PROGRESS

2020019252 김나현

MAY 20th

- VocalLock: Sensing Vocal Tract for Passphrase-Independent User Authentication Leveraging Acoustic Signals on Smartphones
- Nauth: Secure face-to-face device authentication via nonlinearity
- SoundUAV: Fingerprinting Acoustic Emanations for Delivery Drone Authentication
- EarEcho: Using Ear Canal Echo for Wearable Authentication
- Proximity-Proof: Secure and Usable Mobile Two-Factor Authentication
- Acoustic Fingerprinting Revisited: Generate Stable Device ID Stealthily with Inaudible Sound
- Do you hear what i hear? fingerprinting smart devices through embedded acoustic components

- SoundWave: using the doppler effect to sense gestures
- Voice In Ear: Spoofing-Resistant and Passphrase-Independent Body Sound Authentication
- Lippass: Lip reading-based user authentication on smartphones leveraging acoustic signals
- S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol
- Lip reading-based user authentication through acoustic sensing on smartphones
- EchoFace: acoustic sensor-based media attack detection for face authentication (In) secure Acoustic Mobile Authentication

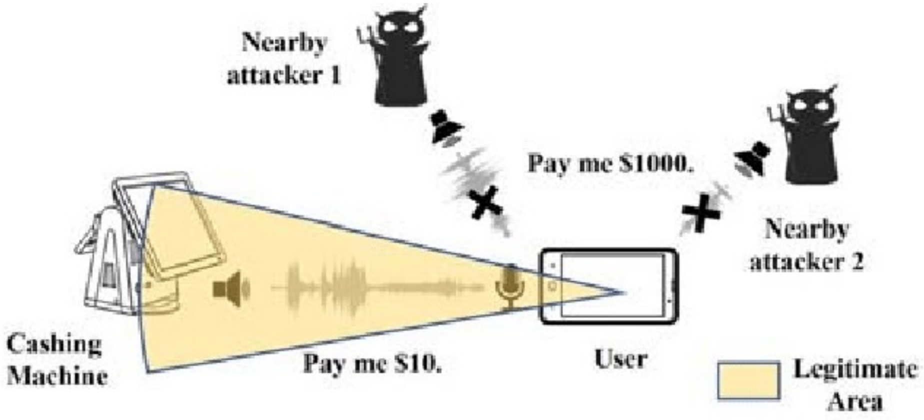
1. VocalLock: Sensing Vocal Tract for Passphrase-Independent User Authentication Leveraging Acoustic Signals on Smartphones (2020)

We propose a user authentication system, **VocalLock**, which senses the **whole vocal tract** during speaking

to identify different individuals in a **passphrase-independent manner** on smartphones leveraging acoustic signals.

VocalLock characterizes both the **static shape** and **dynamic movements** of the vocal tract during speaking, and then constructs a passphrase-independent user authentication model based on the unique characteristics of vocal tract

2. NAuth: Secure face-to-face device authentication via nonlinearity



We present **NAuth**, a nonlinearity-enhanced, location-sensitive authentication mechanism for face-to-face D2D communication even in the middle of a crowd, within which an attacker may hide.

The verification scheme guarantees **device authentication consistency** by extracting **acoustic nonlinearity patterns** (ANP) while the validation model ensures **device legitimacy** by measuring the **time difference of arrival** (TDOA) at two microphones.

3. SoundUAV: Fingerprinting Acoustic Emanations for Delivery Drone Authentication

Existing authentication schemes based on digital certificates have been shown to be compromised by security breaches on certificate authorities.

Thus, we propose **SoundUAV** as a second factor of authentication for drones that leverages **uniqueness in acoustic emanations**(attributed to hardware defects in motors) to fingerprint drones, even within the same make and model.

4. EarEcho: Using Ear Canal Echo for Wearable Authentication

With the goal of seeking a more unobtrusive wearable authentication method that the users can easily use and conveniently access, in this study we present **EarEcho** as a novel, affordable, user-friendly biometric authentication solution.

EarEcho takes advantages of the **unique physical and geometrical characteristics of human ear canal** and assesses the content-free acoustic features of in-ear sound waves for user authentication in a wearable and mobile manner

5. Proximity-Proof: Secure and Usable Mobile Two-Factor Authentication (2018)

Current mobile 2FA solutions all require some form of user effort which may seriously affect the experience of mobile users, especially senior citizens or those with disability.

We propose **Proximity-Proof**, a secure and usable mobile 2FA system **without involving user interactions**.

Proximity-Proof automatically transmits a **user's 2FA response** via inaudible OFDM-modulated acoustic signals to the login browser.

We propose a novel technique to **extract individual speaker and microphone fingerprints** of a mobile device to defend against the powerful man-in-the-middle (MiM) attack

6. Acoustic Fingerprinting Revisited: Generate Stable Device ID Stealthily with Inaudible Sound

we will present another new and more practical method for the adversaries to generate stable and **unique device ID stealthily** for the smartphone by exploiting the **frequency response of the speaker.**

With carefully selected audio frequencies and special sound wave patterns, we can **reduce the impact of non-linear effects and noises**, and **keep our feature extraction process un-noticeable** to phone owners.

7. Do you hear what I hear? fingerprinting smart devices through embedded acoustic components (2014)

During fabrication, **subtle imperfections** arise in device microphones and speakers, which induce anomalies in produced and received sounds.

We exploit this observation to uniquely **fingerprint individual smartphones** through playback and recording of audio samples.

Our experiments show that not only is it possible to fingerprint devices manufactured by different vendors but also devices that have the same maker and model

8. SoundWave: using the doppler effect to sense gestures

it is still relatively **costly** to deploy robust gesture recognition sensors in existing mobile platforms.

We present **SoundWave**, a technique that leverages the speaker and microphone already embedded in most commodity devices to sense in-air gestures around the device.

To do this, we generate an **inaudible tone**, which gets frequency-shifted when it reflects off moving objects like the hand.

We **measure this shift** with the microphone **to infer various gestures.**

9. Voice In Ear: Spoofing-Resistant and Passphrase-Independent Body Sound Authentication(2018)

voiceprint-based authentication is **vulnerable to voice spoofing attacks** (e.g., replay attacks and synthetic voice attacks).

To address this threat, we propose a new biometric authentication approach, named **EarPrint**, which aims to **extend voiceprint** and **build a hidden and secure user authentication scheme on earphones**.

EarPrint builds on **the speaking-induced body sound transmission** from the throat to the ear canal, i.e., different users will have different body sound conduction patterns on both sides of ears.

10. Lippass: Lip reading-based user authentication on smartphones leveraging acoustic signals(2018)

we explore liveness verification of user authentication leveraging users' lip movements, which are robust to noisy environments.

we propose a lip reading-based user authentication system, **LipPass**, which extracts unique behavioral characteristics of users' speaking lips leveraging build-in audio devices on smartphones for user authentication.

We investigate Doppler profiles of acoustic signals caused by users' speaking lips, and find that there are **unique lip movement patterns** for different individuals.

11. S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol(2017)

One promising solution to authenticate IoT devices is to extract a fingerprint to perform device authentication by exploiting variations in the transmitted signal caused by **hardware and manufacturing inconsistencies**.

We propose a lightweight device authentication protocol named **speaker-to-microphone** (S2M) by leveraging the **frequency response of a speaker and a microphone** from two wireless IoT devices as the acoustic hardware fingerprint.

S2M authenticates the legitimate user by matching the fingerprint extracted in the learning process and the verification process, respectively.

12. EchoFace: acoustic sensor-based media attack detection for face authentication (In) secure Acoustic Mobile Authentication(2020)

we propose **EchoFace**, an effective and robust liveness detection system to enhance face authentication in defending against media-based attacks

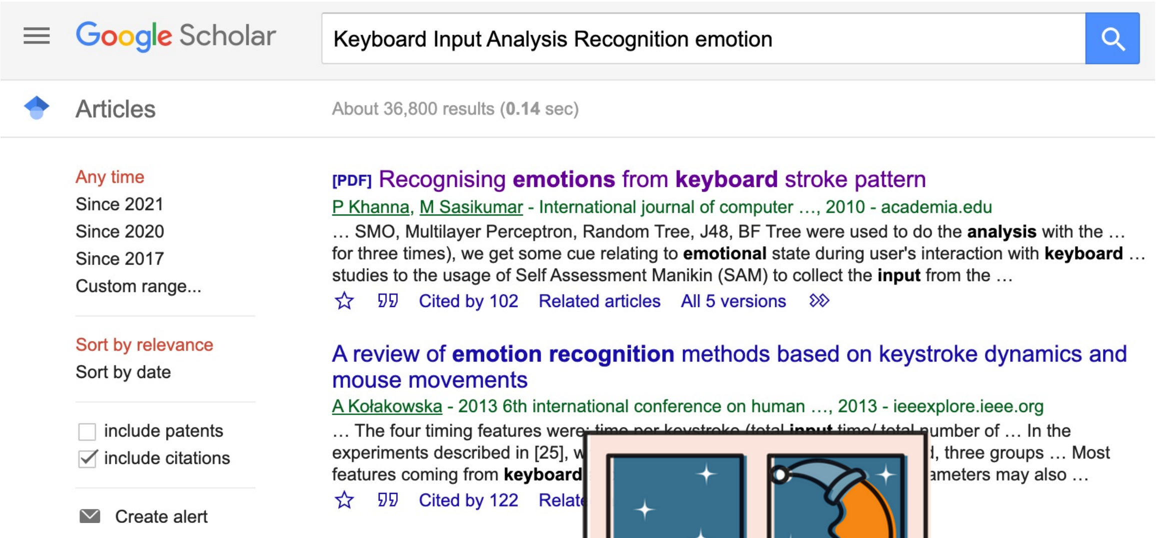
EchoFace uses **active acoustic sensing** to differentiate the uneven **stereostructure** of the face and the flat forged media.

Our proposed scheme effectively extracts the desired reflection profiles from the target.

we propose **effective similarity measurements of reflection profiles** to distinguish live users from forged media, which works robustly under various environmental conditions.

Ideas

- keyboard strokes
  -> Analyzing emotions



Keyboard Input Analysis Recognition emotion

Articles

About 36,800 results (**0.14** sec)

Any time
Since 2021
Since 2020
Since 2017
Custom range...

Sort by relevance
Sort by date

□ include patents
☑ include citations

Create alert

[PDF] Recognising **emotions** from **keyboard** stroke pattern
P Khanna, M Sasikumar - International journal of computer …, 2010 - academia.edu
… SMO, Multilayer Perceptron, Random Tree, J48, BF Tree were used to do the **analysis** with the … for three times), we get some cue relating to **emotional** state during user's interaction with **keyboard** … studies to the usage of Self Assessment Manikin (SAM) to collect the **input** from the …
☆ 99 Cited by 102 Related articles All 5 versions

A review of **emotion recognition** methods based on keystroke dynamics and mouse movements
A Kołakowska - 2013 6th international conference on human …, 2013 - ieeexplore.ieee.org
… The four timing features were: time per keystroke (total **input** time/ total number of … In the experiments described in [25], w … l, three groups … Most features coming from **keyboard** … ameters may also …
☆ 99 Cited by 122 Relat

- Keyboard Input Recognition (ATM, password)

- Breathing sound -> Analyzing sleep stages, disorder