irdeto
Building a Secure Future.™

Datasheet

MITIGATING AUTOMOTIVE CYBERATTACKS

How automotive cyberattacks would have looked if Irdeto's connected transport security solutions had been applied.

The frequency of cyberattacks on the connected transport industry shows rapid growth. The number of reported cases increases daily, ranging from security assessments by ethical researchers to real-world attacks by financially-motivated hackers or those with malicious intentions. Irdeto has solutions.

Irdeto's Secure Environment assumes perimeter security is compromised and focuses on uniquely protecting everything else. With multilayer security, it safeguards critical files and app data, and prevents hackers from adding malicious code, modifying executables and scripts, and reverse engineering.

Irdeto's Keystone is a secure system that integrates directly with the vehicle's settings. This allows vehicle owners to create and control policies around multi-user vehicle access, settings and usage, which enables new business models.

Below, we look at some of the recent, notable attacks. We also detail the key methods that were employed and how Irdeto's security solutions would have mitigated the risks.

Method	Mitigation
CAN message injection via mobile app. In March 2018, a vulnerability in a couple of Volkswagen mobile applications enabled hackers to inject CAN messages. A malicious attacker could use this to take control of car systems.	**Secure Environment** has teamed up with SafeRide whose vSentry is the industry-leading, multilayer cybersecurity solution for connected and autonomous vehicles that combines a state-of-the-art deterministic security solution with a groundbreaking AI profiling and anomaly detection technology to provide future-proof security. Secure Environment also allows OEMs and Tier 1s to define who can access resources and provides telemetry reports for all security events.
Car2Go app hacked leading to stolen vehicles. In April 2019, less than a year after the Chicago-based car-sharing app was launched with 400 Daimler cars, it was discovered that the Car2Go app had been hacked and 100 cars were missing. The specifics of the hack are unclear; it appears the hackers tampered the app to unlock the doors. While there was a 29-square mile drop-off zone defined, the cars were never limited from leaving that area.	**Keystone** is a secured system that allows vehicle owners to create and control policies around multi-user vehicle access, settings and usage. It provides components on the vehicle-side, cloud-side, and a Secure Mobile Engine on the smartphone-side that is designed to resist direct and indirect attacks. It also provides policy-setting geo-fence capabilities that restrict the cars to the intended geographic location.
Two Peugeots stolen using relay attack. In April 2019, two Peugeots with keyless entry and push button start were stolen using a relay attack. The criminals used a box that relays the signal of a car key to gain entry and start the vehicle.	**Keystone**'s three component (mobile, cloud, vehicle) solution includes protection against relay attacks by taking the proximity of the user device into account.

© 2019 Irdeto. All Rights Reserved.

Instrument cluster attacked to roll back odometers. In April 2019, it was discovered that over 1.6 million cars had odometers that had been rolled back. Using an inexpensive electronic device to hack into the car's computer, a technician demonstrated that he could erase 100,000 miles in less than 30 seconds. Such an attack could not only artificially inflate the value of a vehicle, but the erased history could impact the vehicle's warranty and safety.	**Secure Environment** includes a system-wide anti-debug feature. Attackers would not have been able to use the device to hack into the system without first spending a lot of effort trying to defeat the anti-debug feature. Additionally, any binaries modified, either in-memory or on-disk, are disallowed, making any data modification intrusion difficult.
Sniffing CAN to add new features. In May 2019, a research-based hacker used a PCAN-USB adapter to connect to the car's OBD-II port. He shifted into and out of reverse to observe which messages were transmitted on the network. By identifying and injecting the right message, he was able to hack in a forward-looking camera no matter what gear the car was in.	**Secure Environment** (SE) allows OEMs and Tier 1s to add access protection to their resources during integration time; for example, the CANBUS. Customers can define the resources (files, dev_node, etc.) and what can access them. SE's telemetry events report for all security events can detect the early research phases and allow a response. Furthermore, SE's partner, SafeRide, provides extensive monitoring of the CANBUS.
Crashed Tesla vehicles expose personal data. In March 2019, a security researcher extracted unencrypted video, phonebooks, calendar items and other personal data from crashed Tesla vehicles that are sold at junkyards and auctions.	**Cloakware Software Protection** (CSP) offers whitebox encryption and transformation technology, as well as unique secure storage for personal data. Even if the data remained in the re-sold vehicles, it would not be easily accessible or understandable.
New cars found to be vulnerable to keyless entry hacking. In March 2019, a research group ranked new cars on how vulnerable their keyless solution is. Six of the 11 tested were ranked as 'poor.' Vulnerability to relay attacks was specifically mentioned as lacking.	**Keystone** addresses relay attacks as well as other common attack approaches, including Man-in-the-Middle and Man-at-the-End attacks. It also protects common entry points such as BLE, Wi-Fi, debugging ports and ECU updates.
U.S. Army's armored vehicles have been hacked. A February 2019 Pentagon report shows that unspecified adversaries disrupted certain systems on armored vehicles via a cyberattack.	While details of the cyberattack were not reported, it seems likely that the attacks affected the vehicle's data-sharing, navigation, or digital communications capabilities. **Secure Environment** would have ensured these applications were not tampered.

A CASE STUDY: HOW DIFFERENT KEEN SECURITY LAB'S SECURITY ASSESSMENT OF BMW CARS WOULD HAVE LOOKED IF IRDETO SECURE ENVIRONMENT AND SOFTWARE PROTECTION HAD BEEN APPLIED.

On May 22, 2018, Tencent Keen Security Lab released an "Experimental Security Assessment of BMW Cars". They discovered vulnerabilities of varying severity. Their success path followed a general flow of attacks that leverage physical access, as shown on the right.

While this study focuses on a particular vehicle type and success path, it is only one example of the many approaches that threaten connected transportation. The methods used and available Irdeto mitigations discussed are not limited to this specific case.

Gaining root shell via a local interface yields

…more access to the details of implementation of the remote services running on the target which yields

…the discovery of a remote vulnerability in the target and development of the exploit in-situ thanks to the root shell; which ultimately yields

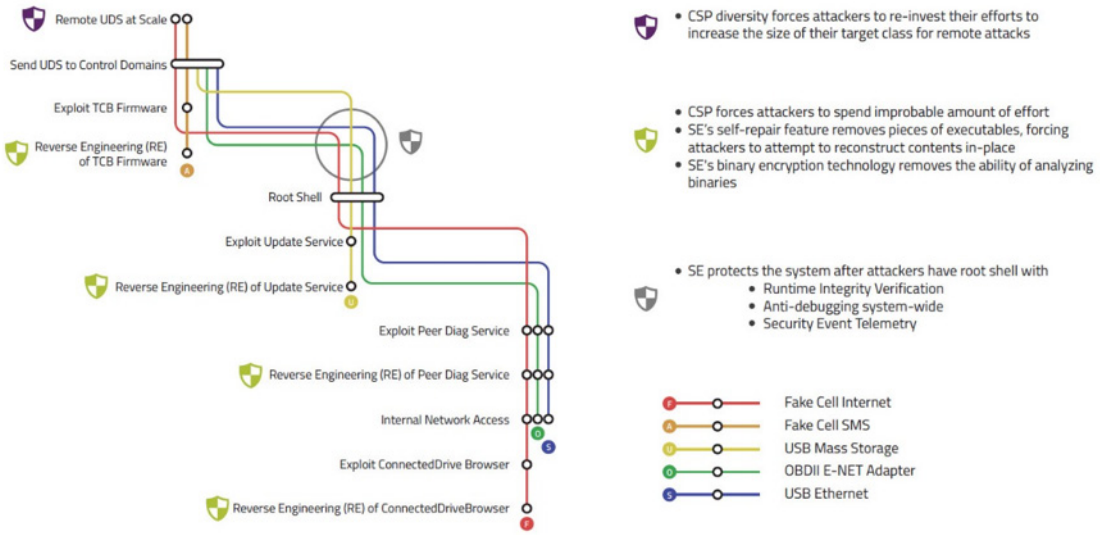
…the ability to deploy an exploit remotely and at scale

© 2019 Irdeto. All Rights Reserved.

Method	Mitigation
Abuse of the update service to deploy privileged executables. The Keen Lab researchers used update services to run their own executables. From the current details, it isn't clear whether Keen Lab exploited a vulnerability to gain control of an update service or abused the update service by bypassing its upgrade payload signature checks.	Secure Environment includes runtime integrity verification, which prevents the use of any executable code unless it has been signed. Even if the update service had such a critical flaw that package signatures were not being exhaustively checked – integrity verification would prevent attackers from running any tools or executables. Integrity verification at load-time and runtime ensures that a start-up check is never trivially bypassed.
Debugging target processes to explore and identify vulnerabilities and test exploits. It is clear that the Keen Lab researchers were using gdb on the hu-intel target (in Figure: Memory Corruption in Bluetooth Service).	Secure Environment includes a system-wide anti-debug feature, which would have prevented attackers from using the gdb tool to debug any target processes without first spending a lot of effort. In addition, since unsigned executables are not permitted to run, the attacker must defeat multiple defenses to use the debugger.
Redeploy a remote attack at scale. The Keen Lab researchers demonstrated the applicability of a remote exploit in both the ConnectedDrive browser and the NGTP SMS processing of the TCB firmware. Though not undertaken by the team of ethical hackers, criminal attackers would most certainly use this to attack multiple targets of the same class remotely.	Cloakware Software Protection (CSP) uses parametrized data transformations which can be seeded for randomization. CSP preserves code functionality, resulting in multiple compiled binaries of a program, which are functionally equivalent but also diverse in their implementation. This can thwart re-use of attacks at scale, forcing attackers to re-invest their time and resources to grow the size of the target class for their remote attacks.
Early investigation phases. The researchers were 'poking around' in the systems, exploring capabilities.	Secure Environment (SE) includes a telemetry events report for all security events and the ability to tailor security policies for individual systems. Had SE been deployed, security operations for the connected vehicle manufacturer could have detected the early research and responded. They could have locked down the target system or opened it up temporarily only to shut it down later, causing the attackers to waste their time and resources.

© 2019 Irdeto. All Rights Reserved.

Reverse engineering of E-NET peer diagnostics service. The Keen Lab researchers reverse-engineered the E-NET service to identify a vulnerability, which enabled them to develop an exploit. Reverse engineering of firmware. The researchers obtained the raw firmware of at least the TCB. They noted that this was “tough reverse engineering work.” They did not report how they obtained the firmware. Microprocessors don’t often have readout protections, or the protections can be bypassed with physical attacks (e.g. glitching).	Cloakware Software Protection uses data and control-flow program transformations to raise the bar for reverse engineering to improbable levels of effort. Particularly when considering high-privileged processes that parse network or local inputs, integrating CSP will force a much higher investment of time and resources on the part of the attackers. More often than not, this pushes the attackers towards other targets.
Leveraging a Root Shell on the Target. The Keen Lab researchers took advantage of the root shell they obtained to deploy new executables, explore system resources and inspect memory contents of all processes.	Secure Environment’s (SE) threat model assumes the attacker has control of the shells that have root privilege. SE realizes the system security enhancing features through multiple mutually-reinforcing user space agents. These agents are self-protected with multi-layer anti-tamper techniques using Cloakware Software Protection. Instead of at the end of an intrusion, attackers with a root shell find themselves at the beginning of a large effort to attack the rest of the system.



For more information about Connected Transport by Irdeto, please visit: Irdeto.com/connected-transport/

© 2019 Irdeto. All Rights Reserved.