Encryption and Key Management

Arshad Noor, StrongAuth, Inc.

PHOTO

Governance, Risk & Compliance Track – Session G31

Abstract:

The disciplines of encryption and key-management have existed for more than 2 decades, but the IT industry is seeing the use of cryptography at unprecedented levels due to regulations such as PCI-DSS, 201 CMR 17.00, etc, throwing many crypto-neophytes into this complex arena. As a result, there are many flawed implementations, misconceptions and misunderstandings about how to use cryptography effectively to protect sensitive data.

Five years after PCI-DSS became mandatory for companies dealing with credit cards, we continue to witness breaches in systems declared to be PCI-compliant. Encryption - a component of the DSS - is recognized to be an effective solution to mitigate the risk of sensitive data falling into wrong hands; yet, why do systems continue to get breached despite using encryption?

This presentation will explore the technical details of this discipline to explain some basics, pitfalls, best practices and the current state-of-the-art of encryption and key-management. Using this information, attendees will be able to better determine if systems using cryptography are well protected or using cryptography in an insecure manner.

Target Audience:

The presentation is geared toward stakeholders (e.g., security, compliance and financial professionals) involved in day-to-day compliance efforts, and anyone interested in gaining insight into the PCI Data Security Standard (PCI DSS).

Skill level ranges from intermediate to advanced.

COBIT Objectives:

IT PROCESSES - Deliver and Support
DS5 Ensure Systems Security

Speaker Bio:

Arshad Noor is the CTO of StrongAuth, Inc, a Cupertino CA-based company that specializes in enterprise key management. He is the designer and lead-developer of StrongKey, the industry's first open-source Symmetric Key Management System, and the StrongKey Lite Encryption System - the industry's first appliance combining encryption, tokenization, key-management and a cryptographic hardware module at an unprecedented value. He has written many papers and spoken at many forums on the subject of encryption and key-management over the years.