Computer Crime Investigative Unit
U.S. Army Criminal Investigation Command

Cybercrime Prevention Flyer

Contact Information:
Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571.305.4482 [DSN 240]
Fax: 571.305.4189 [DSN 240]

E-mail

CCIU Web Page

CID Cyber Lookout
On Point for the Army

DISTRIBUTION:
This document is authorized for wide release with no restrictions.

"DO WHAT HAS TO BE DONE"

CPF 0002-16-CID361-9H **23 March 2016**

Auto Hacking—It's Not a Myth

There is nothing quite like the feeling of wheeling down the open road, blazing a path to your destination, streaming tunes on your interconnected entertainment system. You're in control! But how much control do you really have?

Auto manufacturers use microprocessors, small computers, to control and integrate your vehicle's functions. Windshield wipers, cornering stabilizers, automatic emergency breaking, engine management, tire pressure monitors and many other functions are interconnected. Your entertainment system that connects with your mobile phone, that connects to your GPS, that connects to the Internet, that becomes a mobile hot-spot is also controlled by the same microprocessors that control your car's functions. Your car is a rolling computer with its own operating system that connects to the Internet!

It's no secret that computers can be hacked. And your computer operated, fully connected, Internetworked car is not immune.

While the financial incentive for auto hacking is unclear, vehicle hacking is real. According to a recent Internet Crime Complaint Center (IC3) public service announcement, motor vehicles are increasingly vulnerable to remote exploits.

Vulnerabilities in your vehicle's wireless communication equipment, your mobile phone and your vehicle's operating system are potential points for compromise. Your vehicle's diagnostic port, that connector the mechanic connects the "code reader" to, is a direct connection to your car's internal control systems.

Examples

- A disgruntled employee of a vehicle sales center compromised a Web-based vehicle immobilization system and either disabled the vehicles or made the horns honk on more than 100 vehicles.
- Researchers, using free software and readily available equipment, remotely tracked a vehicle by hacking the vehicle's tire pressure monitoring system. They were also able to trigger the vehicle's warning lights.

Mitigating the Vulnerabilities

When a vulnerability represents an unreasonable risk to safety, manufacturers sometimes issue recalls. However as vehicle owners, you can take the following steps to reduce your vehicle's cybersecurity vulnerabilities:

- Ensure you vehicle's software is up to date through a trusted and reputable maintenance service provider
- Check for vehicle recalls even after the warranty has expired
- If you maintain your own vehicle and install updates or make modifications to vehicle software, be mindful that any changes could introduce new vulnerabilities
- Ensure your mobile devices, which you may connect to your vehicle, have the latest software and security updates
- Use discretion when connecting third-party or after-market devices to your vehicle
- Familiarize yourself with the wireless systems available in your vehicle

Additional Information:

Vehicle Identification Number (VIN) Recall Information, National Highway Traffic Safety Administration
Vehicle Safety Information, National Highway Traffic Safety Administration
Motor Vehicles Increasingly Vulnerable to Remote Exploits, IC3
U.VA. And State Police Partner to Prevent Car Hacking, University of Virginia

ICE

CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide us with feedback.

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flyer (CPF), along with the views and opinions of authors, products or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations. Such links are provided consistent with the purpose of this CPF.