How the NCSC thinks about security architecture

Richard C explains how an understanding of vulnerabilities - and their exploitation - informs how the NCSC assesses the security of computer systems.

Richard Crowther

The NCSC has a security architecture team who consult on the design and operation of some of the most important computer systems in the UK; systems that handle the UK's most sensitive information and provide some of the most critical functions.

The current team has an impeccable pedigree and continues to build on thought-leading knowledge and techniques developed over more than a decade.

Although we're very clear what we mean by the term 'security architecture', we find there are differing views within the industry. And this can lead to a mismatch in expectations when we - to give one example - interview candidates for a security architecture role.

This blog defines what the NCSC mean by 'security architecture'. If you subscribe to a different school of thought, that's fine, but we're passionate about what we believe is a practical approach, particularly when we need to get the most out of a brief engagement with a system owner.

Our definition

The NCSC define security architecture as:

*The practice of **designing** computer systems to achieve **security goals**.*

For the majority of our engagements, these security goals are to:

- make initial compromise of the system difficult

- limit the impact of any compromise
- make disruption of the system difficult
- make detection of a compromise easy

An attacker can attempt to subvert **technology**, **people** and **processes** to undermine security, so security architecture must consider all the technology, people and processes relating to a computer system.

Of course, it is not enough for a system to only be secure. It needs to meet user needs, be cost effective, and account for any other constraints relevant to the scenario. Therefore, we always aim to design a system to be 'secure enough' whilst balancing these other aspects too.

The role of a security architect

Our security architects combine broad technical and security skills with strong business analysis and communication skills. This combination means they are capable of a range of activities, such as:

- Designing or reviewing whether security controls for a computer system are suitable; this is based on an understanding of both use and context, and how the system will likely be attacked
- Researching and developing new techniques or tools to address the more systemic security problems
- Advising technical leaders on cyber security when making strategic decisions

The role is **not** just about giving security advice; it is about making security *effective*. This means supporting our partners and customers, working with other professions towards a shared goal.

Understanding vulnerabilities and how they are exploited

Security architecture is primarily a technical discipline. To judge whether a system is difficult to compromise or disrupt, you need to know how it would likely be attacked. To do this, you need to understand how vulnerabilities occur and how they are exploited. If an attack would be too easy, then the system may need to be designed, configured or operated differently in order to mitigate the risk.

When it comes to understanding vulnerabilities in technologies, security architects need to know how to find out about *known* vulnerabilities. They should also be able to make reasoned judgements about how likely it might be to discover previously *unknown* vulnerabilities. In the NCSC, we're fortunate in that most of our security architects have had some experience of working alongside our world-class vulnerability research team. This gives the architects invaluable insight into:

- what makes finding vulnerabilities in some technologies easier than others
- understanding platform-level mitigations that make exploitation of vulnerabilities significantly harder

Of course, there's an element of subjectivity involved in making these judgements, but being able to call upon our vulnerability research team to give a second opinion on our judgements is priceless.

Security architects will also look for flaws in the way systems are used, built and maintained. And when it comes to mitigating any issues we identify we can use a combination of technical, procedural or operational controls to do so.

It's worth saying that whilst I'm confident we normally make sound judgements about how difficult it would be to find and exploit a vulnerability, I'm concerned that this is more an art than science, at present. To help address this we're keen to see and support academic research to improve the scientific rigour in this area.

We use patterns and principles

Like other technical disciplines, we like to use standard design patterns to solve standard problems. Over the years we've developed several patterns to help with common security problems, like the problem of importing information from an untrusted source without accidentally importing malware, or exporting information from a computer system without accidentally releasing more than intended.

Some of our preferred patterns are baked into the guidance on this website, such as our currently preferred remote access architecture which is used in our end user device guidance. Over the next couple of months we'll be working towards releasing more of these patterns on our website.

Patterns are great for common problems, but we often find ourselves working on systems that are unique. For these bespoke cases we have a portfolio of design principles. If you use your imagination you can apply the vast majority of these principles to other types of computer system or industrial control system. Again, we plan to publish a more generic set of security architecture principles later this year.

WRITTEN BY

Richard Crowther
NCSC Deputy CTO

PUBLISHED

5 April 2018

WRITTEN FOR

Small & medium sized organisations

Large organisations

Public sector

Cyber security professionals

PART OF BLOG

Inside the NCSC