Browser Security Track @ OWASP Summit 2011 (15:15 - 15:40 Thursday Feb 10)

Browser Enduser Warnings

L Adamski == Lucas Adamski, Mozilla
I Fette == Ian Fette, Google
T Gondrom == Tobias Gondrom, IETF
J Nagra == Jasvir Nagra, Google
J Schuh == Justin Schuh, Google
J Hodges == Jeff Hodges, PayPal
R Hansen == Robert Hansen, SecTheory

[About this document] These are the raw notes from the Summit discussion on HTML5 Security. All the cited people have had the chance to edit these notes but there may still be errors and misunderstandings in here. Along with the notes from the other browser security sessions – Site Security Policy, DOM sandboxing, HTML5 Security, and EcmaScript 5 Security – these notes will be the foundation of the forthcoming Browser Security Report. If you have any questions regarding this document, please email john.wilander@owasp.org.

[Session started with a a few screen shots from Chrome, Firefox, and Internet Explorer showing bad SSL certs and private browsing]

I Fette: Buy a cert. Don't make us show that warning. Certs are $10, which often is less than hosting. Users see this warning all too often. As browsers we cannot skip warning the user.

J Hodges: The warnings say the user may be in danger. Research shows the UI doesn't work. My wife too. They have no context. They have no clue of what the padlock or green means.

I Fette: So what is "In danger"? In most cases you're not in danger but there are cases where you are.

L Adamski: Red works. With that we can at least say "Something's wrong, don't continue".

J Hodges: PayPal likes red. We support the "Don't continue" warning. We also use HSTS.

I Fette: Right now a few sites use HSTS and they're well managed. But what about the others? What should we do differently?

J Hodges: I don't have the paper references right now. Research have looked in to warnings signs at work places and such. You have to connect to the user's brain. You need to do serious research. Completely new stuff may be the solution.

Example from New Zealand bank: Cert expired for 12 hours. 300 customers tried to log in. 299 clicked through the warning.

J Hodges: We want a preloaded white list for HSTS in all browsers.

I Fette: How many entries should we have on that list? We cannot have a 2 billion entry white list.

J Schuh: We tried skull and bones for mixed content. That was disruptive and we got enormous amounts of negative feedback.

J Hodges: You browser guys should coordinate your efforts.

J Nagra: Are you saying we should coordinate our *disruptive* efforts to find good enduser warnings? That will not happen.

J Hodges: MItM is occurring. We're collecting data.

From the back of the room: Why not leave the error message design to the app developer? Good messages differ between cultures.

I Fette: What if this is the rouge site? That site will not give an error message but rather "You're our millionth visitor, please click OK".

T Gondrom: Would be nice if browsers behaved the same way, even disruptively. But it's a competitive thing.

I Fette: Yeah, PayPal once said "Don't user browser X because it doesn't support EV".

J Hodges: I did not work there at the time.

L Adamski: Coordination is fine. But that cannot hinder us trying out things. We haven't figured out the right UI paradigms for communicating security risks. We need to experiment more, instead.

I Fette: There have been coordination initiatives, for instance when to show lock and when not to show lock. The ideas are 4-5 years old and locked into the spec.

L Adamski: Regarding the padlock. If you define an icon that means "universally safe" it'll get into the *page* contents in no time.

R Hansen: We need a roadmap for DNSSEC and how it will be signaled in the browser. With all the root CAs out there the PKI is crumbling.

I Fette: If you're under DNSSEC, a signed top level domain, and you include a file with a cert fingerprint Chrome will treat your cert as if signed by a recognized root CA.

J Hodges: TLS gives integrity and confidentiality of the channel and authentication of the site.

From the back of the room: Is Google sharing the knowledge on moving to TLS on for instance GMail?

J Hodges: Adam Langley has written quite a lot about it. While the $ cost might not be high on moving to TLS there's a significant pain-in-the-*** cost to get your site working. PayPal has gone 100% SSL. But I checked for my personal page and it was a pain even if I provided the cert.