Abstract

In 2010 security researchers with the EFF collected the certificates of all of the publicly-visible SSL certificates on the IPv4 internet and published their analysis and data-sets from their research. This work made it clear to the world how extensively PKI is used to facilitate commerce on the web but it also raised he concern that there were as many as 650 organizations capable of issuing publicly trusted certificates on the internet.

While this conclusion is exaggerated as many of those certificates and keys are in-fact operated by the same organizations that their certificates are ultimately issued by, the conclusion that there has been an un-needed expansion of the number of keys that are technically trusted to issue certificates for SSL for the entire Internet is sound.

To address this problem one of the steps that is needed is the application of least privilege principals to how one designs and manages publicly trusted keys and certificates. Thankfully in the late 90's the foundation for addressing much of this problem was developed as a means to enable the Federated PKI in use by the U.S. Federal Government.

For the last year we have been working to broadly deploy X.509 Name Constraints' along with other least privilege design principals to our customers PKIs both internally managed by our own staff as well as those on premise. This talk will explore these concepts, the client support for them, the challenges we have experienced in their deployment and identify the remaining issues that must be addressed to obtain the full benefits of this approach.

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