Cracked SSL?

PANELISTS:

Ivan Ristic, Director of Engineering, Qualys, Inc.

Marsh Ray, Senior Software Development Engineer, PhoneFactor

Gerv Markham, Governator, Mozilla

Phillip Hallam-Baker, VP and Principal Scientist, Comodo

MODERATOR:

Ben Wilson, DigiCert and CA-Browser Forum

Session ID: STAR-108

Session Classification: Advanced

Overview

- Vulnerabilities
  - Protocol-based (TLS Renegotiation)
  - Implementation-based (e.g. mixed content)
  - Practice-based (Certification Authority bad practices)
- Solutions and Remedies
  - Those Currently Available (e.g. RC4 with TLS 1.0)
  - Those In Development / Deployment
    - Online Certificate Status Protocol (OCSP) Stapling
    - HTTP Strict Transport Security (HSTS)
    - Content Security Policy (CSP)
    - Improved security and audit requirements for CAs
  - Those Being Discussed (DANE, CAA, CT, etc.)

Acronym Guide

- CAA = Certification Authority Authorization (DNS Resource Record)
- CSP = Content Security Policy
- CT = Certificate Transparency (Issuance Logging)
- DANE = DNS-Based Authentication of Named Entities
- DV, OV and EV = Domain-Validated, Organization-Validated, and Extended Validation SSL Certificates
- HSTS = HTTP Strict Transport Security
- OCSP = Online Certificate Status Protocol

Take-Aways

- Check Systems (Your Own and Those of Others)
- Analyze Code and Configurations for Vulnerabilities
- “Tweak” System Configurations and Code
- Support Implementation of Newer Versions of TLS and other emerging Protocols
- Patch and/or Replace Systems
- Web Security based on SSL/TLS Continues to Evolve and Improve