MOTHERBOARD

MORE FROM **CRASH**

Blimp Deflates, Catches Fire, and

Cars Are Crashing a Lot Better Than They

The First Tim Humans Cras

Researchers Hack Car Infotainment System and Find Sensitive User Data Inside

Contacts, call logs, text messages and other information from paired phones was stored unencrypted.

SHARE TWEET

Lucian Constantin
Nov 16 2017, 7:42am

Image: Shutterstock

People who are worried about their security will use a secure phone, lock down their computer, and use strong passwords for their online accounts. But how many people have considered that their car could be leaking their most sensitive data?

A researcher who recently decided to investigate his car's infotainment system found that it was not designed using modern software security principles, yet it stored a lot of personal information taken from his phone that could be valuable to hackers.

Executing code on the car's infotainment unit was extremely easy by connecting a USB flash drive with specially crafted scripts. The system automatically picked up those files and executed them with full administrative privileges.

Car enthusiasts have used the same method in the past to customize their infotainment systems and run non-standard applications on them, but Gabriel Cîrlig,

a senior software engineer at security firm Ixia, wanted to understand the security implications of this technique.

What he found was a major privacy issue where call histories, contacts, text messages, email messages, and even directory listings from mobile phones that had been synchronized with the car, were being stored persistently on the infotainment unit in plain text.

Mobile operating systems like Android and iOS go to great lengths to protect such data by restricting which applications have access to it or by allowing users to encrypt their devices. All that security could be undone if people pair their devices over Bluetooth with an infotainment system like the one found in Cîrlig's car.

Cîrlig and an Ixia colleague Ștefan Tănase decided to go even further and investigate how the car's infotainment unit could be potentially abused by an attacker or even law enforcement to track users and obtain information about them that they couldn't otherwise get from their mobile devices.

The researchers presented their findings Friday at the DefCamp security conference in Bucharest, but declined to disclose the car make or model because they're still in the process of reporting the privacy issue they found. However, they mentioned that the car was made by a Japanese manufacturer.

Cîrlig told me that there is a firmware update available that blocks the USB attack vector on his car, but installing it requires going to a dealership. This means that a large number of cars will likely never be patched.

The infotainment system itself is a hacker's paradise and is more powerful than most embedded devices, including home routers. It has a Cortex-A9 CPU with 1GB of RAM, as well as Wi-Fi and GPS. The operating system is based on Linux and has a fully functional Bash command-line shell with all its usual utilities. On top of that, there are various debugging tools, including for the GPS, that the system's developers did not bother to remove, according to Cirlig.

It looks like technology that was created in a rush without any concern for security engineering, Cîrlig told me. "A production system, at least for a car, should be completely locked down."

He thinks that some of the software design choices were driven by convenience, like the storing of unencrypted user sensitive data indefinitely instead of requesting it again from the phone when the device is in proximity.

In addition to data copied from mobile devices, Cîrlig found other sensitive information on the infotainment unit, such as a list of favorite locations the car has been driven to or from, voice profiles, vehicle status information, and GPS

coordinates.

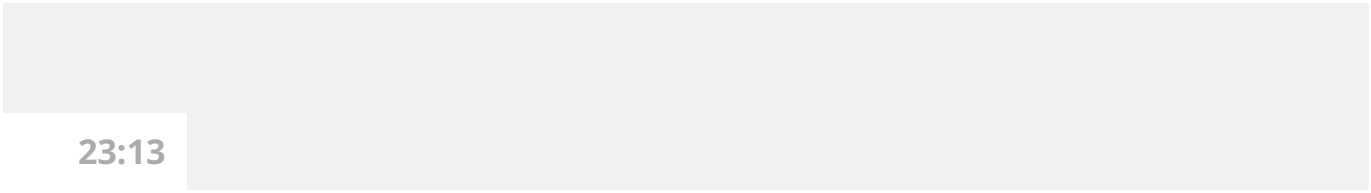
For their presentation, Cîrlig and Tanase showed a proof-of-concept malware program—a Bash script—that when executed via USB, continuously looked for open Wi-Fi hotspots, connected to them and could exfiltrate newly collected data. By combining this malware with location data from the GPS, an attacker could also track the car in real time on a map.

To make things worse, the rogue script is installed as a cron job—a scheduled task on Linux—and is persistent. Even if the infotainment system is reset to factory defaults, cron jobs are not removed, the researchers said.

Hackers could take the attack even further and create a USB worm, where a compromised infotainment system could infect all USB dongles plugged into it and potentially spread the infection to other cars, Cîrlig said. Or the car could be used in a wardriving scenario, trying to automatically exploit Wi-Fi networks and other systems it encounters, he said.

The development of infotainment systems is usually outsourced to third-party electronic component suppliers and not made by the automobile manufacturers themselves. Other researchers have shown in the past that there are ways to jump from the infotainment systems to more critical electronic control units (ECUs)—the specialized embedded computers that control a car's functions.

The auto industry continues to work using outdated programming principles and very old technology stacks that would be unacceptable today in a modern software development environment; and that needs to change, Cîrlig said. "For someone like myself who has a software development background, that style of coding looks ancient, from the age of the dinosaurs."



Frozen Faith: Cryonics and The Quest to Cheat Death

Find us in the future.

LIKE MOTHERBOARD

NET NEUTRALITY

To Save Net Neutrality, We Must Build Our

Own Internet

We must end our reliance on big telecom monopolies and build decentralized, affordable, locally owned internet infrastructure.

Jason Koebler
Nov 21 2017, 7:52am

Image: Lara Heintz/Motherboard

The Federal Communications Commission will announce a full repeal of net neutrality protections Wednesday, according to the ***New York Times*** and several other media outlets. It is possible that a committee of telecom industry plutocrats who have from the outset made it their mission to rollback regulations on the industry will bow to public pressure before Wednesday, but let's not count on it.

It is time to take action, and that doesn't mean signing an online petition, upvoting a Reddit post, or calling your member of Congress.

Net neutrality as a principle of the federal government will soon be dead, but the protections are wildly popular among the American people and are integral to the internet as we know it. Rather than **putting such a core tenet** of the internet in the hands of politicians, whose whims and interests change with their donors, net neutrality must be protected by a populist revolution in the ownership of internet infrastructure and networks.

In short, we must **end our reliance** on big telecom monopolies and build decentralized, affordable, locally owned internet infrastructure. The great news is this

is currently possible in most parts of the United States.

There has never been a better time to start your own internet service provider, leverage the publicly available fiber backbone, or build political support for new, local-government owned networks. For the last several months, **Motherboard has been chronicling** the myriad ways communities passed over by big telecom have built their own internet networks or have partnered with small ISPs who have committed to protecting net neutrality to bring affordable high speed internet to towns and cities across the country.

A future in which ISPs are owned by local governments, small businesses, nonprofit community groups, and the people they serve are the path forward and the only realistic way of ending big telecom's stranglehold on America.

In Detroit, the **Equitable Internet Initiative** is building community-owned wireless internet infrastructure in towns that big telecom won't touch. Hundreds of towns have built their own internet service providers. Rural communities are **putting wireless internet antennas** on top of mountains, grain silos, and tall trees. The

fastest internet connections in the United States are provided by local governments, not big telecom. In Southern California, Tribal Digital Village is **using unused television spectrum** to deliver internet. All over the country, big telecom is being rejected and subverted, and you do not need to have a pile of money, an army of lawyers, or a degree in network engineering to take action.

Motherboard has and will continue to celebrate and amplify these projects, but that is not enough. Starting immediately, we will:

- Begin researching and publishing technical articles and videos that explain how new wireless networking hardware and software works, how to use it, and how to use currently available, affordable technology to start your own small internet service provider.
- Speak to activists, entrepreneurs, lawyers, technologists, networking engineers, and politicians who have navigated the technical, legal, and political hoops required to start community-owned internet service providers. We will use those conversations to create clear instructions for how you can empower yourself to do the same.
- Begin creating a comprehensive guide to the various new technologies and methods of creating decentralized internet infrastructure, which will be released next year.

If you want to help or partner with us, **please get in touch**.

DIY MESH-NETWORKS BROADBAND INTERNET BROADBAND LAND

Related Articles

BIG TELECOM

Verizon Wants the FCC to Overturn State Internet Privacy Laws

NET NEUTRALITY

More Than 80% Of All Net Neutrality Comments Were Sent By Bots, Researchers Say

FCC

Internet Activists Urge Congress to Fire Trump's FCC Chief Ajit Pai

NET NEUTRALITY

To Save Net Neutrality, We Must Build Our Own Internet

Find us in the future.

LIKE MOTHERBOARD