Speaker Details

Name: Rick Andrews, Symantec Corporation
Title: Technical Director

Presentation Specifics

Emerging Technology Space (e.g., User Interfaces): Clarity on requirements for all actors in the CA system

Title of Presentation: CAs Alone Do Not Provide Trust

Presentation Description (max 300 words):
Recent high-profile attacks against the Internet PKI system have resulted in increased scrutiny and requirements imposed on Certificate Authorities (CA). Yet by focusing on only one of the actors in the trust system, we may not materially improve security. This presentation will address the broader scope of issues across the trust landscape from the perspective of a leading CA.

Our reliance on audits of CAs is commendable, yet many attacks have succeeded against CAs with up-to-date audits. We may benefit by examining other industries to create and apply improved audit regimes, not to simply block the attacks of the past, but to anticipate future attacks.

Browser vendors have a crucial role to play in the trust model, yet we lack standards on security-related browser behavior. And we see wide variance in desktop and mobile browsers. Those vendors should be free to innovate on user interface, but should comply with best practices for underlying security checks. Audits of browser security behavior should be considered.

In addition to CA/Browser Forum requirements, each browser vendor has its own root certificate policy. Multiple policies make it more difficult for CAs to comply. We will be more successful at enhancing security if we can make the system less complex with a common set of policies or best practices.

Finally, mobile devices are the new frontier, yet screen area constraints result in less security information being displayed to mobile browser users. More Internet transactions are moving beyond mobile browsers to company-specific mobile apps or social networking sites. Recent investigations have shown that many mobile apps and software development kits fail to handle SSL certificate checking properly. Security best practices for mobile developers should also be explored.

Internet security can only be improved by taking a holistic view of all the actors in the trust system.