In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Certificate Reputation: Cryptographic Analysis of Public Keys and Certificates in Use

by

Dr. Brian A. LaMacchia

Microsoft Corporation

U.S.A.

Date	**:**	**28 Jan., 2014 (Tue.)**
Time	**:**	**11:00am - 12:00noon**
Venue	**:**	**Room 833 Ho Sin Hang Engineering Building** **The Chinese University of Hong Kong**

Abstract

One of the propagation mechanisms used by the FLAME malware was enabled by an MD5 hash collision attack against a portion of the Microsoft PKI. Microsoft Research personnel were involved very early on in the analysis of the FLAME malware and the development of Microsoft's corporate response. Following FLAME, we began developing tools for automatically collecting and analyzing cryptographic objects to facilitate detecting potential attacks. The first tool we are developing, CertRep, analyzes X.509v3 certificates gathered from the public Internet as well as participating enterprises. CertRep's database of certificates is gathered by new features added to the Internet Explorer 11 and Windows 8.1 versions of the Microsoft SmartScreen client protection service. In this talk I will introduce CertRep and the new SmartScreen features and then describe how we are using CertRep along with cryptographic analysis techniques including batch GCD and MD5 hash collision detection to monitor for problematic crypto implementations and attempts to subvert public certificate authorities and PKIs.

Biography

Dr. Brian A. LaMacchia -- "bal" to his friends -- is one of a handful of applied cryptographers at Microsoft. Brian leads the Security & Cryptography team within Microsoft Research's Extreme Computing Group (XCG); his organization conducts security- & crypto-related research and advanced development. Brian is also a founding member of the Microsoft Cryptography Review Board and consults on security and cryptography architectures, protocols and implementations across the company. Before moving into Corporate R&D, Brian was the architect for cryptography in the Windows Security group. Prior positions Brian has held at Microsoft include Development Lead for .NET Framework Security and Program Manager for core cryptography in Windows 2000. Before joining Microsoft, Brian was a member of the Public Policy Research Group at AT&T Labs--Research in Florham Park, NJ. Brian received S.B., S.M., and Ph.D. degrees in Electrical Engineering and Computer Science from MIT in 1990, 1991, and 1996, respectively.

**** ALL ARE WELCOME ****

Host: Professor Sherman S.M. Chow (Tel: 3943-8376, Email: smchow@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)