**Title:**

**Alexa can I Trust you?**

**What is the research problem?**

Alexa is a voice device that enable customers to interact with the device in a more intuitive way using voice command. Such devices are categorized as IVA (Intelligent Virtual Assistant). This paper studies the security aspects and privacy threats by such IVA use, which are now becomes more common with each day and emphasizes on its importance.

**Evolution of IVA**

* IoT devices are considered to be the predecessors of IVA’s. IoT devices in turn have evolved from half a century old Chatbot’s programmed to pass the Turing test.
* With Chatbot’s the interaction with in writing via a chat interface.
* Keywords or combination of keywords was the trigger point to initiate a series of event based on the rule set.
* Today’s IVA in turn comprehend voice and are capable of triggering far more complex set of events.

**Defining modern IVA’s**

* There are many other terms coined around these category of IoT devices. However for the modern class of these devices, although the communication/hearing/listening is done by a device in the proximity of the user, but such devices are always assisted by an artificial intelligence/brain which sits in some virtual space i.e. Cloud environment, hence Virtual
* With the continuous input, more often these devices are continuously evolving hence Intelligent.
* Hence these devices are named as Intelligent Virtual Assistant in this paper.

**Well Known IVA’s**

* Amazon Alexa
* Apple Siri
* Google Home, Google Assistant
* Microsoft Assistant Cortana

These devices are classified into two categories

1. Built-in IVS’s that use multi-purpose devices i.e. Siri, Cortana
2. Standalone IVA’s that use dedicated devices, rest of the devices listed

**Overview/main points of the proposed approach/architecture**

* Voice assistant devices such as Google Home, Apple’s Siri and Amazon’s Echo devices are readily available in the market space and expected to reach a market value of 1.2 billion by 2020.
* IVA’s have open an altogether new space where the end-user can talk to machines as if it were a human and in turn the machine comprehends the user command and execute it such as ability to play music, maintaining user schedule, ordering online, control household devices.
* For doing this, the devices continuously monitor/listens the user voice for keywords. Is it stored? Where is this data stored? Its accessibility?
* Otherwise also these conversations are solely to be kept between the user and the device. But the right question is are they?
* The papers cites one of the example where customer’s voice was continuously monitored and a false command was registered which lead to updating the Wikipedia site with wrong information.

**Identifying Threat vectors of an IVA**

* The paper studies/analyses the security vulnerability by verifying how these devices handle actual people’s voice.
* IVA vendors are actually storing voice data of the end users, thus making it possible to be misused.
* This data can be used to identify users, impersonate them and get access to their system, home.
* To understand these threat in details and there implications the papers studies the ecosystem of such IVA device in detail.

**IVA Ecosystem**

* One of the IVA’s which the papers has studies is Amazon’s Alexa
* The main component of these devices are divided into two components
  + The Client side
    - Alexa enable device
    - A companion app that needs to be installed on the user device of choice
  + The Cloud side: The intelligent assistant which operated on the Cloud environment
* These user commands are stored in the cloud in text as well as voice format, which are accessible from the companion device through app
* Additionally packet analysis of the data on the cloud and firmware/software on the on the device was also carried out as a part of this paper.

**Rogue IVA’s**

* Wiretapping the Internet:
  + Sniffing the network traffic between client’s companion application and the cloud may expose user’s security and privacy data.
  + Even though the traffic is encrypted, various patterns including payload sizes and data rates could be utilized for identifying user’s behavior such as turning on the device, the idle status, talking to the assistant, listening to music, ordering products or services.
* Compromised IVAs:
  + DDoS attacks against Dyn LLC exploited vulnerabilities of 10s of millions of home-embedded devices such as webcams and DVRs, infecting them with Mirai botnet, and turning these devices into an army of bots used to attack Dyn’s systems.
* Malicious voice commands:
  + Although these systems are evolving but it is difficult to perfectly recognize user’s voice. If a malicious person can come close enough to the targeted IVA-enabled device, he or she may be able to fool the system into thinking that the real owner is the person speaking.
* Unintentionally recorded voice:
  + To better understand and evolve these systems, voice sample are recorded and transmitted, so it’s possible to eavesdrop on some private conversation unintentionally. Here the user does not have the control of what audio gets transmitted.

**Conclusion:**

With each day more and more devices are getting connected to the internet and there is a growing need to understand the security and data privacy threats from such smart devices. Not much has been done in this area and the paper highlights the need of the same.