精读

VELODY: Nonlinear Vibration Challenge-Response for Resilient User Authentication (CCS'19)

Summary

- **Basic concepts:** Acoustic vibration has different harmonics and intermodulation under different acoustic emulation. The attenuations at different frequencies is different when going through different multipath.
- Hand-surface vibration vibration responses: ***uniqueness***, contributed by physiological characteristics of human hands, and ***nonlinearity***, whose complexity prevents attackers from predicting the response protocol.

Details

- Four kinds of attacks
  - zero-effort attack
  - imopersonation
  - raw signal replay attack
  - synthesis attack
- Challenge desing
  - requirments: distinguishable (among users); distinguishable (among challenges) + unpredictable
  - chirp + sinusoidal wave
- Feature processing
  - alignment and segment + bandpass filtering
  - Ceptral feature (MFCC) + Statistical feature of ceptral feature (mean, variance,...)
- Classification (OC-kNN, an instance-based classifier)
  - mapminmax --> weight --> distance dj --> threshold estimation
- Evaluation
  - Hardware: Surface (copper plate lying on a ploymer foam pad), Stimuli (loudspeaker), Receiver (two contact microphones (accelerometers))
  - data collection: 15 subjects, three data collection sesssions (intra/inte-days), fixed hand shape for consistent alignment
  - train/test:
    - intra-day: with 30min apart
    - inter-day: with 5 days later to collect 3rd session as the testset while the formar two session as the trainset.
  - Metrics: FNR (usibility), FPR (security), EER (FNR==FPR)

Strength

- Solve the problem: human biometrics are non-resilient by introducing a ***challenge-response biometric authentication***
- A new perspective of human biometrics: a dynamic view (challenge-response)

Weakness

- the position of hands/speaker/receiver
- the sound level of the speaker
- authentication time
- when a new user entrolls. the thresholds should be re-calculated? Or the threshold only correlates with the baseline response without hand contact?
- the evaluation about the three kinds of synthesis attack is not convictive.

Inspiration

Nonlinear vibra-response --> nonlinear mm-response

1. **mmWave-based Palmprint (Tag-based)**

- device: IWR1642 or 120GHz radar
- Goal:
    - authentication
    - recover pixel-level palmprint

2. **mmWave-based Fingerprint (Tag-based)**

- device: 120GHz radar

3. **challenge-response auth in hardware fingerprint?**

泛读

Short-Range Audio Channels Security: Survey of Mechanisms, Applications, and Research Challenges

Vocie Controllable System

- Voice capture + Speech recognition + Cmd execution
- Activation Stage ("Hey Google") + Recognition Stage (NLP)

Active attacks

- Malware (attack against the voice assistant): strong limitation about the execution of the malware
- Unintelligitble but Audible audio signal: audible and white box (assumes some knowledge of the victim's speech recognition system by the attack)
    - Overcome some limitations

- Inaudible-Dolphin Attack (Modulated on Ultrasonic)
- Voice conversion spoofing attacks: mimic the user's voice wihout modifying its content

Passive attacks (Covert listening deivce)

- Recovery printed words on dot-matrix printers, but not ink-jet or laser printers (microphone, 10cm, ML-based, contexct)
    - similar attack on manufacturing system
- Keyboards (Limited real applicatbility by the proximity)
    - keystroke-Sounds-based + fft feature + Neural network
    - Improved (unlabled keystrokes + Cepturm feature)
    - Keystroke-Position-based (No training phase but Statistical properties of English language)
        - [Handwriting on the same]

Defense

- Synthetic sounds: white noise/random sounds to pollute the side-channel, or dedicated sounds to cheat the attacker.
- Masking sound: should be evaluated against Independent Component Analysis (ICA) attack.
- Usability discussion: addtional components, extra action of the user (degradation on user experience)

VibWrite: Towards Finger-input Authentication on Ubiquitous Surfaces via Physical Vibration (CCS'17)

summary

VibWrite enables finger inputs on ubiquitous surfaces to authenticate both the password and the user. It integrates passcode, behavioral and physiological characteristics and surface dependecy together to achieve the authentication.

Solved problem

1. Enable authentication on ubiquitous surfaces with a low-cost hardware solution (vibration motor and receiver)
2. Enable both password-auth and user-auth at the same time. (Extract user-dependent feautures from the vibration)

Main idea

1. A challenge-response solution
2. Extract user behavioral and physiological feature from the vibration (in the frequency domain).
3. cm-level location discrimination, unique features are embedded in a user's finger pressing at different lcoations on a solid surface