Toward Context-aware Security for Individual Information Systems

Van-Tien Nguyen, Guillaume Doyen, Van-Tien Nguyen, Renzo E Navas, Eric Alata, Daniela Dragomirescu

Toward Context-aware Security for Individual Information Systems

Van-Tien Nguyen[1], Guillaume Doyen[2], Renzo E. Navas[2], Eric Alata[1], Daniela Dragomirescu[1]
[1]*INSA Toulouse/LAAS-CNRS, Toulouse, France* [2]*IMT-Atlantique/IRISA, Rennes, France*
{van-tien.nguyen, ealata, daniela}@laas.fr; {guillaume.doyen, renzo.navas}@imt-atlantique.fr

***Abstract*—For a few decades, the multiplicity of Internet services humans consume are increasing, leading people to actually manage their own Individual-oriented Information System (IIS), whose server sides are spread over the internet and operated by different service providers. The security of such systems is essentially service-centric while the user is the focal point of all their usage. If some user-centric solutions exist to date, they are either (1) restricted to some particular services, ignoring a global user activity, (2) intrusive, by requiring a complete instrumentation of user-side terminals, or (3) too specific by requiring the cooperation between the client interface and the server side. To cope with these limitations, we propose to develop a novel approach which consists in monitoring encrypted network flows issued by a user terminal and correlating this network activity with some external contextual information related to the user activity. Due to the lack of existing comprehensive datasets, our ongoing work consists in designing a long-term measurement campaign with real users using smartphones augmented with body sensors while facing security breaches such as malware activity or smartphone theft.**

***Index Terms*—Intrusion Detection System, Biometrics, Mobile, Individual-oriented**

I. Introduction

An individual utilizes multiple Information Systems (ISs) in their everyday activities, like emailing, banking, social networking, e-commerce, and more. Normally, each IS requires users to register an account to be identifiable in this system's digital realm. These systems usually retain user's sensitive information, such as passwords, email, or address. Thus, security techniques to secure users' online assets need to be deployed. Security solutions in the literature concentrates on securing one IS interacting with numerous users. Consequently, the security measures describe therein are associated solely with the interactions between an individual and a specific IS. The subject of securing a single individual that uses multiple ISs, independently of an IS security instantiated on a case-by-case basis, is an open challenge. Our proposition implies a transition in perspective, moving from system-centric security approaches towards an individual-oriented security framework.

To date, user-centric security solutions exhibit limitations: firstly, they may be constrained to some specific services, ignoring the user's global activities; secondly, they adopt an intrusive approach, necessitating the thorough instrumentation of the user side; and thirdly, they mandate collaboration between the client and server components. To cope with these limitations, we propose to develop a network-based intrusion detection system which consists in monitoring network flows issued by a user terminal and correlating this network activity with some external contextual information related to the user activity. The proposal emphasizes transparency to the user, and respects the confidentiality of all information systems' encrypted data. Due to a lack of public datasets with both network and (biometric) contextual data, we design a data collection campaign wherein each individual is equipped with a smartphone and body sensors to perform their daily (physical and digital) activities.

The rest of this work is arranged in two sections: Section II emphasizes the state of the art, whereas Section III presents our current work and perspectives.

II. Definition and State of the art

Kim and Ammeter [1] defined a personal information system as a system including three elements: (1) A user, (2) a personal engine that is an artifact having an understanding of the user, and (3) a task or function being done. However, this description presumably covers a single information system located on a mobile device and used by a single user. As such, it does not integrate either other physical devices taking part in user services or the link between a person and all information systems it interacts with. Consequently, we define the new terminology of an **Individual-oriented Information System (IIS)** as *a combination of three types of elements: (1) one person, (2) digital elements (i.e., information systems) that interact with the person, and (3) physical elements (e.g., a smartphone, smartcard, or computer) that the person uses to interact with digital elements*. Different threats target IIS, such as impersonating a legitimate registered user by stealing its personal information, hosting malware whose stealthy activity cannot easily be distinguished from the legitimate one, or physical device theft. In the rest of this section, we explore the state of the art of different aspects covering IIS security.

A. WBAN security

A Wireless Body Area Network (WBAN) is a wireless networking system using Radio Frequency (RF) to connect tiny nodes with sensor or actuator capabilities inside, on, or around a human body [2]. A WBAN is attached to an individual, facilitating the acquisition of body metrics, which can be subsequently transmitted to remote servers for additional analysis. Furthermore, a person's physical and physiological signals also serve as input features for numerous security methods, including authentication and key management [3].

All of the WBAN security studies focused on the security of the internal WBAN system or the WBAN's connection to a distant server (e.g., a healthcare system). None investigated the role of body measures in improving network security, particularly between a single user and many (non-WBAN) ISs.

B. Continuous Authentication

Many non-WBAN solutions for Continuous Authentication (CA) based on users' physical measures have been offered as an extension of biometric authentication in WBAN. CA is a security technique that monitors user behaviors at frequent intervals during a session and assesses if the user is legitimate [4]. Hernández et al. [5] identified two types of user-related features utilized in authentication: behavioral features (voice, gait, keystroke, mouse movement, etc.) and biological features (blood, heart, face, iris/pupil, etc.). According to reviews from [4], [5], there are three types of scenarios in CA. First, Web-based systems verify whether an interacting user is legitimate. Second, mobile devices verify whether the current user is the device owner. Last, smart environments verify the legitimacy of the user being presented. CA focuses on defending one IS against unauthorized users' activity. From our individual-oriented perspective, securing the interaction of an individual/user with many ISs will imply a high cost: either one CA solution per IS or a federated CA effort between all ISs—Federated CA: a field missing in the literature.

C. IDS in mobile devices

IDS is a mature field in security. Based on different system topology placement, i.e., host-based (HIDS) and network-based (NIDS), IDS approaches leverage features from several data sources to detect anomalies [6]. While HIDS analyzes a host's system calls and log files, NIDS utilizes network traces, e.g., network packets and flows, to diagnose anomalous events. Biometric data has been employed in certain recent works [7]–[9] to secure wireless body area networks. These proposals employ previously learnt changing patterns of the physiological data (heart, blood) and can detect forgery attacks on their future values.

An IDS should be agnostic to the unencrypted content of applications or information systems, as the payload is encrypted at the application layer (i.e., end-to-end). According to [10], several device-related contextual features are proposed for IDS in mobile devices, such as phone call/SMS-related information, device state, CPU utilization, battery, etc. However, the association between network flows and user-related behavior aspects has not been investigated in the literature.

III. Our approach

Real-world data is imperative for formulating and assessing a security solution for an IIS. However, dedicated datasets covering both users' network behaviors and their physical activities are missing. Thus, we first propose a measurement campaign to collect data from realistic use cases. Then, we advocate the design of a dedicated IDS that incorporates physiological metrics as innovative detection attributes.

A. A dataset of realistic scenarios

In our study, we examine two scenarios: (1) an intruder stealing the victim's mobile device and attempting to carry out some unauthorized digital activities, such as creating network flows from the legitimate device to the server of a legitimate information system; and (2) some malware applications running in the background, while the legitimate user is still using the mobile device, and carriyng out malicious digital activities.

Our custom mobile application gathers data from three sources: (1) network flows, (2) built-in sensors and device states of the smartphone, and (3) WBAN sensor data. We employ students and ask them to install the application and do their everyday activities. We emulate the attack scenarios by (1) requesting a student to use another's phone and conduct diverse digital activities and (2) installing harmless software acting as spyware/malware. This public dataset will be used to validate our proposal, and serve both the community of CA mechanisms and intrusion detection systems.

B. Proposal: Enhancing IDS using body measures

We examine an individual NIDS that integrates human contextual physical and physiological data. Machine learning and deep learning algorithms are methodologies used in IDS and would probably be a building block of our solution. The proposal is locally stored on the smartphone device, i.e., close to the user, and is agnostic of the external ISs/encrypted application traffic. Ultimately, the evaluation of the IDS will be conducted utilizing our acquired public dataset.

References

[1] D. Kim and T. Ammeter, "Predicting personal information system adoption using an integrated diffusion model," *Information & Management*, vol. 51, no. 4, pp. 451–464, 2014.

[2] D. M. Barakah and M. Ammad-Uddin, "A survey of challenges and applications of wireless body area network (wban) and role of a virtual doctor server in existing architecture," in *2012 Third International Conference on Intelligent Systems Modelling and Simulation*. IEEE, 2012, pp. 214–219.

[3] M. S. Hajar, M. O. Al-Kadri, and H. K. Kalutarage, "A survey on wireless body area networks: Architecture, security challenges and research opportunities," *Computers & Security*, vol. 104, 2021.

[4] L. Gonzalez-Manzano, J. M. D. Fuentes, and A. Ribagorda, "Leveraging user-related internet of things for continuous authentication: A survey," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–38, 2019.

[5] L. Hernández-Álvarez, J. M. de Fuentes *et al.*, "Privacy-preserving sensor-based continuous authentication and user profiling: a review," *Sensors*, vol. 21, no. 1, p. 92, 2020.

[6] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, 2019.

[7] "Online anomaly detection in wireless body area networks for reliable healthcare monitoring," *IEEE journal of biomedical and health informatics*, vol. 18, no. 5, pp. 1541–1551, 2014.

[8] A. Verner and D. Butvinik, "A machine learning approach to detecting sensor data modification intrusions in wbans," in *2017 16th IEEE international conference on machine learning and applications (ICMLA)*. IEEE, 2017, pp. 161–169.

[9] M. U. H. Al Rasyid, F. Setiawan, I. U. Nadhori, A. Sudarsonc, and N. Tamami, "Anomalous data detection in wban measurements," in *2018 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC)*. IEEE, 2018, pp. 303–309.

[10] A. Shabtai, U. Kanonov, and Y. Elovici, "Intrusion detection for mobile devices using the knowledge-based, temporal abstraction method," *Journal of systems and Software*, vol. 83, no. 8, pp. 1524–1537, 2010.