

Re: xml-security vs. native security

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-03/2297.html>

From: Anne & Lynn Wheeler (lynn_at_garlic.com)

Date: 03/29/05

Date: Tue, 29 Mar 2005 06:19:43 -0700

Bruce Stephens <bruce+usenet@cenderis.demon.co.uk> writes:
> *And yes, the whole thing (most definitely including the very relevant*
> *X.509) always seems way too complex to me. (I still have no idea what*
> *nonRepudiation is supposed to mean in a certificate.)*

well, in the mid-90s ... there was some push that if the consumer digitally signed a financial transaction ... and if the relying party (merchant) could find any certificate for the consumer's public key that contained the nonRepudiation bit ... it would shift the burden of proof from the merchant to the consumer in any dispute. It appeared to be a ploy trying to get the merchants to underwrite the enormous cost of a PKI deployment for consumer certificates (since shifting the burden of proof in disputes represents a significant cost).

besides the whole issue of the verification of a digital signature simply implies some form of "something you have" authentication (i.e. the verification of a digital signature implies that the originator has access and used the corresponding private key) ... and by itself can't carry with it the meaning of a human signature (observed, read, understood, agrees, approves, authorizes) there is the whole issue the standard PKI related protocols have no provision for proving which certificate somebody originating a digital signed message ... actually included in a transaction.

assuming it did come to have any meaning, one attack is for a merchant to convince some certification authority to issue certificates with the nonRepudiation bit turned on ... for all public keys that the merchant happened to encounter. Since the attached certificate is normally part of the signed message in standard existing PKI protocols ... there is no proof as to which certificate a consumer might have actually appended to any digital signed message.

--

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