DigiCert EV SSL Certificates protect users from SSLstrip and man-in-the-middle attacks

SSL Certificate Authority Answers New Digital Threats Presented at Black Hat Conference

LINDON, UT (February 20, 2009) — On Wednesday, February 18 at the Black Hat conference in Washington, D.C., an independent hacker known as Moxie Marlinspike presented a software tool called SSLstrip designed to remove the SSL protection from websites using advanced man-in-the-middle attack methods. DigiCert, a major worldwide provider of SSL Certificates, replied that Extended Validation (EV) SSL Certificates help users to recognize and steer clear of such attacks.

Marlinspike demonstrated how the SSLstrip program can intercept connections between a web browser and a trusted website, then serve the web browser the contents of the trusted site without trusted SSL encryption. The webpage could potentially be loaded unsecured (http) or spoofed with a low-assurance SSL certificate on a fraudulent domain name, similar to a phishing attack. Therefore, it is possible that the pages would still load with a padlock in the browser. SSLstrip could potentially be effective at stealing sensitive information including usernames, passwords, or credit card information in situations where man-in-the-middle attacks are possible such as in Onion Routing configurations and Wi-Fi networks.

SSLstrip does not demonstrate a weakness in SSL encryption, but rather takes advantage of users who fail to look for trusted SSL encryption when sending sensitive information over the Internet. This problem has been exacerbated by the use and distribution of low-assurance certificates.

In anticipation of such problems DigiCert joined with the other major Certification Authorities and Browser developers to establish Extended Validation Certificates. EV Certificates are all vetted rigorously to guarantee authenticity of websites and strong encryption. EV certificates are recognized by major web browsers such as Internet Explorer, Firefox, Opera, Safari, and Chrome. All of these browsers distinguish EV-secured websites by easily identifiable means. For example, the website address bar of Internet Explorer 7 will turn green to certify that the user is connected to an EV-secured website.

“The proper use and recognition of EV certificates effectively resolves the weaknesses exposed by both phishing and man-in-the-middle attacks,” explained Christopher Skarda, DigiCert’s Vice President of Operations. “In this way, EV certificates help to protect users against identity theft. Also, EV certificates help online companies to establish the trust and protection that their customers have learned to expect.”

About DigiCert, Inc.
DigiCert, Inc. is a leading provider of enterprise-grade, high-assurance, 256-bit SSL Certificates trusted by many national and state governments, educational and medical institutions, and Fortune 500 companies around the world. DigiCert’s commitment to innovation and value provides clients with peace of mind backed by a 100% money-back guarantee and live 24-hour phone, chat and email support, along with intuitive GUI certificate management. Located in Lindon, Utah, DigiCert is a WebTrust Certified Certificate Authority, a member of the CA/Browser Forum, the Authentication and Online Trust Alliance, and the W3C Consortium.