How to get into your car's electronics

Craig Smith's Car Hacker’s Handbook shows how to identify network security risks, exploit software vulnerabilities, and gain a deeper understanding of the software running in our vehicles.

The early chapters provide a significant amount of technical information around the CAN network (Photo: No Starch Press)

Modern cars are more connected than ever before. Infotainment and navigation systems, diagnostics, Wifi, software assisted steering, and other innovations form a complex network that helps make driving a breeze. But these innovations also expose modern vehicles to attacks by hackers that jeopardize the safety and security of millions of vehicles. Craig Smith has written a 300-page handbook for car hackers published by No Starch Press (USA). It is a guide for penetration testers.

The book provides the reader with a detailed overview of the computer systems and embedded software ubiquitous in today’s new cars. The author describes the numerous entry points where a hack can occur. Starting with CAN, the infotainment system, the engine control unit (ECU), and more.

The target audience for this book is really people who have a working knowledge of programming and who are familiar with Linux. Smith makes things easy to follow but some people would probably be lost if they are interested in cars but new to programming. On the other hand, if you want to learn how to analyze a CAN network, this book is probably what you need.

If you do want to get into making some real modifications to your car, this book is a good first step though. Nowadays, many computers control the car. This book explains what they do, how they are organized, and how to monitor your vehicle for better understanding. This book isn't going to turn you into a professional hacker, but when you're done reading you'll have a better understanding of how cars really work and how to probe a bit deeper into them.

The Car Hacker’s Handbook is available as a Kindle edition (€ 24.32) and a soft-cover version (€ 37.99). The author, Craig Smith, runs Theia Labs, a research firm that focuses on security auditing and building hardware and software prototypes. He is a founder of the Hive13 hackerspace and Open Garages. Craig is a frequent speaker on car hacking and has run workshops at RSA, DEF CON, and other major security conferences. He has worked for several auto manufacturers, where he provided public research on vehicle security and tools.