Rogue Network Detection ?!?

- RND is een *eerstelijns* detectiesysteem tegen afluisteren/misbruik van WiFi door Rogue Networks en MitM-attacks
- Detectie (vast of mobiel) met gangbare Android™ apparatuur
- Geeft meldingen door aan meldkamer
- Na constatering kan verdere expertise ingeschakeld worden

Wat is een Rogue Network?

- Een nep-netwerk binnen het gebouw, terrein of complex, al dan niet aangesloten op eigen bedrijfsnetwerk. Dit is de “Man-in-the-middle” tactiek.

- Of juist daarbuiten, op een andere locatie, bijvoorbeeld waar personen op sleutelposities gaan vergaderen of dineren, of bij hun woning. Misbruik van in het verleden op het apparaat opgeslagen profielen.

- Of met een “publiek” SSID zomaar ergens waar veel mensen passeren zoals CS, RAI, of net buiten het Hilton. Ook hier misbruik van opgeslagen profielen.

“Voordelen” Rogue Access Point

- Complete communicatie van apparaat (notebook, mobiel, tablet) kan worden afgetapt, geen 'flarden uit de ether'.
- Je bent al door de eerste beveiligingsschil heen, namelijk WPA(2)/PSK of (L)EAP. Dat scheelt een stuk decoderen!
- Je kunt communicatie met servers bestuderen ten behoeve van reverse engineering, bijvoorbeeld om een phishing-site te maken.

De detector (1)

- Mobiele apparatuur draait op Android ™ platform, draait dus op zowel budget-tablets als op MIL-spec en/of high-end apparatuur.
- Vaste montage op basis van 2.4 & 5 Ghz ontvangers met externe antennes.
- Op afstand (meldkamer) wordt functie ingesteld op mobiele detectors.
- Werkt op zich unattended maar geeft ook beeld en eventueel akoustisch signaal.

De detector (2)

Kan:

- “vast” worden gemonteerd bij bijvoorbeeld ingang/receptie, vergaderruimte
- in auto worden ingebouwd voor surveillance
- Draagbaar/mobiel gebruikt worden voor ronde etc

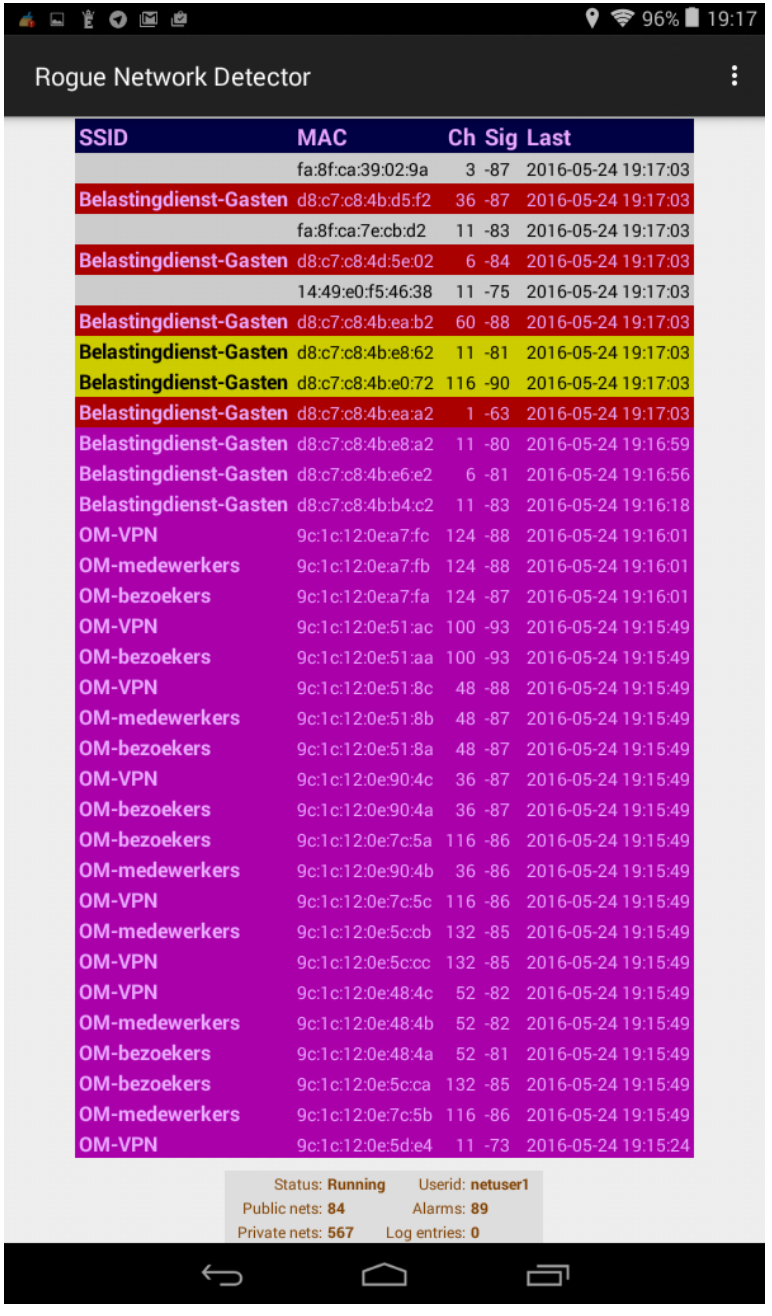
- Ingebouwd en/of mobiel is het zéér geschikt voor periferie-beveiliging

De detector (3)

Kan scannen op:

- Specifieke SSID's van bijvoorbeeld bedrijf
- (... óók op perfect gespoofde MAC's)
- “Publieke” SSID's zoals OV, hotels, andere grote aanbieders
- “Hidden” networks, inclusief probing
- Netwerken zonder beveiliging: “NONE”
- Locale inventarisatie
- Penetration Testing Devices (PenTest)

De detector (4)



Hak5 Pineapple PineAP

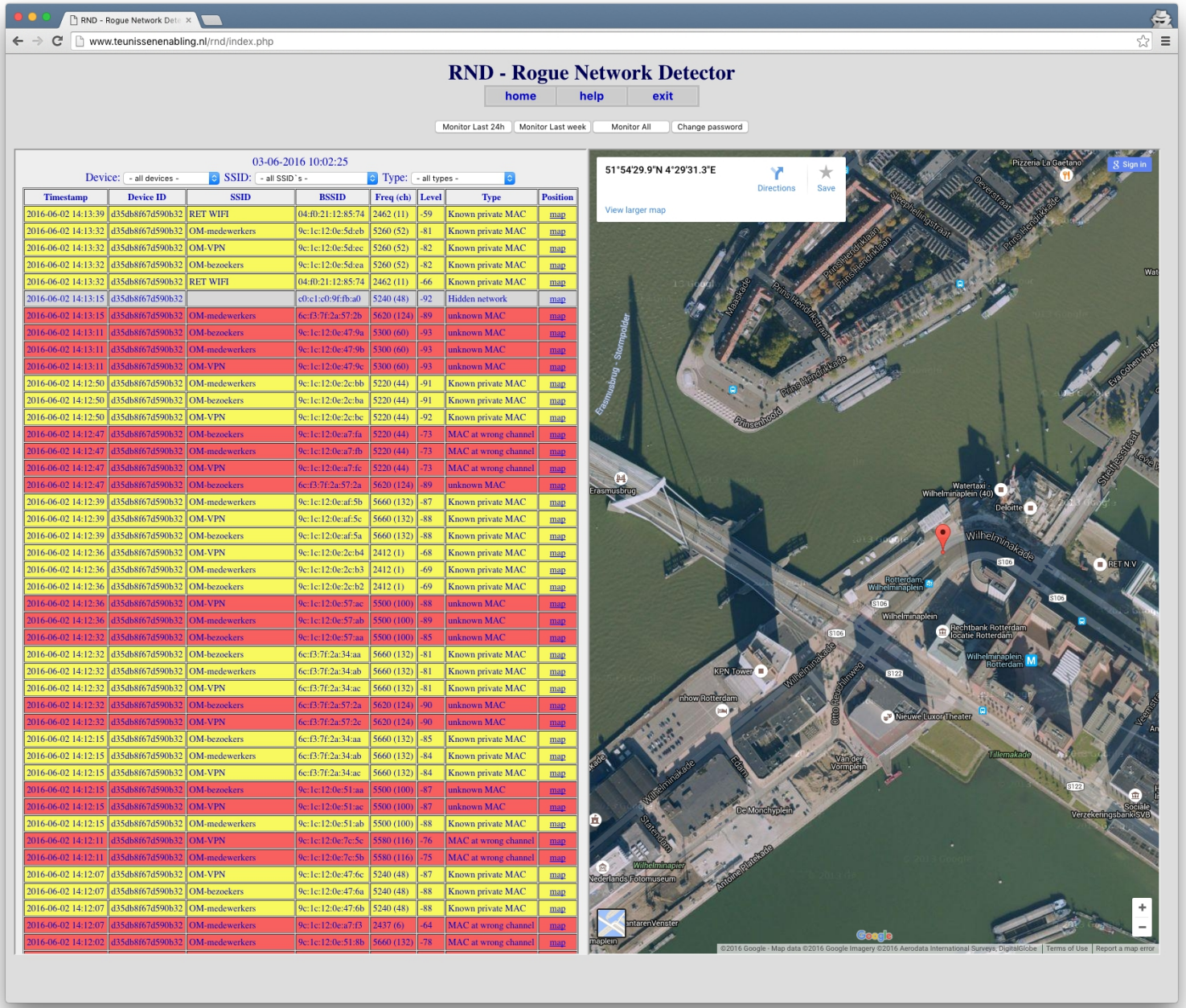
Pineapple (div soorten) is een PenTest device = Penetration Testing. Goedkoop, zeer effectief, zeer verkrijgbaar

- Afzonderlijke aanval op specifiek netwerk kan RND detecteren
- RND kan echter óók detecteren of ergens een Pineapple aan het werk is, bijvoorbeeld tijdens surveillance

De meldkamer (1)

- Eén of meerdere userid's kunnen op dezelfde tag loggen, en één of meerdere userid's kunnen dat in de meldkamer bekijken.
- Een userid kan op meerdere detectors worden gebruikt (in meldkamer te onderscheiden op device-id)
- Hierdoor kan een systeem gebouwd worden wat slechts beperkt wordt door de capaciteit van de database en de webserver.

De meldkamer (2)



Timestamp	Device ID	SSID	BSSID	Freq (ch)	Level	Type	Position
2016-06-02 14:13:39	d35db8f67d590b32	RET WIFI	04:f0:21:12:85:74	2462 (11)	-59	Known private MAC	map
2016-06-02 14:13:32	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:5d:eb	5260 (52)	-81	Known private MAC	map
2016-06-02 14:13:32	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:5d:ec	5260 (52)	-82	Known private MAC	map
2016-06-02 14:13:32	d35db8f67d590b32	OM-bezoekers	9c:1c:12:0e:5d:ea	5260 (52)	-82	Known private MAC	map
2016-06-02 14:13:32	d35db8f67d590b32	RET WIFI	04:f0:21:12:85:74	2462 (11)	-66	Known private MAC	map
2016-06-02 14:13:15	d35db8f67d590b32		c0:c1:c0:9f:fb:a0	5240 (48)	-92	Hidden network	map
2016-06-02 14:13:15	d35db8f67d590b32	OM-medewerkers	6c:f3:7f:2a:57:2b	5620 (124)	-89	unknown MAC	map
2016-06-02 14:13:11	d35db8f67d590b32	OM-bezoekers	9c:1c:12:0e:47:9a	5300 (60)	-93	unknown MAC	map
2016-06-02 14:13:11	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:47:9b	5300 (60)	-93	unknown MAC	map
2016-06-02 14:13:11	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:47:9c	5300 (60)	-93	unknown MAC	map
2016-06-02 14:12:50	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:2c:bb	5220 (44)	-91	Known private MAC	map
2016-06-02 14:12:50	d35db8f67d590b32	OM-bezoekers	9c:1c:12:0e:2c:ba	5220 (44)	-91	Known private MAC	map
2016-06-02 14:12:50	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:2c:bc	5220 (44)	-92	Known private MAC	map
2016-06-02 14:12:47	d35db8f67d590b32	OM-bezoekers	9c:1c:12:0e:a7:fa	5220 (44)	-73	MAC at wrong channel	map
2016-06-02 14:12:47	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:a7:fb	5220 (44)	-73	MAC at wrong channel	map
2016-06-02 14:12:47	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:a7:fc	5220 (44)	-73	MAC at wrong channel	map
2016-06-02 14:12:47	d35db8f67d590b32	OM-bezoekers	6c:f3:7f:2a:57:2a	5620 (124)	-89	unknown MAC	map
2016-06-02 14:12:39	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:af:5b	5660 (132)	-87	Known private MAC	map
2016-06-02 14:12:39	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:af:5c	5660 (132)	-88	Known private MAC	map
2016-06-02 14:12:39	d35db8f67d590b32	OM-bezoekers	9c:1c:12:0e:af:5a	5660 (132)	-88	Known private MAC	map
2016-06-02 14:12:36	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:2c:b4	2412 (1)	-68	Known private MAC	map
2016-06-02 14:12:36	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:2c:b3	2412 (1)	-69	Known private MAC	map
2016-06-02 14:12:36	d35db8f67d590b32	OM-bezoekers	9c:1c:12:0e:2c:b2	2412 (1)	-69	Known private MAC	map
2016-06-02 14:12:36	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:57:ac	5500 (100)	-88	unknown MAC	map
2016-06-02 14:12:36	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:57:ab	5500 (100)	-89	unknown MAC	map
2016-06-02 14:12:32	d35db8f67d590b32	OM-bezoekers	9c:1c:12:0e:57:aa	5500 (100)	-85	unknown MAC	map
2016-06-02 14:12:32	d35db8f67d590b32	OM-bezoekers	6c:f3:7f:2a:34:aa	5660 (132)	-81	Known private MAC	map
2016-06-02 14:12:32	d35db8f67d590b32	OM-medewerkers	6c:f3:7f:2a:34:ab	5660 (132)	-81	Known private MAC	map
2016-06-02 14:12:32	d35db8f67d590b32	OM-VPN	6c:f3:7f:2a:34:ac	5660 (132)	-81	Known private MAC	map
2016-06-02 14:12:32	d35db8f67d590b32	OM-bezoekers	6c:f3:7f:2a:57:2a	5620 (124)	-90	unknown MAC	map
2016-06-02 14:12:32	d35db8f67d590b32	OM-VPN	6c:f3:7f:2a:57:2c	5620 (124)	-90	unknown MAC	map
2016-06-02 14:12:15	d35db8f67d590b32	OM-bezoekers	6c:f3:7f:2a:34:aa	5660 (132)	-85	Known private MAC	map
2016-06-02 14:12:15	d35db8f67d590b32	OM-medewerkers	6c:f3:7f:2a:34:ab	5660 (132)	-84	Known private MAC	map
2016-06-02 14:12:15	d35db8f67d590b32	OM-VPN	6c:f3:7f:2a:34:ac	5660 (132)	-84	Known private MAC	map
2016-06-02 14:12:15	d35db8f67d590b32	OM-bezoekers	9c:1c:12:0e:51:aa	5500 (100)	-87	unknown MAC	map
2016-06-02 14:12:15	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:51:ac	5500 (100)	-87	unknown MAC	map
2016-06-02 14:12:15	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:51:ab	5500 (100)	-88	Known private MAC	map
2016-06-02 14:12:11	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:7c:5c	5580 (116)	-76	MAC at wrong channel	map
2016-06-02 14:12:11	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:7c:5b	5580 (116)	-75	MAC at wrong channel	map
2016-06-02 14:12:07	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:47:6c	5240 (48)	-87	Known private MAC	map
2016-06-02 14:12:07	d35db8f67d590b32	OM-bezoekers	9c:1c:12:0e:47:6a	5240 (48)	-88	Known private MAC	map
2016-06-02 14:12:07	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:47:6b	5240 (48)	-88	Known private MAC	map
2016-06-02 14:12:07	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:a7:f3	2437 (6)	-64	MAC at wrong channel	map
2016-06-02 14:12:02	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:51:8b	5660 (132)	-78	MAC at wrong channel	map

De meldkamer (3)

03-06-2016 10:02:25

Device: - all devices - SSID: - all SSID`s - Type: - all types -

Timestamp	Device ID	SSID	BSSID	Freq (ch)	Level	Type	Position
2016-06-02 14:13:39	d35db8f67d590b32	RET WIFI	04:f0:21:12:85:74	2462 (11)	-59	Known private MAC	map
2016-06-02 14:13:32	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:5d:eb	5260 (52)	-81	Known private MAC	map
2016-06-02 14:13:32	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:5d:ec	5260 (52)	-82	Known private MAC	map
2016-06-02 14:13:32	d35db8f67d590b32	OM-bezoekers	9c:1c:12:0e:5d:ea	5260 (52)	-82	Known private MAC	map
2016-06-02 14:13:32	d35db8f67d590b32	RET WIFI	04:f0:21:12:85:74	2462 (11)	-66	Known private MAC	map
2016-06-02 14:13:15	d35db8f67d590b32		c0:c1:c0:9f:fb:a0	5240 (48)	-92	Hidden network	map
2016-06-02 14:13:15	d35db8f67d590b32	OM-medewerkers	6c:f3:7f:2a:57:2b	5620 (124)	-89	unknown MAC	map
2016-06-02 14:13:11	d35db8f67d590b32	OM-bezoekers	9c:1c:12:0e:47:9a	5300 (60)	-93	unknown MAC	map
2016-06-02 14:13:11	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:47:9b	5300 (60)	-93	unknown MAC	map
2016-06-02 14:13:11	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:47:9c	5300 (60)	-93	unknown MAC	map
2016-06-02 14:12:50	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:2c:bb	5220 (44)	-91	Known private MAC	map
2016-06-02 14:12:50	d35db8f67d590b32	OM-bezoekers	9c:1c:12:0e:2c:ba	5220 (44)	-91	Known private MAC	map
2016-06-02 14:12:50	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:2c:bc	5220 (44)	-92	Known private MAC	map
2016-06-02 14:12:47	d35db8f67d590b32	OM-bezoekers	9c:1c:12:0e:a7:fa	5220 (44)	-73	MAC at wrong channel	map
2016-06-02 14:12:47	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:a7:fb	5220 (44)	-73	MAC at wrong channel	map
2016-06-02 14:12:47	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:a7:fc	5220 (44)	-73	MAC at wrong channel	map
2016-06-02 14:12:47	d35db8f67d590b32	OM-bezoekers	6c:f3:7f:2a:57:2a	5620 (124)	-89	unknown MAC	map
2016-06-02 14:12:39	d35db8f67d590b32	OM-medewerkers	9c:1c:12:0e:af:5b	5660 (132)	-87	Known private MAC	map
2016-06-02 14:12:39	d35db8f67d590b32	OM-VPN	9c:1c:12:0e:af:5c	5660 (132)	-88	Known private MAC	map