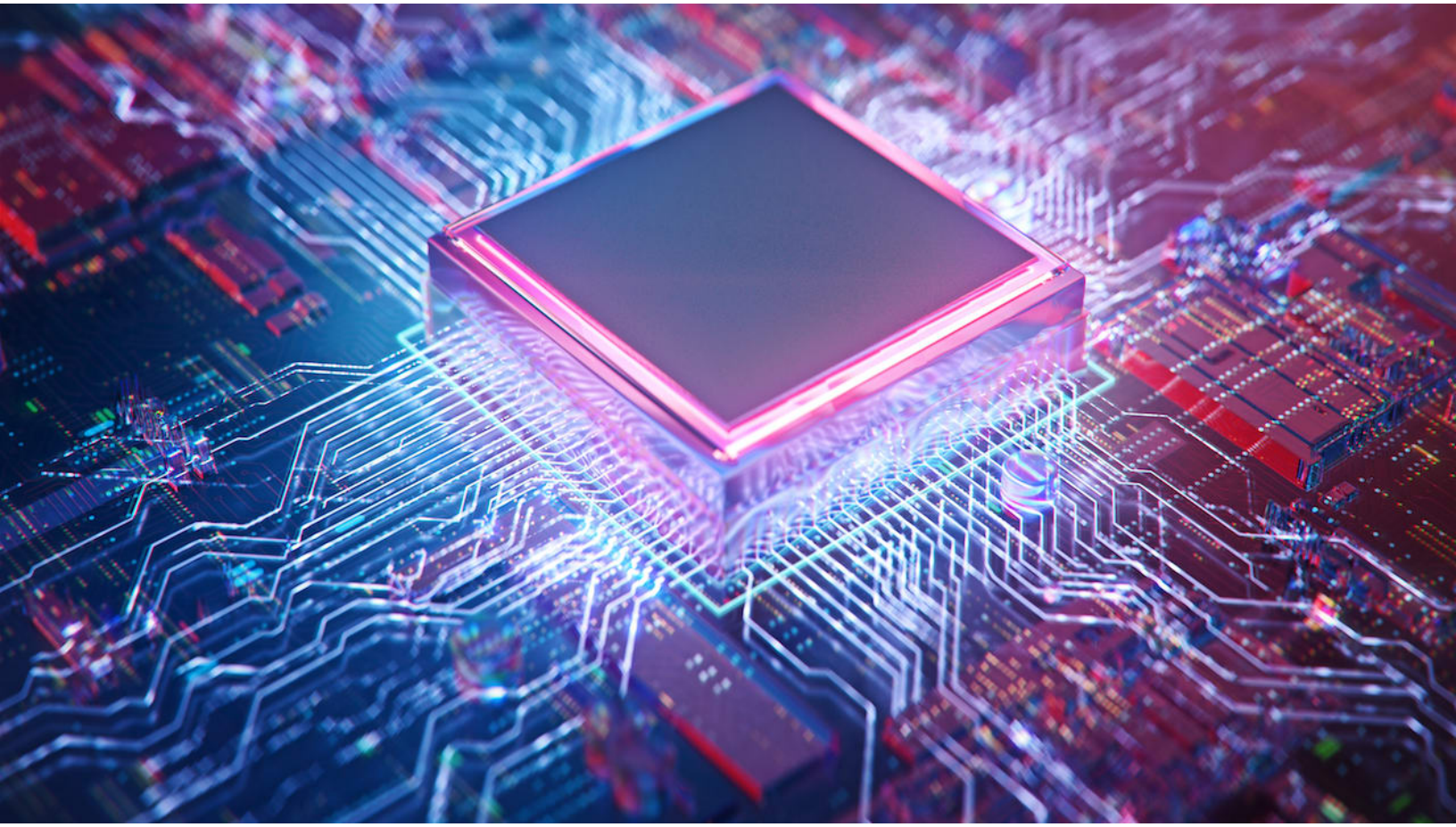

Royalty-free stock illustration ID: 1196754286

Mar 16, 2021 17:33 GMT

Research spotlight: Hardware and embedded systems

We recently published our annual research report from our global head of research, Jennifer Fernick, detailing research spanning a number of areas, including hardware and embedded systems security, applied cryptography, programming languages, machine learning, mobile privacy, cloud and container security, exploit development, industrial control systems/OT security, threat intelligence, and beyond.

In our follow up research spotlight series, we're looking into some of the key

areas in a little more detail. In this instalment, we hear from Rob Wood, technical vice president at NCC Group, for more on our research into hardware and embedded systems, including the issues that exist within hardware and embedded systems, how attack surfaces can be limited, and what ongoing work is needed to address ever-evolving security threats.

What threats or security issues do hardware and embedded systems need to defend against?

This is highly context dependent. Understanding the threat model of your product is vital to knowing which defences you must implement. There are significant differences in attacker profiles – for example, a situation where a journalist's smartphone is lost or stolen and physically accessed is different from a smart light switch that is only affected by local wireless or remote network attacks. Therefore, the defences that must be implemented will also have varying requirements. Needless to say, understanding this up front at the requirements stage can save a lot of pain down the line.

For any network connected device, the remote interfaces need to be hardened as much as possible. Strong authentication and encryption are expected, but so too are patching, fuzz testing, and attack surface reduction.

Many devices today run a variety of third-party code, be it applications on your smartphone or smart TV, or simple javascript in your browser or webview. This poses interesting challenges to defending the system from malicious code running within its boundaries. Adding to this challenge are a recent surge in the discovery of deep hardware architectural issues like Spectre, Meltdown, RowHammer, RamBleed, and more. For any device supporting the execution of third-party code capabilities, code signing, privilege separation, sand-boxing, and other isolation techniques are a must.

For physical attackers, designers need to understand how trivial it is to physically remove the flash memory and dump or modify its contents. Strong hardware-backed data-at-rest encryption is the gold standard countermeasure, and have been considered table-stakes for consumer

devices for many years.

Requiring that the attacker invest in invasive silicon attacks or more complex fault injection or side channel analysis can significantly raise the cost to the attacker, and thereby reduce the number of attackers interested in compromising your devices and users.

Above all, be sure that such an attack on one device does not lead to a compromise of all devices (like the recovery of a shared secret) – ensure that the attacker needs to expend their exploitation effort again for every device so that such attacks cannot scale. Most modern platforms provide all the features necessary to implement defences against physical attacks, however too often these features are just not enabled by the original equipment manufacturers (OEMs).

How can we limit the attack surface of hardware and embedded systems?

Limiting the attack surface is a vital step in any product design process. There are two main strategies to be used here: attack surface reduction, and feature hardening.

The goal of attack surface reduction is to remove as much functionality that is not needed in the product as possible. Choose your components like your SoC and operating system with care, preferring vendors with strong security maturity. But even still, SoC and platform vendors implement many features to help sell their products to the widest possible set of OEMs. And they do not know your product, and so there is a risk that you will inherit features and functionality that you simply do not need in the product. Removing these from your firmware builds is important.

A second form of attack surface reduction is in the deployment configuration: disabling features by default can lead to significant improvements in terms of the exposed attack surface for customers who choose not to use certain

functionality.

Many products, especially consumer devices, contain huge numbers of network-exposed features that are enabled by default, and thereby give an attacker opportunities to exploit potential vulnerabilities in these interfaces. By providing products with features in a disabled state, and requiring that users opt in before enabling them, the exposure can be limited for users who do not need every feature turned on.

For every feature you do include, and allow the user to enable, you must also do your best to harden it as much as possible. Start by patching and making sure you have the latest versions of any dependencies like libraries and other third-party components. Make sure any exposed interfaces have strong authentication mechanisms in place, encrypt traffic where appropriate, are tested thoroughly for security vulnerabilities, and wherever possible, implement exploit mitigations to dampen the effects of any vulnerabilities that remain.

What work is NCC Group doing to combat threats in this space?

Our researchers have carried out some incredible work over the past 12 months to delve into the issues that are still very much present in hardware and embedded systems. This includes a tool developed by Jon Szymaniak to aid product engineers, and security researchers when analysing a customised, product-specific build of the U-Boot bootloader. As part of this work, Jon has explored in-depth how open source software can be made safer and more secure.

As well as this, Ilya Zhuravlev and Jeremy Boone released a blog which explored their methodology for characterising the boot process of the MediaTek MT8163V system-on-chip (64-bit ARM Cortex-A), as well as the design of a cheap apparatus that is capable of reliably producing a fault injection attack against the SoC. Our results showed that the MediaTek BootROM is susceptible to glitching, which allows an adversary to bypass signature verification of the pre-loader.

Finally, we also published a research report on the Zephyr real-time operating system (RTOS). In this report we analysed Zephyr's overall security posture, and documented 25 vulnerabilities that were discovered, some of which are remotely exploitable and could result in a full device compromise.

What work needs to be done to ensure the impact of vulnerabilities continue to be minimised or mitigated?

Devices and systems are rarely designed and built in isolation. The hardware ecosystem is a complex web of hardware and software vendors. With the pressures of cost and time-to-market, pushing as much of the security work upstream to vendors wherever possible is an important strategy.

There are few things more frustrating than inherited vulnerabilities. Selecting vendors that can demonstrate their security posture through reputation and transparency can help immensely. Look for vendors that have clear signals that they take security as seriously as you do, such as public vulnerability disclosure programmes, regular security advisories and patches, long-term product security support commitments, and support for public facing device certification programmes such as the ioXt Alliance.

By encouraging vendors to improve their security posture, not only will your product security improve, but the entire ecosystem can reap the benefits. This will have a noticeable impact on the quantity and severity of vulnerabilities that affect the end users of our technology.

NCC Group provides security consulting services to all aspects of the product development ecosystem, working closely with chipset and platform vendors, and device OEMs alike throughout the product and component lifecycle.

If you'd like to find out more about our hardware and embedded systems research and more, download our annual research report here.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970