucesso na obtenção de um exploit tivemos que procurar outros meios. Iniciamos os testes agora com objetivo de travar o Echo Dot através de DoS, usando o t50 que permite realizar ataques DoS usando apenas uma máquina, executamos o comando **t50 --flood --tubo -S** onde a nossa máquina vai enviar dezenas de pacotes TCP com a flag SYN onde obriga o alvo a responder. A aplicação rodou por 10 min e após isso fizemos uma solicitação a Alexia, verificamos que houve uma demora da alexia em processar a solicitação, porém ainda sim houve uma resposta.

Por último utilizamos o **tcpdump** para captura de pacotes vindo do Echo Dot, usamos o seguinte comando **tcpdump -i wlan0 192.168.0.143 -w echo.cap.** Esse comando captura pacotes do Echo Dot e salva em um arquivo, com isso iniciamos o tcpdump e fizemos algumas solicitações a Alexa e ao final do teste o tcpdump não identificou nenhum pacote provindo do Echo dot, provavelmente pelos dados serem criptografados.

3.1.3 Vulnerabilidade por API

A assistente virtual do Echo possui diversas funcionalidades para responder solicitações e controlar dispositivos inteligentes, mas para que essa experiencia se torne melhor ainda para os usuários, foi criado as skill Alexa, que são habilidades que funcionam como um aplicativo que é desenvolvido através da Alexa Voice Service API (uma interface de programação para criadores de software terceirizados que possam desenvolver produtos associados aos serviços da amazona Alexa). Essas skill podem ser instaladas ou desinstaladas através do aplicativo da Alexa do seu smartphone. Para que os desenvolvedores criem uma skill é necessário que:

a) Um nome para que a Alexa saiba quando invocar a habilidade;
b) As ações por comando de voz que os usuários tem para interagir com a habilidade;
c) Que as ações disponíveis na habilidade sejam baseadas em nuvem para que o serviço de nuvem da amazona aceite as solicitações e consiga agir sobre elas.

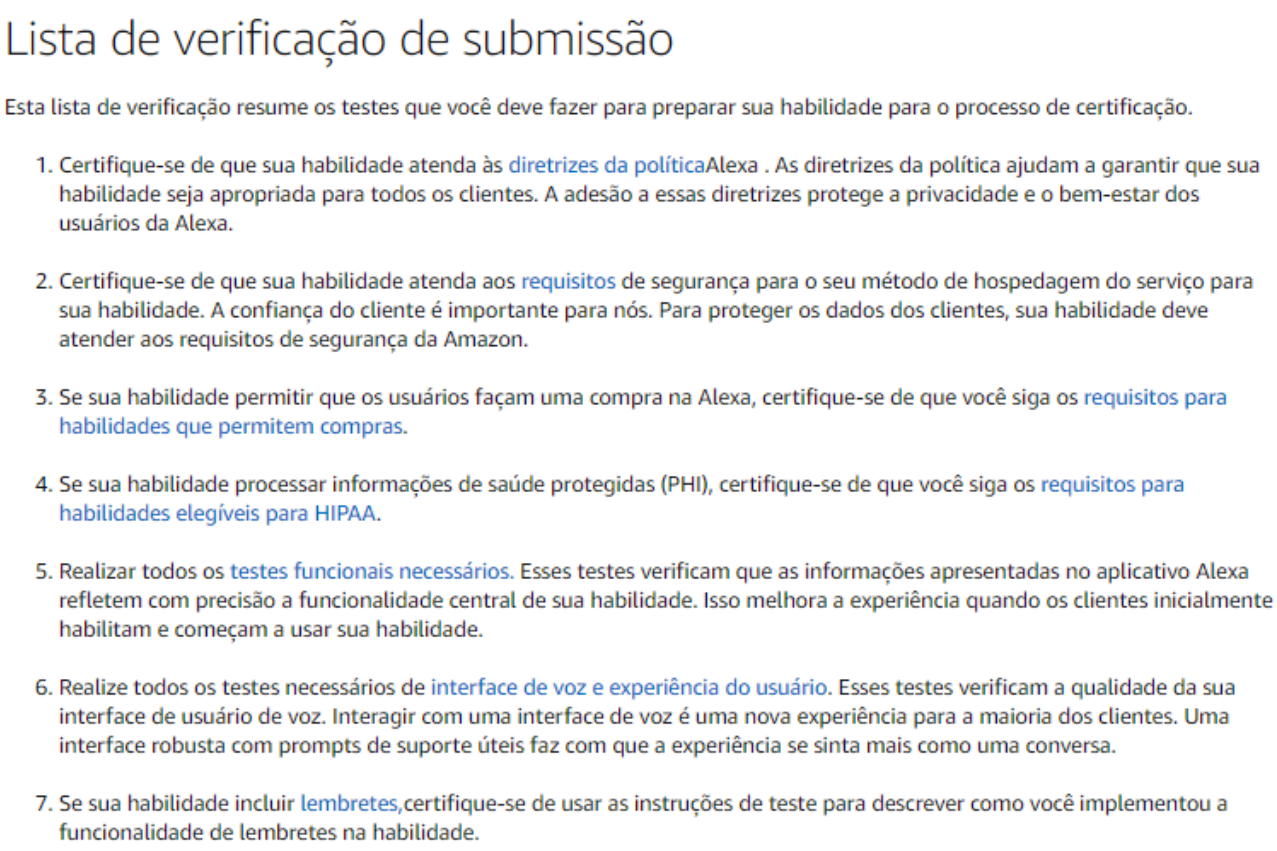
Apesar de que essas habilidades de terceiros possam proporcionar uma melhor experiencia no uso do Echo dot tendo novas funcionalidades, do mesmo modo surge novas ameaças à segurança e privacidade do usuario, como é dito no artigo Hey Alexa, is this Skill Safe?: Taking a Closer Lookat the Alexa Skill Ecosystem, pelos pesquisadores da Universidade Estadual da Carolina do Norte, da Ruhr-University Bochum e do Google. Os pesquisadores dizem “Identificamos várias lacunas no ecossistema atual que podem ser exploradas por um adversário para lançar novos ataques, incluindo registro de nome de desenvolvedor arbitrário,

ignorar APIs de permissão e fazer alterações no código de back-end após a aprovação para acionar intenções inativas”.

Porém o porta-voz da Amazon se pronunciou para alguns portais de noticia dizendo “Que a empresa conduz análises de segurança como parte da certificação de habilidades e possui sistemas para monitorar continuamente habilidades ao vivo em busca de comportamento potencialmente malicioso, sendo assim todas as habilidades ofensivas que identificamos são bloqueadas durante a certificação ou rapidamente desativadas”.

Em nossos testes vimos que para que possamos publicar uma habilidade é necessário enviar a skill para a Amazon onde é analisado e verificado se a skill atende os requisitos necessários das politicas de segurança da Amazon. Estes requisitos são demostrados pela figura 5.

Figura 7 – Requisitos para publicação de uma skill



Lista de verificação de submissão

Esta lista de verificação resume os testes que você deve fazer para preparar sua habilidade para o processo de certificação.

1. Certifique-se de que sua habilidade atenda às diretrizes da políticaAlexa . As diretrizes da política ajudam a garantir que sua habilidade seja apropriada para todos os clientes. A adesão a essas diretrizes protege a privacidade e o bem-estar dos usuários da Alexa.
2. Certifique-se de que sua habilidade atenda aos requisitos de segurança para o seu método de hospedagem do serviço para sua habilidade. A confiança do cliente é importante para nós. Para proteger os dados dos clientes, sua habilidade deve atender aos requisitos de segurança da Amazon.
3. Se sua habilidade permitir que os usuários façam uma compra na Alexa, certifique-se de que você siga os requisitos para habilidades que permitem compras.
4. Se sua habilidade processar informações de saúde protegidas (PHI), certifique-se de que você siga os requisitos para habilidades elegíveis para HIPAA.
5. Realizar todos os testes funcionais necessários. Esses testes verificam que as informações apresentadas no aplicativo Alexa refletem com precisão a funcionalidade central de sua habilidade. Isso melhora a experiência quando os clientes inicialmente habilitam e começam a usar sua habilidade.
6. Realize todos os testes necessários de interface de voz e experiência do usuário. Esses testes verificam a qualidade da sua interface de usuário de voz. Interagir com uma interface de voz é uma nova experiência para a maioria dos clientes. Uma interface robusta com prompts de suporte úteis faz com que a experiência se sinta mais como uma conversa.
7. Se sua habilidade incluir lembretes,certifique-se de usar as instruções de teste para descrever como você implementou a funcionalidade de lembretes na habilidade.

Fonte: Amazon Developer (2021)

4 RESULTADOOS

Diante da nossa proposta de testes iniciais demostramos algumas dessa possíveis vulnerabilidades. Vimos que referente as vulnerabilidades por som o dispositivo Echo dot é bem limitado. Os dados não são salvos nele e sim em nuvem onde é processado as informações, descartando a possibilidades de pedir por voz dados pessoas ou altera-los. Com tudo vimos que é possível de fazer ataque de

força bruta para romper o sistema de PIN de autenticação da Alexa. Esse ataque é um processo que pode ser demorado dependendo do PIN escolhido pelo usuário, sendo assim dificulta a tentativa de realizar esse ataque sem o possível invasor ser descoberto. Mas isso não deixa de ser um ponto falho no sistema da Amazon.

Já na vulnerabilidade por redes, ao qual pretendíamos tentar capturar alguns dados na hora que fosse solicitado algo a Alexa, percebemos de início que a comunicação da Alexa do Echo com os servidores em nuvem da Amazon possuía diversos serviços como VPN e proxy que dificultavam a tentativa de rastrear a comunicação até esses servidores, além disso era criptografada os dados com um protocolo TLS, isso dificultou os softwares de sniffers que conseguissem capturar algum pacote quando e feita as solicitações a assistente do Echo. Julgamos importante ainda fazemos mais alguns testes para verificamos se a possibilidade de decifrar essa comunicação.

Na vulnerabilidade por API, que consistem na criação de skills maliciosas afim de obter vantagens ou usar como ferramenta para ter acesso a rede de terceiros. Iniciamos pesquisas sobre o desenvolvimento e publicação das skills. A Amazon incentiva pessoas e empresas na criação de skills, por isso há uma quantidade imensa de material no próprio site sobre o desenvolvimento de uma habilidade. Após ler diversos matérias sobre, verificamos que é muito complicado de criar uma skill maliciosa e publica-la pois segundo o artigo da Amazon developer “Certify and Publish Your Skill” antes de qualquer skill ser publicada ela passa por vários testes afim de verificar se há qualquer tipo de irregularidade ou vulnerabilidade. Com tudo ainda é possível encontrar futuramente novas brechas que possam driblar o sistema de análise da Amazon.

5 CONCLUSÃO

O surgimento de um crescente número de assistentes virtuais e dispositivos da internet das coisas que se conectam entre si, criou-se uma preocupação referente a integridade e confiabilidade desses aparelhos. Direcionamos nossa pesquisa para o dispositivo Echo dot, uma caixinha de som inteligente, que através de testes de vulnerabilidades, por som, por rede e por API chegamos à conclusão que as políticas de segurança que foram implementadas pela Amazon são satisfatórias. O grande mérito da Amazon não é o dispositivo em si, que possui uma construção simples, lidando apenas com a parte de reconhecimento da voz, gravação e reprodução, e sim o que acontece nos bastidores nos servidores em nuvem da Amazon, onde possui diversos serviços para tornar a experiencia do usuário a melhor possível, com confiabilidade.

Mesmo não encontrando pontos de vulnerabilidades circunstanciais, julgamos importante a necessidade de mais pesquisas destinadas a prever e melhorar possíveis vulnerabilidades futuras, já que se trata de uma tecnologia que está em constante atualizações onde pode acabar surgindo falhas que possam ser exploradas.

6 REFERÊNCIAS

AMAZON SUPPORT PAGE. Disponível em: https://amzn.to/1R5WgXP. Acesso em: 25 jun. 2020.

ALI MONTAG. REVISTA **CNBC MAKE IT**. ARTIGO **FORMER NSA PRIVACY EXPERT: HERE'S HOW LIKELY IT IS THAT YOUR AMAZON ECHO WILL BE HACKED** Disponível em: https://cnb.cx/2wK6J7w. Acesso em: 1 jul. 2020.

AMAZON. **Certify and Publish Your Skill.** Disponível em: https://developer.amazon.com/en-US/docs/alexa/certify/certify-your-skill.html. Acesso em 8 de Abril de 2021.

GOKSEL CANBEK, N.; MUTLU, M. E. **On the track of Artificial Intelligence: Learning with Intelligent Personal Assistants. Journal of Human Sciences,** [S. l.], v. 13, n. 1, p. 592–601, 2016. Disponível em: https://www.j-humansciences.com/ojs/index.php/IJHS/article/view/3549 Acesso em: 9 mar. 2021.

HAUSWALD, J., LAURENZANO, M. A., ZHANG, Y., LI, C., ROVINSKI, A., KHURANA, A., DRESLINSKI, R. G., MUDGE, T., PETRUCCI, V., TANG, L. & MARS, J. (2015). **Sirius: An open end-to-end voice and vision personal assistant and its implications for future warehouse scale computers. In Proceedings of the Twentieth International Conference on Architectural Support for Programming Languages and Operating Systems. p.223-238. ACM.** Disponível em: https://www.researchgate.net/publication/277918492_Sirius_An_Open_End-to-End_Voice_and_Vision_Personal_Assistant_and_Its_Implications_for_Future_Warehouse_Scale_Computers. Acesso em: 9 mar. 2021.

LENTZSCH, Christopher; SHAH, Sheel Jayesh; ANDOW, Benjamin; et al. Hey Alexa, is this Skill Safe?: Taking a Closer Look at the Alexa Skill Ecosystem. **Proceedings 2021 Network and Distributed System Security Symposium,** 2021. Disponível em: https://www.ndss-symposium.org/wp-content/uploads/ndss2021_5A-1_23111_paper.pdf. Acesso em: 11 de abril 2021.

MALTEGO. **Increase the Speed and Precision of Complex SOC Investigations.** Disponível em: https://www.maltego.com/reduce-your-cyber-security-risk-with-maltego/. Acesso em: 12 Abril 2021

MORENO, Daniel. **Introdução ao Pentest**. 2. ed. atual. e aum. [*S. l.*]: Novatec, 2019. 378 p. ISBN 978-85-7522-461-1.

PINOLA, Melanie. **The Most (anda Least) Common PIN Numbers and Numeric Passwords. Is Yours One of Them?** Lifehacker. Disponível em: https://lifehacker.com/the-most-and-least-common-pin-numbers-and-numeric-pas-5944567. Acesso em: 10 abril. 2021**.**

PremProxy. **WHAT IS SOCKS PROXY?** 2021. Disponível em: https://premproxy.com/socks-list/. Acesso em: 6 junho. 2021.

SPENCER SOFER. ARTIGO **THIS IS HOW ALEXA CAN RECORD PRIVATE CONVERSATIONS**. Disponível em: https://bloom.bg/2IJN68G. Acesso em: 29 jun. 2020.

TANENBAUM, Andrew. **Redes de Computadores**. 5. ed. atual. [*S. l.*]: Pearson, 2011. 581 p. ISBN 978-85-7605-924-0.

VENEMA, Wietse. TCP WRAPPER: Network monitoring, access control, and booby traps. **Tcp wrapper**, [*s. l.*], 8 abr. 1997.