Guardian Security Assessment

Degree programme: BSc in Computer Science
Specialisation: IT Security
Thesis advisor: Prof. Dr. Benjamin Fehrensen
Expert: Dr. phil. nat. Igor Metz (Glue Software)
Industrial partner: RUAG, Bern

Mobile devices are integral to modern business environments, making them prime targets for cyber-attacks. This thesis introduces a transparent and repeatable framework for evaluating mobile security, focusing on network communication. Using real-world scenarios and traffic analysis, it establishes a baseline for future assessments and benchmarks of solutions like RUAG's GUARDIAN to support continued improvement in mobile cybersecurity.

Introduction

Mobile devices are vital in personal and professional contexts, often containing sensitive business data. While companies may issue dedicated work devices to isolate corporate information, these often lack strong security, leaving them vulnerable to threats like malware, unauthorized access, and data leaks. To address this, RUAG developed GUARDIAN, a secure mobile platform with a custom OS and secure apps for core business functions like email, messaging, and document handling. GUARDIAN ensures data protection and compliance within a tightly controlled environment.

Goal

This thesis aims to create a transparent, repeatable baseline for evaluating mobile security, allowing for a rigorous comparison of secure mobile solutions like GUARDIAN against three mainstream Android devices:
(a) Pixel running GrapheneOS (b) Stock Pixel (c) Samsung Galaxy with Knox management
The evaluation framework includes:

1. – Automated, repeatable use cases simulating diverse real-world scenarios
2. – Network traffic capture setup to reliably log all device communications
3. – Analysis environment to systematically examine and interpret the data

Use Case Execution

Four scripted scenarios were run on each device using ADB with Python to ensure consistent testing.

- No Use: Device left idle for one hour to observe background activity.
- Normal Use: Popular apps installed and trusted websites visited (15 min).
- Risky Use: Malware without permissions and unsafe browsing (15 min).
- Malicious Use: Full-permission malware and access to harmful sites (15 min)

These scenarios covered a range of real-world behaviors from benign to hostile.

Traffic Capture Setup

All traffic was routed through a secure Linux-based environment:

- VPN (WireGuard): Provided Always-On VPN with static IPs per device.
- Transparent Proxy (PolarProxy): Decrypted HTTPS traffic via TLS interception.
- Packet capture and analysis tool (Arkime): Captured and indexed all network activity for session-level analysis.

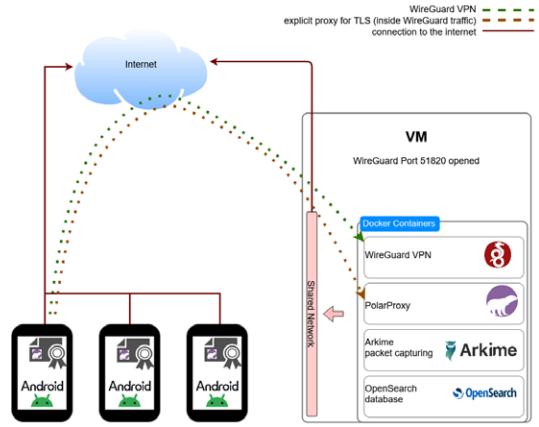
This setup ensured complete logging of device communications.

Analysis Environment

Post-capture, traffic was analyzed using Malcolm, an open-source traffic analysis suite enabling protocol insights and threat detection:

- Uploaded PCAPs were enriched and visualized via OpenSearch dashboards.
- Anomalies and behavioral differences across devices and scenarios were highlighted.

This allowed direct, data-driven comparison of each mobile platform's security posture.



Capture setup

Mosè Ferrazzini

Benjamin Aija Siegenthaler

Steven Mike Zehnder