TABLE OF CONTENTS

1 Executive Summary

2 Threats to the Connected Car

3 How Hackers Attack
   • Reverse Engineering
   • Tampering with Code

4 Application Shielding: Fortifying the Connected Car

5 Intertrust’s Products for Connected Car Security
   • whiteCryption®
   • Seacert™
   • Personagraph™
Executive Summary

The global market for connected cars will grow by 270% by 2022 with 125 million passenger cars expected to ship worldwide between 2018 and 2022. By 2020, it’s estimated that UK, France and Germany will reach 100% connected car penetration. Growth in the European region is due to the eCall mandate which requires new cars to automatically dial the 112 emergency number in the event of a serious accident. While North America and Europe lead in the highest percentage of shipments, China accounts for 32% of shipments.

The list of connected features enjoyed by consumers that add more opportunities for security attacks include streaming radio, Wi-Fi access points and remote-control mobile phone applications. However, with these conveniences comes responsibility. The recent death of a woman in Arizona who was struck by an Uber in autonomous mode has put a spotlight on what can go wrong in connected vehicles as manufacturers seek to introduce more high-tech features to remain competitive to car buyers. Not surprisingly, 68% of Americans are fearful of cars with self-driving features.

The increasing number of smart features built into cars opens door to a serious threat - hacker attacks. Because connected cars are linked with the Internet and its crucial parts are interconnected over a network, adversaries have the potential to remotely access and manipulate the data being exchanged leading to a number of problems, such as leaked personal information, overcoming vehicle’s security mechanisms, or even full remote control of the car.

This white paper describes the potential threats in modern connected cars, the ways hackers attempt to tamper with the data and software, and the solutions to these threats. Finally, this paper will focus on Intertrust’s robust solution to protecting connected cars – a set of software tools that are intended to increase application-level security and render hacker attacks extremely difficult and expensive to execute.

Threats to the Connected Car

Innovative automakers, software developers, and tech companies are transforming the automotive industry. Drivers today enjoy enhanced entertainment, information options and connection with the outside world. As automobiles move towards more autonomous capabilities, the stakes will raise in regards to security. Even if cars are not entirely driverless, the functions will become increasingly dependent on applications, connectivity, and sensors. Vehicle-to-vehicle (V2V) and Vehicle-to-Infrastructure (V2I) allow the car to communicate with other cars and infrastructure such as traffic lights. Vehicle speed adjustments, telematics, and AI voice recognition and interfaces will become common features.

The rapid increase of these technologies inevitably creates the risk of hackers gaining access and control to the essential functions and features of those cars and utilizing information on drivers’ habits for commercial purposes without the drivers’ knowledge or consent.
Here are some of the risks for connected cars:

**Stealing personally identifiable information (PII):** Today, sensors generate 25 GB of data per hour and this is expected to double considering there will be 200 sensors installed in connected cars by 2020, up from 100 sensors in 2015. Once autonomous vehicles become mainstream, the 17,600 minutes Americans spend driving annually will equate to 300 TB of data per year. Financial information, personal trip information, location information and entertainment preferences are just some examples of PII that can potentially be stolen through a vehicle’s system.

**Connection security:** Like other connected devices, vendor implementation flaws are often exploited by researchers for proof-of-concept attacks. However, it is inevitable that these will be followed by real life attacks. The current poor state of security on connected cars creates a tempting target for cyber criminals.

**Manipulating a vehicle’s operation:** Catastrophic incidents resulting in personal injury and lawsuits may surface in the near future. Well-known cybersecurity researchers Charlie Miller and Chris Valasek have demonstrated several proof-of-concept attacks where they were able to control the braking and steering of a car by accessing the adaptive cruise control system. Although costly and with a lower likelihood than data breaches and unauthorized entry, this sort of attack has now been proven possible to a global audience.

**Unauthorized vehicle entry:** Car thieves now have a new way to gain entry into locked vehicles. Many vehicle technologies have opted to replace physical ignition systems with keyless systems using mobile applications or wireless key fobs. These new access mechanisms mean that methods of obtaining illicit entry include intercepting the wireless communication between the vehicle and the mobile application or between the wireless fob and the vehicle to gain entry credentials, among other methods. The New York Times has documented methods such as wireless key emulation devices and “power amplifiers” that increase the range of the wireless signal looking for the entry credentials. If the owner is in a house or other location close to the car, criminals can then gain entry when their wireless fob responds.

**Mobile application security:** As more automobile manufacturers release mobile applications that communicate with cars, mobile applications are quickly becoming a major target for malicious behavior. One example of a flaw in a mobile application happened when Nissan had to pull its NissanConnect EV application for the Nissan Leaf. The poor security of the application allowed security researchers to connect to the Leaf via the Internet and remotely turn on the car’s heated seating, heated steering wheel, fans and air conditioning. In an electric car, this meant the possibility a malicious actor could drain the battery of an unsuspecting owner. Mobile applications themselves can be vulnerable in a number of ways. According to Gartner, 75% of mobile applications would fail basic security tests. Mobile operating systems themselves are a source of concern – over the last four years, there has been a 188% increase in the number of Android vulnerabilities and a 262% increase in the number of iOS vulnerabilities.

---

5. [http://illmatics.com/remote%20attack%20surfaces.pdf](http://illmatics.com/remote%20attack%20surfaces.pdf)
7. [http://www.wired.co.uk/article/nissan-car-hacked](http://www.wired.co.uk/article/nissan-car-hacked)
8. [https://www.gartner.com/newsroom/id/2846017](https://www.gartner.com/newsroom/id/2846017)
THE FAILURE TO PREVENT REVERSE ENGINEERING AND TAMPERING IN CONNECTED CAR SYSTEMS LEADS TO BROKEN SECURITY, LIABILITY, AND EVEN RISK TO HUMAN LIFE. APPLICATION SHIELDING IS THE SOLUTION FOR PROTECTING SENSITIVE DATA AND PREVENTING HACKS IN MODERN CARS.
How Hackers Attack

In order to understand threats to the connected car, we must understand what hackers are trying to achieve. Hackers will mount different kinds of attacks to achieve different kinds of goals. The most dangerous goal might be to bypass controls in safety critical systems, such as steering, brakes, and transmission. But hackers might also be interested in obtaining valuable pieces of data that are managed within the car software, such as personally identifiable information (PII) or car trip and performance statistics. While data can be protected with cryptography, this only shifts the problem from protecting the data directly to protecting the cryptographic keys.

Hackers employ two fundamental techniques when attacking: reverse engineering and tampering. If the hacker tries to bypass the business logic, they have to find where in the application the business logic resides; that requires reverse engineering. Then they must tamper with the application to bypass that logic.

Reverse Engineering

If the hacker is trying to steal sensitive data or cryptographic keys, they have to know where to look in the application. Unless those secrets are obvious, hackers need to reverse engineer the application to find them.

Reverse engineering plays a central role to almost every hacker when attacking applications. Reverse engineering is extraordinarily hard work. The people who do it have a large toolset and focused mind. Their goals are totally different from the goals of software engineers. For example, they are not concerned with fixing bugs; instead, they introduce artificial bugs into the compiled code to see how it breaks. Hackers are familiar with common structures in compiled code. They might look for a string corresponding to an error message related to their objective (e.g. “Engine failure” or “Anti-lock brake system disabled”) and trace where that string is used. They leverage sophisticated techniques such as static analysis which helps them understand the overall structure of the code, where the functions are located and how they are called from other functions.

Tampering with Code

If hackers have physical access to a device, they can directly tamper with the application. Consider how you might bypass business logic. Often, the way this is done is by making one small change to the application. Consider the following code:

```plaintext
if (getTachometerRPM() > 4500) {implementVTECSwitchover();}
```

If the hacker is able to identify this particular piece of code, then they can often bypass it by any number of ways, typically at the assembly language level:

- Inverting the logic of the conditional jump:

  ```plaintext
  if (getTachometerRPM() < 4500) {implementVTECSwitchover();}
  ```

- Replacing the test with a tautology:

  ```plaintext
  if (true) {implementVTECSwitchover();}
  ```

They might also replace function calls to functions of their own design. For example, they might trick the application into calling their own version of `implementVTECSwitchover()`, which executes some part of code they are after.
Application Shielding: Fortifying the Connected Car

Application shielding is the process of adding security functionality directly to mobile applications so that they can withstand hacker attacks independently from the surrounding environment. Application shielding combines prevention, detection, remediation and prediction to go beyond basic best practices to deliver the highest level of mobile application security available today.

As more applications, connections and sensors run in the untrusted environment of the connected car, heightened security measures are apt to follow. By 2020, 30% of enterprises will use application shielding to prevent intrusion, tampering and reverse engineering\(^\text{10}\). Application shielding is ideal for high-value applications to prevent the crippling effects one hack can have on auto manufacturers when brand and company trust are at stake.

Application shielding utilizes the following main methods:

**Obfuscation:** The term “obfuscate” means to render obscure, unclear or unintelligible. The goal is to remove as much of the structure as possible that would be familiar to reverse engineers, to make the code as confusing as possible while keeping functionality the same. Control flow obfuscation modifies the basic structure of how subroutines are called. For example, calls to subroutines could be replaced with computed jumps and functions can be inlined. Symbols for function names can be replaced with random strings.

**Integrity protection:** One of the cornerstone mechanisms of application shielding is to prevent attackers from making any modifications to the application code. That is exactly the purpose of integrity protection. To achieve this, several sophisticated methods are used. For instance, hundreds of very small functions can be embedded into the code, which calculate checksums of fragments of code and compare them to the checksums stored at compile time. Another method is to add a signature of the code to the executable and, at run time, verify if the code matches the signature.

**Whitebox cryptography:** This is a highly specialized form of anti-reverse engineering, in which a special cryptographic library provides strong protection for cryptographic keys. In white box cryptography, the underlying mathematics of the cryptographic operations are obfuscated in such a way that the keys never appear in the clear. Standard operations such as encryption, decryption, key unwrapping, and digital signature creation and validation can all be done with white box cryptography techniques, protecting the keys even if the device is jailbroken or rooted.

**Debugging:** One of the primary tools hackers use to reverse engineer code is debuggers. Normally used by legitimate software engineers to find bugs in code, debuggers give hackers a powerful tool from which to reverse engineer code. Debuggers generally work by setting interrupts at specific points in an executable, thus modifying the executable. Application shielding inserts numerous anti-debug checks into your protected application. These checks take into account the unique indications of the target platform that may identify the presence of a debugger.

**Jailbreak and rooting detection:** Jailbreaking and rooting are similar terms that describe the process of gaining privileged access to a device and overcoming its software and hardware limitations established by the vendor. A jailbroken or rooted device can be used to install a modified version of a car manufacturer’s mobile application, which could be used to execute malicious activities with the vehicle. Therefore, the standard security practice is to prevent the application from running on jailbroken and rooted devices by employing a number of smart detection checks inserted into the code.

Intertrust’s Products for Connected Car Security

With over 20 years of experience in digital security, data privacy, trusted computing and data governance, Intertrust Technologies Corporation is well positioned to support automobile manufacturers as they proactively move to address privacy and security in the age of the connected car. Our visionary and innovative technologies are available and integrated to ensure end-to-end protection and governance for data as automotive systems speak to one another, other automobiles and the cloud.

whiteCryption®

whiteCryption, a subsidiary of Intertrust, is a leading provider of application shielding solutions to prevent hackers from reverse engineering and tampering with code. We specialize in world-class advanced obfuscation, runtime application self-protection (RASP), and white box cryptography solutions for mobile applications, desktop applications, firmware and embedded applications.

Our application shielding portfolio consists of two products:

- **whiteCryption® Code Protection™** provides application developers with a comprehensive suite of anti-reverse engineering and run-time application security protections to help protect your applications. Code Protection is easy to use and requires no significant changes to the code itself or the existing build chain. Since Code Protection secures source code before it is compiled, protected builds can easily be delivered to an electronic control unit, mobile device, and any other device or application in your connected car ecosystem.

- **whiteCryption® Secure Key Box™** is an advanced white box cryptographic library that protects cryptographic keys for critical security functions such as device authentication, secure communications, and data encryption. With Secure Key Box, cryptographic keys are never in the clear in use, in transit or at rest, preventing hackers from stealing your keys and using them to masquerade as users, snoop on secure communications, or unlock content that is critical to your business. Secure Key Box is easy to use; it is a drop in cryptographic library that functions in the same way as common cryptographic libraries, such as OpenSSL or LibTomCrypt.

Our products are backed up by superlative support and professional services to help you achieve your business goals quickly and efficiently. Market leaders have deployed whiteCryption tools in mission critical situations in major automotive, banking, finance, healthcare, and media and entertainment applications around the world. Our technology protects millions of devices and applications, protecting personal information, crypto algorithms running in hostile environments and sensitive intellectual property; we extend the secure perimeter around applications beyond where traditional technologies have gone. whiteCryption is an important weapon in protecting you and your customers from unwanted intrusion and misappropriation of personal information and data.

Learn more about whiteCryption at: [https://www.intertrust.com/products/application-shielding](https://www.intertrust.com/products/application-shielding)
Seacert™

Founded over a decade ago by Intertrust, Seacert provides public-key infrastructure (PKI), specializing in large-scale key provisioning for device identities. Seacert’s services are used by leading media and entertainment companies, manufacturers of automotive, healthcare, and other types of IoT devices. Seacert credentials are embedded in hundreds of millions of devices and applications worldwide.

Seacert services include:

- **Public Key Infrastructure (PKI):** We provide standard PKI services, including creation and management of root certificates and certificate authorities, certificate signing requests, and certificate revocation services. Our services meet the highest industrial quality standards certified to both Webtrust and ISO 9001 standards.

- **High-Volume Device Identity Provisioning:** We provision millions of devices every day with cryptographically secure identities and authorization credentials. We provide both factory floor provisioning with bulk key delivery and field provisioning through our cloud-enabled provisioning services. In the last 12 years we have shipped over 5 billion keys to market without error.

- **Custom Design:** Unlike other PKI providers who focus on delivering standard TLS/SSL certificates or employee credentials, we focus on creating device personalities that meet the needs of the complex ecosystems of stakeholders in the device. Our customers typically have unique requirements for device personalities that include multiple keys, both symmetric and asymmetric, authorization credentials, custom X.509 extensions, and custom secure delivery designs. Our experts work with you to design a management and delivery infrastructure that meets your unique needs.

Seacert delivers these PKI services at a fraction of what it costs for an organization to create their own services internally, and we deliver these services with state-of-the-art security and business continuity controls.

Learn more about Seacert at: https://www.intertrust.com/products/key-provisioning

Personagraph™

Connected cars collect a significant amount of data and can interface with multiple aftermarket devices. Financial information, personal trip information, and diagnostics are just some of the data that can be accessed through a connected vehicle. Personagraph, a subsidiary of Intertrust, offers a cloud aggregation layer for all of the data points generated from on-board devices and sensors. Personagraph’s analytics deliver a comprehensive dashboard providing end-to-end insight allowing for useful services of value to drivers and passengers as well as automobile and aftermarket accessory manufacturers. The Personagraph platform provides technology for consumers to manage how their data is used as well as ensure personally identifiable information is not collected or exposed. Personagraph also allows manufacturers the ability to create private data marketplaces, giving them full control over how their data is used.

Car manufacturers, for the first time, are getting a sense of who their drivers really are and where they go. Driving provides unprecedented amount of contextual data. Through our proprietary data inferencing, Personagraph can take mobile signals and provide insight about an audience. We can reveal a car owner’s interests, preferences, and perhaps most interestingly, when they are most likely to purchase a new car.

Learn more about Personagraph at: https://www.intertrust.com/products/audience-platform
About Intertrust Technologies Corporation

Copyright Information:
Copyright © 2004-2018, Intertrust Technologies Corporation. All rights reserved. All trademarks are the property of their respective owners.

Contact Information:
Intertrust Technologies Corporation
920 Stewart Drive, Suite #100
Sunnyvale, California 94085, USA

https://www.intertrust.com