DEFCON 19 Trip Report

SUMMARY:

1. Increasing awareness and interest in vehicle network vulnerabilities. Multiple vulnerabilities are accessible via existing in vehicle wireless systems.
2. Cloud services are vulnerable due to the distributed nature of the Cloud services. But techniques exist to rapidly detect problems and alert vendors to correct.
3. Password is fast becoming useless due to the continued reduction in cost of Graphics Processing Units and Quantum computing.
4. Increased awareness of the Connected Vehicle Program
5. Vulnerabilities have been identified in both Transit and Freight systems that have not been exploited by the greater hacker community.

DETAILED DISCUSSIONS

Automotive hacking is gaining visibility

Instructor: Robert Leale

Robert Leale www.canbushack.com conducted a full day workshop on CANBUS, its function, and how it can be exploited to gain privileged access to vehicle systems.

27 people attended the CANBUS Hack workshop: 14 with no experience, 4 OEM/Vehicle systems, 4 penetration 'testers', 1 attorney, 5 unknowns. This was an extensive overview to the hacking community on the characteristics of the vehicle CANBUS. It got into substantial details on how to gain access to the network (function of each wires on the ODB2 port), and the binary data type used to read and access information to the vehicle system. Particular focus is on how the diagnostic mode can be utilized to gain access to privileged information on the Electronic Control Unit (ECU) and to modify its content. Modification of the ECU isn't really new; this is very similar to what aftermarket modders have been doing to adjust vehicle engine performance (race tuning for street racers).

Two of the attendees at this workshop is working with a major auto manufacturer (Subaru?) to address a vulnerability in their remote entry system. A cloned GSM base station intercepted wireless door opening and engine start command from a wireless key fob. Apparently a replay attack was able to open the door and start the engine on a targeted vehicle. It was unclear if the intercepted data packet was encrypted, apparently it did not utilize authentication to proof it originated from a trusted party.

Compromise of Ford Sync via the Microsoft AutoPC System

Presenter: Tyler Cohen

Demonstrated the vulnerability of the Microsoft AutoPC, which is a Windows CE based operating system. An IntelliDrive video from the RFK Stadium press events was shown to an audience of 300 to 400 attendees. Questions from the attendees included:

a) Can it be used as a means to transmit virus
b) Can a "Pineapple" (MITM network sniffer) be used on it.

Follow on discussion with presenter being attempted.

Cloud Services vulnerabilities

Cloud services cannot use tradition outer layered defense such as Intrusion Prevention Systems (IPS). IPS is still needed, but substantial protection is needed for threats are from inside the cloud array. There isn't a whole lot the user of the cloud service can really do, this really depends on the cloud service provider. The presenter made additional test of three major cloud service providers to show the difference in support performance in case of problem. A list of protection software was listed that can help identify when a breach exists in your Cloud Service.

Economic of password cracking:

8 character passwords are essentially useless. Nvidia graphics card can crack it in just over 414 hours at a cost of ~$2000. Amazon EC2 cloud services can also be use, taking 3x longer but 75% of the price. At 10x the number of resources, the time is just over a day using a GPU and just under three days using cloud services. At 500x the GPU system can crack the 8 character password in less than 30 minutes; Cloud service will crack it in just under 90 minutes. This assumes a completely random set of 8 characters (upper+lower+number+special characters) Most passwords are not completely random. Just the use of a Capital first letter will significantly reduce the length of time required to crack a 8 character password.

Based on current trend and development in Quantum Computing, the presenter do not see an alternative to two factor authentication.

Overview of FIPS-140

One of the 14 certification lab operators gave an overview of the Federal Information Processing Standard – 140. There are several take away that can be applied to the Connected Vehicle program. The current version is FIPS-140 revision 2 (FIPS-140-2). The Standard covers cryptographic standards with regards to key management and more interestingly, standards for physical component protection and tamper resistance. A number of vulnerability discussed at this DEFCON relies on access to base components and identification of vulnerabilities by targeting the OEM part suppliers. The standard for physical component protection and tamper resistance should be examined for suitability to future systems to increase the cost to potential attackers.

Vulnerability of Aircraft Flight Control System and Autopilot

<u>Presenter: One World Labs</u>

Presentation was made on how ground equipment can be compromised and used to inject changes to the autopilot, engine control unit, and other ancillary systems. Aircraft determined to be vulnerable (tested) were: 747-8 and 737. The presenter discussed not in great detail, but techniques are possible where the autopilot can be compromised and vulnerability exploited where manual over ride can be prevented. Based on examination of available ECU logic, it is possible for the ECU to issue a thrust reversal command to the engine nacelle while in flight. But it was unclear to the investigators if there are other failsafe that will prevent this from occurring. Even if fail safe are present, it maybe possible to attack the airline by tampering with the cabin pressurization system such that lost of consciousness can be brought on to most of the passengers.

Follow on discussion with presenters:

<u>Chris Roberts and Jay Weber of One World Labs, Colorado Springs, Colorado.</u>

OWL Labs in their presentation mentioned a DEFCON-18 presentation where they spoke to the possibility to hack Tractors and Busses. They identified the use by Cummins of a WiFi based engine diagnostic system for fleet and enterprise operations. This is a continuation of the use of WiFi in the transit fleet I first identified in 2004. Unfortunately in this case, the WiFi lacks authentication and other security required to block untrusted agent access. OWL did not release codes needed to exploit this vulnerability in DEFCON-18. However, four RTC transit buses were made to stop on Las Vegas Boulevard several weeks after the talk. Chris Roberts noted the event had characteristics (by impersonating the access point used at the RTC fuel depot and ordering the Cummings ECU to stop the engine) that indicated to him this may be caused by someone hacking the bus based on his talk.

Similar vulnerability was observed on the 16th Street Mall transit route in Denver Colorado. In this case, they have attempted to contact the local transit agency but the transit agency has not been receptive to their approach. I have allowed them to forward my contact information to agencies in any future contact about discovered vulnerabilities so I can moderate the discussion betwen the two parties.

I have plans to contact both Las Vegas RTC and Denver area transit agency to determine if they are aware of these events. This needs to be done to verify the claims from OWL. It's possible that these agencies do not realized they were compromised,

OWL has also investigated into the vulnerabilities at Truck Weight Stations which also uses some form of wireless system for manifest management. Their initial investigation is indication a method maybe possible for a third party to tamper with the electronic manifest.

<u>Meeting with Washington State University and University of California at San Diego</u>

"Comprehensive Experimental Analyses of Automotive Attack Surfaces" – USENIX 20th

I met this team at the Q&A session of the Ford Focus talk. This group presented their paper at a formal security conference (USENIX 20th) in San Francisco three days after DEFCON. This work was not presented at DEFCON. This is the same team that developed CarShark last year that showed how via the OBD port they were able to compromise the ABS system on a vehicle. Their new paper discussed how the vehicle system can be compromised remotely using the build in wireless network. They were also able to show how by using the same method used by aftermarket ECU modders they were able to develop a inter-CANBUS exploit. This effectively overcomes any security by separating CANBUS network currently used by vehicle manufacturers. Their paper is included here as an appendix. But the following are key items: The vehicle can be compromised using any of the wireless system on the vehicle; TPMS, Bluetooth, cellular radio, wireless key entry systems, It can also be compromised from the entertainment center using a USB drive, a compromised PMP, or a CD player. Any ECU can be accessed once the network is breached.

They mention IntelliDrive in the paper as a future area needing research, but did not elaborate further. The next stage in their research is on how to harden the vehicle environment.

<u>Still trying to contact Tyler Cohen for additional discussion on Ford Sync vulnerabilities.</u>

Specific thoughts for Connected Vehicle program

1) What is the point of the "Trust" - What exactly are we protecting? If we try to protect everything, we're protecting nothing. All it takes is one crack to break the whole thing. The entire system needs to be resilient even when trust and authentication are compromised.
2) The use of PKI key for authentication and encryption should be minimized. The less exposure, the less opportunity it can be compromised. The use of this technology should be limited to first responders and public service agencies as the number of units are much lower and positive control can be exercised.
3) The security and authentication system needs to be upgradeable. Vehicle and field devices will outlast viable encryption standards. Field devices can expect multiple upgrades to authentication and encryption over the service life of the equipment and installation.
4) Separation of CANBUS for vehicle functions is no longer sufficient to protect vehicle systems.
5) Physical system must be protected. Attacks can be developed not by targeting the OBE system, but the subcomponent vendors. FIPS-140 can help make this type of attack more challenging.
6) OBE needs to be tamper resistant, and self-destruct of tampered with. We need to come up with a design that won't inadvertently kill the OBE for self-servicing of the vehicle.
7) Trust can be enhanced using a context based model. A context based security method was a submission to the Connected Vehicle Challenge by UC Berkeley – we should investigate the possibility of extending their work.
8) RSE must be 100% trusted, they are stationary and have a higher exposure to targeted attack - greater efforts are needed to harden the RSE.
9) We need to investigate the possibility of bringing in three groups, One World Lab, Washing State University & University of California San Diego, and the professional group Tyler Cohen represents at DoD for an outside look at the vulnerability of the Connected Vehicle system as proposed. We need to gain a better understanding what potential vulnerabilities are and determine the risk/benefit/cost to eliminating these vulnerabilities.