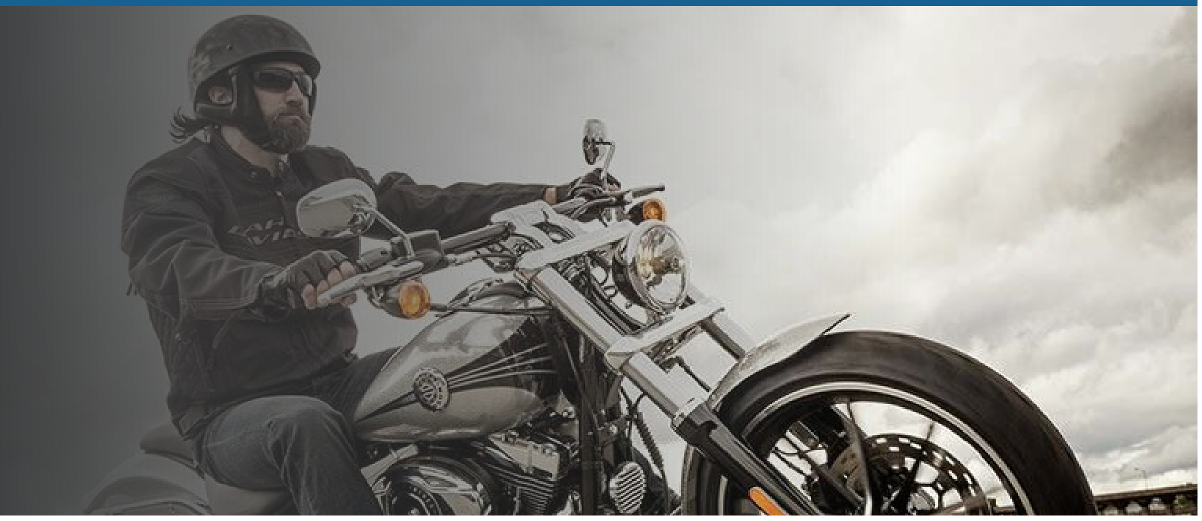
HH◦ MOTORCYCLES

Building trust in a software world.

Security Innovation Secures
Motorcycle Performance.

Biker's Rejoiced



PROJECT

Motorcycle Ignition Control System (ICS) Reverse Engineering

CUSTOMER CONCERNS

The motorcycle's ignition control system (ICS) governs the spark timing to ignite the engine's fuel-air mixture. The client needed to understand if the system could be reverse-engineered to tweak the performance of the motorcycle, such as increasing horsepower by adjusting spark timing or altering the rev limits.

THE MISSION: WHY WE HACKED IT

The ignition control system on this motorcycle, a Suzuki Katana, was being investigated for potential performance tuning. The system was embedded within a sealed box and controlled the timing of the ignition sparks via a microcontroller. The client wanted to reverse engineer the system to modify the engine's performance. The goal was to learn more about the ICS and determine if it could be reprogrammed to boost performance without compromising reliability.

THE BREAKDOWN: WHAT WE FOUND

We approached the reverse engineering process by:

- **Hardware Deconstruction:** Attempted to physically access and probe the circuit board within the sealed ignition control system to understand how it operated.
- **Microcontroller Identification:** Identified the microcontroller governing the system, despite challenges caused by the protective sealing, and searched for debugging or reprogramming interfaces.

DURING TESTING, WE UNCOVERED SEVERAL CRITICAL ISSUES:

- **Sealant Protection Mechanism:** The system was heavily sealed with materials designed to deter reverse engineering, which led to some damage when trying to access the board.
- **No Debug Interface:** Despite thorough testing of potential interfaces, there was no straightforward method to reprogram the microcontroller or extract the firmware.
- **Limited Firmware Accessibility:** The microcontroller utilized mask ROM, meaning the firmware was hardcoded and could not be extracted without advanced techniques like decapping

BY REMEDIATING THESE ISSUES, THE CLIENT WAS ABLE TO:

- **Pivot the approach to Black Box Testing:** By simulating the inputs and measuring the outputs (e.g., camshaft position and throttle), the client successfully inferred the ignition timing algorithms.
- **Build a Custom Simulator:** The client created a custom microcontroller system to mimic the ICS behavior and explore performance tuning possibilities.

As a result, the client gained a deeper understanding of how the ICS controlled the engine's performance and could start building a new, programmable system to improve power and efficiency. While direct reprogramming wasn't possible, the black-box approach provided valuable insights into how to modify the ignition timing for enhanced performance.