Proceedings of the 19th International Conference on Cyber Warfare and Security (ICCWS), Johannesburg, South Africa, 26-27 March 2024

On the zero-trust intranet certification problem

Badenhorst, Danielle P
Council for Scientific and Industrial Research (CSIR)
Meiring Naude Drive, Pretoria, 0184
Email: DBadenhorst@csir.co.za

Securing corporate networks and ensuring the trustworthiness of network resources are critical security concerns for organisations in today's interconnected digital landscape. The zero-trust security model is an approach to designing and implementing ICT systems which prescribes that clients and servers cannot be trusted automatically, even when connected to networks traditionally considered trusted. The implementation of the zero-trust model within the corporate intranet requires a secure method to verify the identity of local servers. On the Internet, trust in the identity of public servers is established by well-known public Certificate Authorities (CAs), which issue digital certificates to securely identify servers. However, local intranet servers exist within the internal address space of the network. Consequently, it is impossible to naturally obtain digital certificates for these servers, validly signed by a public CA, without publicly disclosing sensitive information such as intranet server Domain Name System (DNS) records. This leaves organisations with the option of relying on endpoint management systems to install custom CA root certificates on all corporatre browsers or, in some cases, ignoring the problem altogether. In this paper, we draw on practical experience in the deployment of cybersecurity devices in corporate intranets to formally define the intranet certification problem. We specify five requirements that a solution to this problem must satisfy. We then conduct a comprehensive review of existing candidate solutions and academic research relevant to the intranet certification problem. Specifically, existing ICT systems for public key infrastructure and endpoint management are identified and evaluated with respect to their ability to meet the stated requirements for solving the intranet certification problem, as well as their cost. Our study reveals that solutions that meet the technical and security requirements of the intranet certification problem are beyond the reach of smaller private sector companies and public sector organisations in underdeveloped and emerging economies. The high cost and technical expertise required for their implementation and management render these solutions impractical. Consequently, by relying on servers with self-signed certificates, these entities inadvertently leave their servers susceptible to impersonation, information theft, and unauthorised resource access, thus violating the fundamental principles of the zero-trust model. We conclude that a gap exists for a simple, cost-effective, and easily managed solution to the intranet certification problem.