Authentication of "What" - Not Just of "Who"

Message posted to the Temple University School of Law E-mail List on Digital Signatures
By Daniel Greenwood
Thursday, 26 March 1998

To create a signature, a central legal element is the "intent" of the signer, as manifested by some affirmative action - like scripting a manual signature or, potentially, clicking a button. Digital signature implementations focus energetically on creating proof that the action occurred - but have failed thus far to adequately address the deeper issue of assuring and, if necessary, proving "intent." I think the best way to assure (and hence be able to prove) something as ineffable as intent is to design systems that make the underlying context, implications, gravity, etc. of the transaction plainly obvious to any awake human. UDAC is a shot at providing this second, more complex, level of assurance. I should think that PKI advocates who hope to sell their wares as products/services that are going to create a "legal" signature would be thankful for this timely and topical contribution to the evolution of electronic authentication. For a long time people have lamented the lack of good off the shelf software that implements digital signatures in a user friendly manner (or at least "user aware"). It is clear to me that authentication technology requires innovations like the one proposed in UDAC in order to mature as viable and widely deployable.

I suspect that the focus on non-repudiation of identity is misplaced because that is just a lesser (often negligible) sub issue of electronic authentication. To test this theory, I have been quickly looking over case law involving signature disputes and reviewing citizen complaints to Massachusetts state government (where I work) that are based on signatures. Sure enough, the vast majority of disputes involve people who admit that they were the person that "signed" the record in question - but who contest the meaning of the signature. There is a mismatch between the real problems and the nature of solutions by digital signature advocates. Don't get me wrong - I am also in favor of using digital signatures as an authentication technology, but I perceive that we are experiencing a significant opportunity cost by allocating our resources to answer the wrong question.

Digital signatures are often cited as a method of achieving "non-repudiation." Non-repudiation is not merely the sum of an encrypted digest of data verifiable with reference to a properly issued public key certificate. This type of authentication technology is necessary, but not sufficient to solve the "repudiation" issue. I would first recast the issue as something more like "non misunderstanding" (from which repudiation is one possible outcome). The real trick is to create systems that allow prevention or rapid resolution of the types of misunderstandings (real or claimed) that lead to disputes over whether a given person is to be bound by or held to an electronic authentication.

These misunderstandings, and not a raw denial purportedly based on forgery, are the major source of disputes. These are the disputes that will end up raising transaction costs by clogging our complaint lines, slowing service channels, creating animosity, and - when really unlucky - bringing us into litigation. I suggest that we will end up with a seriously sub optimal authentication infrastructure unless the systems are designed to maximally preclude or resolve the source of this type of misunderstanding. To the extent that infrastructures are needed, this level of the interaction (involving UI design with UDAC type controls) must be treated as a critical part of the whole system.

Beyond creating signatures that will withstand the acid test of litigation, it seems to me that the really important foundation that needs to be laid is based on the "user experience." Every case that ends up in

litigation begins with a dispute. The vast majority of disputes never end up in litigation and are therefor never directly subject to the exhaustive analysis required when legally enforcing an electronic or digital signature. I think the majority of effort in industry, academia, the bar and government should be focused on building systems that reduce or resolve disputes by enhancing system usability/understandability in the first place.

It has been said on this list that things like the ceremony provided by UDAC would only be necessary for high stakes transactions. I think the opposite is more accurate. Namely, the multitude of online environments in which we will find ourselves in the future will work or burn based on the effectiveness with which they deal with more subtle issues of context and transactional implications. Perhaps, the more high stakes transactions may need less of this type of UI because reasonable people will more likely be held to have known what they were getting into when more value is on the line. The ceremony surrounding signing a constitutional amendment or high dollar contract, for example, is largely bounded by non signature related extrinsic information with which to prove the event occurred. This extrinsic data exists precisely because it is a high stakes activity. However, I imagine that UDAC type componentry would also be extremely helpful for higher stakes transactions as well.

- Daniel Greenwood

[the above message was sent in reply to the following message]

Bob Jueneman wrote:
>
> Ben,
>
> The ceremonial aspects, completely with transcription,
> memorialization, and archiving are certainly important
> if the President is signing an international treaty, or an
> amendment to the Consitution.
>
> However, they become increasingly less important as
> the importance of the document that is being signed itself
> descends the scale. Few would argue that you need a notary's
> seal on an application for a fishing license, even in Utah. :-)
>
> It certainly isn't clear to me that a prudent concern for
> protection against fraud and possible violation of one's privacy
> rights demands such ceremonialization in every case ¯ unless
> perhaps you are selling your house to GSA. I certainly ought
> to be able to order a US Coast and Geodetic Survey map for
> $4.00 without such elaborate, and yet potentially easily
> compromised mechanisms as you have described.
>
> As I argued in the article submitted to Jurimetrics, coauthored
> by myself and Prof. R. J. Robertson and entitled "Biometrics
> and Digital Signatures in Electronic Commerce" BOTH
> digital signatures AND a number of biometric techniques,
> explicitly including signature dynamics, are potentially
> subject to a rather long list of ways in which they could be
> compromised, especially if used alone, and less so if they are used

> together. But the fact that any one technique, notably including
> even a notarized wet ink signature, can be successfully
> attacked under certain circumstances is not sufficuent
> justification to discard it. A very careful analysis of the risks
> and threats vs. the cost benefits have to be performed.
>
> I will certainly grant that you are indefatigable and an effective
> lobbyiest (I assume you are registered?) and advocate in
> advancing your particular client's interest. But I forget who
> it was that said "It's a poor lawyer that can't argue both sides
> of the question."
>
> Cordially,
>
> Bob
>
> Robert R. Jueneman
> Security Architect
> Novell, Inc.,
> Network Services Division
> 122 East 1700 South
> Provo, UT 84604
> 801/861-7387
> bjueneman@novell.com
>
> >>> Ben Wright <Ben_Wright@COMPUSERVE.COM> 03/25 1:40 PM >>>
> The US General Services Administration is building a public key
> infrastructure, one of the aims of which is to allow citizens to engage
> legally binding digital signatures. In reply to GSA's request for
> comments, we submitted the following to argue that PKI signatures don't
> work as legal devices unless they are created in the context of
> human-meaningful ceremonies and the ceremonies are transcripted and
> archived.
>
> What do you think of our argument?
>
> --Ben Wright
>
> [snip]