2023 IEEE | DOI: 10.1109/DSN58367.2023.00035
2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) | 979-8-3503-4793-7/23/$31.00 ©2023

Targeted Privacy Attacks by Fingerprinting Mobile Apps in LTE Radio Layer

Jaejong Baek
Arizona State University
Tempe, AZ, USA
jaejong@asu.edu

Pradeep Kumar Duraisamy Soundrapandian
Vellore Institute of Technology
Chennai, Tamilnadu, India
pradeepkumarst@gmail.com

Sukwha Kyung
Arizona State University
Tempe, AZ, USA
skyung1@asu.edu

Ruoyu Wang
Arizona State University
Tempe, AZ, USA
fishw@asu.edu

Yan Shoshitaishvili
Arizona State University
Tempe, AZ, USA
yans@asu.edu

Adam Doupé
Arizona State University
Tempe, AZ, USA
doupe@asu.edu

Gail-Joon Ahn
Arizona State University
Tempe, AZ, Country
gahn@asu.edu

***Abstract*—We investigate the feasibility of targeted privacy attacks using only information available in physical channels of LTE mobile networks and propose three privacy attacks to demonstrate this feasibility: mobile-app fingerprinting attack, history attack, and correlation attack. These attacks can reveal the geolocation of targeted mobile devices, the victim's app usage patterns, and even the relationship between two users within the same LTE network cell. An attacker also may launch these attacks stealthily by capturing radio signals transmitted over the air, using only a passive sniffer as equipment. To ensure the impact of these attacks on mobile users' privacy, we perform evaluations in both laboratory and real-world settings, demonstrating their practicality and dependability. Furthermore, we argue that these attacks can target not only 4G/LTE but also the evolving 5G standards.**

***Index Terms*—LTE, 4G, Fingerprinting, Privacy, Cellular, Machine Learning**

I. Introduction

Mobile communication signals permeate the airwaves as the number of devices and users increases while an average user spends almost 4 hours on their mobile devices every day [1]. Information that we send across these airwaves and the mobile applications with which we send it discloses intimate details (the radio layer) [4]. This means that previously-proposed attacks will only work when the attacker can access either *the victim's mobile device* or *the base station* the victim's device is connected to, where the attacker can sniff and analyze the transport layer traffic that is not protected by LTE encryption. In this case, compromising cell phones or breaking into base stations can be challenging in the real world. However, is this really necessary?

In this paper, we demonstrate that the physical channel of LTE alone is sufficient to carry out previously-proposed privacy attacks to identify which mobile applications are in use on a device. Because our attacks function on the physical layer of LTE, they can be carried out through self-deployed sniffers directly on the exact traffic transmitted *in the air*, and *do not require physical or logical access to user equipment or network nodes*. They also do not require the cooperation of mobile vendors. Worse, these techniques scale with the number (and coverage) of deployed sniffers, and by correlating the use of messaging applications between different devices, we could detect communication between targeted users. The capabilities that we describe in this paper allow an adversary