# ET4394 Wireshark assignment W11

Pradhayini Ramamurthy (4180437) and Hans Okkerman (4290453)

***Abstract*— This report details the procedure, results and analysis of the Wireshark assignment on security (W11) executed by group WN2. WiFi packets were sniffed using airodump-ng while traveling across parts of the country on a train and a bus. The captured data was analyzed for trends in security protocols, encryption and authentication methods. The most prevalent configuration was found to be the WPA2 security protocol implementing the CCMP encryption method and the PSK authentication method.**

## I. Introduction

For the Wireless Networking course of Delft University of Technology an analysis had to be done on WiFi networks. This report covers assignment $W11$ which concerns extracting the used security types per access point. To extract the required information dedicated software such as Wireshark and airodump-ng are used on a laptop which is carried through several areas to record data from nearby networks.

The rest of this report is built up as follows: First the used software, hardware and data collection process are discussed. Next, the results of filtering the recorded data are shown. Finally conclusions are drawn about the used security of the networks.

## II. Data collection

### A. Tools

The hardware used during this assignment was a DELL XPS 13 laptop running $Ubuntu16.04$ and containing an $IntelWireless8260$ adapter that conforms to the IEEE 802.11 standard. Data collection was initially performed using Wireshark and tshark, with the wireless interface configured to operate in the $monitoring$ mode. However, as the data captured with these tools did not provide much insight into the security aspects of the monitored WiFi Access Points (APs), it was decided to use airodump-ng from the aircrack-ng package. There were three main advantages to making this choice. First, with airodump-ng the WiFi interface could be configured to operate in the $monitoring$ mode with little to no extra effort, unlike Wireshark which required a separate script to enable this configuration. Second, airodump-ng allowed the capture of data from multiple channels by doing an automatic, timed, channel hopping. This was both easy to configure (simply by omitting the $channel$ parameter specification) and fruitful in terms of the gathered data. Finally, the data dump from a run of airodump-ng provided information on the basic security configurations of an AP, in addition to the details provided by Wireshark.

### B. Environment

The analysis done for this assignment for focused on capturing data from a wide and varied geographical area, represented by the train route between Breda and Eindhoven and a bus route inside the city of Eindhoven. Several trial runs were done on both routes and the final data analysis was performed on a set of captures executed during the peak travel hours on a weekday. A few obvious expectations were confirmed with respect to the data trends from a superficial glance at the type and quantity of the data gathered. For instance, the density of WiFi APs inside a densely populated urban area such as Eindhoven was much higher than the distribution over the long and sparsely populated train route. This resulted in the number of observed unique APs over the 20 minute bus ride being over twice as many as the number observed in the 40 minute train ride. In contrast, the number of devices (202 devices) that were probing for a recognized, available AP on the train route was nearly 4.4 times the number of devices (46 devices) doing the same on the bus route. This could clearly be attributed to the number of mobile devices within range at the time of measurement.

### C. Data Format and Characteristics

Data collection was done using airodump-ng, configured to scan all channels by default (by periodically hopping channels) in both the 2.4GHz and 5GHz bands. The output was in the csv file format, which was then analyzed. No capture-time filtering could be done with airodump-ng and data filtering was done partly scripted and partly done manually. The following bash script snippet indicates the airodump-np capture. Output CSV files can be found in the group git repository.

```
// startSniffing.sh

# Disable Network Manager
nmcli networking off

# Dump wifi sniffing data from all channels
    in csv format
sudo airodump-ng -b abg -e --write $output
    --output-format csv $interface
```

The data of interest for the security analysis of the wireless networks are given in the columns of $privacy$, $cipher$ and $authentication$ in the captured data dump. $Privacy$ contains the security protocol used by the network. These can be open or not encrypted, WEP which is an older standard that is no longer considered secure, WPA which replaced WEP and WPA2 which replaces WPA and is currently the

most secure. $Cipher$ contains the used encryption protocol of the network. These are either none for open networks, $WEP$, $TKIP$ or $CCMP$. $TKIP$ is used by the WPA protocol and has been considered deprecated since 2009. $CCMP$ is the default encryption scheme for $WPA2$ which replaces $TKIP$, however it is possible to provide $TKIP$ on $WPA2$ to support older devices. Finally $authentication$ contains the means of client authentication to the network. This can be either none for open networks, $PSK$ for regular networks where a password is required to connect and $MGT$ for corporate or other more secure networks. These require a so called $RADIUS$ server which a user has to log on to and provide more information before he can connect to the network.

## III. Results

From the recorded data several distribution profiles can be made based on security protocols, encryption types and authentication types. These will be discussed in the following sections. The measurements are provided in Table I.

### A. Security protocols

Data was first collected while driving by bus through Eindhoven. The distribution of detected network security protocols can be seen in Figure 1. From the Figure it is clear that most detected networks support $WPA2$ or both $WPA2$ and $WPA$ and very few only support $WPA$ or even $WEP$. A rather large amount of open networks was also detected. From the corresponding $ESSID$s it can be shown that a large amount of these networks belong to KPN's $Fon$ network which enables an unencrypted, open AP on the routers of KPN's customers (SSID $KPNFon$) by default. This (from personal experience) is something that a majority of users are unaware of and keep enabled, as seen by the 41 or so such APs. The remaining open networks are mostly "free WiFi" hotspots in stores or cafeterias.

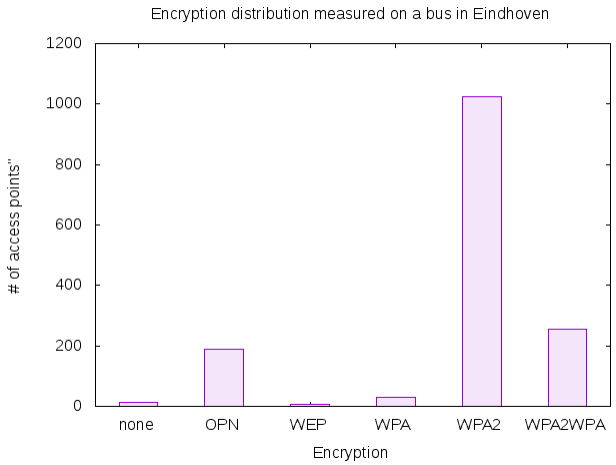


Fig. 1. Security protocol distribution as measured on the bus

In Figure 2 the same data can be seen when traveling by train between Breda and Eindhoven. Roughly the same proportions as before can be observed except for an increase in the relative amount of open networks. Again a large amount of those networks are part of KPN's $Fon$ network or hotspots in stores, but now many "HotspotArriva" and "WiFi in de trein" are available as well. These last two are the open networks in the train as provided by Arriva and NS respectively.

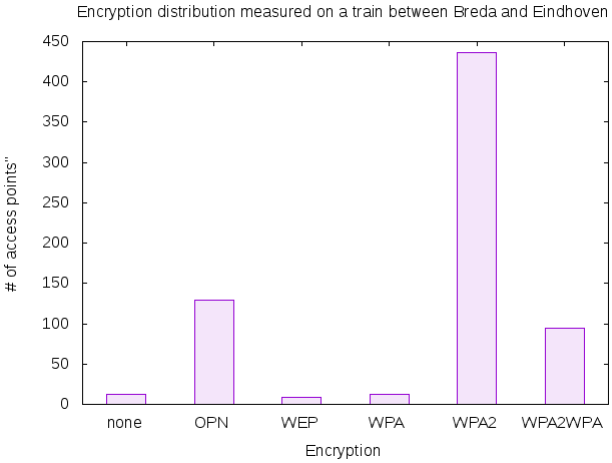


Fig. 2. Security protocol distribution as measured on the train

Figure 3 shows the distributions from the bus and train measurements side by side. Here the larger proportion of open networks as measured in the train is clearly visible.

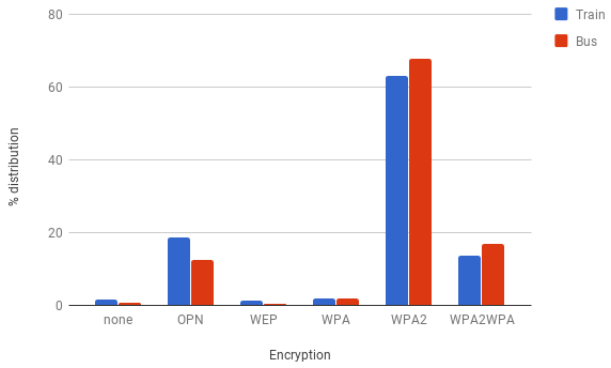


Fig. 3. Security protocol distribution as measured on the train and bus

### B. Encryption types

When focusing on the most common $WPA$ and $WPA2$ protected networks another distribution can be made regarding the used encryption protocol. Figure 4 shows that nearly all $WPA2$ networks as detected from the bus support the $CCMP$ encryption scheme with roughly one fifth supporting both $CCMP$ and the older $TKIP$. Of the networks supporting both $WPA$ and $WPA2$ most support both $CCMP$ and $TKIP$ with roughly one sixth only supporting $CCMP$. Networks that support $WPA2$ but only use $TKIP$ are nearly non-existent, which makes sense as it has been

replaced by $CCMP$ and is only used to support old devices. Very few networks only supported $WPA$, which leads to a lack of usable statistics for these networks as seen in Figure 4. This is however a good sign as it means that not many networks are relying solely on older, deprecated security measures.

Figure 5 shows a similar distribution for the networks detected from the train ride, although it is not entirely clear what causes the difference in proportions between networks that support both $WPA$ and $WPA2$ and use $CCMP$ and $TKIP$, and those that only support $CCMP$. Again, not enough $WPA$-only networks were detected to make a proper comparison.

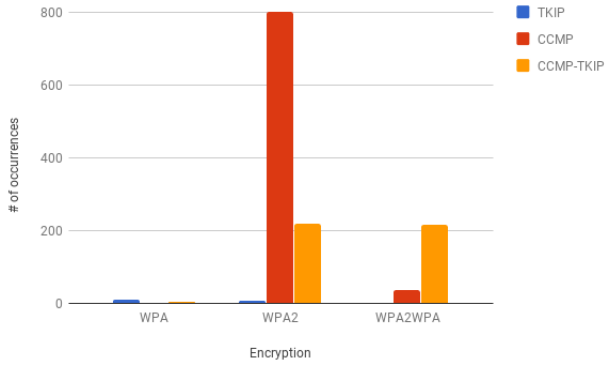


Fig. 4. Encryption distribution as measured on bus

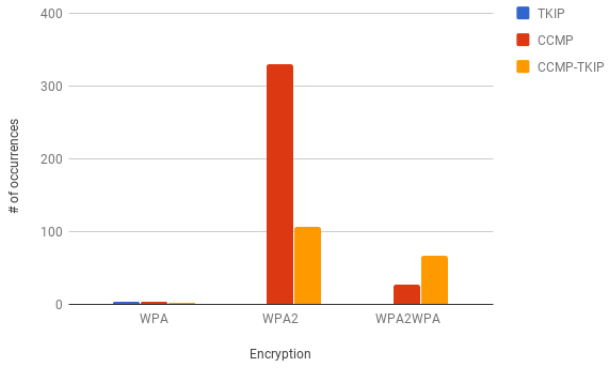


Fig. 5. Encryption distribution as measured on train

### C. Authentication types

$WPA$ and $WPA2$ support two different client authentication methods, $PSK$ and $MGT$. As discussed before, $PSK$ or Pre-Shared Key, is the typical method of authentication used in home networks where users know the password of the network. $MGT$ uses a so called $RADIUS$ server that requires more information from the clients and is often used in corporate or other professional settings. Figures 6 and 7 both show similar results for recordings from the bus and train respectively. It can be clearly seen that the large majority of networks support $PSK$. This makes sense as most home networks use this method. From the $ESSID$s it can be seen that most of the networks that support $MGT$ are called "ziggo". It is expected that this is a similar service as KPN's $Fon$ network, but ran by Ziggo. Another well known network that shows up in the records is "eduroam", which is a good example of the more advanced login requirements of $MGT$ authentication. Finally some companies seem to use the method as well.

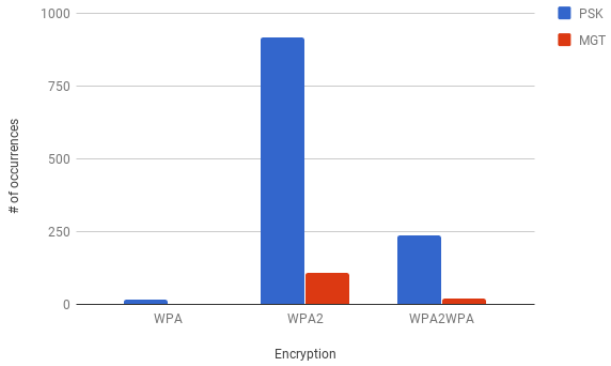


Fig. 6. Authentication method distribution as measured on bus

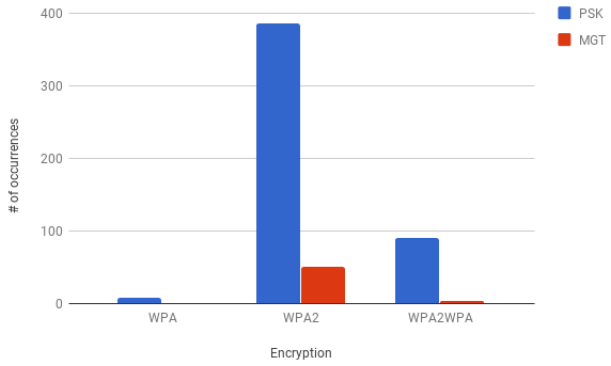


Fig. 7. Authentication method distribution as measured on train

## IV. Conclusion

From the graphs in the previous sections it can be seen that the trends in both populated urban areas and in the sparse rural areas are nearly identical, and only differ in the actual number of Access Points. Open unencrypted networks that do not require any user authentication are mostly provided by KPN's $Fon$ network, public transport companies such as NS with $Wifiindetrein$ and Arriva's $ArrivaHotspot$, city centers ($EHVFREEWIFI$) and shopping centers. Most other personal or office-owned APs are running $WPA2$ or both $WPA$ and $WPA2$, and most of those use either only $CCMP$ or both $CCMP$ and $TKIP$. Authentication is most commonly done using $PSK$ with some corporations using $MGT$. Very few networks still only rely on older insecure standards such as $WEP$ or $WPA$ only, which is a good sign for the overall security of wireless networks.

| | | | Cipher | | | | | | Authentication | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Total | | TKIP | | CCMP | | CCMP-TKIP | | PSK | | MGT | |
| Security Protocol | Bus | Train | Bus | Train | Bus | Train | Bus | Train | Bus | Train | Bus | Train |
| Unspecified | 12 | 12 | - | - | - | - | - | - | - | - | - | - |
| OPN | 190 | 129 | - | - | - | - | - | - | - | - | - | - |
| WEP | 5 | 9 | - | - | - | - | - | - | - | - | - | - |
| WPA | 29 | 13 | 10 | 3 | 1 | 3 | 4 | 2 | 15 | 8 | 0 | 0 |
| WPA2 | 1024 | 436 | 6 | 0 | 800 | 330 | 218 | 106 | 916 | 385 | 108 | 51 |
| WPA2WPA | 255 | 94 | 2 | 0 | 36 | 27 | 217 | 67 | 235 | 90 | 20 | 4 |

TABLE I

DISTRIBUTION OF NUMBER OF OCCURRENCES OF PROTOCOLS IN AIRODUMP-NG MEASUREMENTS