GUIDANCE

Design guidelines for high assurance products

Approaches to the design, development and assessment of products capable of resisting elevated threats.

This guidance recommends approaches to the design, development, and security assessment of products (and systems) capable of resisting elevated threats. It contains a set of principles that can be used to set high level security objectives, which in turn can be used to guide design decisions and development processes.

It's written for organisations that are at risk from these elevated threats, or those seeking to develop products and systems capable of resisting these threats, specifically:

- **buyers** of these products (or independent assessors), to help them gain confidence that a product is capable of resisting elevated threats
- **developers** of product and systems that are intended to protect against elevated threats

This guidance complements the NCSC's existing technology principles (such as those for cloud security, cross domain products, and secure communications), and may be used in conjunction with these to assess the extent to which products offer protection against both commodity and elevated threats.

Note: The ability to gather and validate evidence against these principles is fundamental to their use. The generation and validation of evidence can be achieved in a number of ways that give differing levels of confidence, such as:

- self-assertion by product developers
- validation of presented evidence by a procuring organisation for their own use
- the commissioning of independent validation by a 3rd party organisation.

> **CAPS High Grade assessment**
>
> For certain threat models and technologies the NCSC undertakes independent assessment of products (primarily cryptographic products) that require an NCSC 'High Grade' Certificate. This assessment is performed under the CAPS assurance scheme, which is underpinned by detailed requirements and specifications derived from these principles. Compliance against these is tested in the most rigorous way.
>
> The CAPS requirements and specifications are not available online, so developers looking to develop High Grade products must contact the NCSC for more information.

These high assurance principles can help risk owners to make informed decisions in cases where NCSC CAPS assessment is not appropriate. For example, deployment scenarios that limit the ability of products to meet CAPS requirements, or technology that is not designed to deliver the full range of security functionality required by CAPS.

Commodity vs. elevated threats

Threats to digital systems come from a range of attackers with different capabilities. Much of the NCSC's guidance is focused on defending organisations against **commodity threats** that make use of tools and techniques that are openly available, cheap, and simple to apply. Regardless of their technical capability and motivation, attackers will often turn to commodity tools and techniques first.

Organisations that defend effectively against commodity threats present a very hard target for all attackers, and so any organisation attempting to resist elevated threats should start by ensuring they have the best security posture possible against commodity threat.

For targets that are of particular interest to an attacker (and where commodity threats have been resisted), attackers may seek to develop a range of more sophisticated methods, some requiring long term investment and research. In such cases, we describe products as being subjected to **elevated threats**. These can only be realised by large, well-funded groups (such as high-end organised crime and state sponsored groups) as they require significant investment in skills, resources and capabilities.

High assurance principles

1. **Products should be sourced from trusted suppliers with proven high threat domain knowledge**
   Suppliers of high assurance products should be able to demonstrate their ability to understand and respond to the unique demands of high threat environments. Suppliers should have a deep understanding of the current breadth of capabilities and mode of operation of the most capable threat actors, meaning that known capabilities will naturally be resisted by design. Suppliers should also demonstrate a willingness to keep their knowledge and capability relevant to emerging threats to ensure that future capabilities can be resisted; this may necessitate technology, development, and deployment approaches that support regular maintenance and refresh of deployed products.

2. **Developers' processes should demonstrably meet all accepted good practice**

Regardless of the threats they are looking to mitigate, all developers of cyber security products should use NCSC guidance (such as the NCSC Build Standard.pdf) to help them make sound decisions covering product design, development processes and practices. This should ensure that developers have measures in place to defeat attacks that take advantage of known vulnerabilities, or use well known methods. Developers of high assurance products should make clear how they have applied NCSC guidance, and provide evidence of security claims made.

3 Products should have clearly defined, specific security functionality, with limitations identified

Security functionality should be clearly defined and documented. Functionality should be designed to provide protection against clearly defined threat paths, drawing on their domain knowledge of the capabilities of the most sophisticated threat actors. Scenarios where the product cannot provide protection against an identified threat path should be explicitly declared to enable risk owners to make informed decisions when deploying devices, for example by seeking other mitigations, or accepting risk.

4 Products should support systematic, independent and evidence-based assessment of claimed security functionality

Products should be designed and implemented in such a way that independent inspectors can test security claims by the gathering of evidence. This can be achieved in a number of ways, for example by having modular designs that enable security functionality to be clearly identified and exercised or inspected in isolation, and by using development technologies (eg choice of software languages) that do not obscure functionality.

These features will need to be built into a product's design and development. This does not preclude the use of third party components or libraries, but where these are used (and are directly delivering security functionality), it should be possible to gain the same degree of confidence in their performance, either by reference to the third party provider's evidence, or from the product developer. This evidence-based assessment must be **repeatable** (by for example the use of automated testing) to enable validation of a product's efficacy throughout its full life-cycle.

5 Products should always operate as intended

A product's implementation, configuration, and use should be clearly defined and resilient to provide high confidence that it will always operate as intended. This means products need to demonstrate an ability to protect themselves against errors in implementation and usage, failures, or interference. Where particular threat paths are identified, then resilient protective mechanisms should be evidenced. However in many

cases it is not possible to define all events of these types; therefore generic protective measures should be applied (such as avoidance of single points of failure, diverse implementation approaches and redundant implementations). This need applies to **engineering practices**, just as much as to the **operation** and **design** of a device.

The configuration and intended use of devices should be unambiguous, and proactively support the user and service need, such that high confidence in its correct operation is maintained throughout its full life-cycle.

6 **Products should always be in a trusted state**

A product should be able to validate the integrity of all its component hardware, software, and internal data by reference to an accepted root of trust. When in operation, a device should always be in a recognised state. If either of these are not true, this should be detected by internal or external monitoring, and the device (or wider system) should able to set itself (or be set to) to a known safe state.

PUBLISHED

6 February 2020

REVIEWED

6 February 2020

VERSION

1.0

WRITTEN FOR

Public sector

Large organisations

Cyber security professionals

Small & medium sized organisations