

Live Data Analysis with using VPNService

Fabian Gruber, Béla Lemle

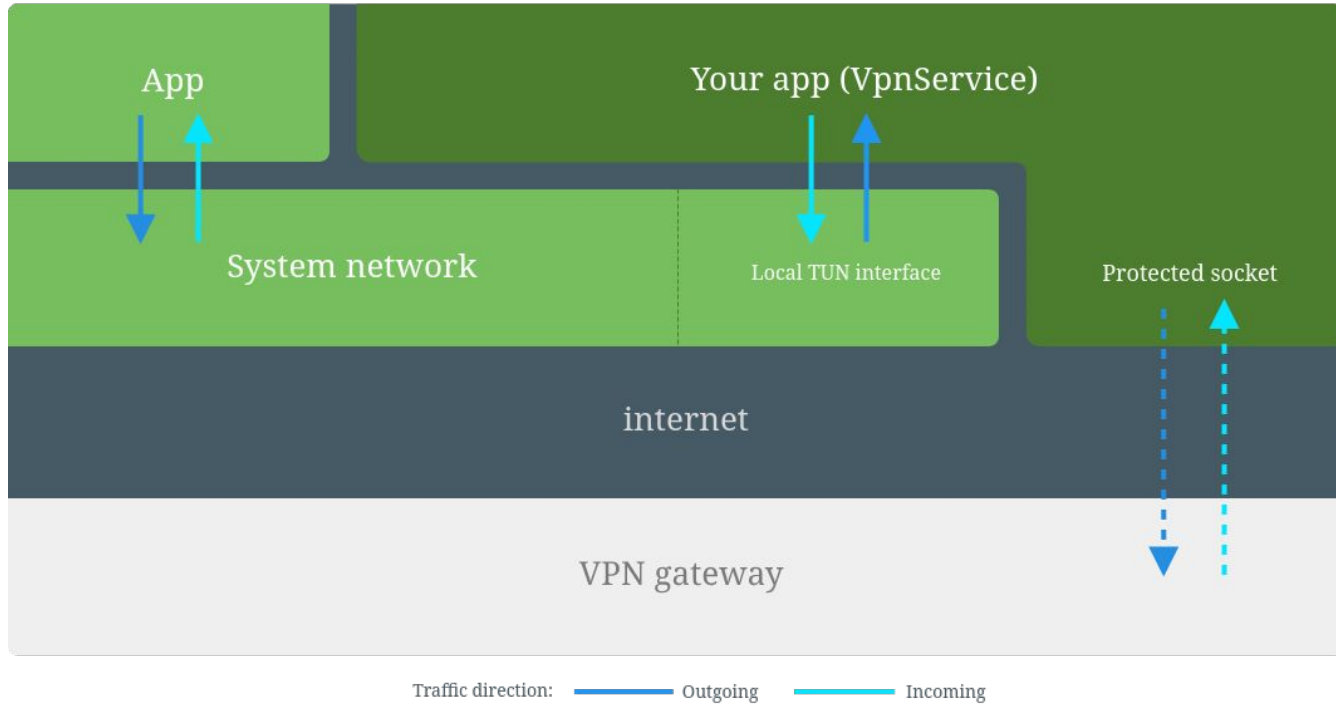
Mobile Security (SS 2023)

Agenda

- VPNService
- Framework and implementation
- Analysis of apps

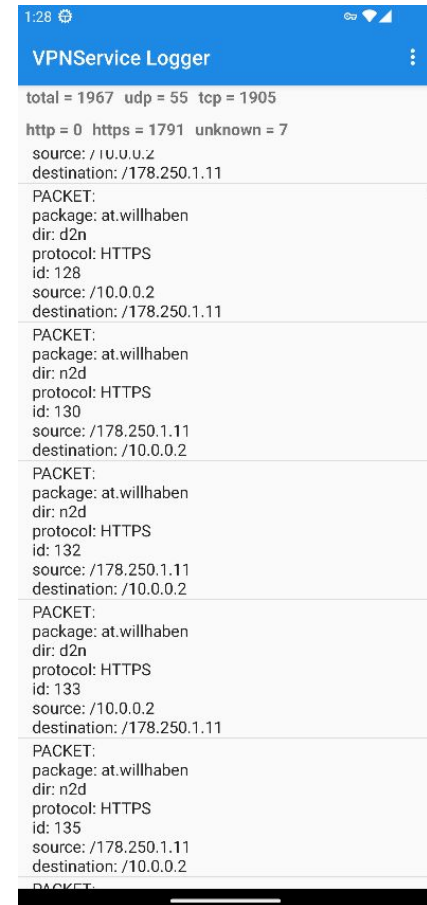
VPNService

- Class for apps to build own VPN solutions
- Virtual network interface, routing rules, addresses, file descriptor
- Read from fd → outgoing packet that was routed to the interface
- Write to fd → injected packets are as if they were received through the interface
- Security measures:
 - user interaction needed to start the VPN service
 - only one service at a time
 - visible on the device if the service is running (system managed)
- BUT no root access required to use it



Implementation

- UI for the live packet analysis
- Differentiate between TCP, UDP, HTTP, HTTPS, DNS packets
- Extract payload of DNS requests
- Specify the app where the packet comes from
- Display packet related data (e.g. source/destination addresses)
- General packet type statistics



Packt and Application Mapping

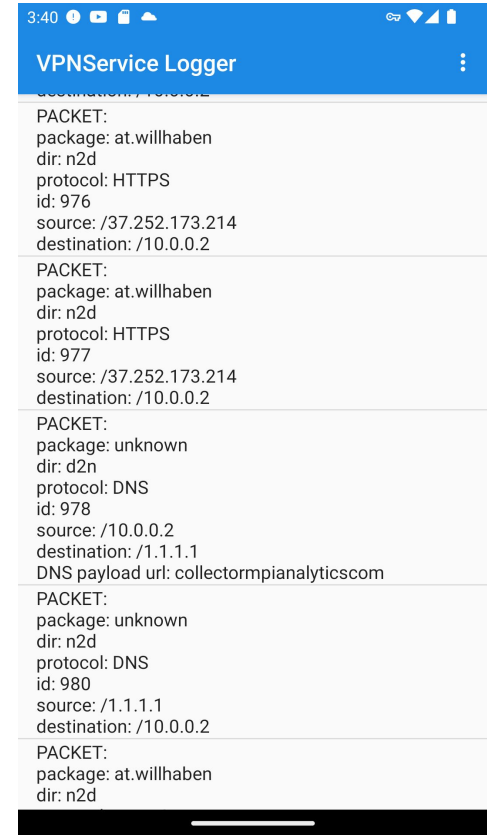
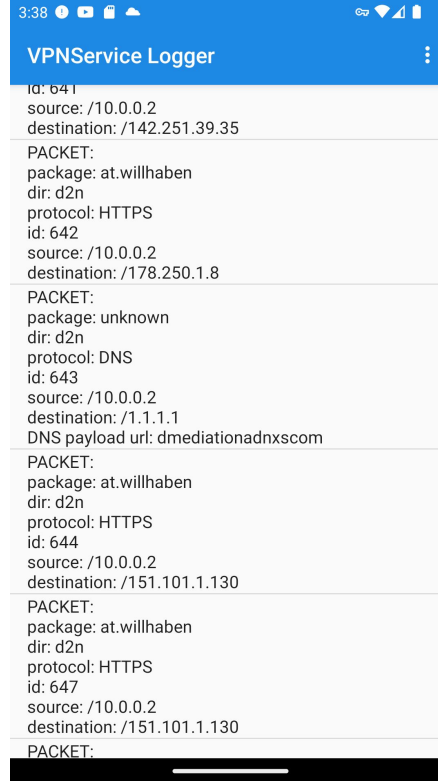
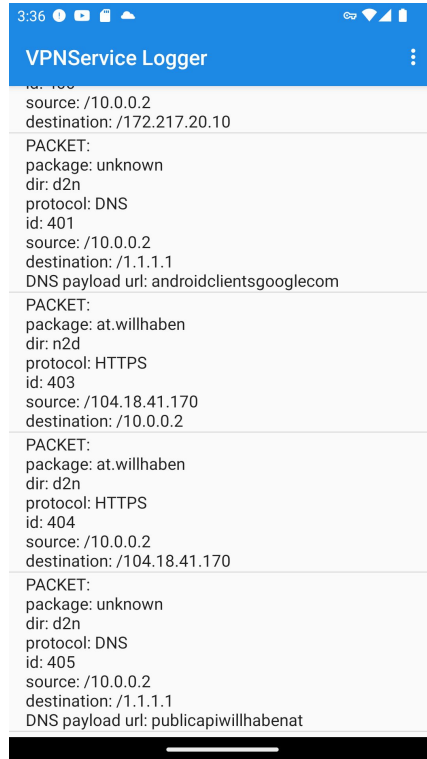
- Pre Android 10 → `/proc/net/tcp`
 - Shows ports and corresponding UIDs
- Post Android 10 → `ConnectivityManager`
 - `/proc/net/tcp` no longer accessible
 - Use `ConnectivityManager` class to get UIDs of connections owners
- Use `PackageManager` to get package names from UIDs

Live Analysis



Packet Analysis

willhaben.at



Packet Analysis

(http app)

Resources

- Based on <https://github.com/mightofcode/android-vpnservice-example>
- VPNService <https://developer.android.com/guide/topics/connectivity/vpn>
- ConnectifyManager <https://developer.android.com/reference/android/net/ConnectivityManager>