Risk detection with a UAV

Yadvir Singh

University of Amsterdam

February 2, 2016

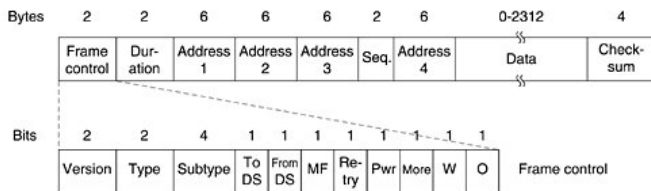Supervised by
Max Hovens & Chris Mavrakis

Introduction

- Company buildings can leak information, including WIFI traffic
- WIFI packet Partly readable
- Use Unmanned Aerial Vehicles (UAV) to capture traffic
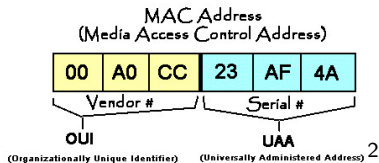
Research question

Which sensitive company info can be deduced from encrypted wireless network traffic and how effective can the use of a UAV be in capturing traffic that is not attainable using conventional WIFI sniffing methods?

802.11 frame

Bytes	2	2	6	6	6	2	6	0-2312	4
	Frame control	Dur-ation	Address 1	Address 2	Address 3	Seq.	Address 4	Data	Check-sum

Bits	2	2	4	1	1	1	1	1	1	1	
	Version	Type	Subtype	To DS	From DS	MF	Re-try	Pwr	More	W	O	Frame control

1

MAC Address
(Media Access Control Address)

00	A0	CC	23	AF	4A

Vendor #   Serial #

OUI
(Organizationally Unique Identifier)

UAA
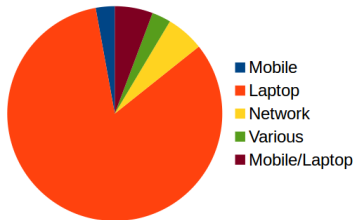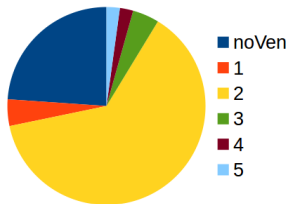(Universally Administered Address)

2

Information extraction
Unique MAC addresses

- Each device has an unique identifier
- Devices can be related to employees
  - Indication of office occupation
  - Activity across the day can be tracked, using timestamps
- Mapping is tricky

Information extraction

Device categorization

- MAC address reveals vendor
- Gives insight into vendor distribution
  - Company may prefer one particular vendor
- Vendors can be linked to device types

Legend (top pie): noVen, 1, 2, 3, 4, 5

Legend (bottom pie): Mobile, Laptop, Network, Various, Mobile/Laptop

Information extraction
Passive movement tracking

- Employees may carry their devices along them
- Devices connect to different Access points (AP)
- Movement tracked by targeting different APs
- Movement can only be tracked at a coarse-grained level

UAV

3
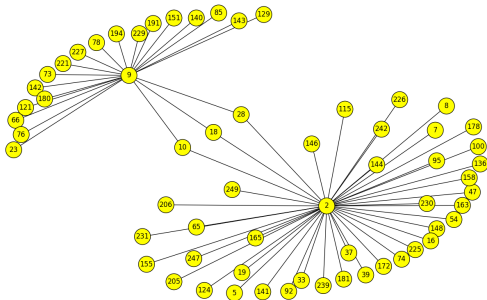
- Booming market (\$ 93 billion in coming decade)
- Often used for aerial inspection
- Different types:
    - Fixed-wing
    - Rotary-wing
    - Flappy-wing
    - Blimp / balloon

4

5

6

7

- Little resistance of regular security measures (cameras, fences)
- Urge to develop interception systems is growing
- Rules and regulations become more strict

8

Conclusion

Conclusion

Overall, different types of information can be deduced from encrypted wireless network traffic. This includes office occupation, vendor usage, coarse grained tracking and traffic flow. To capture such traffic, UAVs can be used due to their manoeuvrability and relative low detection rate. However, efforts are made to restrict the use of UAVs and interception systems are being developed.

Questions

---

[1] http://www4.ncsu.edu/ aliu3/802.bmp

[2] http://thewindowsclub.thewindowsclubco.netdna-cdn.com/wp-content/uploads/2015/04/What-is-MAC-Address.jpg

[3] guowei2014

[4] http://www.dji.com/product/phantom-3-standard

[5] http://www.tudelft.nl/actueel/dossiers/archief/delfly/

[6] https://commons.wikimedia.org/wiki/File:MetaplaneInFlight1.PNG

[7] https://www.thalesgroup.com/sites/default/files/squire/index.html

[8] http://nos.nl/artikel/2084071-hoe-voorkom-je-aanslagen-met-drones-met-een-roofvogel.html