Q&A: Firefox's Kev Needham on Extension Signing

Electronic Design
William Wong
Tue, 2016-11-22 15:37

Digital signatures for device and application extensions aren't new, but their requirement is now the norm. This can have an impact on both users and developers, especially for developers of embedded devices. One of the primary platforms for PCs and embedded systems is Firefox.

To find out more about Firefox's policies and developer support in this area, I talked with Kev Needham.

Related

RSA Digital Signature Software Eliminates Cloning Of Embedded Devices

11 Myths About UEFI

Give System Attackers the Boot

Wong: Why are digital signatures useful and what benefits do they provide to users and developers?

Needham: Signatures are useful for a number of reasons, and the primary benefit is that signing helps Mozilla mitigate the effects of add-ons that negatively influence the user experience (e.g., add-ons that are malicious can significantly impact stability and performance). They do this by giving Mozilla awareness of add-ons that are installable in Firefox, establishing a connection to the developer through the submission process (especially since a developer account is required), and reducing the ability for add-ons to work around the blocklist tools used by Mozilla via polymorphic or existing "guids."

This has two primary benefits for developers: First, it reduces the reuse of their add-on's GUID—a loophole by which bad actors have used to avoid being blocklisted, and second, it gives Mozilla the opportunity to introduce developers to the add-on community at large, and connect them to development support and resources.

Wong: What types of digital signatures are employed within the Firefox environment?

Needham: Extension packages are signed using an X.509 code signing certificate issued to Mozilla. Third-party certificates are not recognized, and the extension source is not encrypted.

Wong: Can users allow the use of extensions that are not signed?

Needham: In some of our products, yes, but both the release and beta versions of Firefox require that extensions be signed, with no supported way for the user to disable signature checking. Our nightly, developer, and extended support releases—targeted at organizations that deploy Firefox—all continue to support the preference that disables signature verification, which is enabled by default in all releases. For developers, we provide unbranded versions of Firefox (generated from the same code base as the release and beta versions) that allow for signature verification to be disabled.

Wong: How does a developer get a signing certificate, and are there different requirements for different types of extensions?

Needham: Developers can use two different methods to get their extension signed, depending on whether the extension will be distributed through a Mozilla website or not.

Listed add-ons are those distributed through https://addons.mozilla.org (AMO), an add-on discovery and distribution site maintained by Mozilla. Listed add-ons submitted by developers to AMO are signed as part of the review and publishing process.

Unlisted add-ons are those that are not intended to be distributed through AMO; each can be submitted as an unlisted add-on the same way listed add-ons are signed, or via a signing service provided by Mozilla as an API.

overview of the extension distribution tracks and their signing requirements is available on MDN as part of Add-ons Review Policy reference.

Wong: Where can developers find out more about the signing process for Firefox extensions?

We maintain a refererence document on signing and distributing Firefox add-ons on MDN at https://developer.mozilla.org/en-US/Add-ons/Distribution. We post regularly on the Mozilla Add-ons Blog, and track our communications about signing and other initiatives around add-ons on the Mozilla Wiki. We also maintain a page for Extension Signing itself, which provides links to our original announcement and follow-up posts, a frequently asked question section, and links to the unbranded builds referenced earlier.

Source URL: http://electronicdesign.com/dev-tools/qa-firefox-s-kev-needham-extension-signing