A Revealed Architecture of camera-based Attacks for Smartphones

Arnold Mashud Abukari
Tamale Technical University
Ghana

Mohammed Amini
FANAP Research Center
IRAN

Francis Martinson
North Dakota State University
USA

ABSTRACT

Smartphones have taken a center stage in the daily activities of individuals and organizations across the world. Despite the positive impacts smartphones come with, the use of smartphones also has serious cyber security implications on the users. One of the most common attacks on smartphones is the camera-based attack. This research paper presents a revealed architectural algorithm highlighting how the camera-based attack are carried out and which functions of the smartphones are being used to aid the attack process. This research work also gives an overview of the global smartphone use and it's reported cyber attack. The generalized smartphone architecture and it's vulnerabilities are also presented in this research paper.

Keywords

Smartphone, cyber attack, camera, vulnerabilities, Architecture, cybesecurity

1. INTRODUCTION

The world has been flooded with Smartphones and other mobile devices in the wake of this digital era. The usage of smartphones have become a part of the human race. Individuals and organisations across the world have integrated the usage of smartphones in their daily activities. Since 2008, the smartphone industry has seen significant growth in usage, the number of models, the number of vendors as well as significant growth in the market size. According to Laricchia (2023), about 68 percent of the global population were smartphone users in the year 2022 with the number of smartphone subscription far exceeding the number of smartphone users. By the end of the year 2022, the number of smartphone subscritions shot up to about 6.5 billion subscriptions and this expected to increase to about 8 billion by the year 2028 (Laricchia, 2023).

Despite the significant increase in the number of smartphones globally, cyber attacks and security threats on smartphones are very alarming. In 2020, according to Ceci (2023), the number of reported cyber attacks on smartphones stood at around 6.5 million attacks.

As reported by Storm (2014), the increase in the cyber attacks and cyber security concerns touches and exploit vulnerabilities in the design, manufacturing and programming of some of the applications that ensure the functioning of these smartphones. Smartphone cameras, speakers and microphones according to Storm (2014) are secretly used and exploited to attack smartphone users. Researchers have identified and demonstrated new security threats in the usage of the front-camera and that of the rear-cameras of smartphones that can be used to capture keystrokes and fingerprints (Storm, 2014). Researchers over the years have modeled attacks on some identified vulnerabilities in smartphones including the front and rear cameras of smartphones. Fiebig, Krissler, & Hänsch (2013) has demonstrated that attackers can abuse the cameras in recent smartphones to capture very valuable data or information from unsuspecting victims. The researchers argued that a front-facing camera can be used to capture keystrokes of users by observing facial reflections (Fiebig, Krissler, & Hänsch, 2013). According to the research, Fiebig, Krissler, & Hänsch (2013) further argued that attackers can exploit the vulnerabilities in smartphone cameras to capture and forge the fingerprints of innocent victims. These security threats in smartphones have serious implications on individuals and organisations as well as governments across the world. Attackers may be able to perform a vast range of malicious activities including biometric systems authentication bypass, falsely implicating people and financial activities.

2. SMARTPHONE ARCHITECTURE AND VULNERABILITIES

There are several components that makes up the Smartphone architecture. Some of the components are generic components and some are peripherals. The Architecture for smartphone has one of the key components called System-on-Chip (SoC) which integrates an application processor, Graphical Processing Unit (GPU), a Crypto-Processor and cache memories. The generalized architecture for smartphones according to Khelif, Lorandel and Romain (2020) can be subjected to various forms of attacks. These attacks are classified into Hardware, Software and Protocol attacks (Khelif, Lorandel and Romain,2020). The software attacks includes the use of malware to steal data from a smartphone or take control by exploiting the vulnerabilities in the operating systems or application software also known as third-party software. The protocol attacks are attacks on wirelesss communication protocols or wired protocols and these includes attacks on Wi-Fi, Bluetooth and USB (Khelif, Lorandel and Romain,2020). The attacks on hardware have also grown exponentially. As reported by Kheli, Lorandel and Romain (2020), physical tempering attacks, fault injection attacks, sidechannel attacks, eavesdropping attacks and instruction skipping attacks are all possible ways attacking smartphones (Elibol, Sarac and Erer,2012). The hardware attacks on smartphones is classified as invasive and non-invasive (Tehranipoor and Wang, 2011).

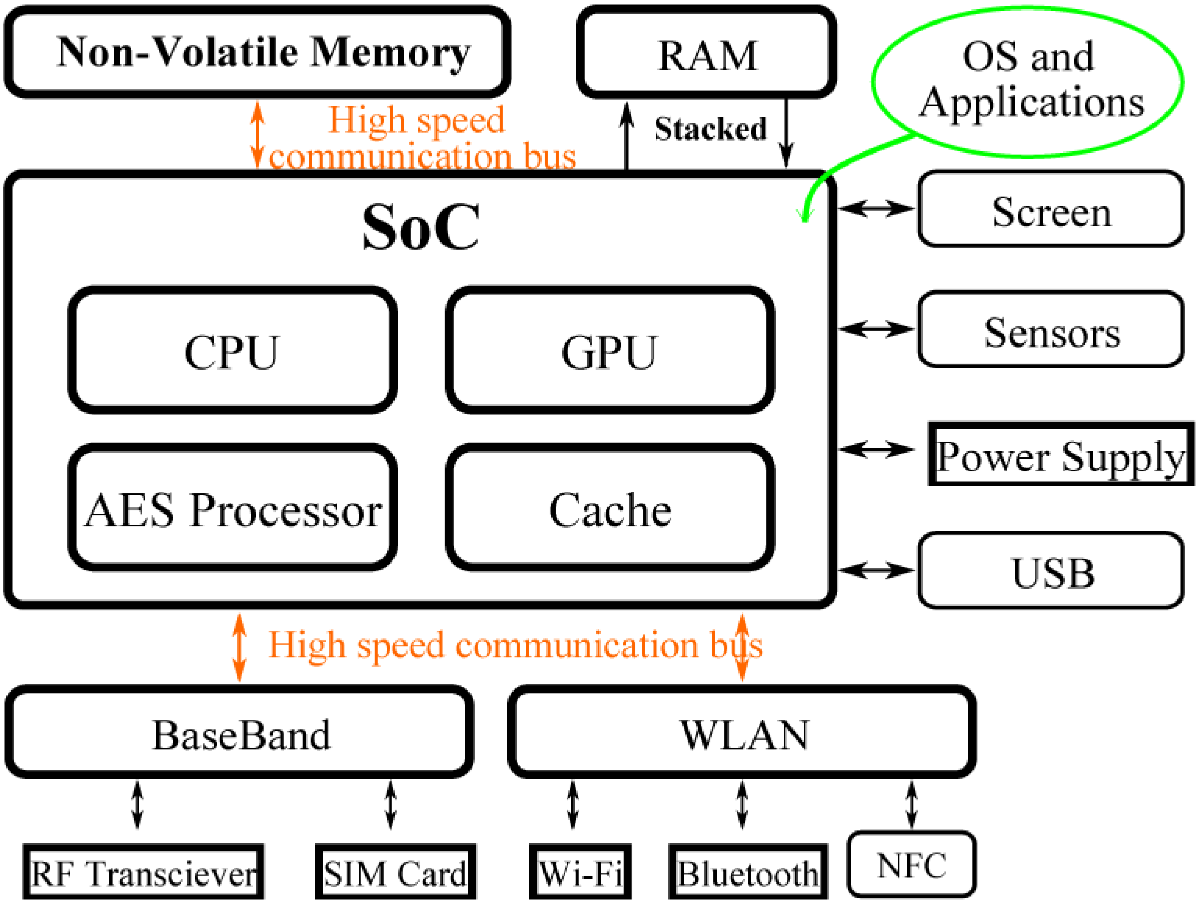

Figure 1: Generalised Smartphone Architecture (Khelif, Lorandel, Romain,2020)

3. SMARTPHONE APPLICATION PROCESSOR

Smartphone Application Processor is a system that has a programmed chip which helps the operating system of the smartphone to operate at its optimal performance level. The Application processor is responsible for executing the application software and instructions from the Operating System (OS) of the smartphone (Bailoo, 2019).

A report by Research and Market (2022), indicates that the global smartphone application processor market was valued at US$15.95 billion as at 2021 and expected to grow significantly to US$29.14 billion by 2027.

Under Market Segment analysis of the report by Research and Market (2022) reveals that Camera holds the highest share of about 35% in the market. This suggest usage of camera in smartphone has taken center stage in the overall use of smartphones and its purchase. According to the report, the growing interest in demand for advanced features in camera in smartphones is as a result of consumers being tech-savvy, enhanced camera functionalities, high end graphics and long battery life among others.

The application processor of smartphone is one of the key targets of attackers or cyber criminals largely due to the growing demand of camera usage in smartphones. This has led to increasing camera-based attacks.

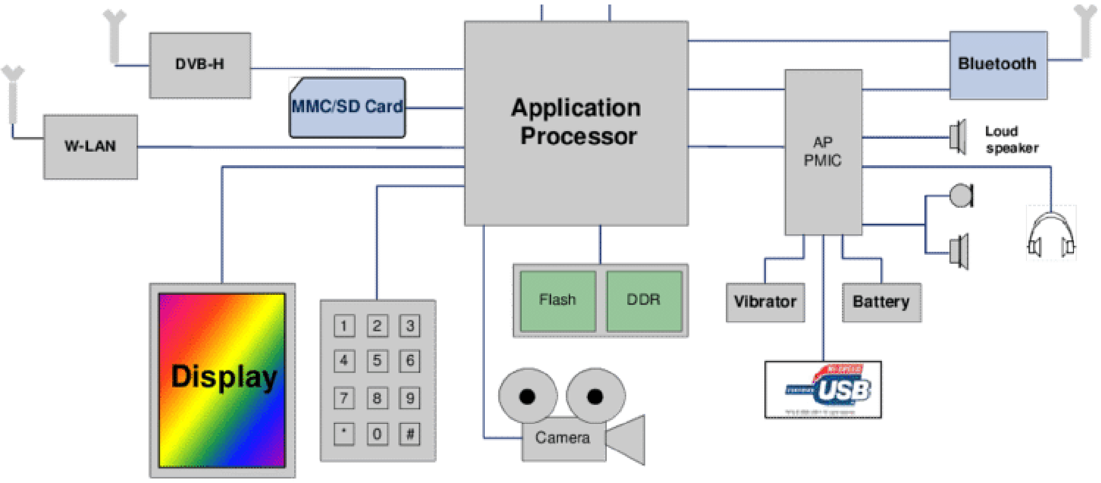

Figure 2: Smartphone Application Processor

4. CAMERA ATTACK ARCHITECTURE

The basic Camera attack architecture contains six parts or processes that are executed sequentially to capture information through the camera to the attacker. These six steps or parts in the camera attack process are modeled to ensure a successful attack without the user suspecting the attack.

The first step to launch a camera-based attack on a smartphone is first of all Detect the Resource utilization of the phone. The CPU, battery status and memory usage are determined before the attack is launched through the camera. Once the application used for the camera-based attack detects very low resource utilization of the smartphone, then it will shutdown any sound or vibration of the smartphone. This is to conduct an attack that will not make a sound or vibrate to raise suspicions during the attack. The malicious software will reduce the volume or deactivated the volume and vibration. In order not let a user become suspicious, the malware will further hide preview of any ongoing activities embarked by the malware. The camera-based attack malware will now store videos and pictures in a hidden folder without the notice of the user, Once the camera-based malware successfully stores the videos and pictures, it will then restore or recover the volume and vibration to their initial state and then send out the videos and pictures through email to the attacker. All these activities are done without the user of the smartphone noticing such attack.

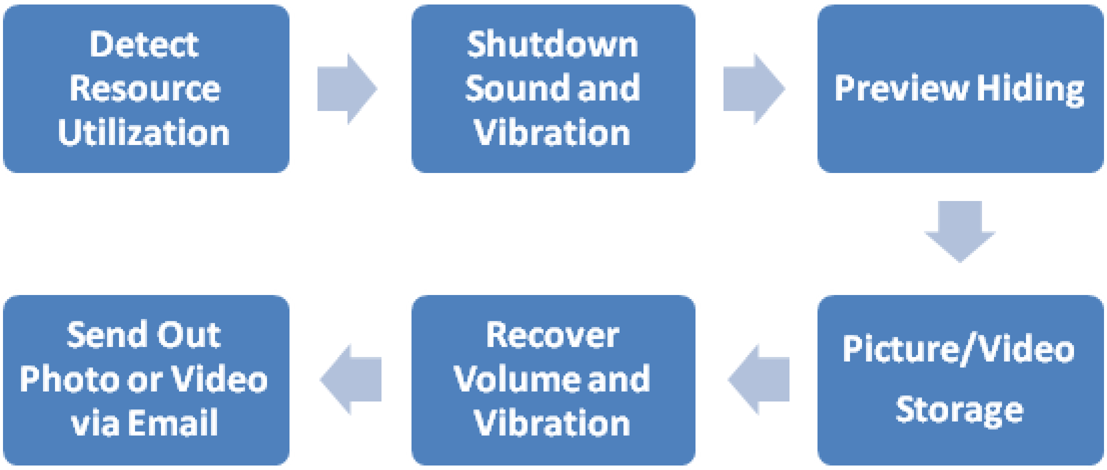
Detect Resource Utilization
Shutdown Sound and Vibration
Preview Hiding
Picture/Video Storage
Recover Volume and Vibration
Send Out Photo or Video via Email

Figure 3: Camera-based attacks architecture (Wu, Du, Wang, Fu, Mbouna, & Kong, 2014).

5. A REVEALED ARCHITECTURE OF THE CAMERA-BASED ATTACK

A typical camera-based attack on smartphones capitalizes on some functions and folders in the smartphones. The camera-based applications developed by attackers utilizes these functions and instruct the functions to act based on the instructions of the malware. The revealed architecture presented in this paper identifies the key functions used in camera-based attack and how they relate in the attack process.

In the attack process of a typical camera-based attack, the spyware or malware first gain access to the *ActivityManager* module of the smartphone and send a request to the *getMemoryInfo()* function of the smartphone. This activity by the malware is to assess the utilization of the CPU of the smartphone. If the CPU is determined to be in used or busy, the attack process is terminated in order not to let the user of the smartphone suspicious. The attack process however continues when the CPU is not in use and a request is sent to *BroadcastReceiver* with *ACTION_BATTERY_CHANGE* to determine the battery level of the smartphone. If the battery level of the smartphone is determined to be adequate, the *AudioManager.STREAM_*SYSTEM is set to 0 and set the *FLAG_REMOVE_AND_VIBRATE* function to flag. This activity by the malware is to remove the sound and vibration status on the smartphone in order not to let the smartphone produce any sound or vibrate during the attack process. The current sound level and vibration status of the smartphone is logged with the purpose to restore them back without the user suspecting anything regarding the attack. Upon a successful logging of the volume and vibration status, the *SurfaceView* is inflated into *View* using a function in smartphones called *LayoutInflater.Inflate()* which eventually changes the WindowManager.LayoutParams. The attacker changes the WindowManager.LayoutParams to work with the new parameters the malware have set without raising any alarm. The malware then set *TYPE_SYSTEM_OVERLAY* and *FLAG_NOT_*FOCUSABLE parameters to reduce the images and videos to be taken to 1 pixel. The *SurfaceHolder* is initialized and either the front camera or back camera is selected to start recording. After a successful recording, the malware restore the original audio and vibration back to the level that is known by the smartphone user. The malware then transmit the collected video and images data and send to the attacker using the *javax.mail()* function as attachment.

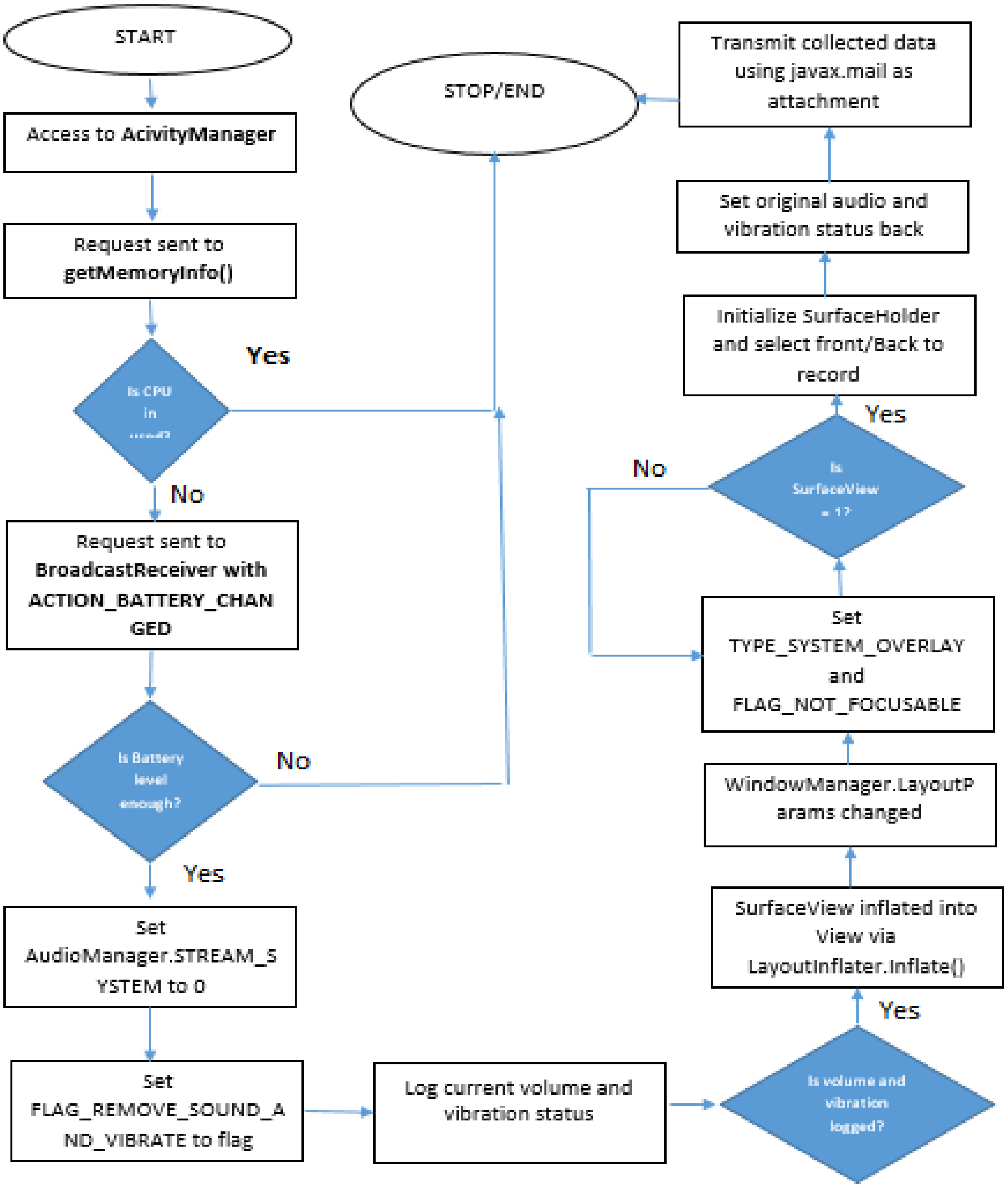
START
Access to AcivityManager
Request sent to getMemoryInfo()
Is CPU in used?
Yes
No
Request sent to BroadcastReceiver with ACTION_BATTERY_CHANGED
Is Battery level enough?
No
Yes
Set AudioManager.STREAM_SYSTEM to 0
Set FLAG_REMOVE_SOUND_AND_VIBRATE to flag
Log current volume and vibration status
Is volume and vibration logged?
Yes
SurfaceView inflated into View via LayoutInflater.Inflate()
WindowManager.LayoutParams changed
Set TYPE_SYSTEM_OVERLAY and FLAG_NOT_FOCUSABLE
Is SurfaceView = 1?
No
Yes
Initialize SurfaceHolder and select front/Back to record
Set original audio and vibration status back
Transmit collected data using javax.mail as attachment
STOP/END

Figure 4: A revealed Architecture

6. CONCLUSION

In this research paper, we study the vulnerabilities in smartphones as well as concentrated on camera-based attacks. The research identified a revealed architecture that is followed and use to develop applications used for camera-based attacks. The functions that are exploited by known camera-based attacks are presented and an algorithm developed and presented in this research paper. To enhance security in smartphones especially the camera-based attacks, a research on defense scheme is recommended.

7. REFERENCES

[1] Laricchia, F. (2023, June 6). Smartphone Statistics: Adoption, Usage, and Market Share. Retrieved from

https://www.statista.com/topics/840/smartphones/#topic Overview

[2] Ceci, L. (2023). Monthly cyber attacks on global mobile users worldwide 2020-2022. Retrieved from https://www.statista.com/statistics/1305965/mobile-users-cyber-attacks/

[3] [3] Storm, D. (2014). New attacks secretly use smartphone cameras, speakers and microphones. Retrieved from https://www.computerworld.com/article/2598704/new-attacks-secretly-use-smartphone-cameras--speakers-and-microphones.html

[4] Fiebig, T., Krissler, J., & Hänsch, R. (2013). Security Impact of High Resolution Smartphone Cameras. Retrieved from https://www.usenix.org/system/files/conference/woot14/woot14-fiebig.pdf

[5] Khelif MA, Lorandel J, Romain O (2020) Hardware Man-in-the-Middle Attacks on Smartphones. Forensic Sci Today 6(1): 012-015. DOI: 10.17352/fst.000016

[6] Elibol F, Sarac U, Erer I (2012) Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system. In 2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO) 1767-1771. Link: https://bit.ly/3cRRCwl

[7] Tehranipoor M, Wang C (2011) Introduction to hardware security and trust. Springer Science & Business Media. Link: https://bit.ly/3bCBlex

[8] Bailoo,A.S (2019). A Quick Introduction to Smartphone Architecture. Retrieved from https://evelta.com/blog/a-quick-introduction-to-smartphone-architecture/

[9] Research and Market. (2022). Global Smartphone Application Processor (AP) Market: Analysis By Operating System (Android, iOS, and Others), By Application (Camera, Gaming, Photo and Video Editing, and Others), By Region Size and Trends with Impact of COVID-19 and Forecast up to 2027. Retrieved from https://www.researchandmarkets.com/report/mobile-application-processor?utm_source=BW&utm_medium=PressRelease&utm_code=97h2th&utm_campaign=1776532+-+Insights+on+the+Smartphone+Application+Processor+(AP)+Global+Market+to+2027+-+Players+Include+MediaTek%2c+Apple%2c+Samsung+Electronics%2c+Huawei+Technologies+and+Lenovo+Group&utm_exec=jamu273prd.

[10] Wu, L., Du, X., Wang, L., Fu, X., Mbouna, R. O., & Kong, S. G. (2014). Analyzing mobile phone vulnerabilities caused by camera. In 2014 IEEE Global Communications Conference (pp. 4126-4130). Austin, TX, USA. doi: 10.1109/GLOCOM.2014.7037454.