Design and Implementation of a Lawful Interception Architecture for B5G Systems Based on Key Escrow

Giuseppe Ungaro*, Francesco Ricchitelli*, Ingrid Huso*†, Giuseppe Piro*†, Gennaro Boggia*†
*Dept. of Electrical and Information Engineering - Politecnico di Bari, Bari, Italy,
†CNIT, Consorzio Nazionale Interuniversitario per le Telecomunicazioni
Email: {*name.surname*}*@poliba.it*

***Abstract*—Law Enforcement Authorities use Lawful Interception to prevent and investigate criminal offenses. But, the adoption of end-to-end encryption makes quite ineffective conventional approaches. To bridge this gap, this work (i) proposes a preliminary and standard-compliant Lawful Interception Architecture for Beyond 5G systems, based on a Key Escrow scheme, (ii) verifies its effectiveness through proof-of-concept tests, and (iii) proposes future research activities in this direction.**

***Index Terms*—Lawful Interception, Beyond 5G, Key Escrow**

I. Problem statement and Proposed Methodology

The adoption of end-to-end encryption in 5G and Beyond 5G systems [1] makes quite ineffective conventional Lawful Interception (LI) techniques based on available 3GPP specifications. Even though a Law Enforcement Authorities (LEA) is still able to intercept communication flows, the captured string of bits remains fully unintelligible. This important problem is under the reflectors of the European Commission [2], researchers and security specialists [3]. This work does not claim to definitively solve the problem! On the contrary, it wants to propose a possible technical solution, which will be of benefit to any future discussion on that topic.

The proposed standard-compliant LI architecture leverages Key Escrow capabilities. The reference mobile network includes the Next Generation Node B, which offers wireless connectivity to the User Equipment through the 5G New Radio interface, and the 5G Core Network. Herein, the User Plane Function hosts the Point of Interception (POI) entity, which is actually able to intercept targeted communications [4]. At the same time, it is assumed that the traffic generated by the UE is encrypted. Hence, the intercepted Content of Communication (CC), to be delivered to the LEA, is encrypted. By managing data encryption via Key Escrow system [5], it is still possible to allow the LEA do decrypt intercepted contents.

The proposed methodology involves three main phases: *key negotiation*, *interception* and *decryption*. Both mobile operator and the Key Generation Center actively participate in the *key negotiation phase*. Thus, end-users can autonomously retrieve the session key and protect the communication via end-to-end encryption. During the *interception phase*, a LEA with a valid interception warranty, interacts with the Mediation and Delivery Function to retrieve details about the targeted communication from the POI, including encrypted CC. Finally, in the *decryption phase*, the LEA decrypts the received encrypted CC by using the session key computed at the beginning.

II. Implementation and Future Activities

A proof-of-concept of the proposed LI architecture is implemented to verify the effectiveness of the proposed approach. Specifically, *Open5gs* and *UERANSIM* are used to emulate 5G New Radio interface and the 5G Core Network, respectively. Moreover, the user has been configured to download an encrypted picture (the targeted traffic) from a remote server. In the core network, the POI uses TCPdump for intercepting data, elaborating the .pcap file, and delivering the resulting CC to the LEA. Finally, the LEA can obtain the plaintext of the encrypted CC.

The goodness of the implementation demonstrates the potential of the conceived solution and also stimulates new discussions in academia and standardization domains. Future research activities will explore the adoption of such methodology in scenarios with network slices and the implementation of interception mechanisms at the network edge.

Acknowledgment

This work has been supported by the PRIN project no. 2017NS9FEY entitled “Realtime Control of 5G Wireless Networks: Taming the Complexity of Future Transmission and Computation Challenges“ funded by the Italian MIUR, and by the project entitled “The house of emerging technologies of Matera (CTEMT)“ funded by the Italian MISE. It has been also supported by the Italian MIUR PON projects AGREED (ARS01 00254).

References

[1] Y. Li, Y. Yu, W. Susilo, Z. Hong, and M. Guizani, “Security and Privacy for Edge Intelligence in 5G and Beyond Networks: Challenges and Solutions,” *IEEE Wireless Communications*, vol. 28, pp. 63–69, 2021.

[2] Council of the European Union and EUROPOL, “Position paper on 5G,” April 2019.

[3] Scientists4Crypto, “Academic letter to the european commission on ”encryption — security through encryption and security despite encryption”,” December 2020.

[4] 3GPP, “3GPP TS 33.127 V18.1.0 (2022-09),” Tech. Rep., September 2022.

[5] K. Han, C. Y. Yeun, T. Shon, J. Park, and K. Kim, “A scalable and efficient key escrow model for lawful interception of IDBC-based secure communication,” *International Journal of Communication Systems*, vol. 24, no. 4.