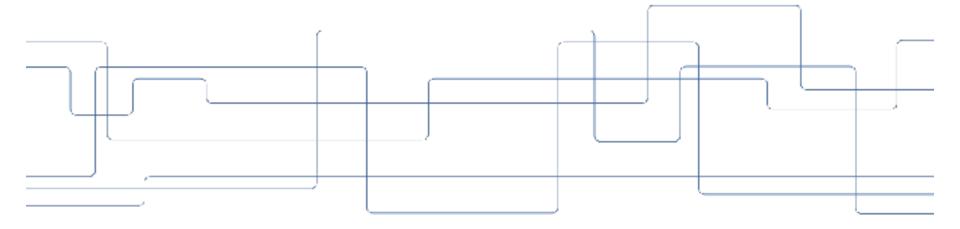
KTH ROYAL INSTITUTE OF TECHNOLOGY



# **Modern vehicle hacking**

Practical demonstration

Fredrik Heiding, KTH Royal Institute of Technology





### Content

- 1. Modern vehicles
- 2. Modern vehicle dongles
- 3. The hack
- 4. Summary



## Modern vehicles

- · Various functions to enhance the vehicle
- View health, performance and driving behavior of the vehicle, unlock or start the vehicle with a smartphone
- Autonomous driving, partly autonomous driving
- Aim to increase the safety, currently more than 1 million annual deaths in car

traffic, many caused by human errors [1]

[1] https://www.asirt.org/safe-travel/road-safety-facts/\_accessed: 2019-09-26



## Modern vehicle dongles

- Make an ordinary vehicle a "smart" vehicle, external device plugged into the OBD-II port
- Different functions, depending on device
- Different manufacturers, different security levels
- Cheap version for  $\sim$ 20\$, more premium versions for  $< \sim$ 200\$
- Our dongle is not made for autonomous driving, but for many other features



### Content

- 1. Modern vehicles
- 2. Modern vehicle adapters
- 3. The hack
- 4. Summary



- Vehicle dongle from AutoPi
- Based on a Raspberry Pi
- Highly customizable and able to work with external hardware such as proximity sensors
- Premium version, retailed around 200\$
- Possible to brute force the wifi password in < 1 second
- Generally good security but human errors and a design flaw

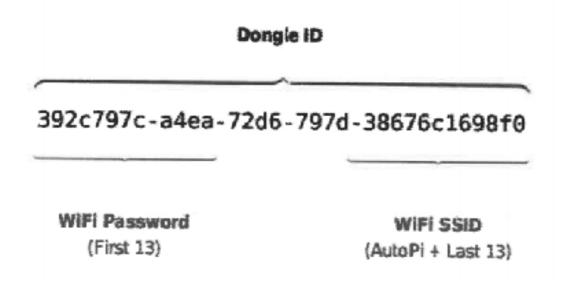


- Dongle ID: 32 character hexadecimal number
- WiFi ID: [AutoPi] + last 13 characters (dash included)
- Password: first 13 characters (dash included)
- 16^12 possible password combinations
- Doing 180k attempts/sec: ~50 years to solve



**Dongle ID** 

The AutoPi Dongle comes with it's own personalized dongle ID. This is what you need in order to activate your dongle and access the AutoPi Cloud. Keep your ID secret, as it gives access to register your dongle.





## Raspberry Pi ID

- The dongle ID is created by making an md5 hash of the device's Raspberry Pi ID
- Raspberry Pi ID, 8 character hexadecimal number, hardcoded in the device, with 8 zeroes padded in front, 16<sup>8</sup> combinations
- Found under /proc/cpuinfo
- By hashing these we get a 16^8 subset of the Dongle IDs
- Doing 180k attempts/sec: ~6.6 hours to solve



#### -38676c1698f0:~ \$ cat /proc/cpuinfo

13	- additional a cut ( proc) charing			
232G226	processor	÷	0	
	model name	:	ARMv6-compatible processor rev 7 (v61)	
	BogoMIPS	:	697.95	
	Features	:	half thumb fastmult vfp edsp java tls	
	CPU implementer	:	0x41	
	CPU architecture		7	
	CPU variant	:	0×0	
	CPU part	:	0×b75	
	CPU revision	:	7	
	Hardvare	:	BCM2835	
	Revision	:	9000c1	
	Serial	:	00000000ad993518	
-38676c1598f0:~ \$			598f0:~ \$	



### Md5 hash

[root@kali:~# echo 00000000ad993618 | md5sum
392c797ca4ea72d6797d38676c1698f0 root@kali:~#



## **Precomputed wordlist**

- · Precompute a sorted wordlist of all the hashes from the raspberry Pi IDs
- A 16^8 subset of the Dongle IDs, 69GB wordlist
- Take the broadcasted WiFi SSID (last 13 characters of the Dongle ID)
- · Go through the wordlist with a binary search algorithms
- Find a Dongle ID where the last 13 characters match the broadcasted WiFi SSID
- Sorted list with 16^8 hashed gives a maximum complexity of log2 16^8 = 32, < 1 second lookup time
- Can exploit any dongle with default WiFi settings

#### Wi-Fi: Looking for Networks... Turn Wi-Fi Off

EXIBEL_579bd6_2.4G	۵.	Ş
2f884e		$\overline{\phi}$
AirLink21C84C		T
AirLink21C84C6G	Ξ.	8
AutoPi-38676c1698f0	θ.	Ş
ESP_DrayTek	Ξ.	Ŷ
EXIBEL_579bd6_5G	θ.	440
Freggelberget2	Ξ.	Ŷ
Fridas_FZ10001001203	۰.	000
Jockes	Ξ.	
KnowiTinnograte	۰.	÷
kungariket	Ξ.	÷
Mitt första LAN	۰.	÷
Tele2Internet-DDC45	Ξ.	
TN_24GHz_C689DF	•	4444
TN_24GHz_D30853	Ξ.	Ŷ
TN_24GHz_EE93A7	•	÷
TN_6GHz_EE93A7	۹.	÷
TN_private_EY7UP7	Ξ.	() e ()
TN_private_HTWPKA	۰.	$\overline{\phi}$
TN_private_KPPTH7	Ξ.	÷.
TP-UNK_89D166		÷
Wiberg_2.4GEXT	0	
Info Other Maturals		

Join Other Network... Create Network... Open Network Preferences...

#### 🤊 🐺 🍥 🗔 🛜

#### Wi-Fi: Looking for Networks... Turn Wi-Fi Off

.

🖮 searchword ist — Java SearchWord list — 90×27

fheiding@fheiding-stp:-//repos/java/searchwordlist\$ java SearchWordlist

\_\_\_\_\_Insut\_SSID-------38676c1698f6[]

EXIBEL_579bd6_2.4G 2f884e AirLink21C84C		0.0.0
AirLink21C84C5G	Α	1
AutoPi-38676c1698f0	Θ.	ę
ESP_DrayTek	Р	÷
EXIBEL_579bd8_50	θ.	÷
Fragge berget 2	Α.	0
Frides_FZ10001001203	θ.	Ŷ
Jockes	8	(jo (j)
KnowiTinnograte	Θ.	ę
kungariket	Α.	Ť
Mitt första LAN	θ.	÷
TN_24GHz_C6B9DF	Θ	ę
TN_24GHz_D30853	θ.	÷
TN_24GHz_EE93A7	Θ.	Ŷ
TN_5GHz_EE93A7	Θ.	ę
TN_private_EY7UP7	۹	÷
TN_private_HTWPKA	Θ.	÷
TN_private_KPPTH7		Ŷ
TP-LINK_89D168	θ	÷
Wiberg_2.4GEXT	Ρ	

Join Other Network... Create Network... Open Network Preferences...

#### ... ଲ 🦻

÷

÷ Ρ

Ŷ Α

000 θ

÷

000

÷

Ŷ Δ

e, Δ

2

P

Α

θ Α

Α

Α

Ρ

Α

ρ

Ρ

P

Δ 2

2

۹

#### Turn Wi-Fi Off

✓ EXIBEL\_579bd6\_2.4G

.

searchwordlist — java SearchWordlist — 90×27

Theiding@fheiding-nbp:-/nepss/jawa/searchwordlist\$ jawa SearchWordlist

-----Isput SSID------38675c169510 Match found: 117.539985 ms1

SSIDE AutoPi-38676c1698f0 Password: 392c797c-a4ea Full hash: 392c797cs4ea72d0797d38070c169818

-----Input\_SSID------

2f884e AirLink21C84C AirLink21C84C5G AutoPi-38676c1698f0 ESP\_DreyTek EXIBEL\_679bd6\_6G Fraggelberget2 Jockes KnowiTinnograte kungariket Mitt första LAN Simonswifi TN\_24GHz\_C5B9DF TN\_24GHz\_D30853 TN\_24GHz\_EE93A7 TN\_5GHz\_EE93A7 TN\_private\_EY7UP7 TN\_private\_HTWPKA TN\_private\_KPPTH7 TP-LINK\_89D166 Wiberg\_2.4GEXT

Join Other Network... Create Network... Open Network Preferences...

0 0.0

• θ Ŧ

٩ Ŷ

0

9

0

۵

θ

0.0

9 ē 🔶

00

0.0

- (b- (b- (b-

#### Turn Wi-Fi Off

✓ EXIBEL\_579bd8\_2.4G 2f884e AirLink21C84C AirLink21C84C5G AutoPi-38676c1698f0 Crowdsurfing ESP\_DrayTek EXIBEL\_579bd8\_50 Fraggelbarget 1 Fraggelberget2 Jockes KnowiTinnograte kungariket. Mitt första LAN TN\_240Hz\_C5B9DF TN\_24GHz\_D30853 TN\_24GHz\_EE93A7 TN\_5GHz\_EE93A7 TN\_private\_HTWPKA TN\_private\_KPPTH7

Join Other Network.... Create Network... Open Network Preferences...

Theiding@fheiding\_wbp:~/repos/java/searchwordlist\$\_java : -----Isput\_SSIB------30070-109810 Patch found! (17.293830 ms) SSIDE AutoPi-38676c169810 Password: 392c797c-a4ca 392c797ca4es72d6797d38670c1698f8 full hash:

-----Isput \$\$10-----

0

The Wi-Fi network "AutoPi-38678c1698f0" requires a WPA2 password.

issword:	392c797c-a4ea				
	🔽 Show pasaword				
	Remember this network				

Cancel	Jol
--------	-----

#### 🤜 🐺 🛞 🖵 🛜

Turn Wi-Fi Off

ſ	✓ AutoPi-38676c1698f0		ę
	21884e	1	Ŷ
	AirLink21C84C		Ş
	AirLink21C84C5G		9
	ASUS_5G		ę
	ASUS_F		÷
	comhem_CDF501		Ŧ
	ESP_DrayTek		ę
	ESP_DrayTek_6 G		ę
	EXIBEL_579bd6_2.4G		ġ
	EXIBEL_579bd6_5G		ę
	Fraggelberget1		ę
	Fraggelberget2		ġ
	Fridas_FZ10001001203		Ş
	Fuffens_EXT		ę
	iMackan_1	1	Ş
	iMackan_3		ġ
	Jockes		Ş
	KnowlTinnograte		ę
	kungariket (		ġ
	Mitt första LAN		ę
	Tele2Internet-DDC45		
	TN_24GH2_1E65A3		÷
	TN_24GHz_C5B9DF		Ş
	TN_24GHz_D30853		ę
	TN_24GHz_EE93A7	1	Ş
	TN_50Hz_EE93A7		ġ
	TN_private_EY7UP7		÷
	TN_private_HTWPKA		÷
	TN_private_KPPTH7	1	÷
	TP-LINK_58C780		÷
	TP-LINK_89D166		4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4

Join Other Network... Create Network... Open Network Preferences...

🔚 searchwordlist — java SearchWordlist — 90x27

#### [fheiding@fheiding-wbp:-//repos/java/searchwordList\$ java SearchWordList

------38676c1698f0 Natch found: (17.293836 ms]

SSID: AutoPi-38676:159878 Passeord: 392c797:-a4ea Full bash: 392c797:a4ea22d6797d34676c1690f8

-----Input SSI0------



## Exploit, what to do when logged in

- · Get GPS location of the vehicle
- Open windows, unlock the doors, start the vehicle, play audio messages ...
- <u>https://www.autopi.io/use-cases/</u>
- Create a vehicle-botnet, dongles automatically connect to other dongles



- Error rate: multiple dongle IDs could have the same last 12 characters
- Negligible, probability of an evenly distributed 32 character hexadecimal hash having the same last 12 characters is 1/16^12
- Still, if that happens, exclude the dongle ID from the search



### Summary

- Generally good security
- Vulnerable because of human error
- CVE-2019-12941
- Visit <u>www.kth.se/nse/ssas</u> for updated info about our projects

Ketwork and Sys	No photonico Q				
2	2	vanit the Chiveleste			
Home Studies Receive	ch Coroperation About KTH Läprary	Soundh			
KIND ASP 2 research a software	Cite 7 Sol 7 Instantic and loans systems and writing and see any 7 instants				
e Schwerz (Jahren Addisouns) Ethical Hacking					
Frojecte	In this context we also adviced breaking for extraction to these too	the late that has been been			
Projects	In this project we do ethical hacking (penetration testing / white hat hacking various devices and systems.				
MAL CENTRE AND A MUCH	,				
Companyer()	Vulnerabilities published				
Million Hacking Integrifield	Ald a Harders is, fourthern Platers 5, Protos Minnars, and Palerit Lage strict costs. AutoPI W1-70/ND and 4G/IEE Systems (Linvaux utilizion to perform)				
etta - Resident information and Control Systems	at take and stimmery attack to gain source to the With activate, which prevales and source to the device				
Sec08 25 Cyber Scoully	Archi Viderberg, Pontas Johnson, and Rebert Experiencies. CPE-accession	Obs Souri			
Thread 9040	Lack 402 Bills sizes have by requery lifesk great associate what is its alience of				
welctive risk and thread	network connection is unavailable.				



# Thanks for your attention