



THE 1997 RSA DATA SECURITY CONFERENCE

SPEAKER BIOGRAPHY

CRYPTOGRAPHERS' Track

Mitigating A Security Flaw in the X.509 Standard

Speaker: **Santosh Chokhani**

President

Cygnacom Solutions, Inc.

7927 Jones Branch Drive

Suite 100W McLean,

VA 22101

Phone: 703-848-0883 Fax: 703-848-0960

Email: chokhani@cygnacom.com

Company Background:

Cygnacom Solutions, Inc. is a small, high-technology company that specializes in information security.

Cygnacom has extensive experience and expertise in design and implementation of public key cryptography applications and associated certification authorities and public key infrastructures. Cygnacom also operates the NIST accredited CEAL laboratory to validate cryptographic modules for compliance with FIPS 140-1. Cygnacom is a member of the IBM alliance on key recovery.

Presentation Overview:

This presentation describes a security flaw in the base X.509 public key certificate and a way to mitigate the flaw.

Speaker Background:

Santosh Chokhani is the founder and President of Cygnacom Solutions, Inc. He is also the director of Cygnacom's CEAL laboratory to validate and test cryptographic products for compliance with FIPS 140-1. He is a member of the International Crypto working Group for the Common Criteria and a member of the Department of Commerce Technical Advisory Committee on Key Management Infrastructure. His research and development interests include infrastructure for applications of public key cryptography for the protection of information and computing resources. Dr. Chokhani holds an M.S. and Ph.D. in electrical engineering from Rutgers University.

PRESENTATION