Advanced Persistent Threats Detection for Mobile Devices

Subjects: Others

Contributor: Amjed Ahmed Al-Kadhimi, Manmeet Mahinderjit Singh, Mohd Nor Akmal Khalid

Advanced persistent threat (APT) refers to a specific form of targeted attack used by a well-organized and skilled adversary to remain undetected while systematically and continuously exfiltrating sensitive data. Various APT attack vectors exist, including social engineering techniques such as spear phishing, watering holes, SQL injection, and application repackaging. Various sensors and services are essential for a smartphone to assist in user behavior that involves sensitive information. Resultantly, smartphones have become the main target of APT attacks.

Keywords: cyber cognitive situational awareness (CCSA) ; Joint Directors of Laboratories (JDL) ; MITRE framework

1. Introduction

Advanced persistent threat (APT), which differs significantly from traditional network attacks, has emerged recently. Cyber attacks, or APTs, known for their ability to steal intellectual property, disrupt critical infrastructure, or cause millions of dollars in damages, are a growing concern [1]. In contrast, traditional network attacks have been employed as cyber attacks for many years to compromise computer network security and steal sensitive information. These attacks exploit network systems and protocol vulnerabilities to gain unauthorized access to networks, steal confidential data, or disrupt normal network operations. The common types of traditional network attacks are denial-of-service (DoS), man-in-the-middle (MITM), sniffing, phishing, and structured query language (SQL) injection [2][3].

According to Powerful Growth, the global APT protection market is expected to reach USD 20,290.7 million by 2027, expanding at a 20.9% compound annual growth rate (CAGR). The global APT defense market is estimated to rise rapidly throughout the forecast period, given the exponential growth of cyber attacks globally, including malware and APTs [4]. Thus, APT is an important threat to be mitigated in mobile and computer systems.

Deliberate, repetitive, and covert cyber attacks that target specific companies rather than random individuals or regular system users are a defining characteristic of APTs [5]. Such complex exploits may not seek immediate gain, instead attempting to acquire covert access over a lengthy period to extract confidential and critical data necessary to achieve the attackers' aims [6]. The incursion of APTs can lead to numerous detrimental organizational consequences, including intellectual property theft, data breaches, critical infrastructure disruption, and potentially complete takeovers of the affected site [7]. Furthermore, governments have regularly supported APT attacks and utilized them as cyber warfare by exploiting vulnerabilities [8]. Smartphone mobile security challenges have emerged due to its pervasive adoption and rapid mobile hardware and software technology advancements. An ongoing concern regarding smartphones is their susceptibility to being the primary target for APT attacks. Most mobile APTs depend on social engineering assaults through sensors, including spear phishing, application repackaging, watering holes, and SQL injection.

Several vulnerabilities lead to APTs, such as heterogeneous mobile network protocols, physical mobile devices, sensors, applications, and services. For instance, smartphones are vulnerable to APT attacks due to insecure communication protocols in mobile networks such as Wi-Fi and Bluetooth. These unencrypted communication protocols make it easier for attackers to intercept and eavesdrop on the communication between devices. In addition, many mobile devices lack built-in security measures such as firewalls, encryption, and intrusion detection systems, leaving them vulnerable to Wi-Fi and Bluetooth attacks and other types of APT attack. Additionally, attackers can use social engineering tactics, such as phishing, to trick users into revealing sensitive information or downloading malicious software [9][10].

Smartphone sensors are essential for gathering, transmitting, and analyzing information in a smartphone application. A smartphone has several sensors and services critical to the user's everyday activities and potentially includes sensitive data. The vulnerabilities in mobile sensors include limited capacity, low-cost sensors, and their nature of always being "ON" [11]. These conditions may lead to increased attack surface as mobile devices' increased connectivity and availability

increase their susceptibility to attacks. Sensors can gather sensitive information, such as location and biometric data, which can be used in further attacks. Furthermore, mobile devices can easily spread malware to other devices in the network, as they are often used to access sensitive information and connect to other networks. Thus, financial and privacy loss and reputational damage are the main impacts that can harm the systems of individuals and organizations. Thus, smartphones have become the principal target of attackers undertaking APT assaults [12] including AndroRat [13], FinSpy [14], and Asacub [15].

2. Overview of Advanced Persistent Threats (APTs)

The targeted attack strategy used by a qualified and skilled adversary to maintain undetected access to critical information exfiltration for a lengthy period is known as an APT. There are various forms of APT assaults, including social engineering techniques such as spear phishing, SQL injection, malware, and watering hole attacks [3]. The term APT offers shorthand for what it is. Traditional assaults lack one or more of these traits.

“Advanced” means the attacks are planned by a team of individuals with many resources, expertise, and funding. The assaults must be simple to be successful. It is common for an attacker to utilize phishing and readily available malware development tools [16][17]. Nevertheless, when necessary, they utilize software, such as zero-day exploits, to target particular vulnerabilities and launch several attacks to gain access. “Persistent” attackers are desperate to access the victim’s systems, applications, and resources. Resultantly, the intruder has full access to the system, including backdoors. If one connection is compromised, others may be opened and used to continue collecting sensitive information. Distinguishing between a threat and an opportunity is also important. Since they are more than software that runs independently, APTs pose a problem [12][18][19].

There are two types of APTs, namely killing and leeching. Leeching occurs when an attacker passively gathers information from a target system without compromising it. An attacker may use a network sniffer to steal sensitive data. Leeching is a sneaky attack that gives attackers information they can use to launch more serious attacks. On the other hand, killing involves actively compromising and disrupting a target system.

Malware can compromise a system, delete important files, or steal sensitive data. Killing is a more aggressive attack that can damage a target system and is easier to detect than leeching [20]. The primary difference between leeching and killing is the attacker’s intent. Leeching is typically motivated by the desire to gain access to information or resources, while killing is motivated by the desire to disrupt or destroy systems and networks. Thus, the tactics used to defend against leeching and killing are different. Preventing unauthorized access is the focus of defending against leeching, while protecting against disruptions is the focus of defending against killing [20].

3. Overview of APT Attacks on Mobile Sensors

Mobile sensors are classified into three types [21]: inertial, positioning, and ambient. **Figure 1** illustrates the classification of smartphone sensors. Inertial sensors on a smartphone are required to control the orientation of the user interface and detect events. Accelerometer and gyroscope sensors can be used to detect events such as device management, tilting, and dropping. Positioning sensors, such as global positioning systems (GPSs) and Wi-Fi, are essential for specifying the location of devices and transmitting information. Additionally, ambient sensors, such as microphones and cameras, must detect and analyze the user’s environment, share documents, and interact with other Internet of Things (IoT) devices that utilize the same technology.

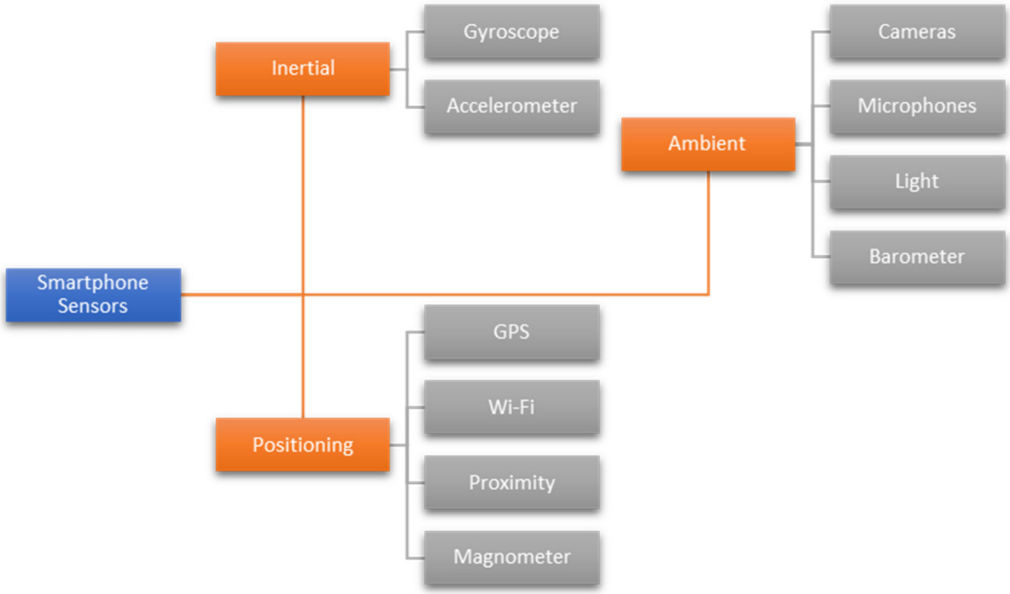

Figure 1. Smartphone Sensor Classifications [12][14].

SMS, MMS, and other telecommunication services such as calls, phone logs, and other services, including the calendar, create a constant data stream. As a result, sensor access is required for various services. Once an attacker obtains or reads these data, the user's protection may be threatened. These features depend on the user's attention [22], and the perpetrator has the ability to execute a highly active APT attack on the mobile to exploit this dependency [12].

Regarding to Zulkifli et al. [22], social engineering can facilitate file transmission and sharing. Among such sensors are Bluetooth connection and the Android beam. The malware also compromises APT target location, environmental sensors, and sensitive data resources. Thus, an APT assault on a mobile phone is a plausible scenario. The Baumgartner et al. [23] assault used an attachment in a spear-phishing email to target a Tibetan activist.

The GPS and Wi-Fi sensors can be compromised due to a flaw. Androrat [13] used application repackaging to target cellphones' GPS, Wi-Fi, camera, and microphone sensors in an assault that affected Turkey and the United States (US). Finally, an assault targeted Bahraini human rights advocates [14] using spear-phishing emails that exploit GPS, Wi-Fi, Bluetooth, and microphone sensors [12].

Vulnerabilities of Smartphone Sensors

Due to the vulnerabilities, an attacker can use smartphone sensors and initiate an APT attack. Vulnerability analysis of sensors discovers and prioritizes these flaws as part of developing security policies and procedures. Several vulnerability spots exist in smartphone sensors, resulting in several cyber attacks launched to take advantage of the vulnerabilities in smartphone sensors. For instance, MIMT and reply attacks can be carried out using communication channel gaps in GPS sensors. The Bluetooth sensor has various vulnerabilities, including LMP/LLP.

Exploiting this vulnerability may allow for executing variant attacks such as hijacking, blue sniffing, or sniffing. Additionally, near-field communication (NFC) sensors are vulnerable to attacks such as eavesdropping and spoofing due to a lack of communication security. Lastly, the vulnerabilities of the camera and microphone sensor have resulted in various security risks, including side-channel attacks and eavesdropping. A strong understanding of the sensors and their vulnerabilities helps designers and users of security systems avoid being targeted.

References

1. Berrada, G.; Cheney, J.; Benabderrahmane, S.; Maxwell, W.; Mookherjee, H.; Theriault, A.; Wright, R. A baseline for unsupervised advanced persistent threat detection in system-level provenance. Future Gener. Comput. Syst. 2020, 108, 401–413.
2. Gervasi, O.; Murgante, B.; Misra, S.; Gavrilova, M.L.; Rocha, A.M.A.C.; Torre, C.; Taniar, D.; Apduhan, B.O. Advanced Persistent Threat Mitigation Using Multi Level Security—Access Control Framework. Lect. Notes Comput. Sci. 2015, 9158, 90–105.

3. Bann, L.L.; Singh, M.M.; Samsudin, A. Trusted Security Policies for Tackling Advanced Persistent Threat via Spear Phishing in BYOD Environment. Procedia Comput. Sci. 2015, 72, 129–136.
4. Powerful Growth: Global Advanced Persistent Threat (APT) Protection Market. Available online: https://www.globenewswire.com/news-release/2021/11/24/2340616/0/en/Powerful-Growth-Global-Advanced-Persistent-Threat-APT-Protection-Market-to-knock-20-290-7-Million-at-a-CAGR-of-20-9-from-2020-to-2027-Research-Dive.html (accessed on 25 December 2022).
5. Ahmad, A.; Webb, J.; Desouza, K.C.; Boorman, J. Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. Comput. Secur. 2019, 86, 402–418.
6. Quintero-Bonilla, S.; del Rey, A.M. A new proposal on the advanced persistent threat: A survey. Appl. Sci. 2020, 10, 3874.
7. Advanced Persistent Threat (APT). Available online: https://www.wallarm.com/what/advanced-persistent-threat-apt (accessed on 10 March 2023).
8. Advanced Persistent Threat (APT). Available online: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/#:~:text=Theconsequencesofsuchintrusions,infrastructures(e.g.%2Cdatabasedeletion (accessed on 20 September 2022).
9. Kibona, L.; Ganame, H. Wireless Network Security: Challenges, Threats and Solutions. A Critical Review. Int. J. Acad. Multidiscip. Res. 2018, 2, 19–27.
10. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. J. Proc. IEEE 2016, 104, 1727–1765.
11. Al-Kadhimi, A.A.; Singh, M.M.; Jabar, T. Fingerprint for Mobile-Sensor APT Detection Framework (FORMAP) Based on Tactics Techniques and Procedures (TTP) and MITRE. Lect. Notes Comput. Eng. 2022, 835, 515–533.
12. Zulkefli, Z.; Mahinderjit Singh, M. Sentient-based Access Control model: A mitigation technique for Advanced Persistent Threats in Smartphones. J. Inf. Secur. Appl. 2020, 51, 102431.
13. Remote Access Tool Takes Aim with Android APK Binder. Available online: https://www.symantec.com/connect/blogs/remote-access-tool-takes-aim-android-apk-binder (accessed on 12 February 2023).
14. The SmartPhone Who Loved Me. Available online: https://citizenlab.ca/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/ (accessed on 15 November 2022).
15. The Asacub Trojan from Spyware to Banking Malware. Available online: https://securelist.com/the-asacub-trojan-from-spyware-to-banking-malware/73211/ (accessed on 1 January 2023).
16. Privacy Assessing Method. Available online: https://www.fireeye.com/blog/threat-research/2013/08/pivy-assessing-damage-and-extracting-intel.html (accessed on 1 January 2023).
17. Spear Phishing Attack. Available online: https://www.fireeye.com/current-threats/reports-by-industry/rpt-spear-phishing-attacks.html (accessed on 12 February 2023).
18. Vukalović, J.; Delija, D. Advanced Persistent Threats—Detection and defense. In Proceedings of the 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 25–29 May 2015; pp. 1324–1330.
19. Jabar, T.; Singh, M.M.; Al-Kadhimi, A.A. Mobile Advanced Persistent Threat Detection Using Device Behavior (SHOVEL) Framework. In Proceedings of the Eighth International Conference on Computational Science and Technology, Labuan, Malaysia, 28–29 August 2021; Springer: Singapore, 2022; pp. 495–513.
20. Rass, S.; König, S.; Panaousis, E. Cut-The-Rope: A Game of Stealthy Intrusion. Lect. Notes Comput. Sci. 2019, 11836, 404–416.
21. Hoseini-Tabatabaei, S.A.; Gluhak, A.; Tafazolli, R. A survey on smartphone-based systems for opportunistic user context recognition. ACM Comput. Surv. 2013, 45, 744.
22. Zulkefli, Z.; Singh, M.M.; Mohd Shariff, A.R.; Samsudin, A. Typosquat Cyber Crime Attack Detection via Smartphone. Procedia Comput. Sci. 2017, 124, 6–8.
23. Android Trojan Found in Targeted Attack. Available online: https://securelist.com/androidtrojan-%0Afound-in-targeted-attack-58/35552/%0A (accessed on 15 April 2023).