WiFi AP security

ET4395
Group WN_2
Pradhayini Ramamurthy (4180437)
Hans Okkerman (4290453)
https://github.com/HOkkerman/ET4394

Assignment

- Record data from many APs
- Determine used security
- Analyze data and draw conclusions

Data collection

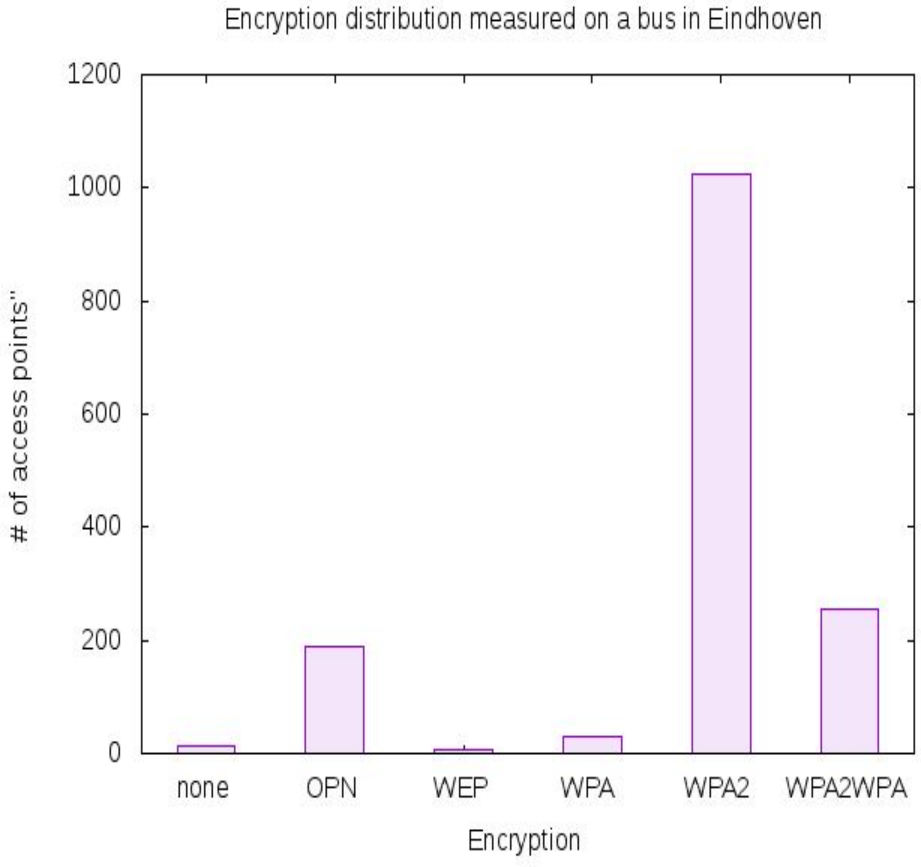
- Laptop running airodump-ng
- Run capture on public transport
- Filter on security afterwards

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

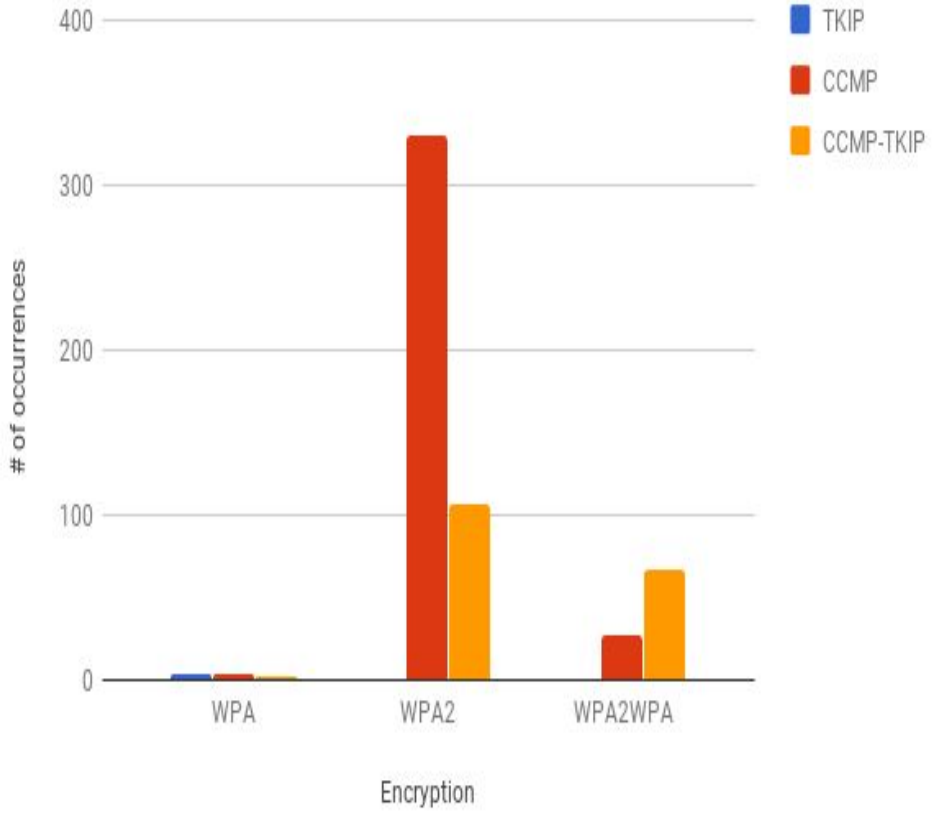
	A	B	C	D	E	F	G	H	I	
1	BSSID	First time seen	Last time seen	channel	Speed	Privacy	Cipher	Authentication	Power	+AC
2	9C:6F:52:36:E8:61	2018+AC0-02+AC0-28 18:40:35	2018+AC0-02+AC0-28 18:40:36	3	54	WPA2	CCMP	PSK	+AC0-65	
3	6A:6F:52:36:E8:62	2018+AC0-02+AC0-28 18:40:35	2018+AC0-02+AC0-28 18:40:36	3	54	OPN			+AC0-65	
4	5A:4D:EA:9C:DB:A	2018+AC0-02+AC0-28 18:40:35	2018+AC0-02+AC0-28 18:40:36	3	54	OPN			+AC0-71	
5	00:1D:AA:C5:4A:38	2018+AC0-02+AC0-28 18:40:34	2018+AC0-02+AC0-28 18:40:35	1	54	WPA2	CCMP	PSK	+AC0-72	
6	38:43:7D:0F:A3:F7	2018+AC0-02+AC0-28 18:40:35	2018+AC0-02+AC0-28 18:40:37	6	54	WPA2	CCMP	PSK	+AC0-75	
7	30:99:35:91:5B:1E	2018+AC0-02+AC0-28 18:40:36	2018+AC0-02+AC0-28 18:40:36	9	54	WPA2	CCMP	PSK	+AC0-76	
8	34:4D:EA:9C:DB:A	2018+AC0-02+AC0-28 18:40:35	2018+AC0-02+AC0-28 18:40:36	3	54	WPA2WPA	CCMP TKIP	PSK	+AC0-76	
9	72:99:35:91:5B:1F	2018+AC0-02+AC0-28 18:40:36	2018+AC0-02+AC0-28 18:40:36	9	54	OPN			+AC0-77	
10	00:15:F2:91:18:73	2018+AC0-02+AC0-28 18:40:37	2018+AC0-02+AC0-28 18:40:37	11	54	WPA2WPA	CCMP TKIP	PSK	+AC0-81	
11	00:02:6F:A0:C5:BF	2018+AC0-02+AC0-28 18:40:35	2018+AC0-02+AC0-28 18:40:35	2	+AC0-1	WPA			+AC0-85	
12	AC:22:05:60:E4:35	2018+AC0-02+AC0-28 18:40:27	2018+AC0-02+AC0-28 18:40:27	52	54	WPA2WPA	CCMP TKIP	PSK	+AC0-58	
13	90:5C:44:CF:27:94	2018+AC0-02+AC0-28 18:40:25	2018+AC0-02+AC0-28 18:40:26	11	54	WPA2	CCMP	PSK	+AC0-63	
14	30:99:35:91:8E:DB	2018+AC0-02+AC0-28 18:40:26	2018+AC0-02+AC0-28 18:40:26	6	54	WPA2	CCMP	PSK	+AC0-68	
15	7A:99:35:91:8E:D8	2018+AC0-02+AC0-28 18:40:26	2018+AC0-02+AC0-28 18:40:26	6	54	OPN			+AC0-69	
16	54:67:51:BC:99:12	2018+AC0-02+AC0-28 18:40:22	2018+AC0-02+AC0-28 18:40:23	1	54	WPA2	CCMP	PSK	+AC0-69	
17	1C:3A:DE:BC:04:A	2018+AC0-02+AC0-28 18:40:25	2018+AC0-02+AC0-28 18:40:26	5	54	WPA2	CCMP TKIP	PSK	+AC0-71	
18	00:13:D4:50:06:FB	2018+AC0-02+AC0-28 18:40:23	2018+AC0-02+AC0-28 18:40:24	8	54	WPA2	CCMP	PSK	+AC0-77	
19	48:BA:4E:70:11:29	2018+AC0-02+AC0-28 18:40:25	2018+AC0-02+AC0-28 18:40:25	11	54	WPA2	CCMP	PSK	+AC0-78	
20	54:67:51:0B:22:DC	2018+AC0-02+AC0-28 18:40:25	2018+AC0-02+AC0-28 18:40:25	11	54	WPA2	CCMP TKIP	PSK	+AC0-78	
21	00:1D:AA:C7:17:B0	2018+AC0-02+AC0-28 18:40:24	2018+AC0-02+AC0-28 18:40:26	3	54	WPA2	CCMP TKIP	PSK	+AC0-81	
22	7A:68:C8:90:8A:04	2018+AC0-02+AC0-28 18:39:36	2018+AC0-02+AC0-28 18:40:23	1	54	OPN			+AC0-81	
23	8C:68:C8:90:8A:07	2018+AC0-02+AC0-28 18:39:12	2018+AC0-02+AC0-28 18:40:23	1	54	WPA2	CCMP	PSK	+AC0-81	
24	54:67:51:0B:23:77	2018+AC0-02+AC0-28 18:40:26	2018+AC0-02+AC0-28 18:40:26	36	54	WPA2WPA	CCMP TKIP	PSK	+AC0-82	
25	AC:22:05:60:E4:63	2018+AC0-02+AC0-28 18:40:25	2018+AC0-02+AC0-28 18:40:26	11	54	WPA2	CCMP TKIP	PSK	+AC0-82	
26	54:FA:3E:BE:CC:A	2018+AC0-02+AC0-28 18:40:24	2018+AC0-02+AC0-28 18:40:24	3	54	WPA2	CCMP TKIP	PSK	+AC0-82	
27	54:67:51:BC:99:0E	2018+AC0-02+AC0-28 18:40:26	2018+AC0-02+AC0-28 18:40:26	36	54	WPA2	CCMP	PSK	+AC0-84	
28	20:89:86:07:4F:46	2018+AC0-02+AC0-28 18:40:25	2018+AC0-02+AC0-28 18:40:25	11	54	WPA2WPA	CCMP TKIP	PSK	+AC0-84	
29	64:D1:A3:4E:1D:73	2018+AC0-02+AC0-28 18:40:11	2018+AC0-02+AC0-28 18:40:23	13	54	WPA2	CCMP	PSK	+AC0-84	
30	F8:04:2E:06:37:A8	2018+AC0-02+AC0-28 18:40:11	2018+AC0-02+AC0-28 18:40:14	6	54	WPA2	CCMP TKIP	PSK	+AC0-70	
31	00:1D:AA:EF:93:E8	2018+AC0-02+AC0-28 18:40:01	2018+AC0-02+AC0-28 18:40:13	10	54	WPA2	CCMP	PSK	+AC0-72	
32	90:5C:44:48:82:76	2018+AC0-02+AC0-28 18:40:02	2018+AC0-02+AC0-28 18:40:14	11	54	WPA2	CCMP TKIP	PSK	+AC0-78	
33	9C:3D:CF:3D:BE:6A	2018+AC0-02+AC0-28 18:40:02	2018+AC0-02+AC0-28 18:40:14	6	54	WPA2	CCMP	PSK	+AC0-79	
34	AC:22:05:19:57:08	2018+AC0-02+AC0-28 18:39:15	2018+AC0-02+AC0-28 18:40:14	11	54	WPA2	CCMP	PSK	+AC0-81	
35	00:1E:E5:83:F9:E6	2018+AC0-02+AC0-28 18:40:02	2018+AC0-02+AC0-28 18:40:14	5	54	WPA2	CCMP	PSK	+AC0-82	
36	54:BE:53:89:9D:0A	2018+AC0-02+AC0-28 18:39:02	2018+AC0-02+AC0-28 18:40:13	3	54	WPA2	CCMP	PSK	+AC0-85	
37	00:14:5C:8E:34:34	2018+AC0-02+AC0-28 18:40:02	2018+AC0-02+AC0-28 18:40:14	11	54	WPA2	CCMP	PSK	+AC0-86	
38	5C:A3:9D:F3:AC:F0	2018+AC0-02+AC0-28 18:40:03	2018+AC0-02+AC0-28 18:40:03	36	54	WPA2	CCMP TKIP	PSK	+AC0-83	
39	28:FF:3E:1A:95:3C	2018+AC0-02+AC0-28 18:40:04	2018+AC0-02+AC0-28 18:40:04	+AC0-1	54	WPA2	CCMP	PSK	+AC0-84	
40	F8:04:2E:06:37:A0	2018+AC0-02+AC0-28 18:40:07	2018+AC0-02+AC0-28 18:40:07	132	54	WPA2	CCMP	PSK	+AC0-85	
41	90:5C:44:48:82:4A	2018+AC0-02+AC0-28 18:40:05	2018+AC0-02+AC0-28 18:40:05	100	54	WPA2WPA	CCMP TKIP	PSK	+AC0-86	

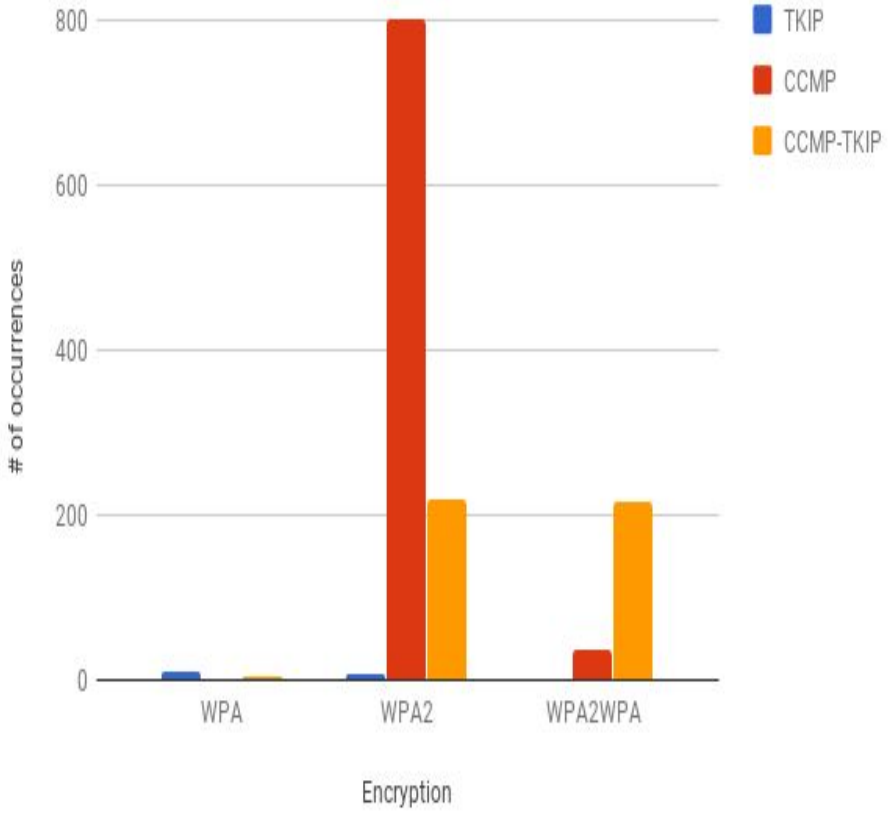
BUSEindhoven-01

Results, security

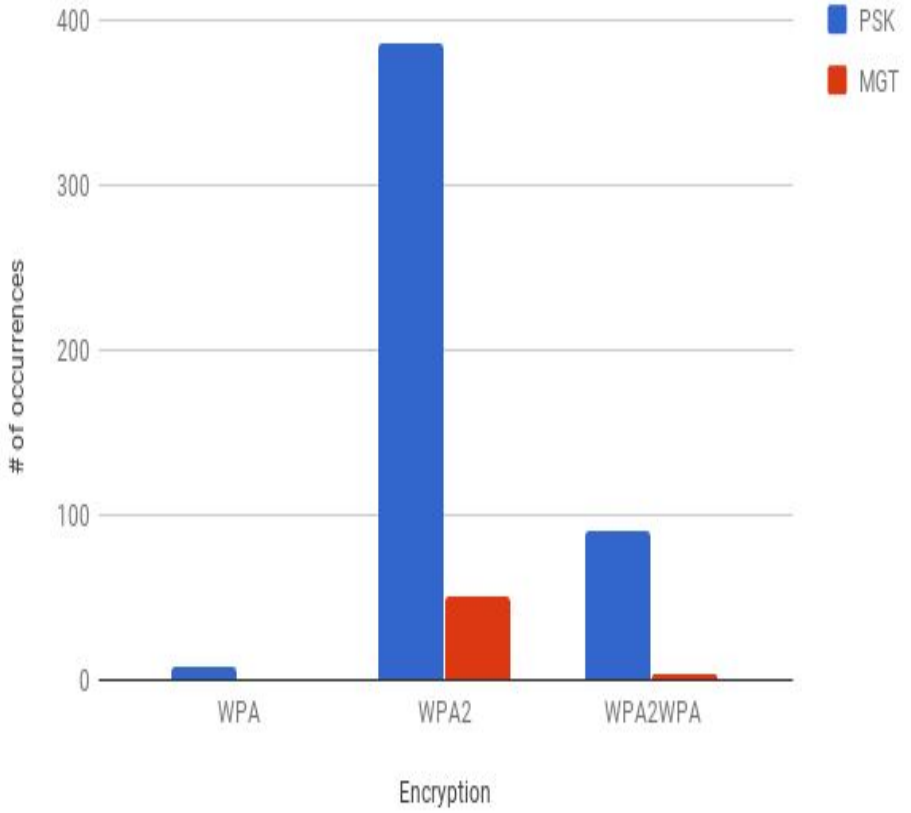


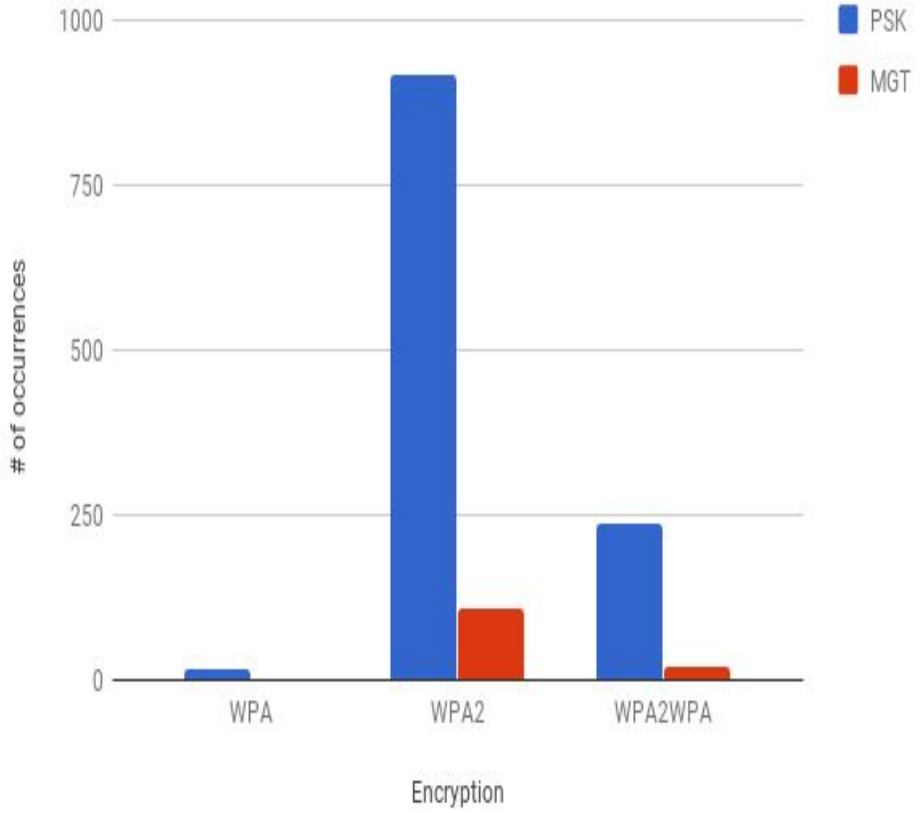
Results, encryption





Results, authentication





Conclusions

-Most run WPA2 or WPA and WPA2
-Very few WPA only or WEP
-Open networks are on purpose
-No networks only support TKIP
-PSK authentication is most common
-Networks seem to be well protected