Statement of the CA/Browser Forum Concerning the EFF's SSL Observatory

The CA/Browser Forum recognizes and appreciates the work of the Electronic Frontier Foundation's SSL Observatory, which was established to collect and report on digital certificate information. The data gathered by the EFF will help analyze certificate issuance practices and, hopefully, identify areas where certification authorities (CAs) can improve security and operations. The CA/Browser Forum, a consortium of certification authorities and browser developers, supports this relatively recent EFF endeavor.

The CA/Browser Forum promulgates rules and policies that certification authorities adhere to when issuing, revoking, and managing certificates. Certificates issued pursuant to the CA/Browser Forum's Extended Validation (EV) Guidelines provide enhanced security over other certificate types as they identify the legal entity that controls a web or service site. This identification significantly enhances cybersecurity by helping establish the legitimacy of an organization claiming to operate a web site, and providing a vehicle that can be used to assist in addressing problems related to distributing malware, phishing, identity theft, and diverse forms of online fraud.

Because EV Certificates provide a higher level of assurance than other SSL certificates, a CA must follow strict rules when issuing an EV Certificate. Certificates that comply with the EV Guidelines display enhanced indication of trust and usually the organization name in the color green in the site name to indicate the heightened level of verification. Some of the requirements include a high level of identity validation, strong algorithm parameters associated with private keys, and annual compliance audits.

In 2010, the EFF reported that more than 99.6% of the EV Certificates that it was able to check fully complied with the EV Guidelines. Although the CA/Browser Forum demands 100% compliance, this small percentage of problem certificates is extremely encouraging considering that the requirements are fairly complex and extensive. Like many reports that members of the CA/Browser Forum receive, thanks in-part to efforts like the EFF's SSL Observatory, the responsible CA members are able to address and correct problematic practices, not only those prohibited by the EV Guidelines, but also other practices that may weaken the security of the Internet. However, it is also important to note that at no time did the non-compliant certificates previously identified ever pose a security risk to consumers.

For example, the major reason for finding non-compliance during the 2010 EFF review was that the certificates had 1024-bit RSA keys instead of 2048-bit RSA keys, the key length required by the EV Guidelines. To date, this is still in accordance with NIST Special Publication 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, which phases out 1024-bit RSA through 2013. (Previous NIST Special Publication 800-57 had advised that 1024-bit RSA keys would be at risk of compromise after 2010.) However, this does not mean that EV certificates containing 1024-bit keys as of January 1, 2011 were compromised or failed to provide adequate encryption. Instead, the NIST recommendation is based on the belief that by 2011, technology would advance to the point that a 1024-bit key was at risk of being compromised.

Additional non-compliant certificates identified by the EFF include EV Wildcard certificates and certificates containing local host names or internal IP addresses. These types of EV certificates

are prohibited by the CA/Browser Forum. Section 10.6 requires the CA to verify that each domain name listed in a certificate "is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA)". Section 8.1.1 expressly forbids wildcard certificates.
The CAs responsible for these certificates have worked quickly and diligently to fix the problem, both from a certificate and operational perspective. Many of the CAs have reported the problem resolved in the following thread:
http://groups.google.com/group/mozilla.dev.security.policy/browse_thread/thread/e1f3be45ffb2d568/320174d2dacfc59c?lnk=gst&q=ssl+observatory#320174d2dacfc59c

The CA/Browser Forum has also taken action, requiring that the CAs responsible for the non-compliant EV Certificates examine their other EV certificates for similar problems. The CA/Browser Forum expects all EV certificate issuers to adopt procedures that prevent these types of mistakes.

The issuing CAs reported that the non-compliant certificates have now been revoked and are no longer functional on the web. CAs use revocation to end the life of a certificate prior to its expiration date and is an emergency process whereby CA's can enforce the proper use of a certificate even after it is installed on an external server. This method acts as a safe guard to protect consumers from unforeseen security risks. Because the certificates were revoked, the problems related to the certificates identified by the EFF have been neutralized.

The EFF also expressed concern over the large volume of certificate authorities. The CA/Browser Forum does not recognize this as a potential problem. All CAs issuing EV certificates undergo an annual independent audit that ensures their compliance with the EV guidelines. In addition, EV-issuing CAs are directly responsible for all of their subordinates. Section 14.1.2 requires that each "CA MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken". The audit covers all of a CA's obligations under the EV Guidelines, regardless of whether the obligation was performed by the CA or a subordinate.

The CA/Browser Forum is currently working towards establishing minimum requirements for all SSL certificates. The minimum requirements will set a baseline requirement for all certificates, antiquating many of the complaints regarding CAs. For example, one of the goals behind the minimum guidelines is to eliminate any non-verified subject information from a certificate, including non-verified subject information asserted through an OU field. Similar to EV, all CAs (including subordinates) will have to undergo annual audits and supervision to ensure compliance with the minimum requirements.

The CA/Browser Forum looks forward to future SSL Observatory data and projects. A publicly available, decentralized observatory and revised datasets will greatly help improve audits and increase security for consumers. The SSL Observatory's work is of great benefit to consumers and businesses worldwide, and we appreciate and welcome their input on any matter.

Sincerely,

The CA/Browser Forum