

Re: xml-security vs. native security

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-03/2264.html>

From: Anne & Lynn Wheeler (lynn_at_garlic.com)

Date: 03/28/05

Date: Mon, 28 Mar 2005 12:36:59 -0700

Bruce Stephens <bruce+usenet@cenderis.demon.co.uk> writes:

> *My guess is that it's the same kind of difference as with OSI: rather
> than checking the signature of the bytes (in BER) you got over the
> wire, you can encode the abstract value in a particular way (DER) and
> check the signature of that.*

which OSI is this ... open system interconnect? ... ISO (international standards organization) model for networking?

ISO has standards for certificates, including requirements for including ASN.1 encoded digital certificates with the transmission of digitally signed financial transactions ... previous reference:
<http://www.garlic.com/~lynn/2005e.html#38> xml-security vs. native security

misc. other references:

<http://www.garlic.com/~lynn/subpubkey.html#rpo>

OSI (as in ISO's OSI model) evolved in the late 70s and early 80s concurrently with the internetworking protocol ... the arpanet/internet had the great switch-over from an early homogeneous (much more OSI-model like) to internetworking on 1/1/83.

in the late '80s several govts. had mandates that the internet be eliminated and the whole thing switched to OSI (US federal government had various "GOSIP" mandates).

in the late '80s I was evolved with trying to get HSP (high speed protocol) accepted as a work item in x3s3.3 (ISO chartered ansi standards body responsible for networking related standards). at the time, ISO had a mandate that networking related standards couldn't deviate/violate from the OSI model.

HSP would:

- 1) go directly from transport/level4 to mac/lan interface
- 2) support internetworking (aka tcp/ip)
- 3) support max/lan interface

sci.crypt: Re: xml–security vs. native security

HSP was rejected based on the ISO mandates because

1) it violated OSI model by skipping the transport/network,
level 3/4 interface

2) it violated OSI model by supporting tcp/ip ... aka OSI was
traditional private homogeneous networking model and didn't include
provisions for internetworking, gateway, etc. ... and therefor HSP
violated the OSI model by supporting internetworking

3) mac/lan interface violates the OSI model with the mac/lan
interface corresponding to approx. the middle of layer 3.
Anything supporting mac/lan interface violates the OSI model.
HSP supported the mac/lan interface, therefore HSP violated
the OSI model.

misc. past comments:

<http://www.garlic.com/~lynn/subnetwork.html#xtphsp>

for a little topic drift ... an unrelated recent post
on xml

<http://www.garlic.com/~lynn/2005e.html#34> Thou shalt have no other gods before the ANSI C standard

misc other xml, html, sgml, gml posts

<http://www.garlic.com/~lynn/subtopic.html#sgml>

--

Anne & Lynn Wheeler | <http://www.garlic.com/~lynn/>