Title: Managing Trust within an Organization
Covering Asymmetric, Symmetric and SSH Key environments

Authors: Gary Moore, Chief Architect Government Solutions, Venafi
Paul Turner, VP Product & Customer Solutions, Venafi

Abstract:

Cryptography touches almost every element in today's business environment. Whether it is protecting information channels for ecommerce, business supply chains or remote employee access or, if it is protecting data assets stored in a cloud-based service, cryptography and the associated keys create an additional level of IT management that many parts of organizations do not understand. The trust within, and of, an organization is based on successfully utilizing these technologies to ensure efficient business operations without exposing vulnerabilities that would lead to service outage, intellectual property or PII data loss, brand damage or possible data destruction or hijacking. This problem has seem dramatic increase in attention due to new methods of attack as well as the expansion of certificates and cryptographic assets in areas of critical infrastructure protection.

The key element to ensuring that an environment is effectively and efficiently managed is to first understand what are the critical assets that are to be protected, what cryptographic assets are deployed to protect these assets and who has responsibility to ensure that these cryptographic assets are maintained in a way that meets the security policy in place. These assets may include symmetric keys, which protect stored data; asymmetric keys which protect data in transit or are used to protect resources from unauthorized access; or SSH keys which protect the channels used to remotely manage the distributed IT environment.

This presentation will discuss the ongoing threat that is presented by not having a well managed cryptographic asset environment and will present an alternative that allows organizations to discover these assets, recognize weaknesses in the environment that are out of policy compliance, assign responsibility for these assets, manage the ongoing lifecycle and allow for cost reduction in an operational environment. Additionally the presentation will look at how this methodology can be used to improve continuity of operations in the event of a compromise of an internal or external certificate authority, allowing for rapid recognition of areas of concern and rapid recovery.