SCIENCE
PASSION
TECHNOLOGY

Live Data Analysis with using VPNService

Fabian Gruber, Béla Lemle

Mobile Security (SS 2023)

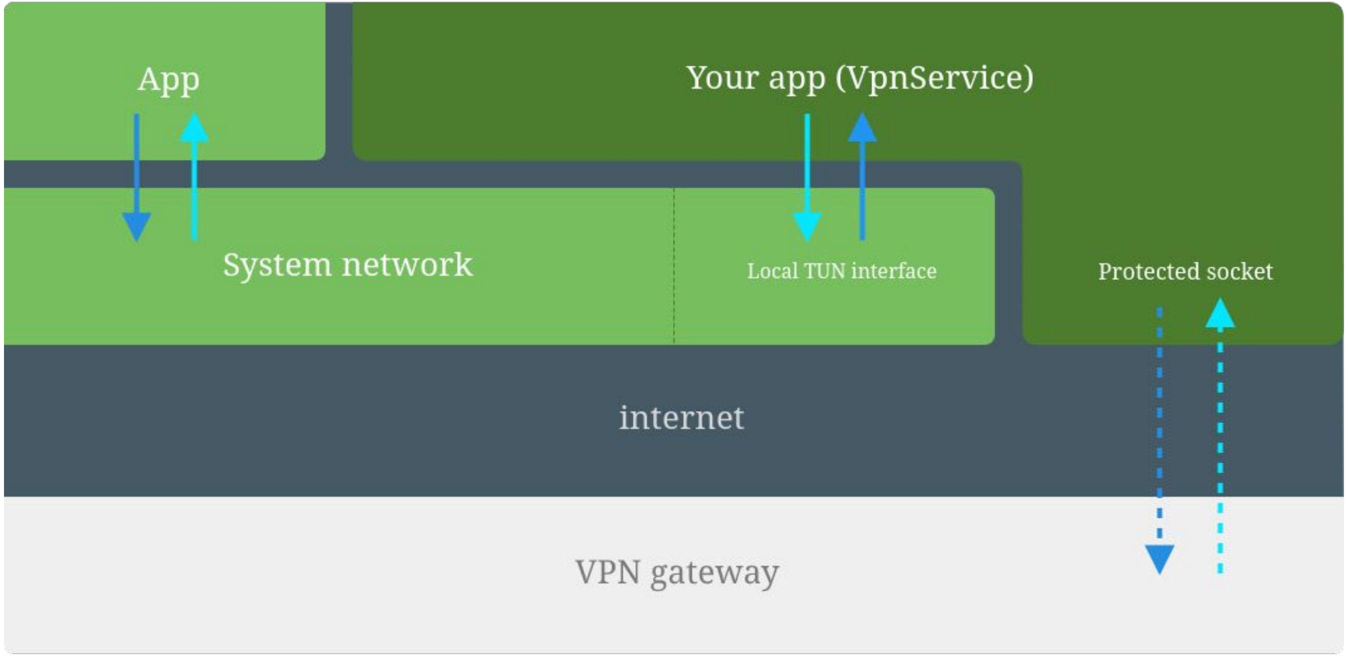
10. June 2023

Agenda

- VPNService
- Framework and implementation
- Analysis of apps

VPNService

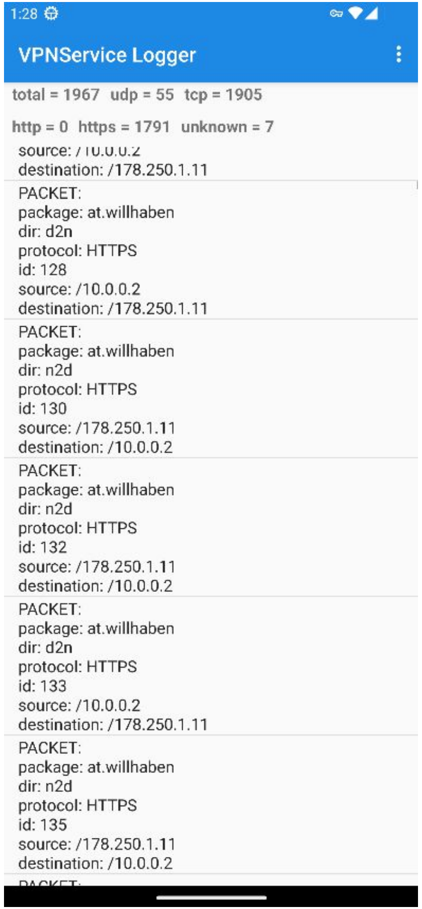
- Class for apps to build own VPN solutions
- Virtual network interface, routing rules, addresses, file descriptor
- Read from fd ➝ outgoing packet that was routed to the interface
- Write to fd ➝ injected packets are as if they were received through the interface
- Security measures:
  - user interaction 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



Traffic direction: Outgoing Incoming

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



VPNService Logger

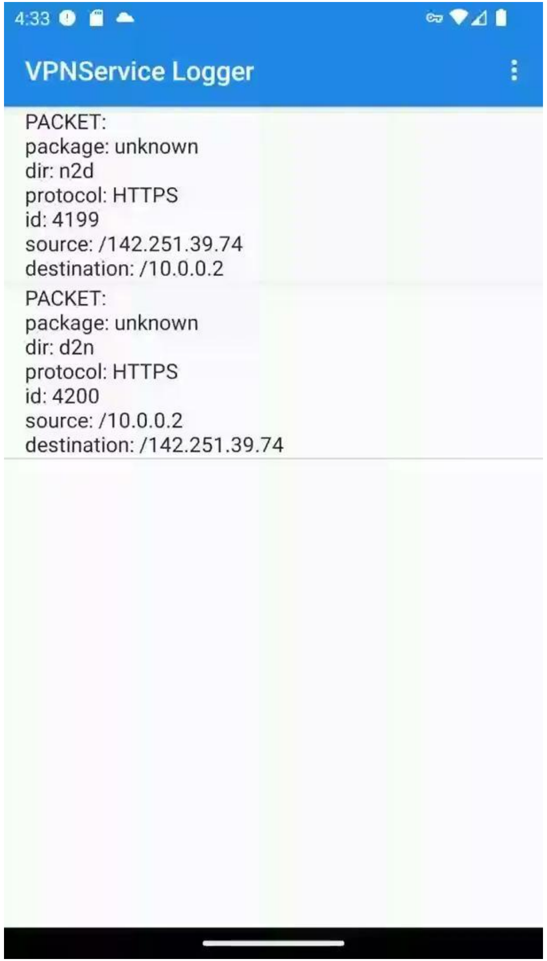
```
total = 1967  udp = 55  tcp = 1905

http = 0  https = 1791  unknown = 7
source: /10.0.0.2
destination: /178.250.1.11
PACKET:
package: at.willhaben
dir: d2n
protocol: HTTPS
id: 128
source: /10.0.0.2
destination: /178.250.1.11
PACKET:
package: at.willhaben
dir: n2d
protocol: HTTPS
id: 130
source: /178.250.1.11
destination: /10.0.0.2
PACKET:
package: at.willhaben
dir: n2d
protocol: HTTPS
id: 132
source: /178.250.1.11
destination: /10.0.0.2
PACKET:
package: at.willhaben
dir: d2n
protocol: HTTPS
id: 133
source: /10.0.0.2
destination: /178.250.1.11
PACKET:
package: at.willhaben
dir: n2d
protocol: HTTPS
id: 135
source: /178.250.1.11
destination: /10.0.0.2
PACKET:
```

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

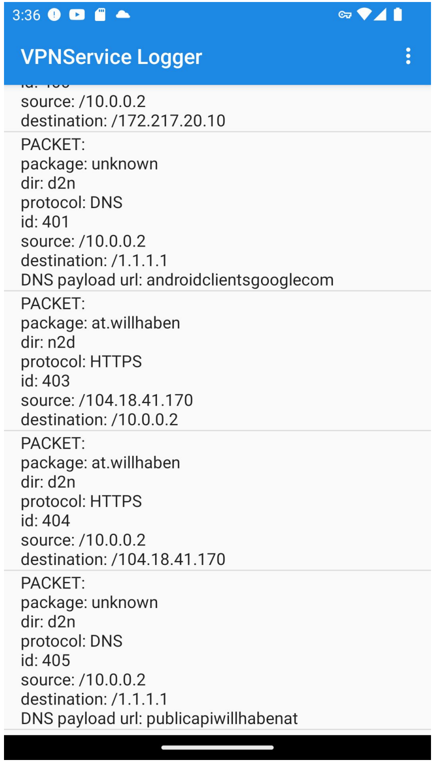
Live Analysis



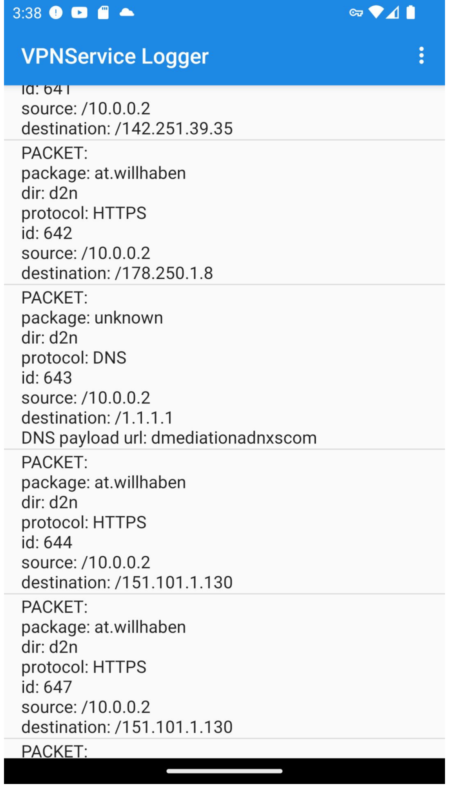
```
PACKET:
package: unknown
dir: n2d
protocol: HTTPS
id: 4199
source: /142.251.39.74
destination: /10.0.0.2
PACKET:
package: unknown
dir: d2n
protocol: HTTPS
id: 4200
source: /10.0.0.2
destination: /142.251.39.74
```

Packet Analysis

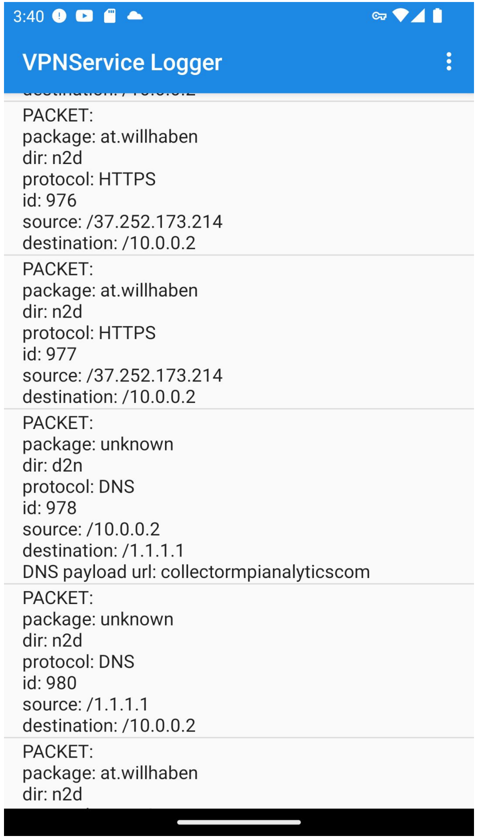
willhaben.at



```
source: /10.0.0.2
destination: /172.217.20.10
PACKET:
package: unknown
dir: d2n
protocol: DNS
id: 401
source: /10.0.0.2
destination: /1.1.1.1
DNS payload url: androidclientsgooglecom
PACKET:
package: at.willhaben
dir: n2d
protocol: HTTPS
id: 403
source: /104.18.41.170
destination: /10.0.0.2
PACKET:
package: at.willhaben
dir: d2n
protocol: HTTPS
id: 404
source: /10.0.0.2
destination: /104.18.41.170
PACKET:
package: unknown
dir: d2n
protocol: DNS
id: 405
source: /10.0.0.2
destination: /1.1.1.1
DNS payload url: publicapiwillhabenat
```



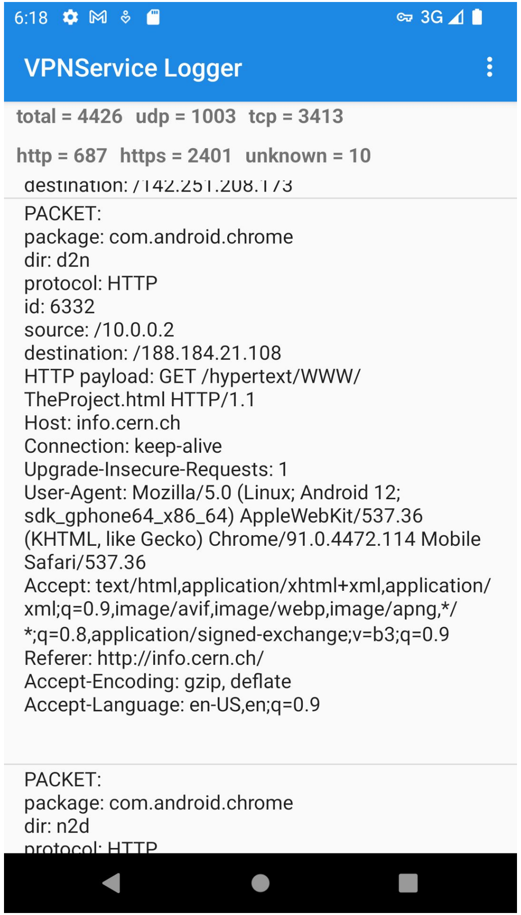
```
id: 641
source: /10.0.0.2
destination: /142.251.39.35
PACKET:
package: at.willhaben
dir: d2n
protocol: HTTPS
id: 642
source: /10.0.0.2
destination: /178.250.1.8
PACKET:
package: unknown
dir: d2n
protocol: DNS
id: 643
source: /10.0.0.2
destination: /1.1.1.1
DNS payload url: dmediationadnxscom
PACKET:
package: at.willhaben
dir: d2n
protocol: HTTPS
id: 644
source: /10.0.0.2
destination: /151.101.1.130
PACKET:
package: at.willhaben
dir: d2n
protocol: HTTPS
id: 647
source: /10.0.0.2
destination: /151.101.1.130
PACKET:
```



```
PACKET:
package: at.willhaben
dir: n2d
protocol: HTTPS
id: 976
source: /37.252.173.214
destination: /10.0.0.2
PACKET:
package: at.willhaben
dir: n2d
protocol: HTTPS
id: 977
source: /37.252.173.214
destination: /10.0.0.2
PACKET:
package: unknown
dir: d2n
protocol: DNS
id: 978
source: /10.0.0.2
destination: /1.1.1.1
DNS payload url: collectormpianalyticscom
PACKET:
package: unknown
dir: n2d
protocol: DNS
id: 980
source: /1.1.1.1
destination: /10.0.0.2
PACKET:
package: at.willhaben
dir: n2d
```

Packet Analysis

Chrome (http://info.cern.ch)

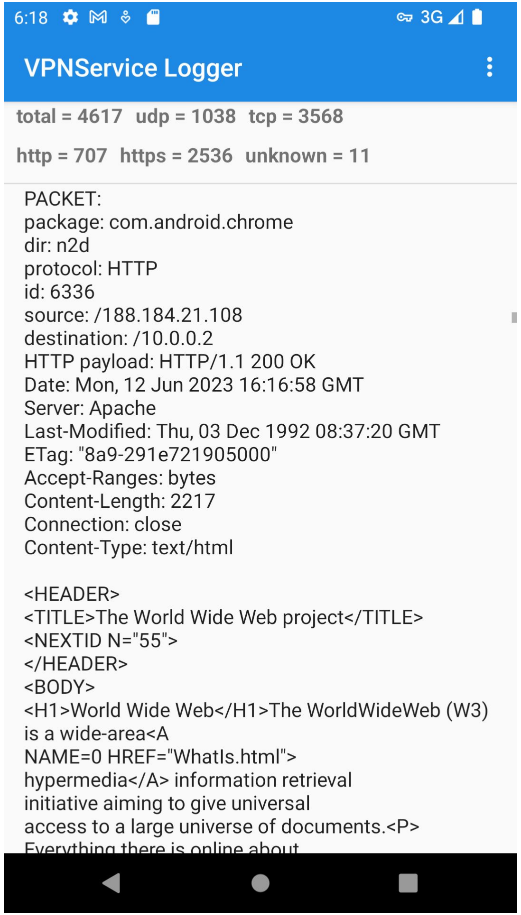


VPNService Logger

```
total = 4426  udp = 1003  tcp = 3413
http = 687  https = 2401  unknown = 10
destination: /142.251.208.173

PACKET:
package: com.android.chrome
dir: d2n
protocol: HTTP
id: 6332
source: /10.0.0.2
destination: /188.184.21.108
HTTP payload: GET /hypertext/WWW/
TheProject.html HTTP/1.1
Host: info.cern.ch
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 12;
sdk_gphone64_x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/91.0.4472.114 Mobile
Safari/537.36
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://info.cern.ch/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

PACKET:
package: com.android.chrome
dir: n2d
protocol: HTTP
```



VPNService Logger

```
total = 4617  udp = 1038  tcp = 3568
http = 707  https = 2536  unknown = 11

PACKET:
package: com.android.chrome
dir: n2d
protocol: HTTP
id: 6336
source: /188.184.21.108
destination: /10.0.0.2
HTTP payload: HTTP/1.1 200 OK
Date: Mon, 12 Jun 2023 16:16:58 GMT
Server: Apache
Last-Modified: Thu, 03 Dec 1992 08:37:20 GMT
ETag: "8a9-291e721905000"
Accept-Ranges: bytes
Content-Length: 2217
Connection: close
Content-Type: text/html

<HEADER>
<TITLE>The World Wide Web project</TITLE>
<NEXTID N="55">
</HEADER>
<BODY>
<H1>World Wide Web</H1>The WorldWideWeb (W3)
is a wide-area<A
NAME=0 HREF="WhatIs.html">
hypermedia</A> information retrieval
initiative aiming to give universal
access to a large universe of documents.<P>
Everything there is online about
```

Resources

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