Voice Security On the Rise

Examining the Path to Secure Voice Automation

Dr. Mi-Sung Cho & Jimi Kang

White Paper | January 2017

alticast

alticast

Contents

Executive Summary

"JARVIS, I'd like to open a new project file." When "Iron Man" first was released, Tony Stark's intelligent voice recognition system named JARVIS was part of a futuristic technology that was truly impressive. What's more noteworthy, however, is the speed at which voice recognition technology has arrived – not just in Hollywood, but in millions of homes around the world.

Examples include "OK Google" on Android devices or "SIRI" on Apple devices, both of which are used daily by many people. These voice recognition technologies make our lives simpler and more convenient -- negating the need for traditional user interface controls, such as keyboards and remote controls, and unifying search across all our devices. This has only become possible because voice recognition has made huge strides in recognizing multiple languages and accents over the last few years.

Voice is trending for navigating the TV media experience, so it only makes sense that using voice for service authentication should follow. In addition to a quick method for authentication, it also can identify the specific person in the household who is watching TV – allowing for a rapid determination of what content that user might want to watch as part of a more personalized experience.

With new technology comes new opportunity for hackers. The security of voice interfaces needs to be a critical component of any voice-driven solution. Voice recognition is vulnerable to cyber-attacks and secure authentication of users' voiceprints is paramount so that private biometrics information and unique voice characteristics can be safeguarded. The confidentiality and integrity for voice recognition systems is critical to ensure secure services.

"It's not just that your voiceprint might be stolen from the system and used to impersonate you elsewhere. Your voice also carries a lot of information — your gender, your emotional state, your nationality." (Bhiksha Raj, Professor of Carnegie Mellon University)

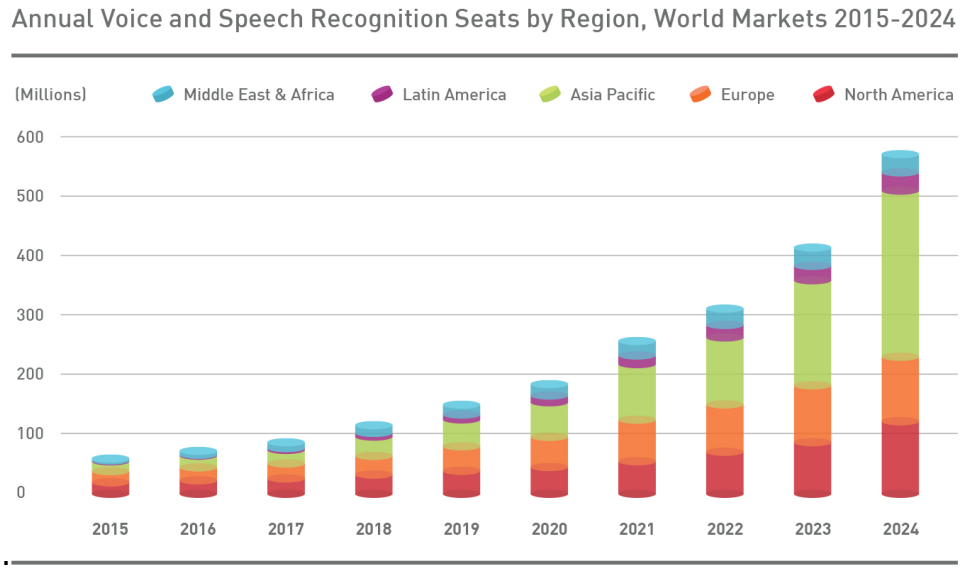
The Path to Voice Biometric Authentication

The terms speech recognition, voice recognition and voice authentication all have different meanings, but how do they differ? Speech recognition identifies what the speaker is saying, for example in speech-to-text applications; voice recognition (or speaker recognition) refers to identification of the speaker; and voice authentication is a security process that authenticates or verifies the identity of the speaker.

Speech recognition is one of the critical factors in the advancement of machine learning (i.e. Artificial Intelligence) technology. Voice-based user interface adoption is accelerating across industries and continents. As voice becomes the primary interface to all devices, appliances, and more, voice hacking can potentially expose an abundance of data. In this new world of voice control, secure voice authentication is essential.

Voice recognition was first introduced in 1950 and by 2000 enough progress had been made to begin to realize the opportunities that had been imagined. Pay-TV's introduction of voice navigation in recent years is considered to be the precursor to a broader expansion of voice-activated IoT services.

Voice recognition accuracy has leapt from 70% in 2010 to 90% in 2016. It is now perceived as the most efficient form of computational input because it enables hands-free interaction. The average person speaks about 150 words per minute, but can only type about 40 words per minute. Using voice as the primary way to interact with not only our mobile phones, but all our 'machines,' will improve productivity and simplify our lives.



Source: Voice and Speech Recognition, Tractica, June 11, 2015

The voice and speech recognition market is expected to grow significantly in coming decades by facilitating AI (artificial intelligence) and IoT, especially as the technology becomes more ubiquitous.

- Most everyone has a voice input device. *According to a Unisys survey, the biometric measures ranked by consumer preference are: voice recognition (32%), fingerprints (27%), facial scan (20%), hand geometry (12%), and iris scan (10%). This ranking seems to confirm that people prefer convenience and familiarity when choosing a biometric technology.*

- Voice control of AI allows for smarter services. Natural language interfaces that allow conversations between humans and machines are becoming more common. As individual data is gathered in these conversations, more personalized recommendations can be made, improving the quality of service and simplifying the life experience.
- Voice assistants including Alex, Siri and OK Google, are all getting integrated for use in gateways for IoT home automation as well as connected cars. Using a central voice controller allows any devices in the network to be easily managed.
- Voice authentication is much faster and more convenient than entering a pass code. Global banks have started launching voice biometrics authentication. A report form Nuance suggests 80% of users feel voice authentication is faster and 90% prefer voice as their primary method.

As these opportunities and others drive market expansion, there is an increasing need to ensure reliability and security. Robust measures are required that will safeguard the confidentiality of private data from two primary threats:

- Identity impersonators who attempt to replicate our voices to get access to important files, private information and even entire networks.
- Device vulnerabilities that allow hackers to hijack a voiceprint to gain entry to the primary device, as well as secondary devices that are connected to or controlled by the primary device.

Vulnerabilities such as these are prompting some security researchers to warn users to disable voice recognition on their devices.

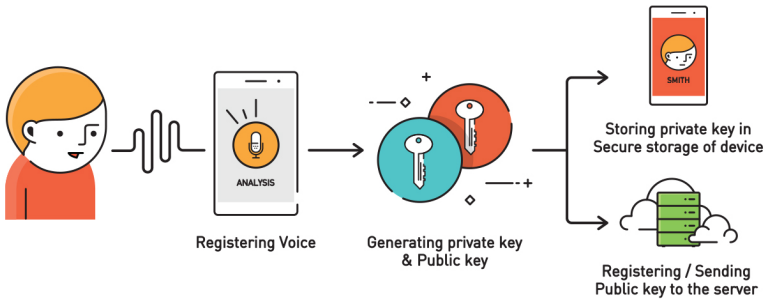
Overcoming Security Vulnerabilities

An example of how voice is becoming the primary user interface to our connected life is the increasing implementation of voice biometrics authentication in the financial industry. It is not enough that these systems simply recognize the voice itself; they also need to be able to authenticate that the speaker who is attempting to access the service is authorized to do so. Robust security and authentication technology is essential to prevent fraud and protect confidential data.

At the same time, it is also important to point out that authentication by voice as a singular method is not viable, as a user may get ill and their voice may be unrecognizable, so a back-up secure method for service access is necessary.

To minimize the likelihood of unauthorized access due to identity impersonators or device vulnerabilities, additional measures are needed to ensure the confidentiality and integrity of the voice data itself. This can be accomplished through a two phase process – registration plus verification/authentication.

- Registration: In this phase, the user's voice biometrics information is stored locally *ONLY* by the client and the authentication data and a public key are stored *ONLY* on the server side.



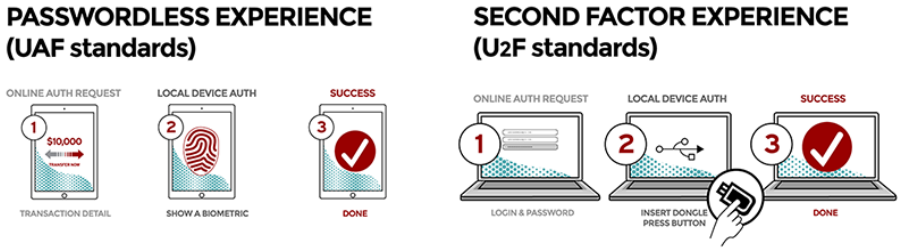
1. A client device sends a message to initiate registration to the server. The user registers his/her voice to the device and both public and private keys are generated.
2. The private key is stored within the secure storage on the client side and the public key is sent to the server in an encrypted form.

- Authentication: After voice biometrics information is registered on the server side, the authentication process is done in 2 phases – Verification and Authentication.

1. The client sends a message to initiate authentication to the server. Then the server returns relevant authentication policy and a 'challenge' created randomly.
2. User verification is completed locally with the stored voice data and a response to the 'challenge' is created and sent to the server encrypted with the private key.
3. The server decrypts the response and completes the authentication process.

Separating the verification process and storing the confidential biometrics data only stored in personal devices eliminates security concerns that could arise by storing that data in a public area. More enhanced security can be done using multi-factor authentication that can combine such methods as fingerprint, voice, retina, and PIN or password. Such protocols are standardized by the FIDO Alliance (Fast IDentity Online) with two different standard protocols – UAF (Universal Authentication Framework) and U2F (Universal 2nd Factor).

- UAF: Passwordless UX with biometrics authentication. Two-factor authentication is also possible by combining biometric and PIN identifiers.
- U2F: Strengthens traditional authentication using ID and password with an additional authentication module on a USB dongle or smartcard.



Source: The FIDO User Experience, https://fidoalliance.org/, Dec 15, 2016

Enriching and Simplifying Lifestyles

With the wide-spread use of mobile devices integrated with biometric capabilities, mobile payment services are becoming increasingly common. Biometrics Research Group estimated that annual transactions on mobile devices will hit US$750 billion globally by 2020, with more than 700 milion consumers using a mobile payment system.

Global banks have started adopting voice authentication solutions for mobile transaction services. In June 2016, Citigroup announced they would roll out voice biometic authentication in Hong Kong for a faster and more convenient user experience. HSBC and Barclays have also introduced this technology for their mobile banking customers.

Recently, many pay-TV operators have started providing voice-enabled media services on their set-top boxes, usually using a microphone in the remote control. Set top boxes also are expected to become gateways for emerging IoT services, providing subscribers with home automation controls and providing personalized TV services. By authenticating different voice profiles, the service provider can offer individualized services for each household member.

For more robust security authentication -- for example secure payment transactions for TV shopping -- two-factor authentication is recommended for example using voice authentication and a PIN number.

Conclusion

Voice authentication is an effective way to identify users for logging into services. Each person's voice is unique, making voice authentication an effective tool for identifying users for fraud mitigation so long as tightly secured processes are used for authentication. To eliminate concerns of voice print hacking, voice biometrics should be stored in a secure area of a device using robust cryptographic algorithms. This information remains locked within the device. Multi-factor authentication can add an extra layer of security for more robust and reliable user authentication.

Alticast is delivering end-to-end media solutions including CAS and DRM for service and content protection. The Alticast security business unit is introducing new technology to operators to expand their business through technological innovation. This includes multi-factor authentication that can be used for IoT and Big Data applications, providing operators the confidence that their subscribers are protected when using any data or transaction applications.

Resources

I. Five Highlights From Mary Meeker's 2016 Internet Trends Report (2016, June 1)
http://www.forbes.com/sites/kathleenchaykowski/2016/06/01/five-highlights-from-mary-meekers-2016-internet-trends-report/

II. The User Experience, FIDO Alliance (2016, December 10)
https://fidoalliance.org.

III. Nuance
http://www.nuance.com/for-business/customer-service-solutions/voice-biometrics/index.htm.

IV. Biometrics Market Forecasts, Tarctica (Q2 2015)

V. Voice Recognition Technology Trend, ETRI (2015, May 20)
http://www.korean.go.kr/

VI. Source Security: Voice recognition – benefits and challenges of this biometric application for access control
https://www.sourcesecurity.com/news/articles/co-3108-ga.4100.html

Contact us today

For more information
please contact one of our regional offices or
visit www.alticast.com
or email info@alticast.com

Alticast Corporation
Seoul, South Korea
Tel +82 2 2007 7827
info@alticast.com

Alticast Inc.
Colorado, USA
Tel +1 720 887 1700
us@alticast.com

Alticast B.V.
Amsterdam, Netherlands
Tel +31 20 240 3190
eu@alticast.com

Alticast Vietnam
Hanoi, Vietnam
Tel +84 165 8737 339
asia@alticast.com