FOREWORD

There was a time in the not-so-distant past when hardware was relegated to the fringes of hacking. Many considered it too difficult to get involved with. “Hardware is hard,” they’d say. Of course, this is true of anything before you become familiar with it.

When I was a juvenile delinquent with a passion for hardware hacking, access to knowledge and technology was often out of reach. I’d jump into dumpsters to find discarded equipment, steal materials out of company vehicles, and build tools described in text files with schematics fashioned from ASCII art. I’d sneak into university libraries to find data books, beg for free samples at engineering trade shows, and lower my voice to sound distinguished when trying to get information from vendors over the telephone. If you were interested in breaking systems instead of designing them, there was rarely a place for you. Hacking was a long way from turning into a respectable career.

Over the years, attention to what hardware hackers could accomplish shifted from the underground to the mainstream. Resources and equipment became more available and cost affordable. Hacker groups and conferences provided a way for us to meet, learn, and join forces. Even academia and the corporate world realized our value. We’ve entered a new era, where hardware is finally recognized as an important part of the security landscape.

Within The Hardware Hacking Handbook, Jasper and Colin combine their experiences of breaking real-world products to elegantly convey the hardware hacking process of our time. They provide details of actual attacks, allowing you to follow along, learn the necessary techniques, and experience the feeling of magic that comes with a successful hack. It doesn’t matter if you’re new to the field, if you’re arriving from somewhere else in the hacker community, or if you’re looking to “level up” your current embedded security skill set—there’s something here for everyone.

As hardware hackers, we aim to take advantage of constraints placed on the engineers and the devices they’re implementing. Engineers are focused on getting the product to work while remaining on schedule and within budget. They follow defined specifications and must conform to engineering standards. They need to make sure the product is manufacturable and that access is available to program, test, debug, repair, or maintain the system. They place trust in the vendors of the chips and subsystems they are incorporating and expect those to function as advertised. Even when they do implement security, it’s extremely difficult to get right. Hackers have the luxury to ignore all the requirements, cause the system to intentionally misbehave, and look for the most effective way to successfully attack it. We can attempt to exploit weak spots in the system, whether through peripheral interfaces and buses (Chapter 2), physical access to components (Chapter 3), or implementation flaws susceptible to fault injection or side-channel leakage (Chapter 4 and onward).

What we’re able to achieve with hardware hacking today is built on the research, struggles, and successes of hackers past—we are all standing on the shoulders of giants. Even as engineers and vendors progressively improve on their security awareness and integrate more security features and countermeasures into their devices, those advancements will continue to be outwitted through the hacker community’s persistence and perseverance. This literal arms race not only leads to incrementally more secure products, it sharpens the skills of the next generation of engineers and hackers.

The message in all of this is that hardware hacking is here to stay. The Hardware Hacking Handbook provides a framework for you to explore its many possible paths—it's now up to you to start your own journey!

Yours in solder,

Joe Grand aka Kingpin

Technological troublemaker since 1982

Portland, Oregon