Threat Intelligence for Bluetooth-enabled Systems with Automotive Applications: An Empirical Study

Madeline Cheah, Jeremy Bryans, Daniel Fowler and Siraj Shaikh

Coventry University

Cybersecurity Group
Centre for Mobility and Transport

Coventry University

Cybersecurity Group

Centre for Mobility and Transport Research

The Cyber Security Group at the Centre for Mobility and Transport (CMT) at Coventry University is a team of multi-disciplinary researchers addressing issues of systems security for automotive, rail and connected infrastructure:

- **CyberOwl**, a new commercial venture spun-out of the group in 2016 that is developing early warning systems for the cyberspace;
- **Automotive Cyber Security collaboration with HORIBA MIRA**, involving a number of doctoral students investigating both testing and design aspects of security on vehicular platforms;
- **Knowledge Elicitation for Railway Safety (KEEP SAFE) (2013-2014),** which was funded by the RSSB to assess the use of safety-related data for effective safety decision-making for rail safety and security

Information: http://www.coventry.ac.uk/research/areas-of-research/mobility-transport/cyber-security/

Outline

- Background
- Methods
- Results
- Threat Case Study
- Discussion

Background

- Modern vehicles are sophisticated, with more connectivity
- One of the most pervasive external facing interface is Bluetooth
  - Estimated to be 21 million vehicles with Bluetooth by 2018 [1]
- Situational awareness is therefore essential

Background

- Bluetooth is exploitable through:
  - E.g. compromising authentication mechanisms
    - Brute force PINs [4]
    - NINO [5]
    - Downgrade attack [5]
  - E.g. range extension [6]
    - CarWhisperer
- Only the first step; the aim is to get into the vehicle

Background

- Wardriving for Bluetooth (aka ``war-nibbling'') has been performed (e.g. [2])
  - Large number of devices (~64,000)
  - Not focused on security or automotive specific
- Another study has looked at Bluetooth implementations in vehicles and aftermarket devices [3]:
  - Information from publicly available manuals

Methods

- In-cabin inspection
  - Head-units only (i.e. native Bluetooth connection)
  - Looked at Bluetooth version
    - <2.0 is legacy pairing (more susceptible to MITM)
    - 2.1+ is Secure Simple Pairing (SSP)
  - Organisationally Unique Identifier (first three bytes of Bluetooth address)
    - For future reconnaissance

Methods

- War-nibbling
  - Automotive aftermarket devices and automotive head-units
  - Bluetooth Cambridge Silicon Radio Class 2 v 4.0 dongle
    - 10 meter range
  - 28 trips (small scale) spanning town centers, highways and car parks
  - Based in the West Midlands area of the UK

Methods

- War-nibbling (continued)
  - Filtering of results (head-units):
    - If the Bluetooth name contained the name of an automotive manufacturer, vehicle model or licence plate number;
    - If the Bluetooth class indicated that it was a handsfree device with telephony, rendering, object transfer or audio capabilities
    - If the OUI indicated that the manufacturer is a known supplier of automotive head-units
  - Filtering of results (aftermarket):
    - If the Bluetooth alias contained the name of a known aftermarket device (e.g. GPS, Radio, OBDII) or the name of an aftermarket carkit;
    - If the Bluetooth class indicated that it was capable of audio, rendering or networking. This is the loosest of the three criteria, as even something that indicates a GPS unit could have a class of 'uncategorised';
    - If the OUI indicated that the manufacturer is a known supplier of aftermarket devices.

Results

Pairing type	*Legacy*		*SSP*		
Version Adopted (Year)	2003	2004	2007	2009	2010
Bluetooth version / *Reg. Year*	<2.0	2.0	2.1	3.0	4.0
2010	1	2			
2011		1			
2012		3	2		
2013		2	2		
2014			4	2	
2015				1	2
2016		1	1	1	
2017					1
Total	1	9	9	4	3

Results

	Duration visible	*Legacy*			*Not Legacy*		
		TC	H	CP	TC	H	CP
Vehicles	<1 min.	52	8		39	12	3
	>1 min.	3	1	1	3		
Total (location)		55	9	1	42	12	3
Total (pairing type)		65			57		
Aftermarket devices	<1 min.	40	6	2	34	6	
	>1 min.	2		4	1	2	1
Total (location)		42	6	6	35	8	1
Total (pairing type)		54			44		

TC = Town Centre, H = Highway, CP = Car Park

Results

Device Type	*No. Found*
GPS	43
GPS (Heavy Goods Vehicles)	4
Telematics (Heavy Goods Vehicles)	15
Diagnostics-OBDII	3
Diagnostics-Other	2
Carkits	30

Discussion

- Easily found devices even with a very low-powered device doing the scanning
- Vehicle head-units had technological lag between implementation and adoption (although it's improving)
  - Average lifetime of a vehicle ~10-15 years
- Aftermarket devices broadcast serial numbers, license plates, personal names, type of device
- Still a goodly proportion (on both counts) using Bluetooth version 2.0 (legacy pairing)
  - which was deprecated in 2014.
- Even with devices that use 2.1 and above, their manuals openly state the use of '0000' or similar for backwards compatibility
  - Makes these devices susceptible to downgrade attack
- Caveats:
  - Not statistically significant; all indicative
  - The makeup of the vehicles found could reflect the popularity of those manufacturers geographically

Threat Case Study

- Highlight the potential threat
- Using Onboard Diagnostic Port devices
  - Also known as OBD-II dongles
- Three were found through war-nibbling
- Studies and reports [3, 7] show that they are insecure
  - Which in turn makes the vehicle itself more insecure

Threat Case Study

- OBD-II is a mandatory port
  - Originally for diagnostics, maintenance and measurement of environmental aspects such as emissions
  - Manufacturers add own functionality for testing and maintenance
  - Controller Area Network (CAN) and diagnostic message injection is possible
  - Effects are based on the vehicular network implementation
    - Gateways
    - Exposed busses

Threat Case Study

- CAN Message injection
  - For practical purposes 3-digit hex CAN ID (which determines message priority) and up-to 8 byte data message
- Diagnostic messages
  - In this case OBD-II commands (SAE J1979)
    - Mode and PIDs
    - 7df CAN ID followed by 02 (data length) and mode (1 byte) and PID (generally 1 byte)
    - So 7df 02 09 02 = VIN number

Threat Case Study

- Connection
  - Bluetooth-enabled OBD-II dongle
    - Containing ELM327 chipset
    - OBD to RS232 interpreter
  - Requires Bluetooth Serial Port Profile (SPP)
  - Send commands through any serial terminal
    - AT commands to configure the dongle
    - CAN or diagnostic messages to affect the vehicle

Threat Case Study

Tested with five different dongles:

Dongle (OBD Port Device)	*PIN*	*Discoverable window*	*Price*	*Chip version*
Vgate Advanced OBD2 Bluetooth Scan Tool	1234, fixed	Always	$13	v2.1
Exza OBD SCAN	1234, fixed	Always	$25	v1.5
Vgate ELM327 Mini	1234, fixed	Always	$15	v1.5
Pumpkin OBD2 ELM327 Bluetooth Car Scanner	1234, fixed	Always	$15	v1.5
Scantool OBDLINK MX Bluetooth	6-digits, dynamic	2 minutes	$100	v1.3a

Threat Case Study

- All dongles bar OBDLINK-MX broadcast as soon as they were plugged in (even if ignition off)
- An example when diagnostic messages were sent in a flood:
  - Ignition on: lights flickered, all electronics non-functional
  - Engine on: engine stalls
  - Non-functional so long as the flood continued
- Dongles returned information from the vehicle when queried even when the 12V battery went to 7V

Discussion

- Aftermarket wireless devices can make vehicles more insecure
  - Fixed unchangeable PINs
  - Downgrade attacks
- Bluetooth device may need to be planted
  - Black box insurance devices
- Bluetooth is short-range,
  - Range extension
  - Other technologies where compromise is easier (e.g. WiFi) or long distance (e.g. cellular)

Summary

- Could find both vehicles and aftermarket devices
  - Technological lag was apparent (from inspection)
  - No correlation with 'premiumness' of the vehicle
- Visible long enough to compromise (with premeditation)
- Aftermarket devices can make a vehicle more insecure (and affect vehicle safety)

References

[1] GSMA, "Connected Car Forecast: Global Connected Car Market to Grow Threefold within Five Years," GSMA, Tech. Rep., 2013. [Online]. Available: http://www.gsma.com/connectedliving/wp-content/uploads/2013/06/cl ma forecast 06 13.pdf

[2] W. Bronzi, T. Derrmann, G. Castignani, and T. Engel, "Towards Characterizing Bluetooth Discovery in a Vehicular Context," in Proc. of the 2016 IEEE Veh. Network. Conf. Columbus: IEEE, Dec 2016.

[3] D. K. Oka, T. Furue, L. Langenhop, and T. Nishimura, "Survey of Vehicle IoT Bluetooth Devices," in IEEE 7th Int. Conf. on Service-Oriented Computing and Applications. Matsue, Japan: IEEE, Nov 2014, pp. 260–264

[4] n—u: The Open Security Community, "Carwhisperer, Bluetooth Attack," 2012. [Online]. Available: http://www.slideshare.net/null0x00/ carwhisperer-bluetooth-attack

[5]] K. Hypponen and K. Haataja, ""Nino" Man-In-The-Middle Attack on Bluetooth Secure Simple Pairing," Proc. of 3rd IEEE/IFIP Int. Conf. in Central Asia on Internet, vol. I, pp. 1–5, 2007.

[6] J. P. Dunning, "Taming the blue beast: A survey of bluetooth based threats," IEEE Security and Privacy, vol. 8, no. 2, pp. 20–27, 2010.

[7]] Argus, "Argus Cyber Security Working With Bosch to Promote Public Safety and Mitigate Car Hacking," 2017. [Online]. Available: https://argus-sec.com/argus-cyber-security-working-boschpromote-public-safety-mitigate-car-hacking

Coventry University

Thank you!

CENTRE FOR MOBILITY & TRANSPORT

Madeline Cheah
PhD Research Student
cheahh2@uni.coventry.ac.uk

Centre for Mobility & Transport
Faculty of Engineering, Environment and Computing
Coventry University
Coventry CV1 5FB