Abstract

The concept of certificate revocation is core to the X.509 trust model however 18 years after its introduction the reality is as implemented and deployed it falls short of its promise to enable an issuer certificate issuers to protect relying parties from malicious actors and miss-issuance

This talk will discuss the findings of a project where I have observed the behavior (https://revocation-report.x509labs.com), up time and performance of revocation repositories for a number of commercial Certificate Authorities for a period of over six months.

Additionally I will overview the revocation behavior of the most common browsers, identifying the gaps as they exist in those implementations.

And finally I will provide a set of recommendations that I believe if followed can address the current gaps which would move us to a world where revocation checking is an effective means of protecting relying parties from known bad actors and miss-issuance.

Presenter

Ryan Hurst is the chief technology officer at GlobalSign. In this role, he is responsible for developing the overall technology vision for the company, product architecture, standards development, compliance and overseeing the engineering and operations organizations.

Prior to joining GlobalSign, Mr. Hurst, a ten-year Microsoft veteran, was responsible for security engineering within the Advertising business. Prior to that he was responsible for integrating security and networking technologies such as cryptography, certificates, smart cards, biometrics, code signing, document signing, and network authentication into Microsoft products.

Mr. Hurst has authored a number of patents relating to security and software design and has been an active participant in the standards community, having co-authored and contributed to standards in forums such as the IETF and the Trustworthy Computing Group.

Ryan M. Hurst
Chief Technology Officer
GMO GlobalSign

email: ryan.hurst@globalsign.com
twitter: @rmhrisk
mobile: 206-650-7926