The end of Eavesdropping Attacks through the Use of Advanced End to End Encryption Mechanisms

Leandros Maglaras & Nick Ayres
School of Computer Science and Informatics
De Montfort University
Leicester, UK
(leandros.maglaras, Nick.Ayres)@dmu.ac.uk

Sotiris Moschoyiannis
Centre for Cyber Security
University of Surrey
Guildford, UK
s.moschoyiannis@surrey.ac.uk

Leandros Tassiulas
School of Engineering and Applied Science
Yale University
New Haven, CT, USA
leandros.tassiulas@yale.edu

***Abstract*—In this article we present our novel Secure Node End-2-End Encryption (SNE2EE) mechanism that is under implementation. This mechanism offers both a software and hardware solution by extending encryption technologies and techniques to the end nodes to increase privacy. The SNE2EE mechanism can address the issues concerning spyware and stalkerware at both the individual and community level.**

***Index Terms*—End to End Encryption, Privacy preservation**

I. Introduction

Current end-to-end (E2E) encryption solutions focus on encrypting data during transmission but not at the physical end nodes (i.e. the user) where data is received and read in cleartext. When an unencrypted message is received there is no confidence that the received message will be read by the intended recipient. Mobile communication devices are vulnerable to physical over-the-shoulder eavesdropping as well as digital eavesdropping often via unknown malware infections. Social media and communication apps are the most frequently consumed application types and account for almost half of global Internet traffic [1]. However, downloaded apps may harbour hidden stalkerware; a category of spyware that enables threat actors to monitor activity and access personal information. According to [2], stalkerware capabilities include recording, monitoring or accessing email, social media, stored media, SMS and chat apps. Notably, they may be used to enable Intimate Partner Stalking (IPS) where perpetrators use stalkerware as a surveillance tool against current or previous partners, perpetuating violence against women and girls [3]. Contemporary E2E encryption is failing to protect privacy, which is enabling mal-actors to use more innovative methods in order to spy on their targets [4]. The SNE2EE project proposes to extend encryption technologies and techniques to the end nodes to increase privacy.

The SNE2EE research proposes end-to-end mechanisms that comprises of four levels:

- The end node mobile device receives an encrypted message
- The received message is not decrypted until specific user Multi Factor Authentication (MFA) intervention
- Once MFA is passed, message is transferred from mobile device to attached screen overlay (or application)
- Once the message has been transferred it is then decrypted

The SNE2EE mechanism addresses several goals. It develops technologies to disrupt mal-actors by introducing a privacy-enhancing technology (PET) that specifically utilises a user-friendly Public Key Encryption (PKE) coupled with biometric authentication. Thereby, it aims to prevent 'front-line' criminals who perpetrate IPS. This research also tackles other forms of spyware and stalkerware at both the micro (individual) and macro (community/society) level. Furthermore, SNE2EE aims to enhance citizens' management of their personal data and protect it against unauthorized access. By providing them with a screen overlay (or application) to address physical over-the-shoulder eavesdropping, coupled with a separate PKE and biometric enhanced display, will help citizens manage threats to their data and privacy.

II. The SNE2EE mechanism

To overcome the weaknesses identified in the previous section we will build the SNE2EE novel solution that can offer holistic end to end privacy of messages exchanged by any two entities utilizing mobile devices without inducing high delays.

Towards these desired abilities, two research goals are formulated as follows:

1) Augmented reality must be efficiently integrated into existing messaging applications in order to make them highly secure.
2) The offered solutions must be user friendly and platform agnostic.

The proposed system will combine encryption technologies with innovative technologies (augmented reality equipment) to decouple privacy preservation of messages from the 'weak' mobile device. In order to achieve holistic end-to-end encryption, we are going to connect external devices to the mobile phone. These security enhancing devices will initially encrypt the message rather than the host device. Once the necessary encryption has been completed the ciphered message is sent to the mobile phone via Bluetooth for transmission. Upon receiving the message at the destination node the cipher text is transferred to the external device, awaiting biometric confirmation before decryption. To safeguard the privacy between

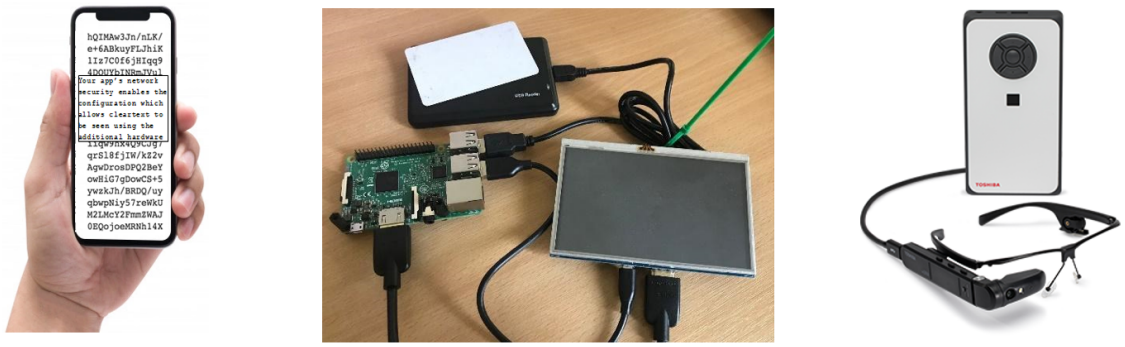

Fig. 1. SNE2EE solutions. A) Software Application for Android Mobile Phones B) Hardware Prototype using Raspberry Pi C) Integrated solution with a set of Smart Glasses developer kit

users, all messages will be encrypted using public/private cryptography models (e.g. Diffie-Hellman). These keys will be generated through a central entity that we will build for the purposes of the project or by using Pretty Good Privacy (PGP) generators.

Privacy is enhanced through PKE mechanisms that can be distributed via peer-to-peer or centralised through a mobile app. To facilitate secure messaging, this research utilises a separate hardware solution (along with an application solution) that incorporates a biometric mechanism which proves the intended recipient's identity [5]. To further enhance privacy, this biometric could form part of a more secure Multi Factor Authentication (MFA) system [6]. We have split the development of the mechanism into three phases.

The first phase is the implementation of the prototype through the use of Arduino, Raspberry Pi, fingerprint scanners, and liquid crystal display screens. This prototype will help us build the main software mechanisms needed for the system while at the same time test basic functionalities and identify early faults and weak points. Moreover, during the first phase we are implementing a pure software solution that will be released as an app for Android mobile phones. During the second phase of the project we will integrate our proposed system a set of Smart Glasses. These glasses include a mini pc, fingerprint reader, microphone and speakers, camera, Bluetooth and augmented reality capability among others. During the last phase of our project we will test the integration of more features into the identification phase of each user in order to further enhance the security of the system.

III. The SNE2EE solutions

The SNE2EE mechanism will offer several holistic E2E hardware and software solutions (See Figure 1). The software solution will be in the form of an app for any Android device and will be available - via a GitHub workspace dedicated to the project – under GNU Lesser General Public License (LGPL), in order to help researchers investigate the efficiency of such a solution and also the integration of it with other PETs.

This research will develop two hardware solutions, one prototype using Raspberry Pi/Arduino and some off the shelf peripherals (fingerprint scanner, Bluetooth connecting device, etc.), and an integrated solution using a set of Smart Glasses (including a developer kit). Also, all the software products developed for the integrated solution of the project, are intended to be open-source and freely available – via a GitHub workspace dedicated to the project – under GNU Lesser General Public License (LGPL). Note that, from an exploitation viewpoint, the SNE2EE solutions could be used after project completion for teaching and knowledge transfer purposes.

IV. Conclusions

In this article we present our novel SNE2EE mechanism that is under implementation. The mechanism that offers both software and hardware solutions extends encryption technologies and techniques to the end nodes to increase privacy. The SNE2EE mechanism tackles other forms of spyware and stalkerware at both in individual and community level. The developed solutions will be freely available in order to be easily used from other researchers in order to further extend the functionality of the prototype and blend it with other privacy or security mechanisms.

References

[1] M. Khader, L. S. Neo, and W. X. T. Chai, *Introduction To Cyber Forensic Psychology: Understanding The Mind Of The Cyber Deviant Perpetrators*. World Scientific, 2021.

[2] C. Parsons, A. Molnar, J. Dalek, J. Knockel, M. Kenyon, B. Haselton, C. Khoo, and R. Deibert, "The predator in your pocket: A multidisciplinary assessment of the stalkerware application industry," 2019.

[3] S. Chan, "Hidden but deadly: Stalkerware usage in intimate partner stalking," in *Introduction To Cyber Forensic Psychology: Understanding The Mind Of The Cyber Deviant Perpetrators*, 2021, pp. 45–66.

[4] T. Isobe and R. Ito, "Security analysis of end-to-end encryption for zoom meetings." *IACR Cryptol. ePrint Arch.*, vol. 2021, p. 486, 2021.

[5] M. A. Ferrag, L. Maglaras, and A. Derhab, "Authentication and authorization for mobile iot devices using biofeatures: Recent advances and future trends," *Security and Communication Networks*, vol. 2019, 2019.

[6] V. Papaspirou, L. Maglaras, M. A. Ferrag, I. Kantzavelou, H. Janicke, and C. Douligeris, "A novel two-factor honeytoken authentication mechanism," in *2021 International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2021, pp. 1–7.