-

Voice UI is the precursor to the coming: brain-to-machine interface. Voice Assistant is the lead-in to the coming: personalized-ambient-smart AIs, services, devices, and environment.

SonoKey is creating pioneering solutions and services for the voice-first and the smart-future.
We found major gaps and needs and will start by solving one of them:
The world’s first user authentication security-key solution for voice assistants. This solution is an important new paradigm for the voice space, and will enable the first personalization of services (i.e. “directly”), which will underpin the next big growth and user experience for the voice space.

Michael Chung, Founder
SonoKey (dba)
Santa Clara, CA
12/3/2020

December 3, 2020

To: Mark Cuban

Re: Voice space, angel-stage, venture opportunity.

Dear Mr. Cuban,

Greetings and thank you in advance for the time and attention to review and to consider this presentation and funding request. I noted your strong interest in the voice space.

The voice assistants and services are becoming ubiquitous and we are at the very early growth stage of the voice UI and voice first era. There are still potentially epic infrastructure opportunities. We are have found 2 such huge opportunities.

One will solve a major overlooked gap which is handicapping the entire space, its growth and user experience. The solution for this is relatively simple and is described in the attached presentation. We are very confident that i**t will be needed by** every voice service and their users.

The second opportunity will expand and extend the entire voice space and more specifically, will help it to the coming "everything and everywhere" smart world of the future. **It will be wanted by everyone. And actually (gulp), it targets and dares to envision the "post-smartphone" era.** (I.e., it is will reduce the need/habit for the smartphone). This is left out of this document for the sake of brevity and **will be sent to you next - please just ask! It is an interesting and bold vision as well.**

Our solutions will help and uplift the entire voice and the smart spaces by increasing the use cases, the revenue, and improving the user experience.

We are a startup-lab in the voice space with several pat. pending. I am a full-time tech-startup entrepreneur for the past 7 years. I create new business models and do "root-research". Previously, I spent 25 years in real estate and retail in New York City. I may now be a top expert in the in the combined paradigms of the voice assistants, the voice UI, smart devices, ambient computing, and data-over-sound.

I invent business models. "I never met a 'problem' I didn't like". I see…opportunities and patterns everywhere. I riff off of existing paradigms and create new values.

We would love to have you to back and advise us. **Thank you again for being so very open, inviting, and welcoming!** And we look forward to any questions you may have.

Yours truly,
Michael Chung, Founder
SonoKey (dba)
917-680-6870
michael@sonokey.com
https://www.linkedin.com/in/chungmojo/

Worlds first direct authentication for Voice assistants and Voice UIs

Overview and SonoKey solution Summary

Solution 1 is for enabling its users to be **authenticated directly in the audio channel** of the voice service or device that they are using. By directly: That the solution uses the audio channels (mics/speakers) to transmit-receive the authentication data -- and can be done at the edge among smart devices, in the cloud and with multiple services, or in combination.

For example, a user can authenticate to the Alexa cloud, directly through the voice assistant speaker that the user is speaking on; or directly to the video doorbell or smart lock from several meters away (e.g. the Amazon RING, Arlo, Google Nest); and similarly communicate with other smart or networked voice responsive or audio capable device or service.

Solution 1 is a "sonic-key" device (or app) that directly and securely authenticates the user in the voice or audio channel of the device or service being used. It is the world's first solution that enables strong identification, authorizations, and authentication in the same channel.

The bill-of-materials for the devices is to range from as low as $2 for disposable-tag key design (e.g., a one-time use or short life), to ~$10 to ~$20 (with optional Bluetooth, WiFi, or UWB).

We will create our own distribution and brand, but also license to the voice space as these are solutions which will expand and uplift the entire space. **The personal device form factor is a must for the best user experience, security, increase uses, and to reduce the need of phones.**

Use case: Personalized and secure service via the voice assistant speaker-gateway

1. User: "**Alexa, please reorder my asthma medicine and pay with Bitcoin in my wallet**".
2. Alexa: "**Please authorize.**" (And, starts to broadcast token/s using data-over-sound.)
3. User: **The user taps the SonoKey wearable or speaks to it with a wake phrase*** such as "SonoKey, please do authorization" and the SonoKey device and Alexa will talk to each other****** and do the authentication protocol -- for example, the Alexa cloud retrieves a token from the medicine service and transmits it, and the device signs and transmits the token back to Alexa speaker; or alternatively the device transmits a secure a token or one-time-use password to Alexa. (*****Optionally, the device can have wake phrase and voice recognition capability. ******The data-over-sound frequency type and range include audible, near ultrasound, and ultrasound and depends on the use cases and purpose.)
4. Alexa and/or the Medicine service: "**Thank you, the medicine authorization is verified and the payment has been signed and posted to the blockchain**."

(At above, three separate services are being used and each can be separately authenticated: Alexa as the voice UI and gateway, the medicine fulfillment, and the payment service.)

Data-over-sound differences/advantages over the NFC, Bluetooth, and UWB

1) Mics and speakers are “the largest installed infrastructure in the world”, open and free;
2) Data exchanged reliably: over-the-air up to several meters or in a phone call or wire;
3) The additional security from the possession and being physically present so that the man-in-middle attack is nearly impossible;
4) Time-of-flight and angle-of-arrival (using 2 mics on the device) are easily calculated using only two devices; also enables “sonic-tethering” of devices; device positions known, etc.

Data-over-sound (DoS) advantages and differences to USB and RF

The SonoKey DoS will be as secure as the USB connection or the NFC or Bluetooth. In fact, we can make it more secure than the RF for some applications due to the proximity over-the-air uses. For example, man-in-middle signal substitution is nearly impossible because the device has to be in possession and present. It can also do challenge and response where a token can be received, signed, and transmitted back, e.g. even for blockchain and private-key uses.

We have additional novel security solutions and innovations that specially fit or leverage the audio channel and the voice space. **For example, even if the voice assistant service is walled** (as nearly all are currently), we have a method (in stealth), to transmit or receive (i.e. tunnel through) in both directions, a security token which is then passed through to the third-party skills(!), and then to authenticate or authorize. This is one of our patent pending methods.

The top problem and opportunity targeted

The voice-services and devices do not directly and with certainty know who the speaker is, and the result is that the majority of the current voice based or voice reliant services, skills, and use cases are not personalized, individualized, or secure.

The personalized and secure services and user experiences are essential for the voice space to grow and to increase the revenues, increase services, and users. Plus, we want to help open the space up – as recently cooperation was announced by Google, Amazon, and Microsoft.

The voice and AI assistants will become the new gateways of our digital lives. This is analogous to how the browsers are gateways and permit the “direct authentication” by enabling the ***direct and secure communication*** to our services such as banking, etc. This direct and strong authentication enables the personalized services, experiences, and our digital life experience. **Direct authentication enables the best experience, revenue, and services for the voice space.**

About the Data-over-sound and, its novel “mating” with the Voice assistants.

Data-over-sound has certain differences and advantages over the radio frequency, such as: a) doing the data exchange directly, b) that the audio channels are open and permits any audio capable smart edge devices or (dumb) networked devices to talk to each other (i.e. no pairing or registration is required as the cloud can handle that), c) ubiquitous*; and physical security of the proximity over-the-air transmission. (*E.g. even a public intercom system can be a channel.)

Data-over-sound technology is proven

In 2017, Google began to use data-over-sound India for a phone based payment solution by swapping out the QR code communication part for the “audio QR” function. Bit rate is about 100 to 300 p/s. (Google white paper: Ultrasonic Communication Using Consumer Hardware. 06/2018)

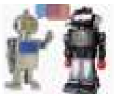
Worldwide, about seven startups are in the data-over-sound space. The best is from ~2005 (French; copsonic.com); next is Lisnr.com, funded to $30 mil (does ~1000 bit/s at the near ultrasound range of ~18k to 19.2kHz); and Chirp.io acquired by SONOS in Jan 2020. Next 2 top are India based and focused on payments, has funding of $10 million. We may infringe on some prior patents, but strongly believe that these are very manageable. We also have broad pats. pending related to our own voice space related solutions and strategies.

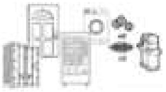
(Note: Data-over-sound will **help the coming shift to passwordless and touchless**. We can make a “sonic-YubiKey” and enable it to do contactless and touchless strong authentication.)

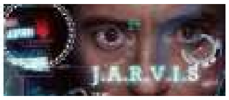
Voice UI and Sound is versatile, open, and…interspecies: human to machine to…

Voice and sound have vast untapped potential and have solutions to be discovered. It will be fun and profitable to bring new fundamental solutions to the world.

Data-over-sound for the direct authentication and the voice UI for the communication:







Our expertise in data-over-sound, voice, ambient computing, smart environment

SonoKey maybe the first to mate the data-over-sound with the voice space -- or at least with the focus and the special insights, and with potentially broad patents and IP.

> *Paradoxically, none of the data-over-sound companies are targeting the voice space.*
>
> *And also, the voice space leaders are not “paying attention” to the need for 1) the user-authentication, and 2) that they are missing out on the personalization and the individualization of the voice assistants, the skills, and voice services.*

Three additional mentionable winds at our backs:

1. **The voice UI is the precursor to the coming brain-machine interface.**
2. **The ambient computing and smart appliances and environments (home, work, and public spaces) is the precursor to the “Star-Trek” future.**
3. **Currently, ALL cloud voice assistant services are walled. However, people will need to access the service directly – as they do now with the web; and there will be a need for the users and the services to authenticate each other. Solution 1 can do this.**

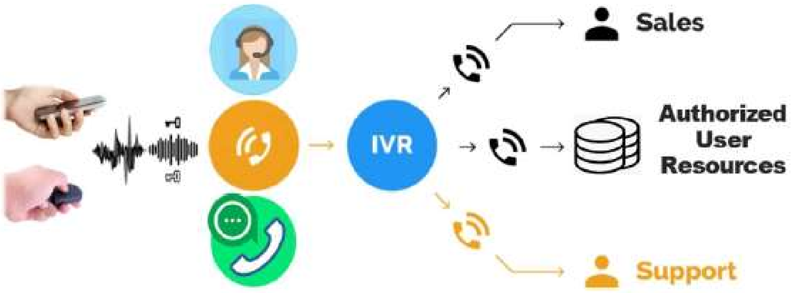
SonoKey is the world’s first authentication solution designed specifically for the voice UI and voice services. SonoKey solutions are key helpers and strategies for these mega new trends.

Addendum: Data-over-sound is hugely versatile

A) One of our goals is to get our DoS communication solutions to be certified for use for FIDO2, WebAuthn, etc. and become a standard.

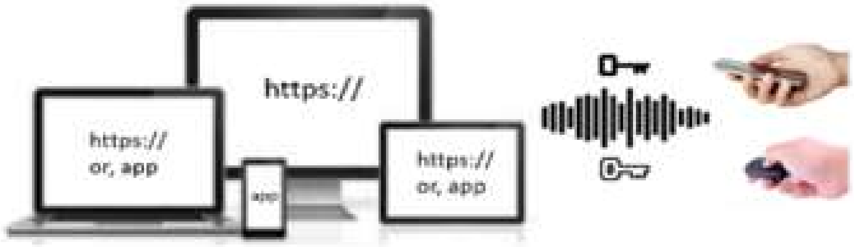
Example 1: Authenticate over any audio channel – frictionless, strong, and secure.

The Solution 1 fob can transmit the user's secret over the phone call so that there is no need to enter the PIN, give the "last 4 numbers of the SSN", etc.:



Example 2: Touchless – Contactless automated/ambient hardware security key.

"Sonic-YubiKey", and also can be fitted to the RSA-SecurID token device. The Solution 1 fob can transmit the user's secret over the browser and log the user on to their web based services:



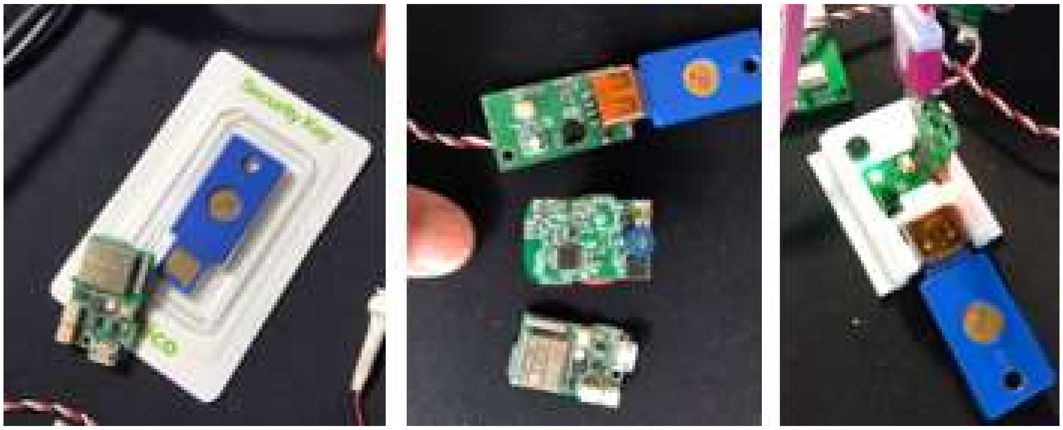
B) Another feature of the data-over-sound is that it can easily do time-of-flight and angle-of-arrival measurements. These can be used to know the distance to the user and the direction. Thus, the things will follow me as I approach them.

This time-of-flight and knowing the proximity of the user is difficult to do with the Bluetooth and UWB devices. Examples new possible uses are:

- A voice assistant speaker can sense if the user has walked into the room and then seems to be stationary (e.g. sitting down), it can then command and provide smart services.
- A smart audio capable security system can follow the users individually around the house, office, or workplace.
- (A side mention: That the microphone and speaker infrastructure is "ubiquitous" makes for imaginative uses. For example, an audio signal can be sent over an intercom system.)

Exhibits: Current benchtop prototyping/mockups

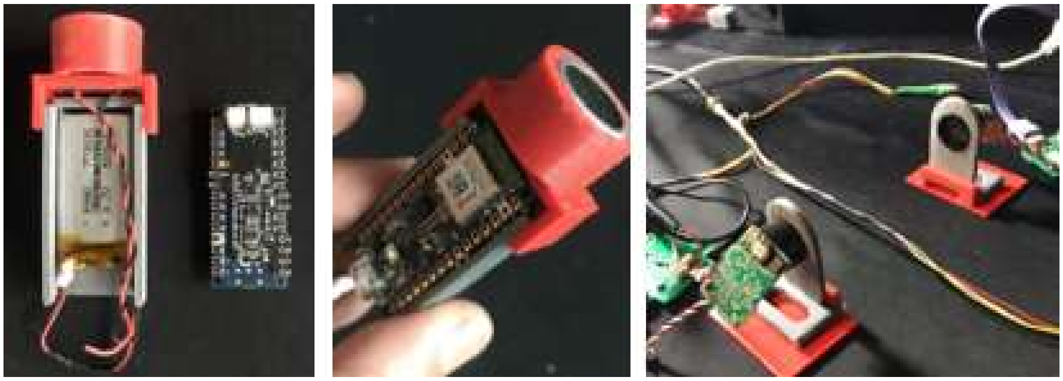
A) "Sonic-YubiKey" concept - retrieve the secret token on YubiKey, send via data-over-sound.



B) POC data-over-sound device; MEMS mics and speakers will be used in the wearable device.

- *User experience benefits and uses include*: contactless and touchless; usable from 1 to several meters distance; the wearer being ambiently identified by smart devices and voice assistants.

- *Security benefits and use include*: easier handling but strong authentication, e.g. no need to insert into USB or manually transfer the PIN or token; the device can be sonically ”tethered” to equipment; also, in an **open (i.e. non-walled) voice services world** the device can be used to reverse-authenticate the external services such as the third party skills and apps.



C) Data communication evaluation tunnel.