Zero-knowledge Armor for Automotive Security
Introduction

When hackers remotely cut the engine of a Jeep Cherokee speeding at 70 miles an hour, the unprecedented security breach made headlines and sent shock waves around the world.

Using a laptop 10 miles away, the attackers first sent bone-chilling cold air through the vents, hijacked the radio, flipped on the windshield wipers and finally shut down the transmission as the Jeep rolled to a stop. While the attack was a stunt to demonstrate how easy it is to hack a car, it was a stunning reminder that semiconductor-laden automobiles are like “souped-up” computers on wheels and can be compromised just like the vulnerable enterprise networks that are attacked on a daily basis.

Data is lost and privacy compromised when a network is hacked, but people may die and property destroyed when cars are hacked. Imagine an ambulance without steering control with a heart attack victim on board; or a fire truck engine suddenly shutting down three miles from a raging wildfire; and what of the brakes that fail without warning on a school bus with innocent children on aboard?

If hackers have their way, these scary scenarios may one day be more like frightening fact than titillating fiction. And while they were once a fantasy, driver-less car controlled by nefarious hackers could one day be accidents waiting to happen when they hit the road in years to come.

rubiconlabs.io

Car Vulnerability Primer

- The system of wires and software protocols acting as the connective tissue between a vehicle's computers and sensors is known as a Control Area Network, or CAN bus.

- The CAN bus network allows data from micro controllers (MCUs) to circulate around the car.

- MCUs transmit sensor and programming data constantly.

- Each MCU is connected to the network and selects what data it needs to perform its task. There is no central hub or routing system, just a continuous flow of data.

- To compromise a vehicle, an attacker simply gains access to any MCU in the system, and then 'hops' around until they find an MCU that talks to the CAN bus.

- Communication is unauthenticated and unencrypted. Once an MCU is compromised, it can assume command of the vehicle.

- Over 90% of vehicles manufactured in 2014 had a wireless network (a doorway into the car).

- Only six automakers in 2014 had any kind of security software in their vehicles.

- Only models made by two companies in 2014 can alert their manufacturers in real time if a malicious software attack is attempted – all others wait until a technician checks at the next servicing.
Declaring Cyber-War

The stark reality is that hackers have quietly declared cyber-war on the automotive industry. A quarter of a billion vehicles will join the Internet of Things (IoT) by 2020, and attacks on them are no longer theoretical. Vehicles have joined PCs and smartphones, and a growing list of devices that get hacked. This is no longer a threat to the industry; it is the new reality of automotive.

As a result, security is now on a fast track to rival the appeal of muscular horsepower, sleek body styling and auto safety. But automakers typically don't have the in-house skill set to uniquely and securely identify devices, protect communication, and securely execute code.

While software alone is not enough to thwart hackers, there are solutions available. Rubicon Labs has developed a breakthrough combination of hardware and software that is a lightweight, scalable and secure cyber-armor solution for automotive security. It is provided royalty-free to automotive semiconductor providers.

rubiconlabs.io

Jeep Hack Analysis

- The attacker determines the IP address of target vehicle (Jeep Cherokee) running on the Sprint network.
- The hacker attacks port 6667 which was left open on the car's cellular network. Fiat Chrysler (FCA) did not require authentication on this port.
- This port gave the attacker access to the vehicle's multimedia system (UConnect). One of the processors in the UConnect system is Texas Instrument's OMAP processor.
- The OMAP processor runs as root. From OMAP they used its SPI interface to jump to the Renesas V850 MCU (inside of UConnect).
- The V850 is directly connected to the CAN Bus. Its firmware was designed to only listen to the CAN Bus. The attacker rewrote the V850 firmware to enable it to send commands to the CAN bus.
- The vehicle is completely compromised due to access to the CAN bus. Note: CAN bus communication is neither authenticated nor encrypted. The attacker now controls almost every component of the car, including the brakes, accelerator, in-dash and under-the-hood electronics.
The “connected” car of today has evolved into a collection of dozens of sensors and semiconductors that control everything from braking, acceleration, airbags, navigation and in-dash entertainment, which can link over the air to the Internet. These unprotected connections to the Internet are in essence an unlocked backdoor for hackers and opens up attack vectors that simply did not exist before: web browser exploits, malicious apps, and cloud service manipulation. Once a hacker gains control of a single sensor or microcontroller, he gains control of the entire electronic network under the hood. This added attack surface is expanding rapidly and creating blind spots for automakers and an open road for hackers who can wreak more havoc than drivers who weave and speed while under the influence.

"Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat"
-Sun Tzu

An Elegant Root of Trust

Rubicon provides an easily integrated key provisioning and protection platform for securing sensors, automotive microcontrollers (MCUs) and central processing units (CPUs). A minimal semiconductor footprint coupled with patented hardware root-of-trust protection means that Rubicon Labs’ on-chip solution can fit into any existing automotive network, such as a CAN bus, or can be designed into next-generation cyber-armor as part of a comprehensive automotive security solution.
Protection starts with zero-knowledge

The foundation of our cyber-armor innovation is a unique coupling of a keyed one-way hash function with a secure memory space. This coupling creates a vault that can be provisioned with a key whose value is never known by anyone or anything, but still usable by the device. This is a **self-provisioning zero-knowledge system** that Rubicon uses as the digital identity of the device.

We use zero-knowledge keys to prove an assertion without revealing any other information. A semiconductor-enforced sandbox is secure because the MCU/CPU can interact with the key only to write data to the input of the keyed hash function and to read the resulting output. Even if an attacker gains access to the CPU/MCU, he/she can never access the zero-knowledge key. The address of the key is never readable, keeping the identity of the device secure.

---

Today's crypto is not zero-knowledge

- Modern cryptography is built on the protection of secrets and keys.
- Zero-knowledge proofs allow someone to prove possession of a key, without actually revealing the key itself, or leaking any other information about the key.
- A common cryptographic mechanism for exchanging secrets between two parties, is called public key cryptography.
- In public key crypto systems (RSA, ECDSA...), a sender and a receiver each have a pair of keys, one published in a database available to everybody (public key) and the other kept secret (private key).
- When a sender wants to securely send a secret to a receiver, they simply lookup the receiver's public key in a database, and encrypt the secret with the receivers public key.
- Encryption with the receiver's public key, places the secret in a vault that only the receiver can unlock.
- The receiver unlocks the secret using its private key, a key that should never be exposed to anyone.
- The problem with public key systems, is that the public and private keys have a mathematical link (known as a one way algorithm). This is the link that allows one key to encrypt (public key), and one key to decrypt (private key).
- The one catch is this: revealing the public key to the world actually leaks information about the private key. This prevents public key cryptography from being zero-knowledge, and may eventually make it incredibly vulnerable to advanced computing attacks.
Secure cloud mirroring

Once zero-knowledge keys are provisioned into the secure execution space of a Rubicon device's core, the key is mirrored in a cloud-based distributed device service (DDS). This allows Rubicon to have authenticated identity that is brokered through the DDS.

The DDS is best thought of as a powerful certificate authority, but based on symmetric cryptography (not public key infrastructure). It brokers trust relationships between devices and has a foundation of zero-knowledge keys. This solves the key and identity-provisioning problem that has challenged vendors, as deployed device numbers have grown larger. Rubicon cyber-armor scales far better than asymmetric/PKI-based keys, and has incredible speeds of execution (a requirement for CAN bus speeds).

For example, a Rubicon Labs-based key exchange executes 3000 times faster than an equivalent RSA 2048 bit TLS handshake. This low-power and high-speed feature is critical for the RTOS requirements of the automobile.

Adoption through donation

Rubicon Labs is enabling this ecosystem by making its hardware architecture readily available to semiconductor device suppliers on a royalty-free basis. Because the company’s architecture is based on symmetric key cryptography and one-way hash functions, it can be implemented on the smallest MCUs – a level of scalability that asymmetric crypto can never achieve. It is also important to restate that every Rubicon Labs device has a secure execution space, so no root key or derived session key is ever in attackable memory.
Authentication, encryption, and secure code execution

Rubicon Labs builds on secure identity by deriving session keys between other Rubicon devices and servers. These session keys are all zero-knowledge based, execute in a secure execution space, and allow for authentication, data encryption, and secure execution of signed binaries that are delivered from the cloud.

In a vehicle, the Rubicon cyber-armor can prevent malicious attacks that use identity spoofing, data manipulation, code/binary replacement, and cloning — the exact attacks seen today in automotive systems. These attacks are possible, and even simple, due to a lack of secure identity, secure communication and secure execution of MCUs on the CAN bus.

Security must come first

It is rare that innovations in design, safety and gas mileage take a back seat to security concerns but the unique risks in automotive now make this a requirement with the advent of “connected” cars. Cyber-security is woefully lacking in automobiles — a four-wheel product that may now represent a new category in the “Internet of Things” segment. It’s time for the auto industry to step on the gas and accelerate the adoption of cyber-armor.
**How to prevent auto hacks**

When the ridges on a house key align with the matching pins of a lock, the tumblers move and the door opens. In a similar way, only when two people identify and authenticate each other can a “conversation” commence on an online matching service.

A similar pairing happens when a vehicle receives matching signals from the Internet, but hackers have shown they can fool the car’s electronics into thinking it is following legitimate commands.

By sending bogus commands to the vehicle’s vulnerable Control Area Network (CAN), hackers can hijack any Internet-enabled auto, truck, ambulance, fire engine or school bus. It’s that simple.

To prevent auto hacks, the CAN bus must be able to authenticate the incoming signal based on a secure identity and then authorize it based on an enforced policy that is bound to the trusted identity. Rubicon’s solution is to provide a hardware root of trust that makes the keys that identify and authenticate commands invisible to all users – and almost impossible to hack.

**How Rubicon stops the Jeep hack**

- Rubicon provides a hardware root of trust that prevents malicious code from executing on the V850. This is analogous to validating the passport of a traveler before they can enter the country.

- Rubicon provides secure identities for automotive MCUs. This uniqueness would allow other MCUs on the CANbus to authenticate messages from other MCUs. Even if the V850 is compromised, it would not be able to send authenticate messages to the Rubicon enabled MCUs on the CANbus.