Practical APP's fingerprinting attack in 5G network

April 16, 2024

1 Introduction

Recent advancements in mobile network technologies, particularly in 5G [1], offer high-speed connectivity and low-latency, leading to their widespread adoption and utilization at the expense of alternatives like Wi-Fi. Consequently, popular apps such as WhatsApp, YouTube, and TikTok increasingly rely on mobile connections to transfer data. Given that these apps handle substantial amounts of personal user data, there's a growing responsibility on mobile communication systems to protect traffic from potential attacks, notably those exploiting vulnerabilities like mobile traffic analysis. Studies indicate that such attacks, including application fingerprinting, can compromise user privacy even when traffic is encrypted. While previous research primarily focused on exploiting implementation differences between apps and collecting internet traffic from public wired networks or Wi-Fi, mobile communication networks are relatively protected due to infrastructure security and data encryption. However, vulnerabilities persist, particularly in the radio link segment where encrypted mobile data can be intercepted using tools like software-defined radio.

Recent studies [2] [3] have demonstrated privacy attacks capable of inferring user activities by analyzing encrypted mobile traffic, presenting challenges due to encryption and the complexity of mobile networks. In response, researchers have developed novel approaches, such as leveraging mobile relay nodes and employing convolutional neural networks (CNNs) to identify app usage patterns from encrypted traffic.

2 Objectives

- Explore side-channel vulnerabilities by traffic sniffing and fingerprinting on the wireless channel.
- Accurately detect a list of apps installed on a victim's phone (alternatively: Web sites visited on the phone's Web browser), and detect the victim's activities as performed within those apps, from observing encrypted mobile network traffic.
- Design and setup the necessary experimental environment, including an emulated 5G core and radio part (note that emulations for both already exist at the chair).
- collect encrypted mobile traffic between the victim and the gNB with a 5G mobile-relay or sniffer as part of the experiment.
- Exploit the collected traffic to train fingerprinting classifiers, then exploit data sniffed from a victim UE to identify both the apps installed on the victim's phone as well as their usage.

3 Methodology

The main methodology will be implementations and actual measurements of 5G traffic in a local campus 5G setup. The chair already runs a 5G emulation testbed, upon which the student can build. The attack vector is using side-channels by traffic analysis using simple machine learning-based classifiers, so there is no need for formal verification or protocol fuzzing, or any other advanced vulnerability detection approach.

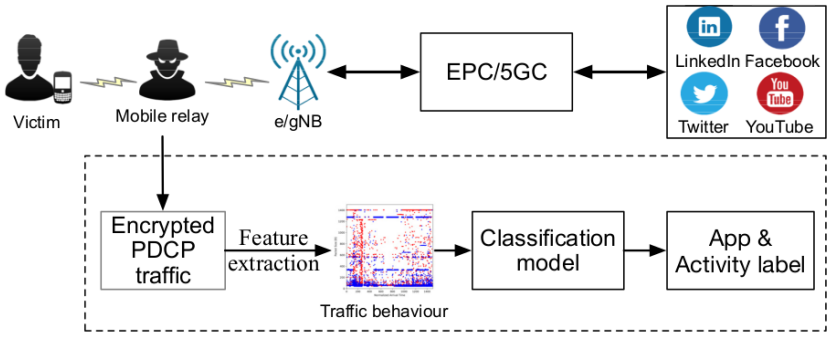

Figure 1: . The attacker sets up a position between the victim and the e/gNB to capture traffic (up). This traffic is processed in order to identify the apps and their activities as used on the a victim UE (down)..

- Literature Review: Conduct an extensive review of existing literature on 5G architecture and protocols.
- Experimental set up: data acquisition setup includes software-defined radio (SDR) with software gNodeb e,g OpenAirInterface 5G Radio Access Network and open source 5G core.

4 Expected Outcomes

- A comprehensive understanding of 5G architecture and protocols.
- setting up a controlled 5G environment.
- Identification of vulnerabilities specific to apps and their activities.
- analysis of the causes that enable fingerprinting and suggestions for protective privacy-enhancing technologies.

5 Conclusion

We will show that adversaries can obtain fine-grained app usage profiles from victims without requiring access to the victim's UE or the mobile network infrastructure. We will further analyze the causes that enable fingerprinting and propose solutions for improved protection.

References

[1] 3GPP, "5g; system architecture for the 5g system (5gs) (3gpp ts 23.501 version 16.6.0 release 16)," 2020.

[2] S. Bae, M. Son, D. Kim, C. Park, J. Lee, S. Son, and Y. Kim, "Watching the watchers: Practical video identification attack in LTE networks," in *31st USENIX Security Symposium (USENIX Security 22)*, (Boston, MA), pp. 1307–1324, USENIX Association, Aug. 2022.

[3] K. Kohls, D. Rupprecht, T. Holz, and C. Pöpper, "Lost traffic encryption: fingerprinting lte/4g traffic on layer two," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '19, (New York, NY, USA), p. 249–260, Association for Computing Machinery, 2019.