"Paul Van Oorschot" <paulv@rogers.com> on 04/18/2005 10:49:05 PM

Please respond to <paulv@rogers.com>

To: <submissions@nspw.org>
cc:
Subject: submission to NSPW'05: Van Oorschot, "Message Authentication by Integrity with Public Corroboration"

Attached please find the PDF of my submission to NSPW'05.

Title: "Message Authentication by Integrity with Public Corroboration"
Author: Paul C. Van Oorschot
Category: Research Paper
Attendance Statement: I will attend if the contribution is accepted.

Justification for inclusion in NSPW:

I believe my submission is appropriate for NSPW, as a Research Paper, for the following reasons. I believe that it represents a significant shift in thinking on message authentication, and potentially has direct application to problems including spam and phishing, possibly providing a very interesting improvement over some recently proposed existing alternatives (the IETF proposals for Sender Policy Framework/SPF, and DomainKeys) to these specific problems. It is somewhat contrarian to standard security proposals, since it does not directly involve the use of a cryptographic key, and also it relies on access control (or integrity) as the basis for message authentication, whereas the standard paradigm is to rely on authentication as the basis for access control decisions.

My submission is not particularly deep in technical details (indeed, the idea itself is not particularly "deep" technically - which is one of its advantages), and thus would not be well-received at a crypto conference. I believe it would also be of little interest to other top security conferences, as many typically require implementations to "prove out" the ideas (e.g. NDSS, USENIX Security), require more fully developed ideas (ACM CCS), or more theoretical justification (IEEE S&P/Oakland). The present idea as documented is also preliminary, and might be considered "too simple" in some other forums. However, in my

experience, it is precisely such "simple" ideas which, when good, have the greatest potential to get deployed, and have true practical impact.

The basic idea of the proposal is for the originator of a message (e.g. an email) to post a hash of the email at some publicly verifiable site. Intended recipients / recipient systems can then cross-check that site as corroboration that the asserted originator was the true originator. For the system to work, the true originator must have the ability to post hashes to the corroborating site, while an attacker must not be able to update or modify entries to this site. Specific problems this proposal seems to have application to include: email with spoofed `From' fields (e.g. as used in spam and phishing); and corroboration of digital signatures, in the case that signature private keys may have been compromised. I believe these specific applications may also stimulate interesting discussions at NSPW, independent of my own proposal.

Sincerely,
Paul Van Oorschot
http://www.scs.carleton.ca/~paulv/

- nspw.pdf