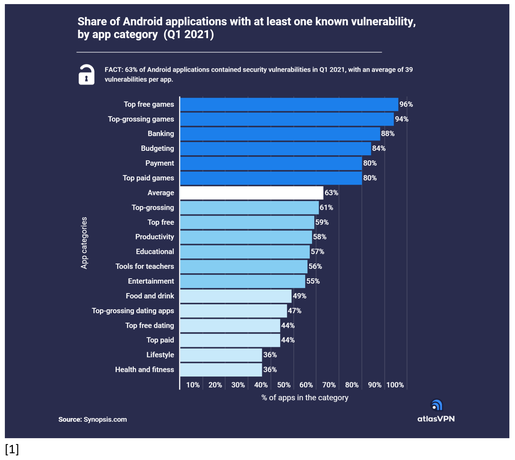
Reverse Engineering of Medical Devices for Innovation and Advancement in Healthcare

David Baldwin, Michael Nowatkowski, Jeffrey Morris, Scott Jordan

Introduction

- Medical technology is rapidly evolving and introducing new functionality and methodologies that suggest a higher risk for common vulnerability exposures(CVE)
- Introduction of functionalities like Wi-Fi, Bluetooth, and internet connectivity require devices to be rigorously evaluated for vulnerabilities
- Subsequently like many other fields cell-phone interconnectivity suggests a significantly higher level of risk to critical infrastructure and data security

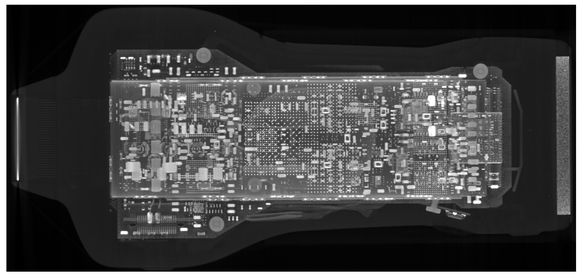


[1]

Methods

The methodology utilized for this study combined analyzing devices communication behavior combined with both thorough software and hardware reverse engineering to understand risks posed through encryption and communication practices, functionality, and programming practices

Highlighting risks, vulnerabilities, and bad practices through reverse engineering and adversary emulation



CT scan of medical device to analyze for subterfuge or other hardware anomalies

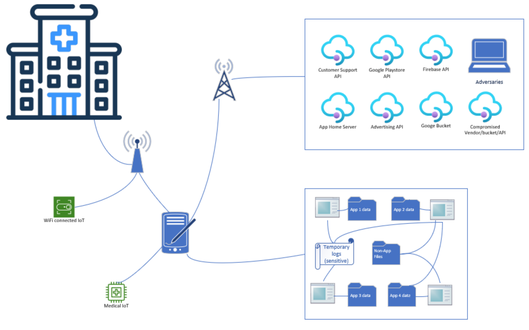
```
public void setGpsInfo(Location location) {
    if (location == null) {
        return;
    }
    setAttribute(TAG_GPS_PROCESSING_METHOD, location.getProvider());
    setLatLong(location.getLatitude(), location.getLongitude());
```

Source code reverse engineered through JADX

Geolocations data extracted and mapped based on server ping backs within an application

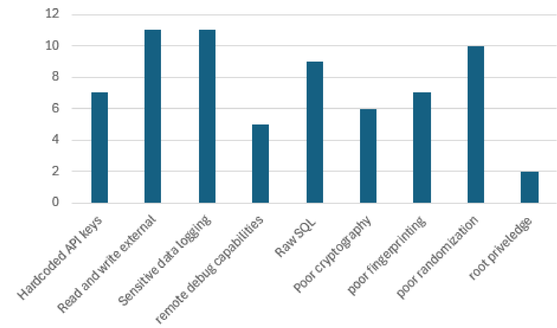
SDK package name	*Ver*	*Vulnerability*	*Vulnerability level*	*Vulnerabilities Number*
Com.amap.api.3dmap	5.0.0	URL hard-coding risk	Low	13
Com.amap.api.3dmap	5.0.0	Dynamic registration of Receiver risk	High	2
Com.tencent.tbs	43646	Risk of using weak SHA-1 algorithm	High	1
Com.tencent.tbs	43646	IP address exposure risk	Medium	3
Com.google.gson	2.8.3	Risk of log data leakage	Low	2
Com.umeng.commonsdk	9.1.0	Database Injection Vulnerability	High	25

Table highlighting risks associated with some Software Developer kits(SDKs)[2]



Results

- we identified multiple attack vectors that can be exploited to geolocate wireless devices. Our analysis of hazardous developer trends uncovering various risks that allowed researchers the ability to reverse engineer several API keys, authentication passwords, other sensitive secrets, and highlighted significant development flaws.



References

1. Kingsley-Hughes, A. The Android Apps on Your Phone Each Have 39 Security Vulnerabilities on Average. ZDNet, July 20, 2021. Available online: https://www.zdnet.com/article/the-android-apps-on-your-phone-each-have-39-security-vulnerabilities-on-average/
2. Gao, S.; Xiao, Y.; He, Y.; Wen, J. Mobile Application SDK Version Detection and Security Alert Based on Multi-partition LSH. Presented at the 3rd Asia Conference on Computers and Communications, 2022.

Acknowledgement

This work was supported by the Laboratory Directed Research and Development (LDRD) program within the Savannah River National Laboratory (SRNL).

Document Number

SRNL-STI-2025-00634