Losing the Car Keys

Wireless PHY-Layer Insecurity in EV Charging

Richard Baker and Ivan Martinovic

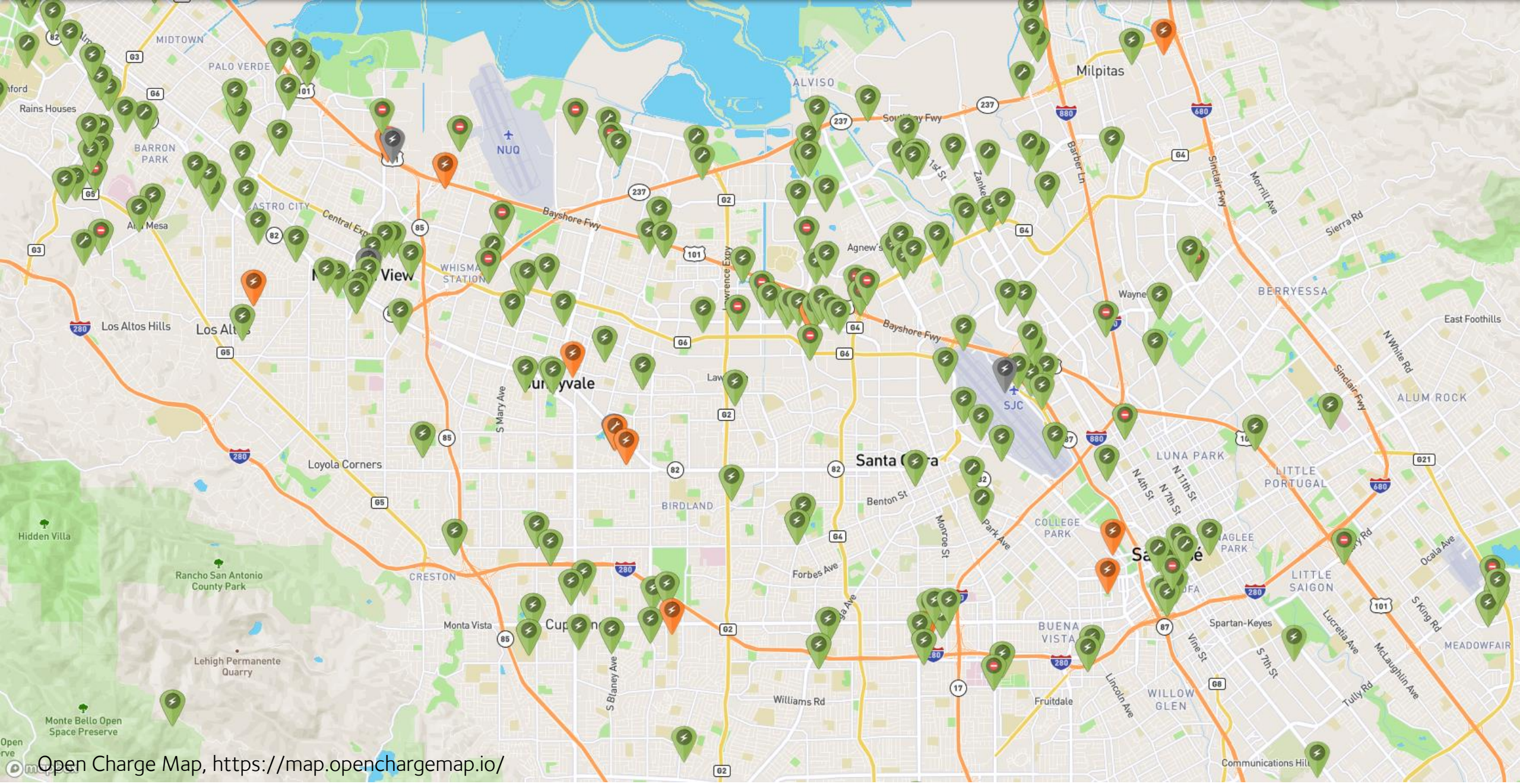
14th August 2019

USENIX Security Symposium

UNIVERSITY OF OXFORD

CENTRE FOR DOCTORAL TRAINING *in* CYBER SECURITY

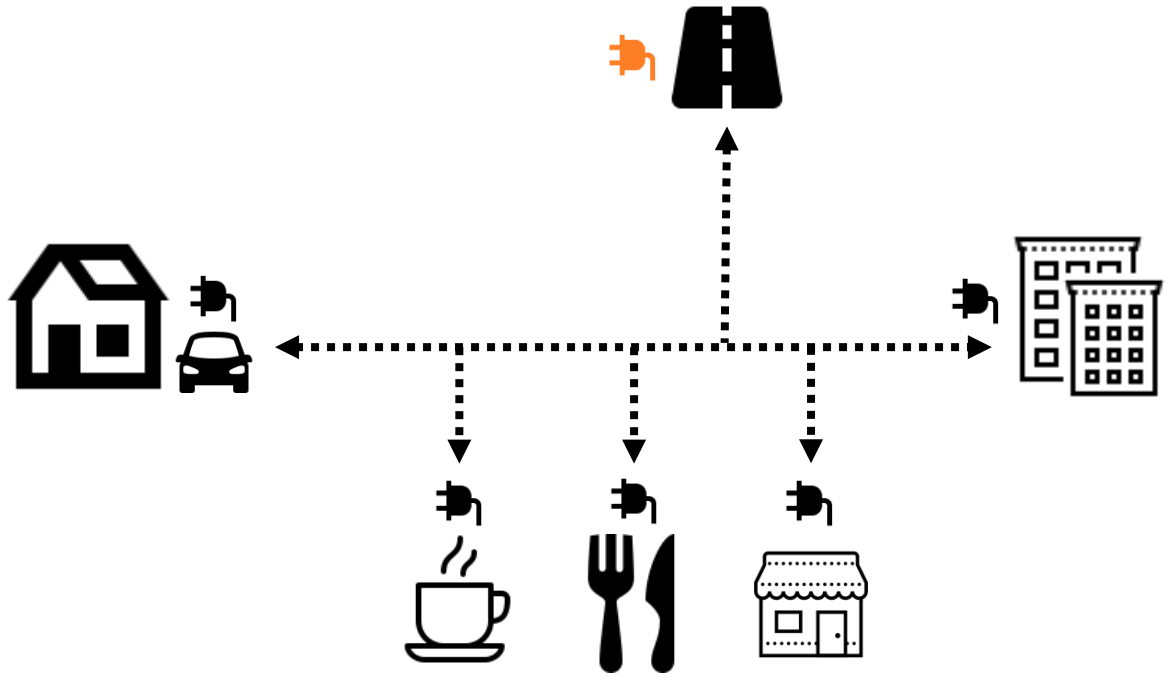
EPSRC
Engineering and Physical Sciences Research Council



Open Charge Map, https://map.openchargemap.io/

Charging everywhere

- Power is only one part of the story
- Deeper integration of charging
  - Reactive charging
  - Vehicle-to-grid
  - Automatic billing (“plug-and-charge”)
  - Additional services on top
- All underpinned by communication
- Secure it early
  - Public/Widespread/Expensive to change
  - Previous work has found serious vulnerabilities in earlier chargers [1,2]



[1] Achim Friedland. Security and privacy in the current e-mobility charging infrastructure, 2016
[2] Matthias Dalheimer, “Ladeinfrastruktur fr elektroautos: Ausbau statt sicherheit“, 2017

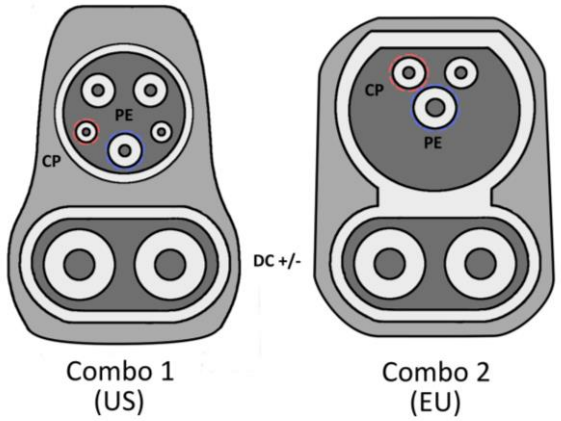

smoov
smoov
smoov
Shell
Recharge
CHAdeMO
50kw DC
CCS
50kw DC
AC
43kw AC
DANGER

Four major DC standards

CCS

EU/US cars

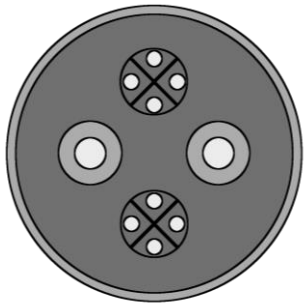
PLC comms. + IP stack



CHAdeMO

Japanese cars

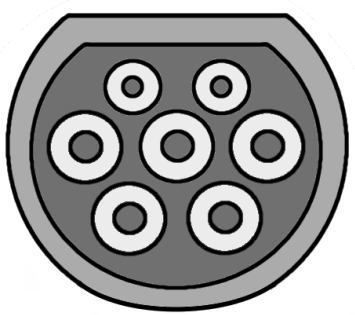
CAN-Bus comms.



Supercharger

Tesla cars

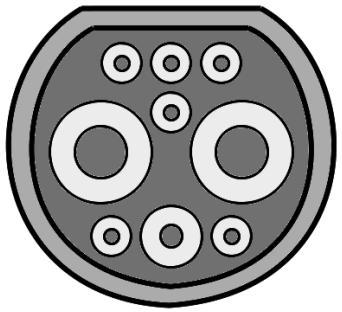
CAN-Bus comms.



GB/T 20234

Chinese cars

CAN-Bus comms.

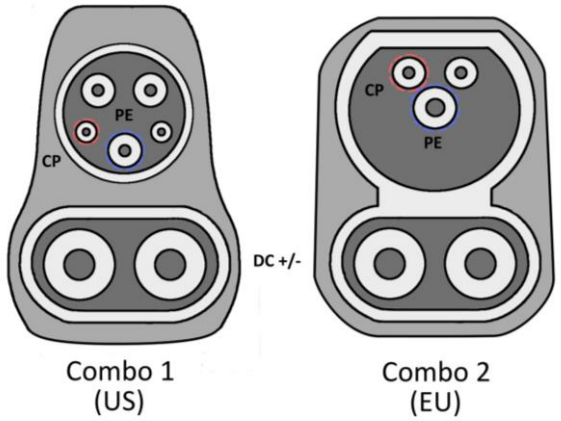


Four major DC standards

CCS

EU/US cars

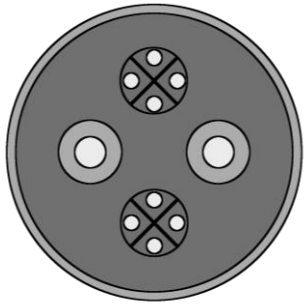
PLC comms. + IP stack



CHAdeMO

Japanese cars

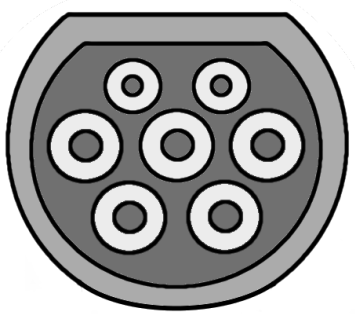
CAN-Bus comms.



Supercharger

Tesla cars

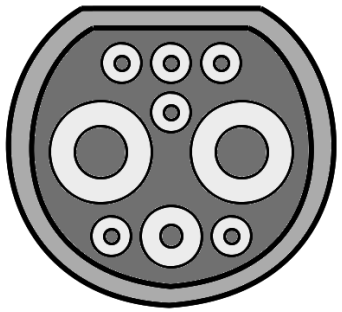
CAN-Bus comms.



GB/T 20234

Chinese cars

CAN-Bus comms.



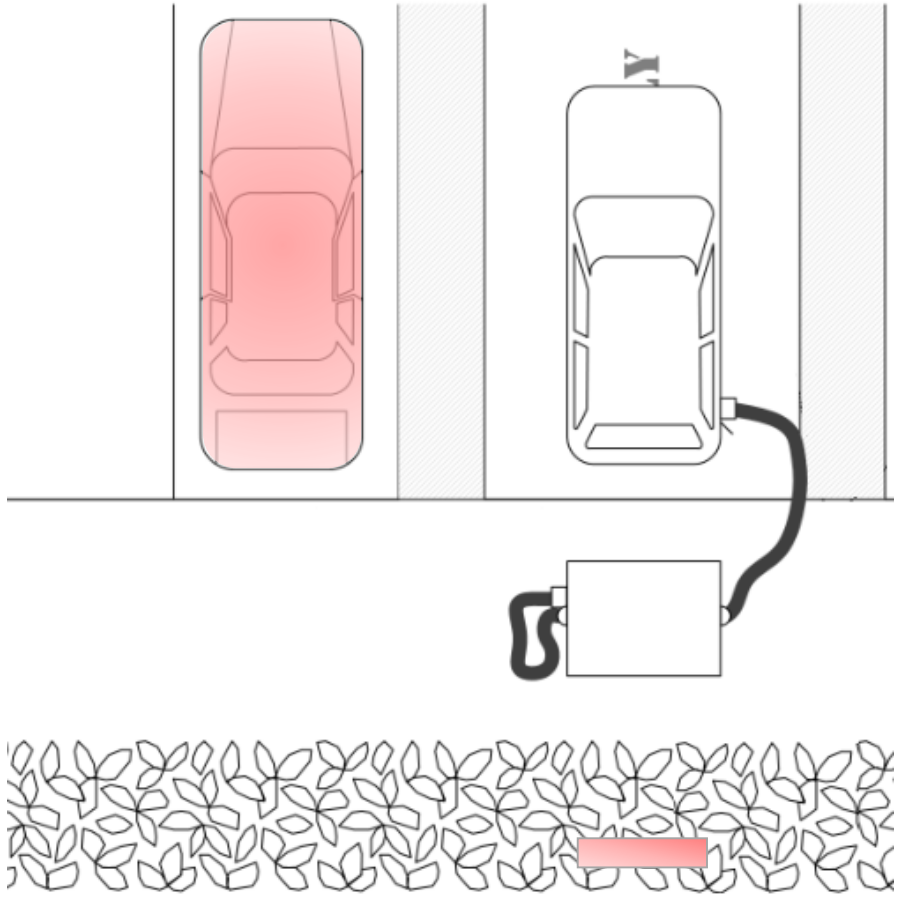
Combined Charging System (CCS)

- Adapts a domestic PLC LAN technology for a new use
  - Shared-key private network model vs. public use case
  - Known to leak signal
- Supported by 7 of the top 10 car manufacturers worldwide [1]
  - About 7,500 chargers in Europe [2]
- Underpinned by DIN 70121 (CCS 1.0) and ISO 15118 (CCS 2.0)
  - Specs differ in support for advanced features
  - Specs match at a physical communications level

[1] OICA Production Rankings
[2] http://ccs-map.eu/

Threat model

- Passive eavesdropping
- Wireless, despite wired system
  - no modification to vehicle, cable or charger
  - deniable as attack behaviour
- Located nearby, either:
  - …in-person : waiting nearby and monitoring live
  - …with planted device : collecting data for upload or later retrieval



Why would someone do this?

- Track people using vehicle MAC address
  - Location privacy
  - Monitor when homeowner leaves
  - Detect specific makes/models
- Observe traffic on platform
  - Internet access as a service, Third-party apps
  - Others have reported SSH, Web management consoles, Telnet available on chargers [1]
- AutoCharge
  - Manufacturer-specific system for automated billing
  - Available at 90 locations across three European countries
  - Users associate vehicle MAC with their account and are billed automatically

[1] Dudek et al., "V2G Injector: Whispering to cars and charging units through the Power-Line", SSTIC2019

Experimental campaign

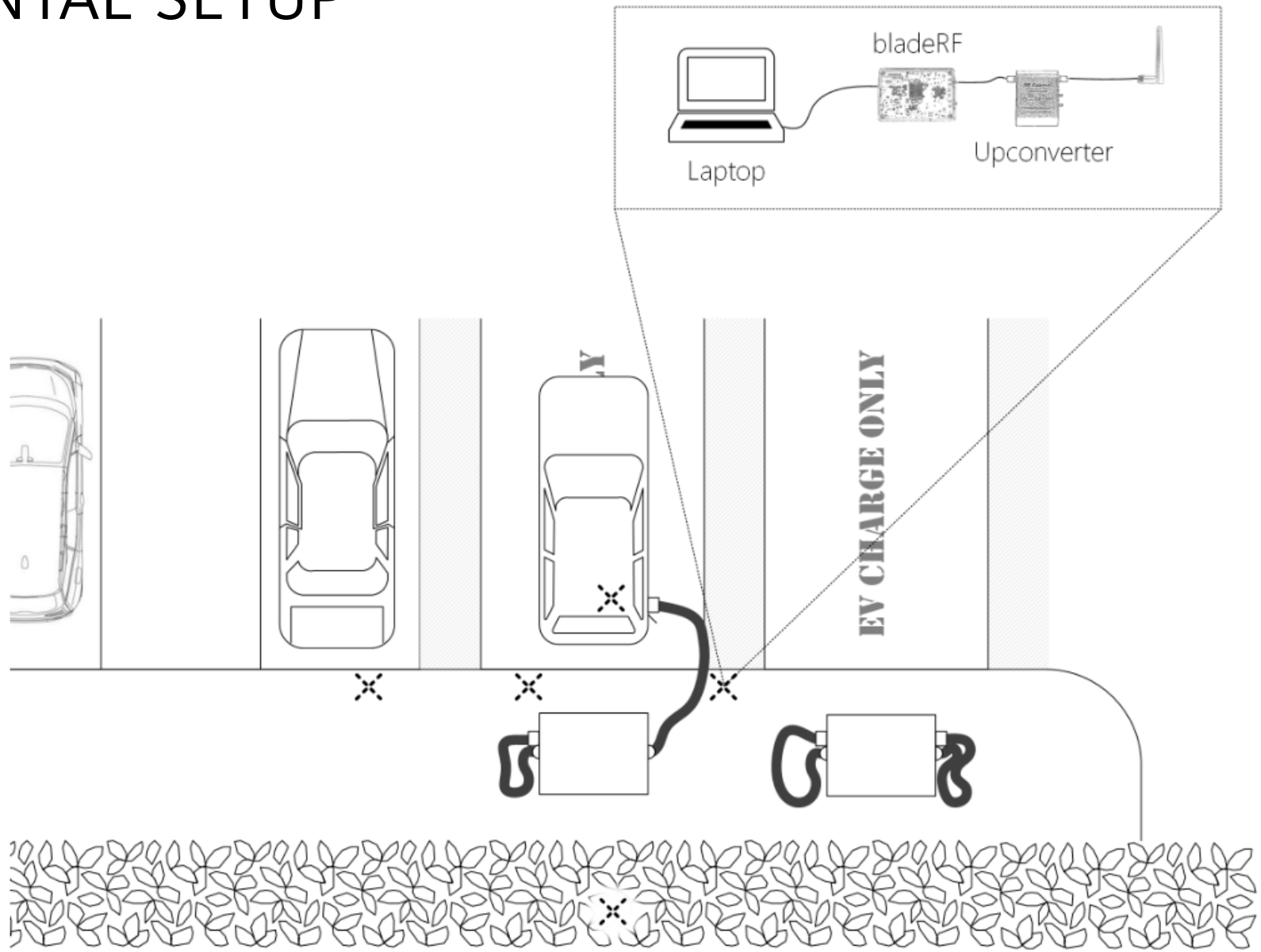
- Three vehicles
  - All vehicles DIN 70121
- 800 miles of driving
- 14 locations, 6 charging networks
  - Service stations
  - Highway rest stops
  - Superstores
  - Hotels
- 54 unique charging sessions

BMW i3

Jaguar I-PACE

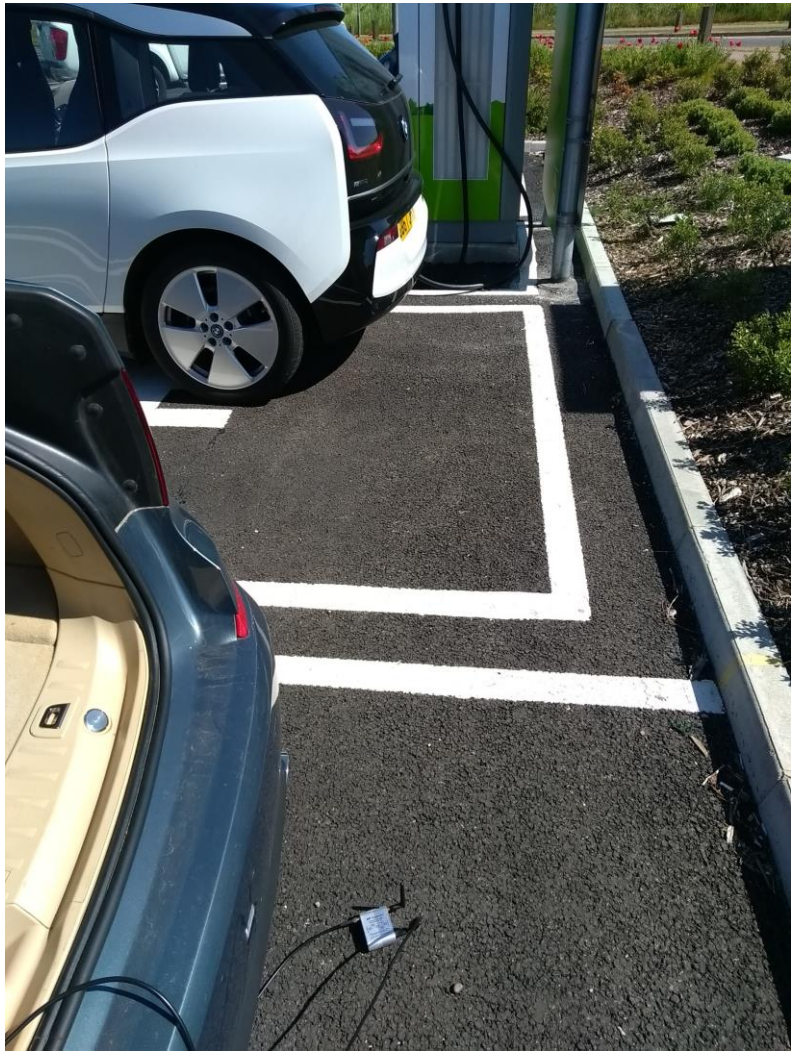
VW e-Golf

EXPERIMENTAL SETUP



Close-range

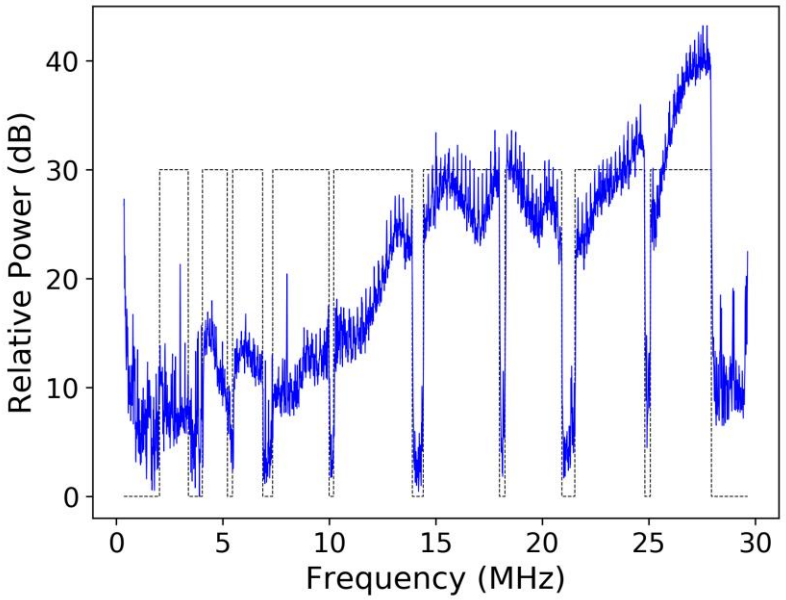
Further away



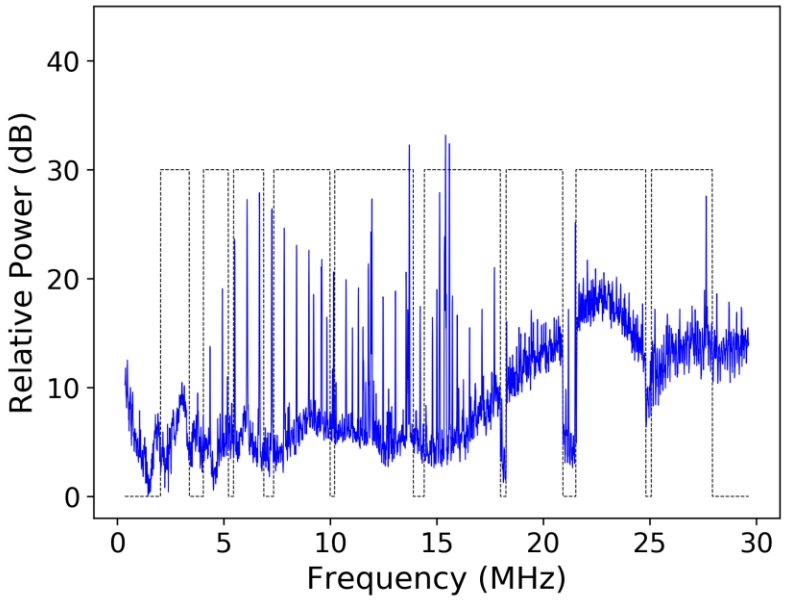
Multiple vehicles at once

Emissions at every site

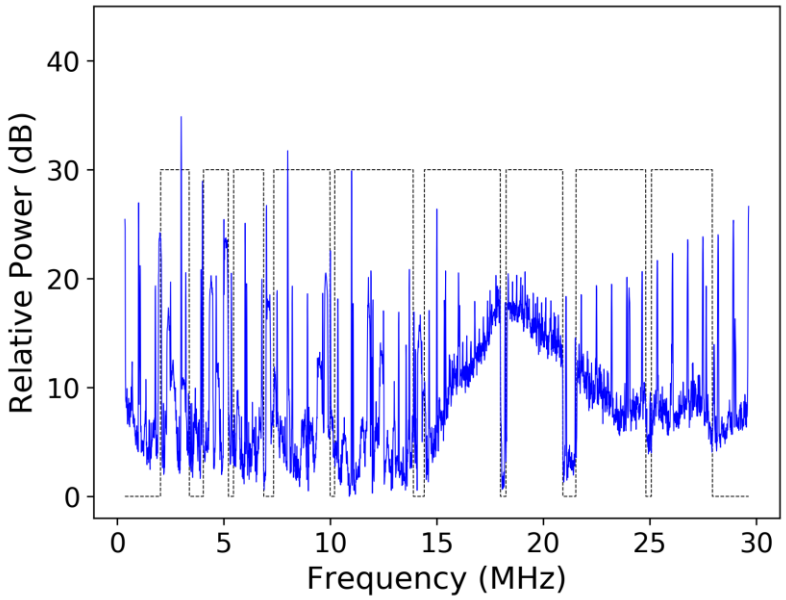
By charging cable



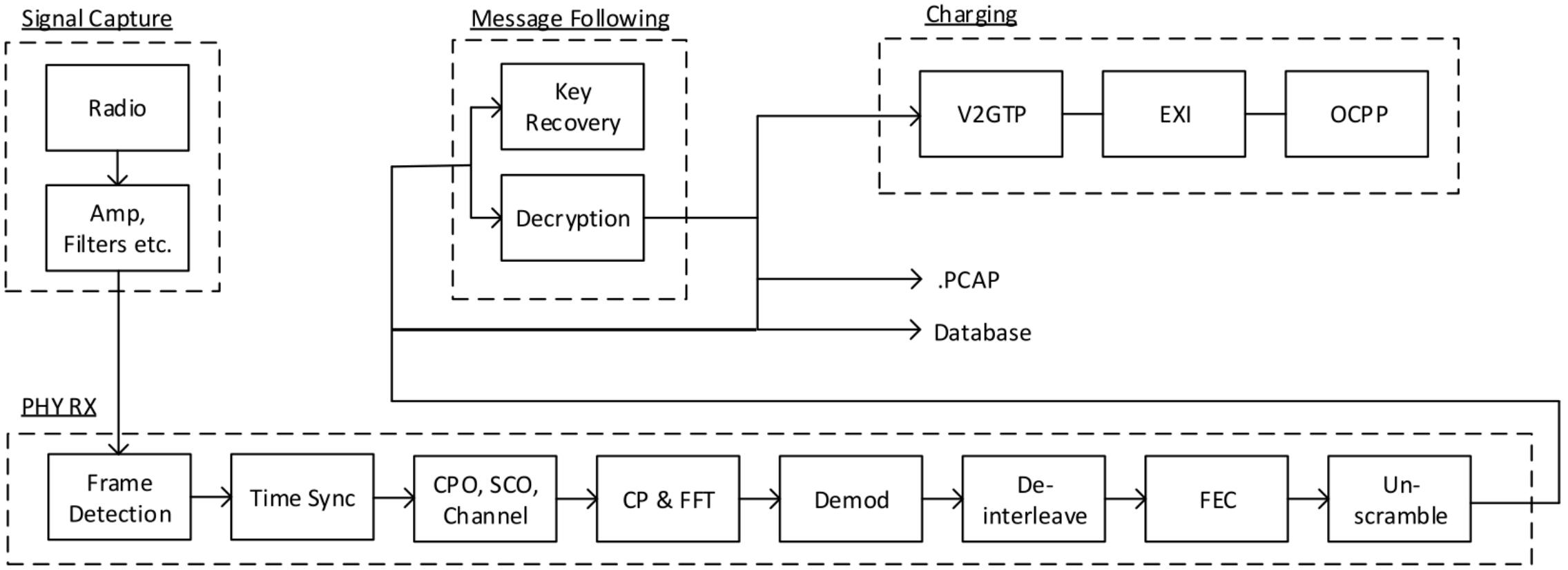
Bay behind



Bay next door



EAVESDROPPING TOOL



Available at: `https://gitlab.com/rbaker/hpgp-emis-rx`

Message recovery

- Counted total packets
- Tested message CRC32 checksums

- Performance varied widely
  - Differences site-to-site
  - Differences run-to-run
- Closer is better
- Far from an optimal setup

Site	Antenna	Peak SNR (dB)	BW (MHz)	Total PPDUs	Data PPDUs	Bi-direc.?	Start?	RX% Mean	CRC32% Min	CRC32% Mean	CRC32% Max
A	In car	15	6	526	272	✓		99.3	1.1	1.8	3.3
B	In car	18	12	1063	567	✓		29.8	0.5	3.3	5.3
C	In car	25	14	2976	1819	✓		99.9	46.6	48.1	50.3
D	In car	10	12	556	293	✓		88.2	1.4	2.3	3.0
E	In car	9	4.5	569	306			100	11.0	11.1	11.2
F	In car	21	12	3660	2009	✓	✓	99.3	27.8	36.8	45.8
	Bay behind	15	8	1434	1430	✓		99.3	**43.5**	43.5	**43.5**
	Outside car	10	10	12987	8255	✓		76.2	34.9	46.6	89.5
	Two cars	14	11	2449	2274			99.1	**24.3**	47.5	70.8
G	In car	19	12	5837	3670	✓	✓	99.0	51.1	60.3	71.4
	Next bay	15	13	4157	2749	✓		99.7	**91.8**	91.8	**91.8**
	By cable	29	23	23984	17246	✓	✓	80.2	52.9	74.0	**99.8**
H	In car	16	12.5	15052	9362	✓		99.2	69.9	71.0	72.8
	Outside car	20	11	16243	10407	✓		99.5	27.7	61.6	**80.6**
	By cable	35	25	19535	14717	✓	✓	92.1	**34.2**	70.0	92.8
	Two cars	15	12	24121	21006			99.6	42.2	71.9	**94.8**
I	In car	20	12	1501	1193	✓	✓	98.0	94.8	97.4	**100.0**
J	In car	20	7	14231	10291	✓	✓	81.0	1.0	33.6	67.9
	Outside car	23	7	1084	935	✓	✓	96.0	49.2	49.2	49.2
K	In car	8	5	1971	1278	✓		92.5	**0.0**†	22.0	38.3
L	Outside car	8	7	3004	1849		✓	25.8	**0.0**	0.0	0.0
M	In car	20	12	13631	9743	✓	✓	98.8	42.4	64.9	82.5
N	In car	24	14	4317	3364	✓	✓	68.3	**0.0**†	44.5	72.6

Values in session startup

- Vehicle MAC
  - Unique per-vehicle
  - Observed stable over 3 months
  - In some cases derivable from other traffic too
- 'NMK' master key
  - Delivered in plaintext, according to standard

	sessionname	filenum	key	hex(val)
1	Dover-ByCable-20180626-PPDUs/file92_882_0.674888...	882	MM_CM_SLAC_Parm_Req.sectype	00
2	Dover-ByCable-20180626-PPDUs/file92_882_0.674888...	882	MM_CM_SLAC_Parm_Req.runid	000792E40051801C
3	Dover-ByCable-20180626-PPDUs/file92_884_0.675775...	884	MM_CM_SLAC_Parm_Cnf.sectype	00
4	Dover-ByCable-20180626-PPDUs/file92_884_0.675775...	884	MM_CM_SLAC_Parm_Cnf.runid	000792E40051801C
5	Dover-ByCable-20180626-PPDUs/file92_884_0.675775...	884	MM_CM_SLAC_Parm_Cnf.ciphersuite	0000
6	Dover-ByCable-20180626-PPDUs/file92_959_0.715344...	959	MM_CM_SLAC_Match.sectype	00
7	Dover-ByCable-20180626-PPDUs/file92_959_0.715344...	959	MM_CM_SLAC_Match.pevmac	F07F0C[redacted]
8	Dover-ByCable-20180626-PPDUs/file92_959_0.715344...	959	MM_CM_SLAC_Match.evsemac	D88039[redacted]
9	Dover-ByCable-20180626-PPDUs/file92_959_0.715344...	959	MM_CM_SLAC_Match.nid	85E10050319D0D00
10	Dover-ByCable-20180626-PPDUs/file92_959_0.715344...	959	MM_CM_SLAC_Match.nmk	1CBE4C23C65A3C3F26121D6D2138751A

PHY TRAFFIC RECOVERY

No.	Time	Source	Destination	Protocol	Length	Info
25	77.1942958	Leopold	Devolo_	HomePlug AV	433	MAC Management, Get Key Request
26	79.500895	Devolo_	Leopold	HomePlug AV	506	MAC Management, Unknown 0x6006
27	79.501734	Devolo_	Leopold	HomePlug AV	435	MAC Management, Get Key Confirmation
28	118.1830795	Devolo_	Leopold	HomePlug AV	60	MAC Management, Unknown 0x6063
29	122.1872735	::	ff02::1	ICMPv6	78	Neighbor Solicitation for fe80::f27f:cff:
30	133.1439733	Leopold	Devolo_	HomePlug AV	60	MAC Management, Unknown 0x6062
31	134.1362364	Devolo_	Broadcast	HomePlug AV	60	MAC Management, Unknown 0x3a
32	-138.974823	fe80::f27f:cff:fe02…	ff02::1	UDP	72	60221 → 15118 Len=10
33	140.1824598	fe80::da80:39ff:fee…	fe80::f27f:cff:fe02…	UDP	90	15118 → 60221 Len=28
34	141.1833232	fe80::f27f:cff:fe02…	ff02::1:ffea:8438	ICMPv6	86	Neighbor Solicitation for fe80::da80:39ff: from f0:7f:0c:
35	-142.1037701	fe80::da80:39ff:fee…	fe80::f27f:cff:fe02…	ICMPv6	86	Neighbor Advertisement fe80::da80:39ff: (sol, ovr) is at d8:80:39:
36	144.1754837	fe80::f27f:cff:fe02…	fe80::da80:39ff:fee…	TCP	78	54164 → 53537 [SYN] Seq=0 Win=3232 Len=0 MSS=1432
37	145.1412059	fe80::f27f:cff:fe02…	fe80::da80:39ff:fee…	TCP	74	54164 → 53537 [ACK] Seq=1 Ack=1 Win=3232 Len=0
38	146.820918	fe80::da80:39ff:fee…	fe80::f27f:cff:fe02…	TCP	78	53537 → 54164 [SYN, ACK] Seq=0 Ack=1 Win=2920 Len=0 MSS=1440
39	-147.1023997	fe80::f27f:cff:fe02…	fe80::da80:39ff:fee…	TCP	116	54164 → 53537 [PSH, ACK] Seq=1 Ack=1 Win=3232 Len=42
40	149.1017369	fe80::f27f:cff:fe02…	fe80::da80:39ff:fee…	TCP	74	[TCP ACKed unseen segment] 54164 → 53537 [ACK] Seq=43 Ack=13 Win=3114 Len=0
41	149.946826	fe80::da80:39ff:fee…	fe80::f27f:cff:fe02…	TCP	86	[TCP Spurious Retransmission] 53537 → 54164 [PSH, ACK] Seq=1 Ack=43 Win=2878 Len=12
42	151.169177	fe80::f27f:cff:fe02…	fe80::da80:39ff:fee…	TCP	97	54164 → 53537 [PSH, ACK] Seq=43 Ack=13 Win=3232 Len=23
43	151.586766	fe80::f27f:cff:fe02…	fe80::da80:39ff:fee…	TCP	74	[TCP ACKed unseen segment] 54164 → 53537 [ACK] Seq=66 Ack=37 Win=3232 Len=0
44	154.793437	fe80::da80:39ff:fee…	fe80::f27f:cff:fe02…	TCP	98	[TCP Spurious Retransmission] 53537 → 54164 [PSH, ACK] Seq=13 Ack=66 Win=2855 Len=24
45	155.454001	fe80::f27f:cff:fe02…	fe80::da80:39ff:fee…	TCP	98	54164 → 53537 [PSH, ACK] Seq=66 Ack=37 Win=3232 Len=24
46	155.489335	fe80::f27f:cff:fe02…	fe80::da80:39ff:fee…	TCP	74	[TCP ACKed unseen segment] 54164 → 53537 [ACK] Seq=90 Ack=64 Win=3232 Len=0
47	157.1630163	fe80::da80:39ff:fee…	fe80::f27f:cff:fe02…	TCP	101	[TCP Spurious Retransmission] 53537 → 54164 [PSH, ACK] Seq=37 Ack=90 Win=2831 Len=27
48	159.1462902	fe80::f27f:cff:fe02…	fe80::da80:39ff:fee…	TCP	98	54164 → 53537 [PSH, ACK] Seq=90 Ack=64 Win=3232 Len=24
49	-159.640024	fe80::f27f:cff:fe02…	fe80::da80:39ff:fee…	TCP	74	[TCP ACKed unseen segment] 54164 → 53537 [ACK] Seq=114 Ack=86 Win=3232 Len=0

…

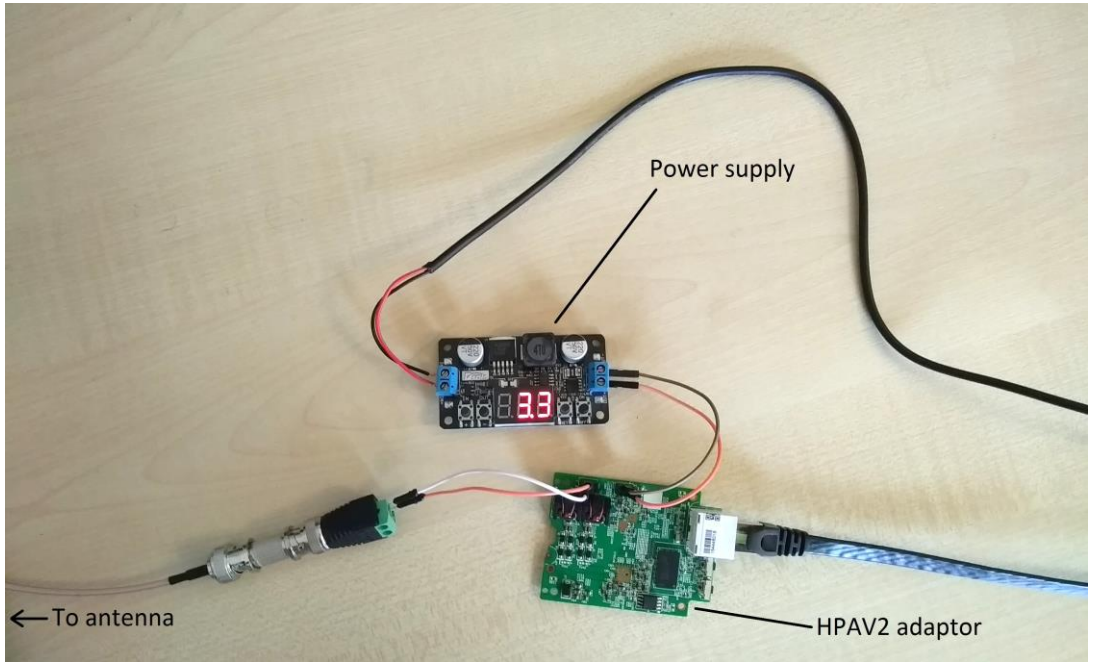
What about other encryption?

- None in DIN 70121
  - Standard limits traffic to only charging control
- ISO 15118 includes complex security model
  - Purpose-built charging PKI
  - TLS mandatory for many use cases (inc. automated payment)
- No universal security provision
  - TLS usage varies by services, payment options and environment
  - Security measures for additional “value-added services” are out of scope [1]
  - Can just build additional services on the IP link

[1] ISO 15118-2, V2G2-638

Can it be done with cheap equipment?

- Our SDR setup was ~$1000 and very slow
- Some chipsets support a “Sniffer Mode”
  - Use a chipset that supports EV messages
  - A bit of hardware modification to connect an antenna
- Have successfully captured in-home PLC traffic at short range
- Cost ~$35



Conclusions

- Wireless threat model for a wired system
- Security model is case-by-case
  - Hard to predict all the use cases – rabid competition to be first
- Available persistent unique identifiers

- Informed all 7 tested manufacturers (received 3 responses)

- Future work on active attacks
  - PHY-layer
  - Protocol attacks

Questions?

richard.baker@cs.ox.ac.uk