THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

COMP RESEARCH STUDENT SEMINAR

Date : 12 July 2023 (Wed)
Time : 2:30 pm - 3:30 pm
Venue : HJ303 (Face-to-face)

Inducing Wireless Chargers to Voice Out for Inaudible Command Attacks

Abstract

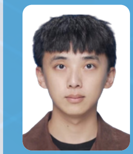
Recent works demonstrated that speech recognition systems or voice assistants can be manipulated by malicious voice commands, which are injected through various inaudible media, such as ultrasound, laser, and electromagnetic interference (EMI). In this work, we explore a new kind of inaudible voice attack through the magnetic interference induced by a wireless charger. Essentially, we show that the microphone components of smart devices suffer from severe magnetic interference when they are enjoying wireless charging, due to the absence of effective protection against the EMI at low frequencies (100 kHz or below). By taking advantage of this vulnerability, we design two inaudible voice attacks, HeartwormAttack and ParasiteAttack, both of which aim to inject malicious voice commands into smart devices being wirelessly charged. They make use of a compromised wireless charger or accessory equipment (called parasite) to inject the voice, respectively. We conduct extensive experiments with 17 victim devices (iPhone, Huawei, Samsung, etc.) and 6 types of voice assistants (Siri, Google STT, Bixby, etc.). Evaluation results demonstrate the feasibility of two proposed attacks with commercial charging settings.

Mr Donghui DAI
PhD student
Department of Computing

About the Speaker

Donghui Dai received his bachelor's degree in Electrical Engineering from Sun Yat-sen University in 2020. He is now a PhD student at the Department of Computing at The Hong Kong Polytechnic University, under the supervision of Dr Lei Yang. His research interest focuses on wireless system and mobile security, including physical side-channel attack, cross-technology communication and UHF RFID beamforming system.

Leaking Arbitrarily Many Secrets: Any-out-of-Many Proofs and Applications to RingCT Protocols



Mr Tianyu ZHENG
PhD student
Department of Computing

About the Speaker

Tianyu Zheng received his bachelor's degree in Information Science and Engineering in 2020 and master's degree in Cyber Science and Engineering in 2022 from The Southeast University. He is now a PhD student at the Department of Computing at The Hong Kong Polytechnic University, under the supervision of Shang Gao. His research interest focuses on applied cryptography, including zero-knowledge proofs and ring signatures.

Abstract

Ring Confidential Transaction (RingCT) protocol is an effective cryptographic component for preserving the privacy of cryptocurrencies. However, existing RingCT protocols are instantiated from one-out-of-many proofs with only one secret, leading to low efficiency and weak anonymity when handling transactions with multiple inputs. Additionally, current partial knowledge proofs with multiple secrets are neither secure nor efficient to be applied in a RingCT protocol.

In this paper, we propose a novel any-out-of-many proof, a logarithmic-sized zero-knowledge proof scheme for showing the knowledge of arbitrarily many secrets out of a public list. Unlike other partial knowledge proofs that have to reveal the number of secrets [ACF21], our approach proves the knowledge of multiple secrets without leaking the exact number of them. Furthermore, we improve the efficiency of our method with a generic inner-product transformation to adopt the Bulletproofs compression [BBB+18], which reduces the proof size to 2 log(N) + 9.

Based on our proposed proof scheme, we further construct a compact RingCT protocol for privacy cryptocurrencies, which can provide a logarithmic-sized communication complexity for transactions with multiple inputs. More importantly, as the only known RingCT protocol instantiated from the partial knowledge proofs, our protocol can achieve the highest anonymity level compared with other approaches like Omniring [LRR+19]. For other applications, such as multiple ring signatures, our protocol can also be applied with some modifications. We believe our techniques are also applicable in other privacy-preserving scenarios, such as multipl ring signatures and coin-mixing in the blockchain.