Creating a secure hardware product be challenging.

However, our embedded systems security specialists can help you to design and test your products to ensure that they meet the level of security expected by you and your stakeholders, including vendors, OEMs and certifying bodies.

NCC Group can engage at all stages of product development including, architecture & design, component selection, supply chain, manufacturing, implementation review and repair services.

Our services include:

- Secure design & architecture review
- Product security testing
- Threat modeling
- Component specification review & recommendations
- Circuit & component level security testing
- Device hacking & security awareness training
- Forensics & data recovery
- Reverse engineering
- Supply chain security
- Secure product manufacturing & repair
- Commercial Product Assurance & Common Criteria foundation grade assessments

We have expert led hardware lab facilities in Canada, the UK & the US and can also provide on-site expertise.

Secure Design & Architecture Review

Embedded devices can often contain and use sensitive data that should be protected from unauthorised access. Examples include:

- IoT devices contain various Wi-Fi and cloud credentials.
- Mobiles and wearables contain biometrics and payment credentials as well as VPN and other sensitive data.
- Media appliances contain DRM keys and other provisioned secrets.
- Point of sale terminals contain payment details and often have access to sensitive backend systems.
- Smart meters contain data directly related to billing.
- Modems, routers and other networking equipment, all carry and are responsible for the digital life of consumers.

All of the above devices also contain the valuable intellectual property of the designers, manufacturers and vendors.

Additionally, protecting the correct operation of the product might be of significant importance. For example:

- Industrial controllers are responsible for a wide range of critical processes and infrastructure.
- In cars, vulnerabilities are direct customer safety concerns.
- Certification compliance mandates correct product operation for many industries e.g. banking and aviation.
Product Security Testing

Due diligence to ensure that your product adequately protects sensitive data is not only a responsible thing to do, it demonstrates good business practice and in some cases can be a contractual or legal obligation. Our hardware labs specialise in:

- Embedded firmware code review & vulnerability assessment.
- Circuit design review and testing.
- Component selection and specification guidance.
- Hardware threat modeling and attack surface mapping.
- Biometric technology integration expertise.
- Secure platform design and architecture review (TPM, TrustZone, etc.).

Supply Chain Security

How can you build a secure product when you do not trust the factory in which you build it?

Today, cost considerations have pushed outsourced manufacturing to the point where at least some portion of your product is guaranteed to be produced in untested factories.

NCC Group has a great deal of experience investigating and mitigating counterfeiting and other rogue supply chain activities.

Post-Sales Support

The life of a product does not end once it is sold. If it has your company logo on it, it has the power to affect your brand.

In order to ensure the best customer experience, we can help you with all of the security aspects of the post-sales lifetime of a product.

This includes issues such as:

- Incident response and root cause analysis
- Product security updates and roll-out
- Forensics and data recovery
- Reverse engineering, design recovery & anti-counterfeiting

For more information from NCC Group, please contact:

+44 (0) 161 209 5200  response@nccgroup.trust  www.nccgroup.trust

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever-evolving threat landscape.

With our knowledge, experience and global footprint, we are best placed to help businesses identify, assess, mitigate & respond to the risks they face.

We are passionate about making the Internet safer and revolutionising the way in which organisations think about cyber security.