Securing the Connected Car Ecosystem

One of the largest automakers selects Arxan to secure connected car apps

One of the largest global automakers embarked on a vision to revolutionize the Connected Car ecosystem, and took bold steps to transform the way mobile apps interact with the Connected Car. Recent demonstrations by security researchers proved, beyond any doubt, that car hacking is a real risk. Increased connectivity has also introduced new risks / attack vectors to the Connected Car ecosystem. The leading automaker realized the need to address the potential threats, particularly the risks associated with usage of the following:

- **Mobile apps using their APIs to access in-vehicle communications and entertainment systems**
- **Software provided for Dealers to interface with cars through the OBD2 port for diagnostics, configuration changes, or on-board software updates**

Challenge: In-vehicle communications and entertainment system hosts high-value or sensitive applications. API libraries facilitate communication and sharing of vehicle data. These API libraries are vulnerable to reverse engineering and tampering attacks and may even result in loss of passenger safety. Attackers can inject malware that may be able to migrate to other in-car networks such as the controller-area-network (CAN) bus which links to the vehicle's critical systems.

Software provided for dealers to interface with cars through the OBD2 port is vulnerable to reverse engineering and tampering attacks. Hackers may be able to abuse these tools to inject malicious code into the ECUs and CAN bus.

Attackers can lift the cryptographic keys used, and use that to build their own rogue apps/software. Their cloned version of the original app/software may have altered functionality, and may intend to gain access to other in-car networks.

> Recent demonstrations by security researchers proved, beyond any doubt, that car hacking is a real risk.

Solution: Arxan delivered comprehensive application protection to mitigate these risks.

Arxan Cryptographic Key/Data Protection

White-box cryptography is a method for securely hiding cryptographic keys even if a hacker has full access to the software. The original key material is converted to a new representation using a trapdoor function (a one-way, non- reversible function). This new key format can only be used by the associated white-box cryptographic software, effectively hiding the key. However, this is not enough – white-box cryptography hides the key securely, but the hacker could still decompile the original application and modify the app or lift out the entire white-box software package and leverage it in a separate app for nefarious objectives.

Arxan Code Protection to Prevent Code-Lifting and Code-Tampering Attacks

Arxan Code Protection, comprised of unique patented guarding technology, hardens the API library to self-defend against reverse engineering or tampering, both statically and at runtime. Arxan's application protection solution, comprised of unique patented guarding technology, hardens the dealer tools to self-defend against reverse engineering or tampering, both statically and at runtime. It can detect if the white-box software is running in the correct (unmodified) application or in a new environment, and make decompiling the app extremely difficult. Arxan's anti-tamper techniques can respond to runtime attacks with customizable actions and notify the owner that the software is being modified.

Results: Arxan's Cryptographic Key/Data Protection has effectively hidden the secret keys used for authentication.

Given the keys are never present either in the static form or in runtime memory, hackers have not been able to gain unauthorized access to the application and/or to any of the in-car networks.

Arxan's Code Protection has "hardened" the client app and dealer tools, making it extremely difficult for a hacker to gain access to the source code and all of the security controls, lift the white-box software package and/or modify the behavior of the application at run-time.

About Arxan Technologies

Arxan is the trusted global leader of Application Attack Prevention and Self-Protection products for Internet of Things (IoT), Mobile, Desktop, and other applications. We help protect our customers against financial loss, brand damage, fraud, IP theft, stolen credentials, fraudulent transactions, unauthorized access, non-compliance with regulatory and industry standards, and more. Our unique patented guarding technology **1. Defends** applications against attacks, **2. Detects** at run-time when an attack is being attempted, and **3. Deters** attacks to stop hackers, send alerts, or repair making customers' applications truly resilient. We are currently protecting applications running on more than 500 million devices across a range of industries, including: financial services, automotive (connected automobiles), healthcare (connected medical devices), digital media, gaming, high tech/independent software vendors (ISVs), and others. The company's headquarters and engineering operations are based in the United States with global offices in EMEA and APAC. **Learn more at www.arxan.com.**