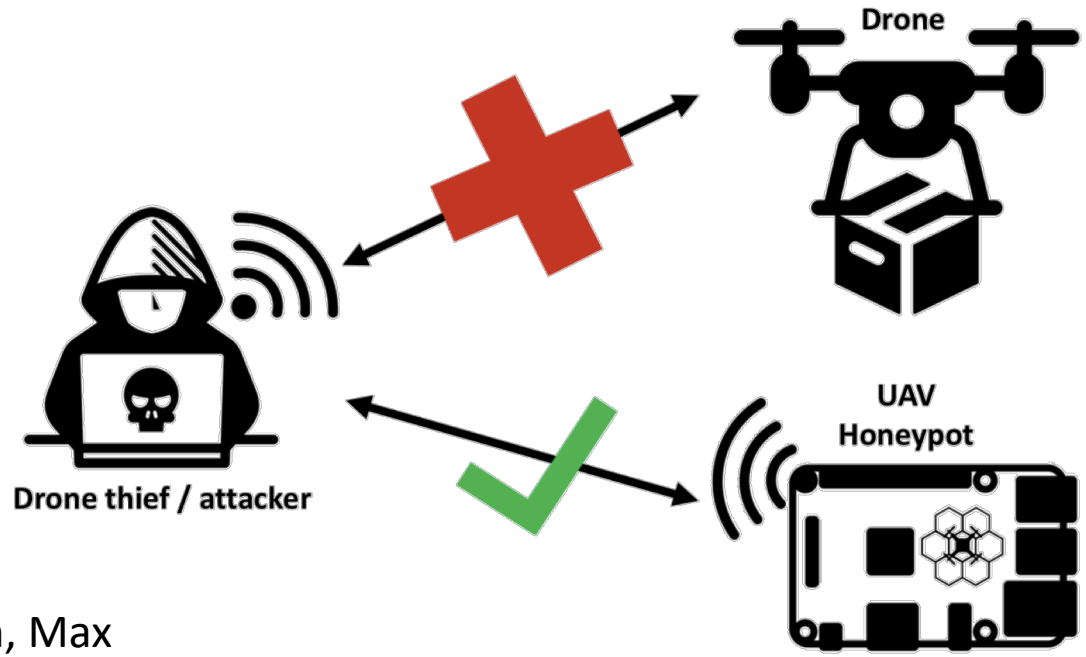
HoneyDrone: a medium-interaction Unmanned Aerial Vehicle Honeypot

DISSECT 2018



Jörg Daubert, Dhanasekar Boopalan, Max Mühlhäuser, Emmanouil Vasilomanolakis

Co-funded by the European Union

Telecooperation Lab

Drones. And why the hack they are relevant in distributed network security.

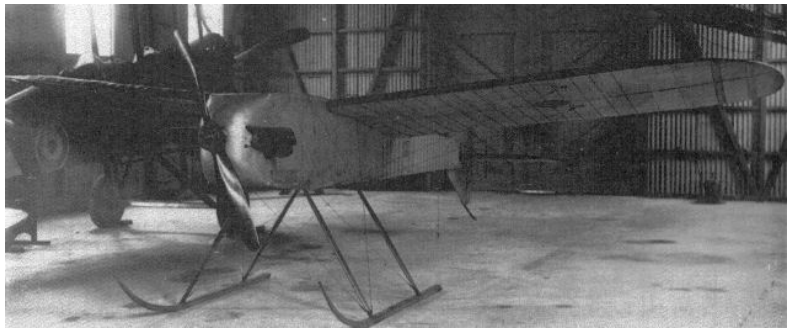
INTRODUCTION

A history of drones (1)

Military

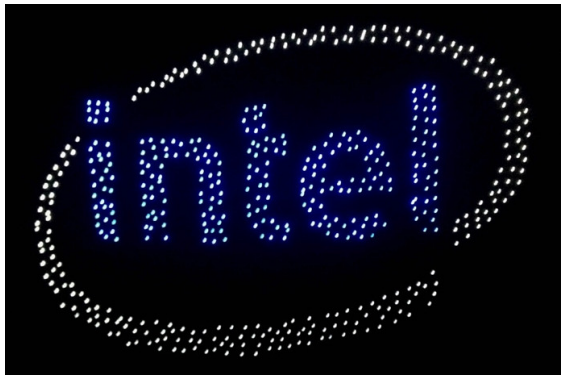
- 1849 unmanned balloons
- 1916 Areal Target (radio controlled!)

Бомбардировка с аэростата. "Воздушное торпедо" О. С. Костовича.



Civil

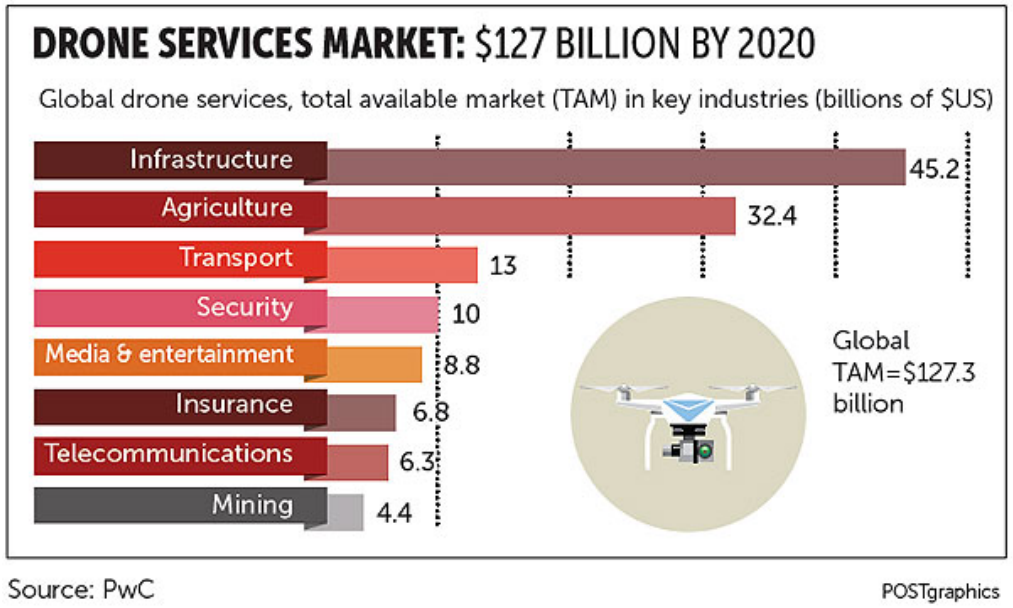
- 2006 MD4-200
- 2006 Foundation of DJI
- 2009 Foundation of 3DR
- 2013 DJI Phantom 1
- 2015 Drone Racing MultiGP & DRL
- 2016 Intel 500 Drone Light Show

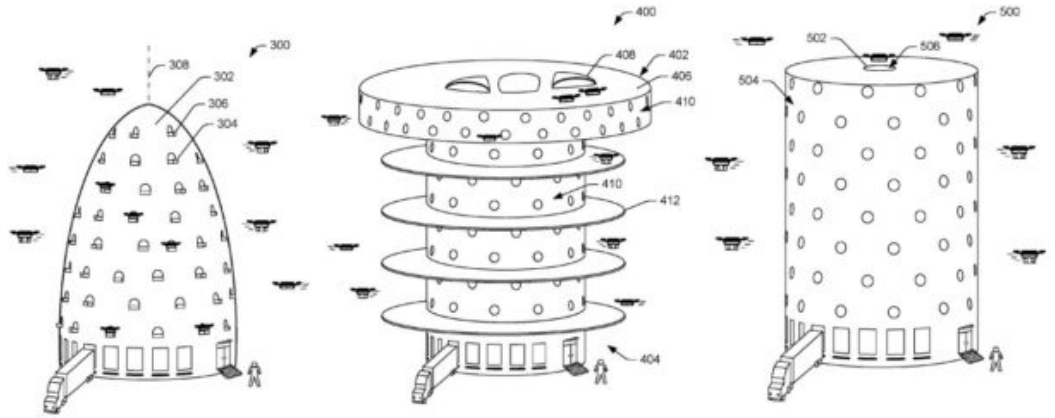


A history of drones (2)

Commercial

- Transport (package drone)
- Forest and agriculture
- Infrastructure maintenance





What we know about drones so far

TECHNISCHE UNIVERSITÄT DARMSTADT

Different types of drones—land, water, air

- Model → drone → UAV → UAS
- Focus and correct term here: **UAV / UAS**

Command & Control

- Live (radio) control
- Planned missions (with monitoring) → radio

UAS are networked systems

- Ground stations, mission control, swarms

Police UAS WEP Wi-Fi

Radio-driven devices get hacked

- 2011, SkyJack, http://samy.pl/skyjack/
- 2016, AR.Drone 2 Wifi Attack, https://github.com/markszabo/drone-hacking
- **Mayhem:** Bebop Wifi Attack, DroneJack, Bebop Dissabler, DeviationTX NRF24L01 Hijack, ICARUS, **Nils Rodday Attack**, Drone Duel, Fb1h2s Maldrone, Aaron Luo DJI Phantom 3 hijack, Voidsec Hacking DJI Phantom 3, DJI Spark hijacking, Sololink Hack, Drone Hijacking by Arthur Garipov, […]

Telecooperation Lab

CYSEC

How to stop these attacks?

TECHNISCHE UNIVERSITÄT DARMSTADT

Make drones more secure?

- Doh! See attack history.

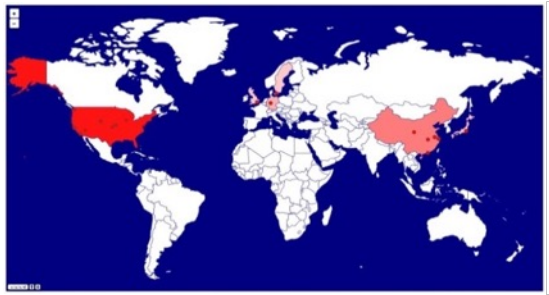
Intrusion Detection Systems (IDS)?

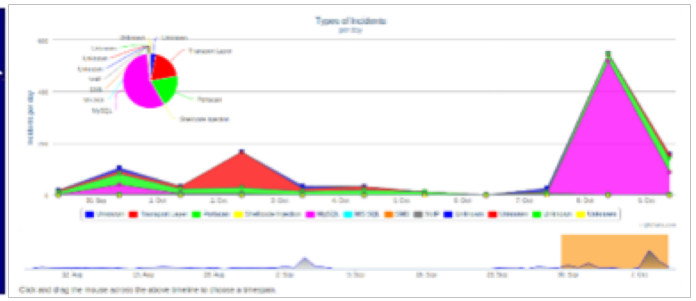
- Where to put?

Honeypots?

Our track record

- TraCINg





- HosTaGe

Telecooperation Lab

CYSEC

Very short.

BACKGROUND

Drone Radio – Protocols

Drone	Network	Application
MicroDrone MD4-200, …	2G, 3G, ?	?
Parrot AR.Drone 2, Bebop 2, Rolling Spider	**IEEE 802.11** Bluetooth	FTP, Telnet, SSH, **MAVLink**
3DR Iris, Solo	**IEEE 802.11**	**MAVLink**
DJI Phantom 3,4, …	**IEEE 802.11** LightBridge	Telnet, FTP, SSH
Globe UAV Copter 7, 8	LTE	?
Others	**IEEE 802.11** IEEE 802.15 SiK Radio (433 MHz, …)	**MAVLink** UAVCAN ?

Wi-Fi—drone specific: vendor BSSID, predefined ESSIDs, IPs, predefined security MAVLink

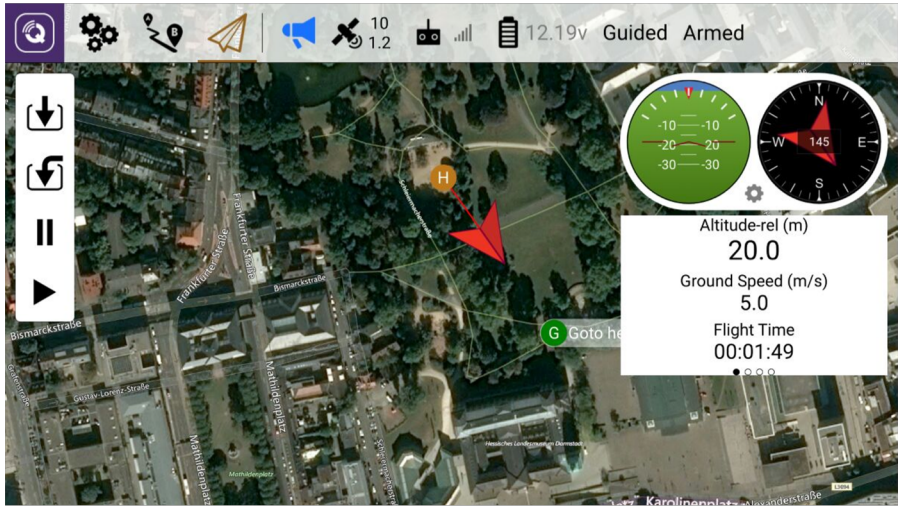
Some MAVLink Background

MAVLINK
MICRO AIR VEHICLE COMMUNICATION PROTOCOL

- Marshalling / serialization library
- Low overhead (8 Byte / packet)
- Over various transport protocols (UART, UDP, TCP)
- Grew over time: now version 2, point-2-point, multicast, pub/sub, CRC, delivery guarantees

Message example:

```
<message id="150" name="RUDDER_RAW">
  <description>...</description>
  <field type="uint16_t" name="position">...</field>
  <field type="uint8_t" name="port_limit">...</field>
  [...]
</message>
```

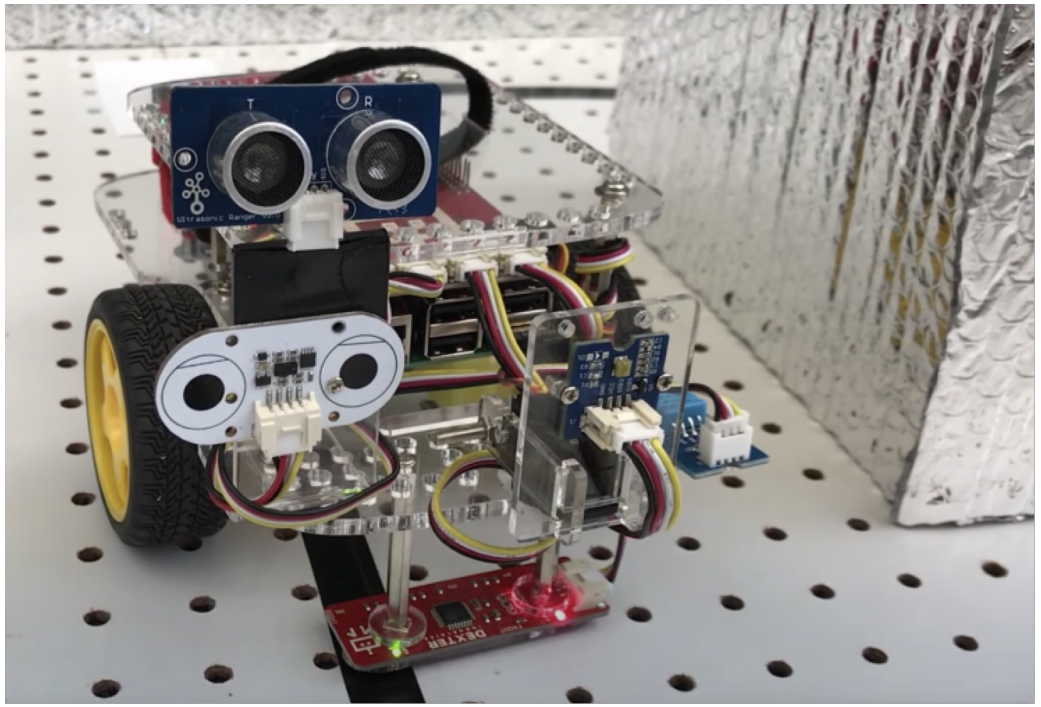


Related Work

- Heralding (credentials)
- Kippo (SSH)
- Kojoney2 (SSH)
- Cowrie (SSH, Telnet)
- HosTaGe (mobile)
- HoneyPy (Web, Telnet, TFTP, SIP, …)
- HoneyWRT (Telnet, VNC, RDP, …)
- Bluepot
- […]

No MAVLink! Hardly Wi-Fi specific.

- HoneyBot, http://www.rh.gatech.edu/news/604462/robot-designed-defend-factories-against-cyberthreats



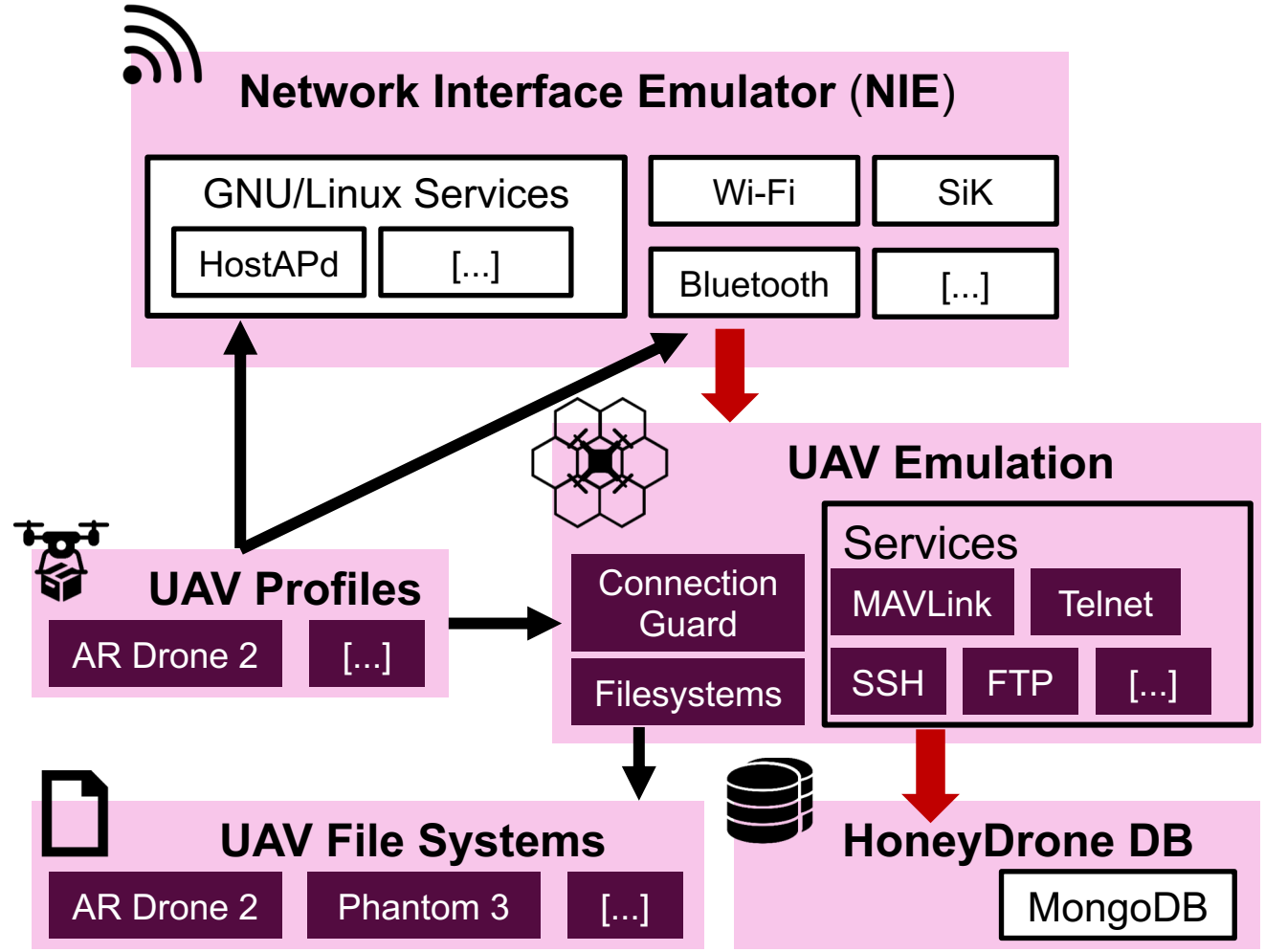
Some background and how it works.

HONEYDRONE

HoneyDrone Design

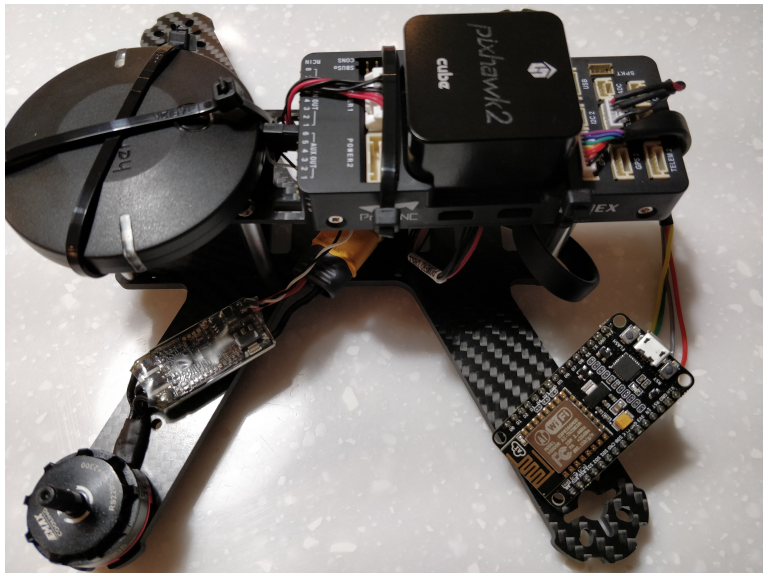
More software

- Python
- Twisted framework
- PyMAVLink (+ MAVLink)
- PyMongo
- MAVProxy
- Arducopter (+ SITL)



HoneyDrone Capabilities

- Low power (3-5 Watt)
- Portable (a UAV can carry HoneyDrone)
- Can lure attacks away from real UAVs
- (Uses the same Wi-Fi as the SkyJack attack)
- Emulate
  - AR.Drone 2
  - Custom UAVs

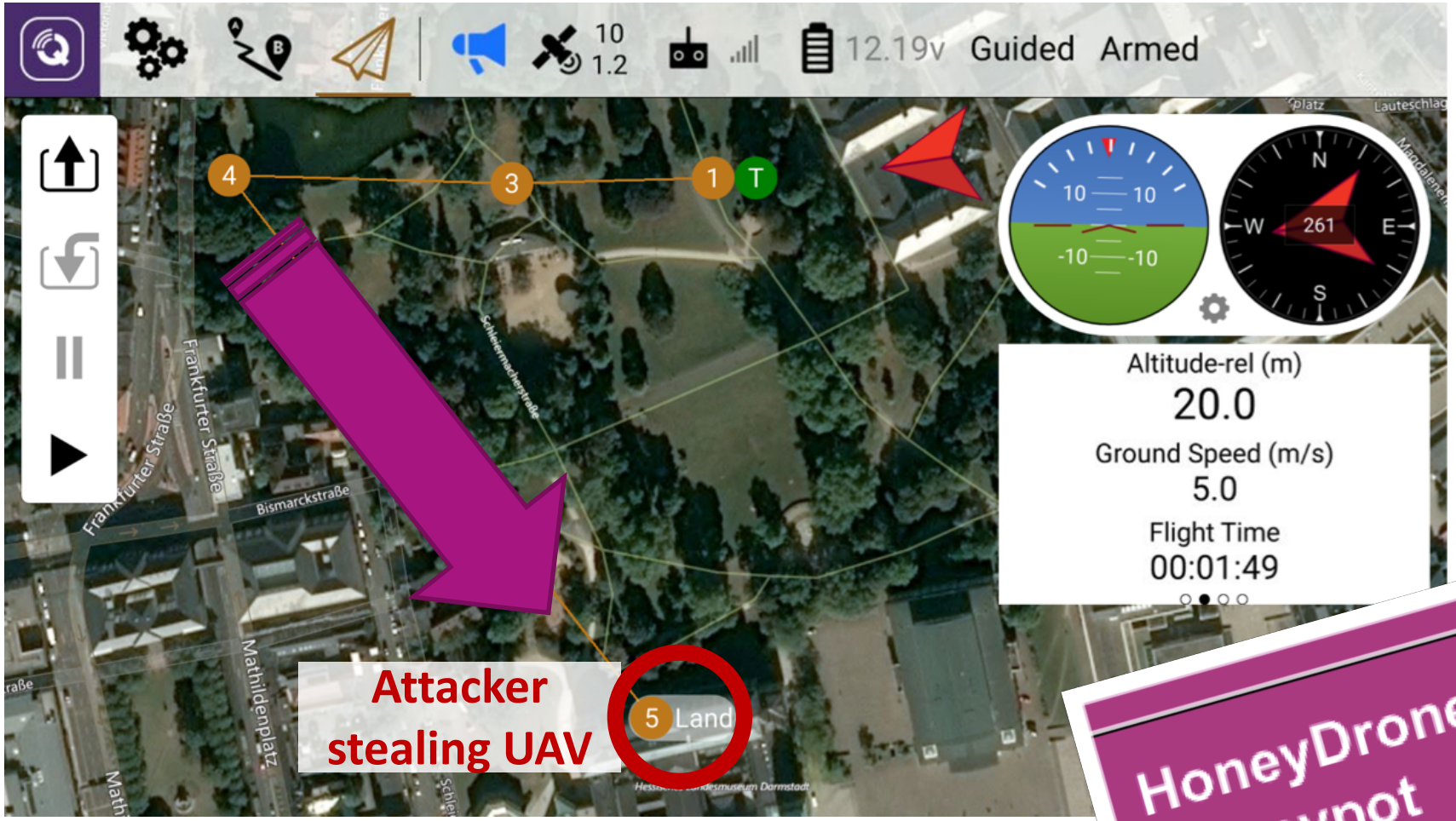


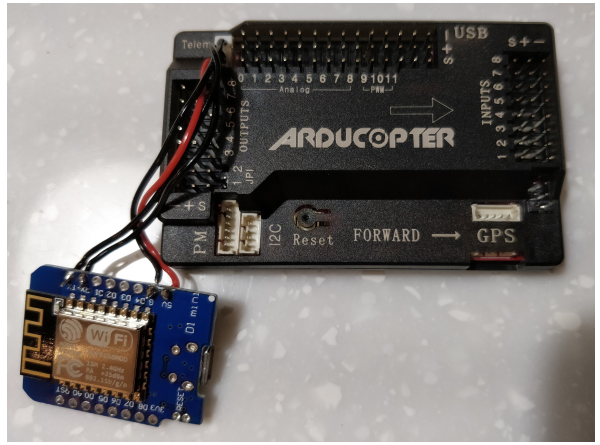
Brief Evaluation (1): Telnet AR.Drone 2.0

```
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.


BusyBox v1.14.0 () built-in shell (ash)
Enter 'help' for a list of built-in commands.

# ls -l
drwxrwxr-x    4 root     root          5688 Jan  1  1970 bin
drwxr-xr-x    4 root     root          1016 Jan  1  2000 data
drwxrwxrwt    4 root     root          3660 Jan  1  2000 dev
drwxrwxr-x    3 root     root          1256 Jan  1  1970 etc
drwxr-xr-x    2 root     root          1064 Jan  1  2000 factory
drwxr-xr-x    3 root     root           536 Jan  1  2000 firmware
drwxrwxr-x    3 root     root           224 Jan  1  1970 home
drwxr-xr-x    5 root     root          2800 Jan  1  1970 lib
drwxrwxr-x    2 root     root           240 Jan  1  1970 licenses
drwxrwxr-x    2 root     root           160 Jan  1  1970 mnt
dr-xr-xr-x   77 root     root             0 Jan  1  1970 proc
drwxrwxr-x    2 root     root           160 Jan  1  1970 root
drwxrwxr-x    2 root     root          2752 Jan  1  1970 sbin
drwxr-xr-x   12 root     root             0 Jan  1  1970 sys
drwxrwxrwt    3 root     root           200 Jan  1  2000 tmp
drwxr-xr-x    2 root     root           232 Jan  1  2000 update
drwxrwxr-x    8 root     root           544 Jan  1  1970 usr
drwxrwxr-x    2 root     root           352 Jan  1  1970 var
#
```

```
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.


BusyBox v1.14.0 () built-in shell (ash)
Enter "help" for a list of built-in commands

# ls -l
drwxr-xr-x 1 root root 4096 2017-12-19 16:04 bin
drwxr-xr-x 1 root root 4096 2017-12-19 16:03 data
drwxr-xr-x 1 root root 4096 2017-12-19 16:01 dev
drwxr-xr-x 1 root root 4096 2017-12-19 16:04 etc
drwxr-xr-x 1 root root 4096 2017-12-19 16:04 factory
drwxr-xr-x 1 root root 4096 2017-12-19 16:05 firmware
drwxr-xr-x 1 root root 4096 2017-12-19 16:01 home
drwxr-xr-x 1 root root 4096 2017-12-19 16:04 lib
drwxr-xr-x 1 root root 4096 2017-12-19 16:04 licenses
drwxr-xr-x 1 root root 4096 2017-12-19 16:01 mnt
drwxr-xr-x 1 root root 4096 2017-12-19 16:04 proc
drwxr-xr-x 1 root root 4096 2017-12-19 16:02 root
drwxr-xr-x 1 root root 4096 2017-12-19 16:05 sbin
drwxr-xr-x 1 root root 4096 2017-12-19 16:01 sys
drwxr-xr-x 1 root root 4096 2017-12-19 16:03 tmp
drwxr-xr-x 1 root root 4096 2017-12-19 16:02 update
drwxr-xr-x 1 root root 4096 2017-12-19 16:01 usr
drwxr-xr-x 1 root root 4096 2017-12-19 16:04 var
# rm -r bin
Deleted /bin
#
```

Brief Evaluation (2): MAVLink Pixhawk





HoneyDrone: a medium-interaction
Honeypot

Conclusion

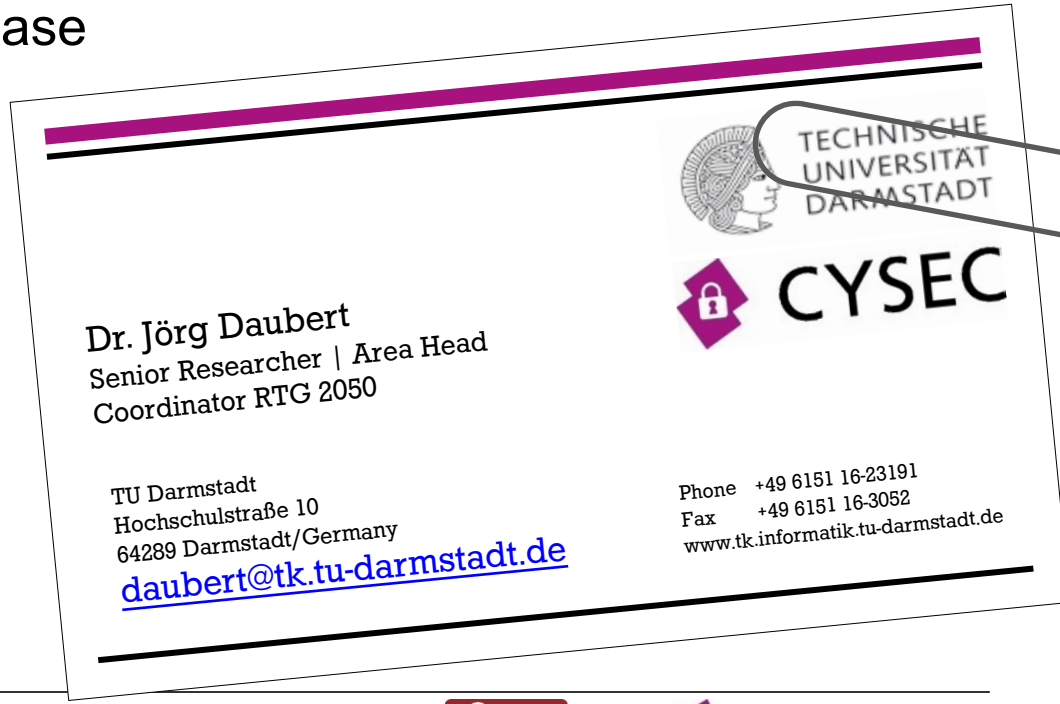
Summary

- Commercial drones besides recreational ones
- 1st honeypot for drones / UAVs
- 1st honeypot to support MAVLink
- Focus on emulating drone Wi-Fi
  - Profile support for common drones
  - Filesystems of drones
- Can emulate a real flight controller

Demo session on Wednesday

Next

- Support more radios
- Multiple instances
- release



Telecooperation Lab

CYSEC