IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

CloudClient – Origins of a Zero Trust Network Deployment for UK Government

Bernard Parsons

Bernard Parsons
CEO and Co-Founder
Becrypt

Biography

Bernard Parsons is the CEO and Co-Founder of Becrypt (www.becrypt.com).

Establishing Becrypt in 2001 with the aim of addressing the growing security requirements of endpoint technology, Bernard has built the company into a leading supplier of end-user device security products and services, with a focus on product assurance, multiple platform support and flexible delivery: from being embedded within the platform, to hosted within the Cloud.

Furthermore, Bernard has ensured Becrypt helps the most security-conscious organisations to be positioned as leaders in enabling value from the use of secure technology.

For his dedication to digital technology, Bernard was bestowed with an MBE in the 2018 New Year's Honours List.

Keywords Zero Trust, Networks, Cybersecurity, Government, NCSC, CloudClient, Cloud
Paper type Research

Abstract

Whilst the concept of Zero Trust (ZT) networks is gaining broad popularity and acclaim, elements of the approach have been quietly adopted and applied within some sensitive government IT environments. The ever-dissolving corporate perimeter has been a driver for the ZT concept, however for parts of government, it is more a case of not placing complete trust in a perimeter even where it can be identified, but instead building a defence in depth architecture that offers better protection and detection capabilities than conventional IT architectures. In this article, the author has captured some insight gained from working with government sector adopters of network models that reduce implicit trust, influenced by a project called CloudClient, run by the UK National Cyber Security Centre (NCSC).

Introduction – defining Zero Trust

The first rule of dealing with a recently popularised phrase, is that no one will agree on an exact definition – perhaps as there are too many different apparent solutions to the problem! The Zero Trust Network, or Zero Trust Architecture model, was created in 2010 by John Kindervag, a principal analyst at Forrester Research. Kindervag emphasised that organisations should not automatically trust users or assets, irrespective of location.

As technology and real world ZT deployments have evolved, it is best to think in terms of the important characteristics of the ZT approach, and how these may continue to adapt. The key point remains that you should no longer implicitly trust a managed entity – be that a device or user – just by virtue of them being, for example, connected to an internal network. This leads to two responses: seeking to have greater trust in the identities managed, and having greater control over how resources are accessed. The relevant tools and techniques include: device identity management, health monitoring, user identity and access management, service segmentation, and traffic inspection.

The desired outcomes include having confidence in both the identity and integrity (health) of a device, combined with the identity of a user that can be verified at a granular service level when a service is accessed, all underpinned by robust security mechanisms that are, as far as possible, transparent to the user and easy to manage.

NCSC CloudClient – A brief history

The predecessor of the UK National Cyber Security Centre (NCSC) initiated a research project a few years back that incorporated many of the characteristics of ZT networks. The objective of the CESG CloudClient project was to facilitate the secure sharing of IT infrastructure across government, allowing an employee of one department to securely access their online services from collaborating organisations. The project required that the health of devices could be measured and validated across organisational boundaries with a high level of assurance, to ensure that no organisation's security posture was reduced through collaboration, and that user identity management would automate the delivery of defined service components.

The first building block of the resulting architecture was a security-focused operating system optimised for accessing online services -– effectively a secure platform to launch a browser. Adopting a browser-based operating system simplifies the process of validating device identity or health, as it becomes viable to cryptographically validate all firmware, operating system and application software components – a task that is problematic for a full-blown general purpose operating system.

The CloudClient project resulted in the end-to-end implementation of a Remote Attestation protocol for a desktop environment compliant with the relevant Trusted Platform Group open standard, using a Trusted Platform Module as a hardware root of trust. At a high level, this means that an organisation can be confident in not just the identity of a device, but its integrity. A device in a known healthy state indicates that no malware or unauthorised software is present.

The CloudClient architecture utilises the SAML (Security Assertion Mark-up Language) authentication protocol that allows collaborating organisations to exchange authentication parameters as part of a federated device identity model. This allows web services to be published that can then create end-to-end encrypted sessions with 3rd party devices at the same level of confidence as internally managed devices. Two factor user authentication is implemented using physical smartcards, with associated policies defining granular authorised service access.

A real world deployment

Whilst CloudClient was a research project, its successful outcomes were subsequently adopted across a number of UK government departments. Well aligned with government's 'cloud first' policy, the 'cloud client' model allowed a number of security benefits to be derived by optimising end user devices for cloud access. However, in addition to security, the need to optimise usability proved a key driver for user adoption. Even with some of the most sensitive government environments, security today needs to be as automated and transparent as possible, whether that is single sign-on, timely certificate management or automated patching. These are all necessary characteristics of a well-designed ZT architecture.

Security operations overheads may also be reduced through the cloud client model, as a light-weight and secured OS can significantly change the security event monitoring landscape. Minimising the software stack with a browser-based model reduces security auditing 'noise' from endpoints, whilst cryptographically enforced health checks provides a very low-volume high-value audit profile. This can offset the potential for increased network traffic logging and inspection as advocated by the ZT model.

With NCSC and wider UK government's preference for commercial off-the-shelf products, Becrypt has been able to productise the project's outputs in the form of an end user device platform called Paradox (no formal endorsement by NCSC implied).

Lessons learned

When moving to cloud and online services, there is a temptation to focus on the benefits that the chosen cloud-based infrastructure can offer. The CloudClient model demonstrated how the typical benefits of security, cost and flexibility can be extended to the end user device infrastructure - when the endpoint needs little more than a browser, it becomes difficult to justify a general-purpose OS, and easier to implement ZT-enabling controls.

However, few organisations would expect or attempt to standardise on all of the architectural components of CloudClient or similar architectures across the entire enterprise, and this has been shown by assessing where Paradox has subsequently been deployed. The pre-requisites to adopting a browser-based OS such as Paradox typically include deploying to 'greenfield' environments, although this can include new software roll-outs to existing hardware. Furthermore, projects typically need to be targeting 'cloud native' communities, or those accessing online applications.

To date, Paradox has been deployed to secure desktops, laptops and kiosks with a range of use cases from standard enterprise access to O365, to the more specialised examples of SOC hosting and control of 3rd party supplier access, providing varied examples of the shift towards a Zero Trust model.