POSTER: No Doppelgänger: Advancing Mobile Networks Against Impersonation in Adversarial Scenarios

Felipe Boeira
Linköping University
Sweden
felipe.boeira@liu.se

Mikael Asplund
Linköping University
Sweden
mikael.asplund@liu.se

Marinho Barcellos
University of Waikato
New Zealand
marinho.barcellos@waikato.ac.nz

ABSTRACT

The expansion of mobile network capabilities throughout the decades has increased people's exposure to the digital world, and the next generations of communication networks are expected to achieve ubiquitous connectivity and immersive use cases. Security and privacy concerns have arisen and are continuously taken into account in the design of mobile networks. However, a relevant limitation currently lies in the use of shared secrets for providing security and privacy to users. Ideally, we believe that users' identities should be immune to impersonation as long as their own devices remain secure, notwithstanding the network operators and other entities potentially being compromised. In this paper, we develop this idea with the objective of providing the non-repudiation property, which represents a mitigation to its dual, impersonation.

CCS CONCEPTS

• **Networks** → **Network protocol design**; **Formal specifications**.

KEYWORDS

mobile networks, security, impersonation, non-repudiation

ACM Reference Format:
Felipe Boeira, Mikael Asplund, and Marinho Barcellos. 2022. POSTER: No Doppelgänger: Advancing Mobile Networks Against Impersonation in Adversarial Scenarios. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22), May 16–19, 2022, San Antonio, TX, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3507657.3529651

1 INTRODUCTION

Mobile networks have undergone tremendous development since their early deployments in the 1980's. While being originated for audio-only transmission at that time, mobile network generations evolved through the decades towards current 5G specifications that can support modern applications that involve low latency, high data rates, and accurate positioning.

As technology becomes increasingly a part of our personal lives, so does concerns about its security and privacy properties. Given the expansion of mobile networks and its use in more applications, attackers have gained more interest and motivation for compromising mobile network operators. Recently, it was uncovered that a group specialised in mobile operators has compromised at least 13 operators worldwide[1]. In addition, in 2015 an attack targeting a manufacturer of Subscriber Identification Module (SIM) cards (which contain each user's secret identity and key) resulted in the compromise of potentially millions of cards[2].

In addition to such malicious actors being able to disrupt security and privacy properties, many countries have also established legal frameworks for supporting lawful interception of mobile communication. Lawful interception is employed by authorised law enforcement agencies in the investigation of serious crimes and terrorism. Because intercepted material may be used in court against an individual, it becomes paramount to guarantee its legitimacy, integrity, and authenticity.

Security standards have evolved substantially towards providing security and privacy properties. However, an intrinsic weakness remains: operators and the supply chain for long-term secrets are assumed to be immune to being compromised by external attackers or malicious insiders. Given that they possess the secrets required to establish the communication, attackers that compromise such secrets may be able to impersonate their users. This potentially leads to the compromise of other services (e.g., instant messaging and social media accounts) through the reception of activation codes through text messages or calls. In 2018, attackers have used similar techniques in Brazil to compromise Telegram accounts of high-profile politicians and members of the judiciary system for political reasons [3]. Likewise, it is straightforward to imagine other scenarios in which impersonation could be used to manipulate political or even war events, conduct incrimination of individuals or perform other cyberfrauds.

To advance upon 5G, the current conceptual discussions of future 6G networks expect it to achieve global connectivity where the physical, digital, and human worlds are unified. This expands the scope of lawful interception, as well as the concerns regarding misuse of digital identities in case of attacks. In this paper, we propose design changes to mobile communication in order to **mitigate the risk of impersonation** by achieving its dual property, non-repudiation. Ultimately, we aim at achieving non-repudiation with the sole assumption that the user keeps it device secure, while operator infrastructure and SIM card manufacturers might be compromised. The remainder of the paper is organised as follows: Section 2

[1] LightBasin: A Roaming Threat to Telecommunications Companies, available: https://www.crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/
[2] Two Billion Owned SIM Cards is a Real-Life Nightmare, available: https://www.kaspersky.com/blog/gemalto-sim-hack/7774/
[3] Telegram voicemail hack used against Brazil's president, ministers: https://www.zdnet.com/article/telegram-voicemail-hack-used-against-brazils-president-ministers/

introduces relevant preliminaries, Section 3 presents our solution design proposal, and Section 4 concludes the paper.

2 SYSTEM AND THREAT MODELS

This section introduces relevant actors in the mobile network ecosystem and the threat model for the development of our solution.

Mobile Network Entities. The current mobile network ecosystem is composed of several participants, including hundreds of operators worldwide, dozens of SIM card manufacturers, mobile device manufacturers, operating system and application developers, and others. We investigate what are the relevant entities that, if compromised, might enable impersonation attacks of mobile users even when their devices remain secure. One fundamental problem lies in having shared secrets, such as the long-term secret key and identity (i.e., the subscription permanent identifier in 5G). We therefore highlight the following entities that are relevant in the context of this paper:

- User Equipment
- Home Network
- Serving Network
- SIM Card Manufacturer

Threat Model and Scenarios. We consider a powerful attacker that may compromise one or more components of the home/serving network, the SIM card manufacturer, or the SIM provisioning protocol or infrastructure. The threat model captures both external and internal attackers, including disgruntled or bribed employees. To exemplify some scenarios, we outline the following:

(1) Attackers compromise an operator's server responsible for SIM provisioning and capture long-term keys and identities
(2) Attackers bribe SIM card manufacturer employee to obtain a copy of generated keys database for a batch of SIM cards
(3) Attackers compromise the base station of an operator
(4) Operator malicious insider leaks the long-term key of governmental agents' devices

3 SOLUTION DESIGN OVERVIEW

In this section we present an overview of our proposal to achieve non-repudiation in mobile networks. We consider the latest standards released by the 3rd Generation Partnership Project (3GPP) and aim to make minimal changes and minimize overhead. The solution comprehends five *components*: setup, authentication and key agreement, communication, handover, and lawful interception and dispute resolution. Given the current space constraints, we only provide the reasoning for the need of design changes in each of the components.

Setup Phase. We assume that the mobile device is either equipped with a new SIM card or a used card for which it has setup before. This allows a user to guarantee that its SIM card has not been previously setup by an attacker, and also prevents an attacker from performing a new setup after the user. Intuitively, the objective of the setup is to generate a fresh pair of Non-Repudiation (NR) elliptic curve keys and to run a setup protocol such that the user and operator obtain mutual commitments for the use of the generated NR keys in subsequent components. Such commitments may be used later in dispute resolution in case of lawful interception operations.

Authentication and Key Agreement (AKA). The AKA design must be adjusted so that the private NR key is used to guarantee non-repudiation even though the attacker has compromised the user's shared secrets. To verify our design, we extend the models by Basin et al. [1] and Cremers and Dehnel-Wild [2].

Communication. Since the attacker may compromise components of the core network of operators, it is necessary to address non-repudiation in the transmission of user data. To achieve that, we perform changes in the Packet Data Convergence Protocol (PDCP) where confidentiality and integrity protection are handled. Given that the introduction of overhead must be minimised, we investigate efficient stream signing schemes.

Handover. As the user equipment moves geographically, handover procedures are performed for deriving new keys and provide stable connection to the user. These protocols must also provide non-repudiation, and to validate our design changes we extend the models developed by Peltonen et al. [3].

Lawful Interception and Dispute Resolution. Lawful interception is conducted by many countries for investigation of serious crimes and terrorism. As these interceptions may be used in court against a potentially honest user, it becomes essential to guarantee its legitimacy, integrity, and authenticity. On a system that provides non-repudiation, a user can use the commitment obtained in the setup phase to dispute any false data the operator might have transmitted on behalf of the user (e.g., due to the compromise of a base station the user was attached to).

4 CONCLUSION AND NEXT STEPS

As mobile networks advance, societies become increasingly connected and our real and digital identities become intertwined. In this paper, we provide arguments for the need of protection against impersonation considering cases where operators might become compromised by attackers. To develop the idea further, we aim to perform design changes to guarantee non-repudiation. To verify the correctness and security of our approach, we will use formal methods by extending state-of-the-art protocol models according to our design changes and introducing more granularity in the entities involved (e.g., by modeling base stations, secure anchor functions, and unified data management components separately) in the protocol in order to obtain the set of assumptions for non-repudiation to hold. Furthermore, as our personal identity becomes bound to digital identities of applications as we use them (e.g., social media and instant messaging), we aim to investigate how a non-repudiation guarantee in mobile network communication may be leveraged in the context of those applications to thwart impersonation.

REFERENCES

[1] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. 2018. A Formal Analysis of 5G Authentication. In *Proceedings of the 2018 ACM CCS* (Toronto, Canada) *(CCS '18)*. ACM, New York, NY, USA.
[2] Cas Cremers and Martin Dehnel-Wild. 2019. Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion. In *NDSS, San Diego, California, USA*. The Internet Society.
[3] Aleksi Peltonen, Ralf Sasse, and David Basin. 2021. A Comprehensive Formal Analysis of 5G Handover. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (Abu Dhabi, United Arab Emirates) *(WiSec '21)*. ACM, New York, NY, USA.