Poster Abstract: Uncovering Mobile User Gait Patterns Through Contactless RF Channels

Huanqi Yang[1], Xinyue Li[2], Jiahuan Chen[2], Mingda Han[3], Weitao Xu[1]
[1]City University of Hong Kong, [2]Xidian University, [3]Shandong University,

ABSTRACT

Gait-based authentication has risen to prominence for its distinctive advantages, becoming an essential security mechanism for mobile devices. These devices typically employ Inertial Measurement Units (IMUs) to capture intricate gait patterns for confirming the identity of users. However, our research highlights a vulnerability: the user's gait data on mobile devices is susceptible to interception through a radio frequency (RF) side-channel, potentially allowing unauthorized access. We introduce `Gait-Snoop` as a proof-of-concept for this novel side-channel attack. `Gait-Snoop` utilizes the RF signals reflected during a user's walk to extract gait information. It then correlates these RF signal patterns with IMU-derived gait data and employs a robotic arm to replicate the gait, aiming to deceive and unlock the targeted mobile devices. Our comprehensive evaluation of `Gait-Snoop` on smartphones demonstrates its capability to mimic IMU gait signals, underscoring the effectiveness and potential risks of such side-channel attacks.

1 INTRODUCTION

Gait recognition has recently attracted attention for its unique benefits as a biometric identifier [2]. Gait, an individual's distinctive way of walking, is shaped by an interplay of anatomical structure, motor skills, and habitual patterns, making it a sophisticated and nuanced biometric. One of the key advantages of gait as a form of biometric authentication is its ability to be measured unobtrusively from a distance, without requiring direct interaction with the person being identified. This non-intrusive aspect ensures a level of security that is both effective and respectful of personal space. In contrast to other biometric systems, gait recognition offers more privacy and tends to be less prone to variability under different conditions, unlike facial recognition which can be affected by various factors such as changes in facial hair, cosmetics, or the presence of accessories. Moreover, the proliferation of advanced technologies has made the collection of gait data more accessible than ever before. Among these technologies, Inertial Measurement Units (IMUs) stand out. Commonly embedded in smartphones and wearable devices, IMUs can capture detailed, high-fidelity gait information. The requirement for user participation when using IMUs also adds a layer of consent, making it particularly well-suited for protecting personal and sensitive assets [1, 5]. Given the high accuracy, ease of use, and security benefits, IMU-based gait recognition is arguably the best approach for biometric authentication. Its integration into commonly carried devices ensures a user-friendly experience, while the need for active user engagement provides an additional safeguard, solidifying its position as a leading solution in the realm of personal security.

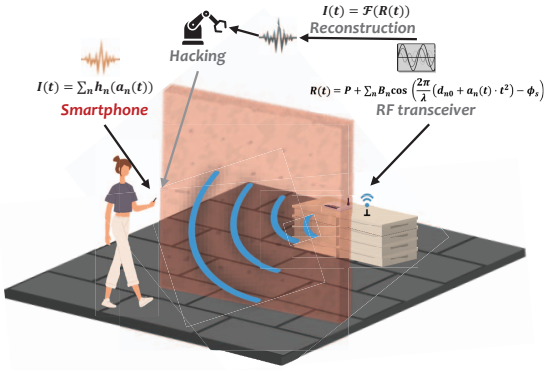

Figure 1: `Gait-Snoop` overview. `Gait-Snoop` uses RF signals to recover the user's gait signals on mobile devices and employs a robotic arm to replicate the gait, aiming to deceive and unlock the targeted mobile devices.

Surprisingly, our research has uncovered a previously unreported vulnerability: the IMU data used for gait authentication on mobile devices can be compromised simply when users are walking normally. This security gap exists because the motion of walking invariably emits radio frequency (RF) signals that inadvertently carry enough information to reconstruct the acceleration patterns associated with a person's gait. The security loophole becomes exploitable when a user walks past an RF transceiver (e.g., WiFi, LoRa). During this process, the transceiver is capable of detecting and capturing the RF signals that correspond to the user's walking patterns. These signals can then be processed to generate data that mimics the gait information typically derived from an IMU. Armed with this simulated IMU data, an adversary could employ a robotic arm to artificially reproduce the user's gait. The ultimate goal of this sophisticated attack is to trick and gain unauthorized access to the target's mobile device by passing the gait authentication checks.

979-8-3503-6201-5/24/$31.00 ©2024 IEEE
DOI 10.1109/IPSN61024.2024.00049

In this paper, our objective is to delve into the potential of RF signals for acquiring accelerometer data of user's gait from mobile devices. Our principal contributions can be summarized as follows:

1) We introduce Gait-Snoop, a pioneering system that uses RF signals to accurately recover the accelerometer data corresponding to a user's gait from a mobile device, thereby hacking the user identification mechanism.

2) We develop a novel method of transforming RF signals into accelerometer signals. We utilize a diffusion model for this transformation. The diffusion model effectively maps the correlation between the RF signals and the corresponding accelerometer signals.

3) The initial evaluation of Gait-Snoop on smartphones validates its proficiency in recovering IMU-based gait signals, highlighting the system's effectiveness and the consequential security implications posed by such sophisticated side-channel attacks.

2 SYSTEM OVERVIEW

In Gait-Snoop, the attacker leverages RF signals to demodulate and capture the user's gait patterns, followed by using a Maximal Overlap Discrete Wavelet Transform (MODWT)-based algorithm to reconstruct a spectrogram that encapsulates the victim's distinctive gait signature. Subsequently, a diffusion model is applied to translate the spectrogram into IMU gait data, potentially allowing the attacker to replicate the user's walking patterns and compromise their privacy. This system overview underscores the complexity of the attack and the considerable threats it poses to the integrity of gait-based authentication systems.

2.1 Attack Triggering Recognition

The detection of walking is determined by observing that human movement typically causes larger fluctuations in the phase differences of the RF signals than those caused by ambient disturbances. When there is no human movement, the fluctuations in the phases are mainly due to noise, which changes slowly over time. A dynamic thresholding algorithm is employed to monitor this noise.

2.2 Eavesdropping User Gaits

Signal Preprocessing. The initial stage of preprocessing involves applying a median filter in conjunction with the Hampel identifier [3] to remove outliers that significantly differ from the expected RF phase values. Subsequently, the MODWT [4] is employed, which effectively diminishes the residual noise in the denoised signal.

Spectrogram Generation. After the signal reconstruction, a spectrogram is created using the Short-Time Fourier Transform (STFT). This process involves segmenting the signal into overlapping windows and computing the Fourier transform for each segment.

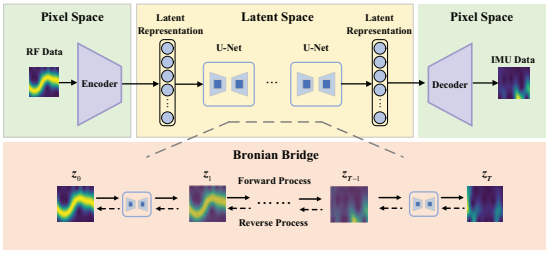

Figure 2: Diffusion Pipline

Diffusion-based Acceleration Reconstruction. Diffusion models have been successful in creating detailed and high-quality images, standing out in areas like changing the style of an image or generating new images based on certain themes. Therefore, we propose a novel method that uses a diffusion process to establish a straightforward connection between RF signals and IMU signals.

Spectrogram conversion. After generating the acceleration spectrograms, we use the Griffin-Lim algorithm iteratively reconstructs the 3-axis acceleration signals.

3 PRELIMINARY RESULTS

We utilize a USRP X310 Software Defined Radio to act as the attacker's tool. The algorithm that carries out the attack is executed on a Raspberry Pi. Our evaluation, conducted across five different mobile devices, indicates that the attack achieves an average gait data reconstruction similarity of 82%. This level of accuracy demonstrates the potential efficacy of our proposed side-channel attack in compromising gait-based security systems on mobile devices.

4 CONCLUSION

This paper introduces a novel side-channel attack that leverages RF signals to acquire a user's gait data from mobile devices. Our approach exploits the vulnerability of gait authentication system on mobile devices, allowing an unauthorized entity to infer gait information about a user.

REFERENCES

[1] Omid Dehzangi, Mojtaba Taherisadr, and Raghvendar ChangalVala. 2017. IMU-based gait recognition using convolutional neural networks and multi-sensor fusion. *MDPI Sensors* (2017).

[2] Ju Han and Bir Bhanu. 2004. Statistical feature fusion for gait-based human recognition. In *IEEE CVPR*.

[3] Ronald K Pearson. 2002. Outliers in process modeling and identification. *IEEE Trans. Control Syst. Technol.* (2002).

[4] Donald B Percival and Andrew T Walden. 2000. *Wavelet methods for time series analysis.* Cambridge University Press.

[5] Weitao Xu, Yiran Shen, Yongtuo Zhang, Neil Bergmann, and Wen Hu. 2017. Gait-watch: A context-aware authentication system for smart watch based on gait recognition. In *ACM/IEEE IoTDI.*