

REPORT 12

An Initial Insight into Information Security on Android Smartphones with a Focus on Information Systems

[ANONYMIZED REPORT – NO IDENTIFYING INFORMATION]

Abstract

Recent social changes have turned the smartphone into a central piece of technology, with complexities linked to essential activities such as instant communication, email management, web browsing, and photo capturing. Despite the benefits, IT experts and managers face challenges in information security, especially concerning information systems. It is important to highlight that Information Systems theories emphasize the importance of security for devices such as the Android smartphone. Researchers suggest that ontologies could be a solution, defining knowledge structures to facilitate shared understanding. The development of an ontology is proposed to assist IT managers in dynamic security on the Android smartphone, focusing on information systems, utilizing a systematic literature review and the Methontology methodology. This ontology aims to standardize concepts and facilitate information sharing for risk analysis, vulnerabilities, and threats.

1. Introduction

The profound transformations in society throughout this decade have promoted a fundamental change in the role of the smartphone, elevating it from a simple device to a central piece of technology, characterized by significant complexity [Betz 2016]. This complexity is essentially linked to a wide variety of vital activities for companies and users in general, including instant communication, email management, web browsing, and photo capturing, among others [Laudon and Laudon 2004] [Da Costa et al. 2022] [Sutter et al. 2024]. However, this technological evolution does not come without its inherent concerns. As users engage in their daily routines, they inadvertently share a substantial amount of personal information with software and hardware providers. These Personally

Identifiable Information (PII), which encompass sensitive data such as residential addresses, dates of birth, photos, and videos, are frequently stored on devices, considerably increasing the risk of exposure to spyware applications and other digital security threats [Sutter et al. 2024].

According to Boscarioli et al. (2017) in the Grand Challenges of IS Research in Brazil 2016–2026 (GrandSI-BR), transparency and interoperability are still persistent challenges in the area of Information Systems (IS). For example, for Eric Trist (2009) there is still a need to understand how data are shared and used. Ludwig von Bertalanffy (2009), in turn, considers the importance of integrated and comprehensive management for different systems on the Android smartphone. Jay Forrester (2009) highlights how different protocols and data standards can affect interoperability and data security between smartphones and other IS.

In this context, the rapid growth of applications for Android Operating Systems further intensifies such risks, especially with regard to interoperability between the various information systems and the Android smartphone.

Based on the results of the SLR, it is intended, through the Methontology Methodology, to develop an ontology to guide IT specialists and managers regarding the importance of understanding the dynamic approach and thus minimize risks and failures due to lack of knowledge of attack trends and vulnerabilities on the Android smartphone [Sutter et al. 2024].

This article is organized as follows: Section 2 presents the theoretical framework; Section 3 describes the Speculative Design methodology; and Section 4 presents the final considerations.

2. Theoretical Framework

2.1. Ontology

Ontology has its origin in philosophy and, according to Almeida and Bax (2023), is the branch of Metaphysics that studies the types of things that exist in the world. The word Ontology comes from the Greek “Ontos,” meaning being, and “Logos,” meaning

word. However, its original term emerged with Aristotle, who defined it as a set of categories to structure specific models of reality.

According to Studer et al. (2024), ontology is described as an explicit formal specification of a shared conceptualization. The word “conceptualization” can be understood as an abstract model of some real-world phenomenon that identifies the relevant concepts of that phenomenon. The word “formal” highlights that the ontology must be machine-processable. In “shared,” it is understood that the ontology captures consensual knowledge which, according to Fensel (2003), should not be restricted to a few individuals, but accepted by a group of people.

2.2. Information Security

The international standard ISO/IEC 27002:2013 [ISO 2013] emphasizes that information security is achieved through the implementation of an appropriate set of controls, including policies, processes, procedures, organizational structure, and software and hardware functions. These controls need to be established, implemented, monitored, critically analyzed, and improved when necessary, to ensure that the business objectives and the organization’s information security are met.

Whitman and Mattord (2009) define information security (InfoSec) as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit this information. They also identify several critical characteristics of information that confer value to organizations. This definition is related to the preservation of Confidentiality, Integrity, and Availability of information, understood as the CIA triad [Malagutti 2016].

The CIA triad constitutes a reference point for evaluating IS security and information security audit processes. Confidentiality ensures that information will only be shared with authorized persons or entities.

3. Speculative Design

In this article, the speculative design methodology was followed according to the stages below [Auger 2013]:

Figure 1. Speculative Design.

3.1. Definition of the Research Theme

In the current reality marked by profound transformations in all spheres of society, information security managers still face many challenges in view of a wide variety of IS. This is mainly due to the popularization of the Android smartphone among employees who carry out their work routines through their most diverse applications.

3.2. Mapping the Current Scenario

To exemplify the importance of this theme, three hypothetical and fictitious scenarios were proposed:

Scenario I

Reports emerge of suspicious behavior and slow performance on Android smartphones belonging to employees of a company that provides services to a non-profit organization. A subsequent investigation reveals that these devices were compromised by a virus disguised as an entertainment application. This threat triggered a series of problems, including the leakage of confidential information and the dissemination of spam through the corporate emails of the respective employees.

Scenario II

A malicious hacker exploited a flaw in Windows remote assistance to invade the computer of a Commercial Area Manager without authorization in an organization that provides IT services to banking institutions. Upon gaining access, the intruder discovered that WhatsApp was installed on the Manager's device and logged into their account. Subsequently, they began sending inappropriate messages to company employees' contacts via WhatsApp, pretending to be the Manager. Even away from the computer, the Manager promptly noticed the inappropriate messages being sent to their contacts, receiving notifications on their Android smartphone. Faced with this situation, the Manager was confronted with the urgency of protecting their

Android device, since the hacker also used WhatsApp on the PC to install invasion programs on it. In addition, the hacker managed to block the Manager's access to the Android smartphone, further complicating the situation.

Scenario III

A hacker used an Android smartphone in a critical operation within a Federal Public Institution to access potentially sensitive information. The device in question was equipped with the Seeing AI application, developed by Microsoft, which offers advanced computer vision features for visually impaired users. During the operation, the hacker modified Seeing AI to map in detail the interior of the building, revealing corridors and restricted areas that would be difficult to access through conventional surveillance methods. Taking advantage of access obtained through the login and password of a high-ranking official, the hacker also captured images of access codes to a critical system. Discreetly, this information was transmitted to a foreign company interested in the technology of that system. After successfully completing the mission, the hacker disabled the Seeing AI application on the Android smartphone and left the site without leaving traces.

3.3. Mapping Signals and Trends

According to the IT Section website, there are five cybercrime trends to monitor in 2024:

- I. States allied with cybercriminals;
- II. Fraud epidemic fueled by data theft;
- III. Victims targeted by multiple attacks;
- IV. Persistence of phishing;
- V. Normalization of criminal behavior among young people.

Thus, these trends demonstrate the importance of information security in the use of the Android smartphone in the context of internal networks of various organizations.

3.4. Definition of the Future

For the future, it is perceived that the management of various IS faces challenges with the number of preexisting, autonomous, distributed, heterogeneous databases and ontologies generated by Artificial Intelligence (AI) [Dias et al. 2020] [Mellal and Saighi 2024]. However, for this to occur in the way IT Managers need in their organizations, it is still necessary to elicit requirements, scenarios, and follow a development methodology. Thus, managing information security on the Android smartphone through a domain ontology focused on IS for applicability in organizations is a challenge.

3.5. Mapping the Future Scenario

Thus, it is intended to investigate how to facilitate understanding of dynamic security functionalities on the Android smartphone so that specialists, IT managers, and their teams can prevent cyberattacks through this device on their respective organizations' internal networks [Da Costa et al. 2022] [Xavier et al. 2024] [Sutter et al. 2024]. Currently, there is practicality in extracting information from an ontology for use in mobile applications, websites, smartwatches, smartphones, smart appliances, virtual assistants such as Alexa (Amazon), Siri (Apple), Cortana (Microsoft), ChatGPT, among others. Such utility can execute queries as in a Database Management System for use by small and medium-sized enterprises [Dias et al. 2021].

3.6. Designing an IT Solution

In this context, the following question arises: How to facilitate understanding of Android security functionalities for specialists, IT managers, and their teams, with the objective of preventing cyberattacks through Android smartphones on their respective internal networks? A solution presented in the literature by researchers is the use of domain ontologies to represent knowledge management in dynamic security on the Android smartphone, facilitating shared understanding among specialists, IT managers, and their teams [Casola et al. 2019] [Meriah et al. 2021] [Laudon and Laudon 2004].

Researchers consider that ontologies can be used as a solution to this problem because they define knowledge structures and promote a shared understanding of a domain, task, or application [Chandrasekaran and Benjamins 1998]. Guarino (1998) defines a taxonomy in which he considers that domain ontologies describe the vocabulary of a specific knowledge domain, defining and characterizing it. The contribution to its use is the standardization of concepts, terms, and definitions, as well as ease of information sharing to make assumptions more explicit and assist in the analysis of knowledge and domain relationships.

3.6.1. SegDinAndroid Ontology

Figure 2. Taxonomy of the Android dynamic security analysis research domain.

The initial SegDinAndroid ontology was developed from an SLR through the taxonomy of the Android dynamic security analysis research domain.

Figure 3. SegDinAndroid ontology with its hierarchy of classes, subclasses, and instances using OWLViz in Protégé.

The SegDinAndroid ontology was developed with the purpose of demonstrating its applicability in industry, in issues related to information security, from the perspective of professionals and researchers, in the context of the Android smartphone.

Three competency questions were preliminarily defined for executing tests with the ontology:

CQ1: How are the concepts related to dynamic security analysis structured in the context of the Android smartphone?

Figure 4. Answer to CQ1 through the SegDinAndroid ontology in Protégé.

CQ2: What are the technologies, models, techniques, or information security tools most used on the Android smartphone?

Figure 5. Answer to CQ2 through the SegDinAndroid ontology in Protégé.

Figure 6. Answer to CQ2 through the SegDinAndroid ontology in Protégé. Continuation.

CQ3: What types of malware are most commonly found in the use of the Android smartphone?

Figure 7. Answer to CQ3 through the SegDinAndroid ontology in Protégé.

4. Final Considerations

In this work, an initial version of the SegDinAndroid ontology was presented for identifying Android smartphone information security elements and indicating their main characteristics. Thus, it is expected that those responsible for managing these Android smartphones will have access to a relevant, technical, and practical body of knowledge that reduces the possibility of error and increases specialization in this topic. Another benefit to highlight is the transfer of knowledge and skills acquired in managing the main technical characteristics of information security expressed in the ontology, which will enable faster learning for interested managers and researchers.

References (*kept verbatim from the original*)

- Auger, J. (2013). Speculative design: crafting the speculation. *Digital Creativity*, 24(1):11-35.
- Betz, C. (2016). *Managing Digital: Concepts and Practices*.
- Boscaroli, C., Araujo, R. M., and Maciel, R. S. P. (2017). Introduction. In Boscaroli, C., Araujo, R. M., and Maciel, R. S. P., editors, *I GrandDSI-BR - Grand Research Challenges in Information Systems in Brazil 2016-2026*, chapter 1, pp. 7-11. SBC.
- Casola, V., Catelli, R., and De Benedictis, A. (2019). A first step towards an ISO-based information security domain ontology. In *WETICE 2019*, pp. 334-339.
- Da Costa, A. M., De Sá, A. O., and Machado, R. C. S. (2022). Data acquisition and extraction on mobile devices - a review. In *MetroInd4.0IoT 2022*, pp. 294-299.
- Dias, R. M. et al. (2020). Oportunidades de KIPO para gestão em sistemas de informação federados. In *ONTOBRAS 2020*, pp. 227-234.

- Dias, R. M., Zacarias, R. O., and dos Santos, R. P. (2021). Ontologia para o gerenciamento de segurança da informação em sistemas-de-sistemas. In *ONTOBRAS 2021*, pp. 273-278.
- Fensel, D. (2003). *Ontologies: A Silver Bullet for Knowledge Management and Electronic Commerce*. Springer.
- Guarino, N., Oberle, D., and Staab, S. (2009). What is an ontology? Springer.
- ISO (2013). ISO/IEC 27002:2013 – Information technology – Security techniques.
- Laudon, K. C. and Laudon, J. P. (2004). *Management Information Systems*. Pearson.
- Malagutti, M. A. O. (2016). O papel da dissuasão no tocante a ofensas cibernéticas.
- Mellal, N. and Saighi, A. (2024). Ontology population using CNN model.
- Meriah, I., Rabai, L. B. A., and Khedri, R. (2021). Towards an automatic approach to ontology design for information security.
- Ramage, M. and Shipp, K. (2009). *System Thinkers*.
- Sutter, T. et al. (2024). Dynamic security analysis on Android. *IEEE Access*, 12.
- Whitman, M. E. and Mattord, H. J. (2009). *Principles of Information Security*.
- Xavier, C. et al. (2024). Understanding the negative effects of social networking mobile app notifications. *HICSS 2024*.