

RE: Protecting XML File While Displayed In Browser

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.security/2004-04/0253.html>

From: Shawn Farkas (shawnf_a_t_online.microsoft.com)

Date: 04/29/04

Date: Thu, 29 Apr 2004 01:07:08 GMT

If you're sending data to the user in IE, there's nothing I'm aware of that will protect it before printing. There may be an IE plugin somewhere that will provide this functionality for you, but by default there's nothing you're going to be able to do.

Even if your signature was enforced, that wouldn't solve the overall problem of ensuring the printed data is from your original source. If the user modified the data, and the signature failed to validate, once you've printed it, the signature is lost, so you have no way to know that its invalid (unless you print a special mark for "invalid document").

Assuming you had some way to protect the data all the way to the printer, once its been printed out you have a whole new set of problems. If someone is really determined to fake the data, what's going to prevent them from scanning it into the computer, and using Photoshop or some other application and dititaly modifying the document, then printing it out again?

This is a pretty difficult problem to solve, I can't think of any good solution off hand, but perhaps some other readers of this newsgroup have suggestions.

-Shawn

http://blogs.msdn.com/shawnf_a

--

This posting is provided "AS IS" with no warranties, and confers no rights.

Note: For the benefit of the community-at-large, all responses to this message are best directed originated.

>From: "John Bowman" <<Remove this before reply> john.bowman@thermo.com>
>Subject: Protecting XML File While Displayed In Browser
>Date: Wed, 28 Apr 2004 07:38:14 -0500
>Lines: 35
>X-Priority: 3
>X-MSMail-Priority: Normal
>X-Newsreader: Microsoft Outlook Express 6.00.2800.1409
>X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1409
>Message-ID: <uM1#t2RLEHA.3052@TK2MSFTNGP12.phx.gbl>
>Newsgroups: microsoft.public.dotnet.security
>NNTP-Posting-Host: host-208-44-151-58.thermo.com 208.44.151.58
>Path: cpmsftngxa10.phx.gbl!TK2MSFTFEED01.phx.gbl!TK2MSFTNGP08.phx.gbl!TK2MSFTNGP12.phx.gbl

microsoft.public.dotnet.security: RE: Protecting XML File While Displayed In Browser

>Xref: cpmsftngxa10.phx.gbl microsoft.public.dotnet.security:5878
>X-Tomcat-NG: microsoft.public.dotnet.security
>
>Hi,
>
>I'm hoping this is the right place to post this Q. So if it's not, please
>direct me otherwise.
>
>I've got a simple win forms app (C#) I've been asked to modify that
>generates numerical scientific data as XML and displays it in a grid
>control. The user is allowed to generate a report of the data. To do this, a
>temp XML file containig the portion of the results to display is apparently
>generated and loaded into the default browser using a style sheet to make it
>look pretty. This is where the user would normally print his/her results.
>Here's the problem. the XML data file is digitally signed, so when the
>browser is loaded w/ the temp XML file, the user could technically modify
>the data (through View Source, or any other text editor) while it's open in
>the browser, then print it in a modified form and no one would ever know
>that the results had been modified for printing purposes. This of course
>defeats the digital signature. Is there any way to "protect" the temp file
>that is loaded into the browser such that NO alterations can be made to it
>between the time it is loaded into the browser and the user chooses to print
>the displayed results?
>
>I'm afraid I'm such a newbie at digital signature stuff that I'm not even
>certain what approach to take here. Is there some other much more "safe"
>approach to displaying and printing signed XML data? The above approach
>certainly has it's holes.
>
>TIA,
>
>--
>John C. Bowman
>Software Engineer
>Thermo Electron Scientific Instruments Div.
><Remove this before reply> john.bowman@thermo.com
>
>
>