

1 / 52 91%

SILENT WEAPONS: EXAMINING FOREIGN ANOMALOUS HEALTH INCIDENTS TARGETING AMERICANS IN THE HOMELAND AND ABROAD

HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM, LAW ENFORCEMENT, AND INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

MAY 8, 2024

Serial No. 118-02

Printed for the use of the Committee on Homeland Security

1 / 18 70%

TARGETED INDIVIDUALS

If you make changes to your account, please log out on the side.

CCx4.0 Creative Commons License

Targeting Program

Lighthouse, Board Member

1 / 16 91%

Eavesdropping on Black-box Mobile Devices: Audio Amplifier's EMR

Hailing Chen¹, Wengang Hu^{1*}, Yipeng Hu^{1*}, Zhengyong Ning¹, Kexin Li^{1,2}, Zheng Qiu¹, Mingyong Duan^{1,2}, Yong Xue³, Dabao Liu⁴, and Ming Li¹

¹ College of Computer Science and Electronic Engineering, Hunan University, Changsha, China
² National Supercomputing Center in Changsha, Hunan University, Changsha, China
³ Nanjing University of Posts and Telecommunications, Nanjing, China
⁴ The University of Texas at Arlington, Arlington, Texas, USA

{chenh1, weng, yipeng, zheng, kexin, duanmingyong}@hnu.edu.cn, yongxue@utep.edu.cn, dabao.liu@gmail.com, mingli@uta.edu

Abstract: Eavesdropping poses serious threats to user privacy and security, such as phone calls, text messages, and confidential meetings. Smartphones are often the main source of personal and confidential information. However, our paper presents the first proof-of-concept, TargetedJust, that demonstrates the vulnerability of targeted mobile devices. The system shows that by using electromagnetic radiation (EMR) from audio amplifiers, it can be exploited as an effective eavesdropping device. Additionally, TargetedJust can be used to capture the EMR from these easily accessible or long distances, and hardware analysis further reveals highly correlated with the device's audio inputs and outputs, and wireless signals, making it a powerful tool for eavesdropping. To address this, we propose a secure communication system that can be used to detect and prevent eavesdropping. The necessary results are comparable to natural and audio speech input, and the system is a wide range of attack scenarios. We also design a 4-building mobile manufacturers.

1. INTRODUCTION

Eavesdropping on mobile devices is a common threat to user privacy. In this paper, we present a novel eavesdropping device that can be used to capture the EMR from these easily accessible or long distances, and hardware analysis further reveals highly correlated with the device's audio inputs and outputs, and wireless signals, making it a powerful tool for eavesdropping. To address this, we propose a secure communication system that can be used to detect and prevent eavesdropping. The necessary results are comparable to natural and audio speech input, and the system is a wide range of attack scenarios. We also design a 4-building mobile manufacturers.

Capítulo nuevo

Nuevas amenazas silenciosas

Luis Enrique Martín Chero

Resumen

En el siglo XXI, la tecnología junto con la biotecnología ofrece nuevos campos para la investigación que a veces parecen ciencia-ficción y con un amplio espectro de posibilidades, siendo muchas de ellas de aplicación dual. Lo que significa que, en mundo de hoy, el dominio militar y biológico sobre la población es el objetivo para conseguir dichos fines, siendo desarrollada por los países más poderosos. Las nuevas amenazas silenciosas q...

From:

<https://wiki.cibertortura.eu/> -

Permanent link:

<https://wiki.cibertortura.eu/doku.php?id=docs:start&rev=1790929553>Last update: **2026/10/02 08:25**