

RE: Signing before Encryption and Signing after Encryption

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-03/msg00282.html>

- *From:* "David Gillett" <gillettdavid@xxxxxxxx>
 - *Date:* Wed, 22 Mar 2006 09:32:11 -0800
-

The property that a hash match is supposed to verify (is this copy the same as the original) is not quite the same as the property that a signature verifies (did this document come from that source). There **are** many applications where one is an acceptable alternative to the other.

However, there have been numerous news items in the last 18 months about the feasibility of engineering hash collisions with several popular algorithms; hashing must be assumed to provide weaker verification of its property than might have been previously assumed. (For now, I've recommended that folks using tools that don't yet do SHA-256 or better should use **both** MD5 and SHA-1 -- I don't think anyone has yet described an engineered collision that works with both.)

Engineering hash collisions is apparently easier than compromising a properly-secured private key used in a good asymmetric algorithm.

David Gillett

-----Original Message-----

From: Craig Wright [<mailto:cwright@xxxxxxxxxxxxxxxx>]
Sent: Tuesday, March 21, 2006 8:03 PM
To: gillettdavid@xxxxxxxx; shyaam@xxxxxxxx;
security-basics@xxxxxxxxxxxxxxxx
Subject: RE: Signing before Encryption and Signing after Encryption

Hello,
Just to be difficult...

David stated "Signing requires a private key". This is correct through feasibility, but it is not technically correct as there are signature schemes that only require symmetric keys. Signing with symmetric keys is a lot more complex and thus more prone to error and has a range of key

RE: Signing before Encryption and Signing after Encryption

management issues. This does not mean that it is not possible.

In fact there are scheme to sign a message using only Hashing algorithms. The simplest of these is to hash the document and keep a list of document hashes (similar to software). A user could check the list to see if the message was valid or if tampering had occurred. A third party could keep the hash tables to ensure that the lists where accurate.

So signing does not require a private key – it just makes it easier. Next it also depends on non–repudiation/repudiation issues. It is easy to sign a document and have a verification that it is unaltered but with no proof that the original signer could not come back and accuse the receiver of forging the document.

An example symmetric scheme could be:

Alice encrypts a message using a symmetric key known to Bob (and Alice only)

Alice hashes the encrypted message

Alice encrypts the (encrypted) message and hash using a symmetric key known to Jim but unknown to Bob Bob receives the hashed and encrypted message.

If Bob alters the message – the hash will not work. Alice can not lie as Jim has a copy.

Key management is a bugger, but still possible (though unlikely)

ANSI X9.17 Notarised Symmetric Keys may be used to sign.

Regards
Craig S Wright

PS There are also hybrid ciphers for signing which are based on a combination of all the above – but this for another post

-----Original Message-----

From: David Gillett [<mailto:gillettdavid@xxxxxxxx>]

Sent: 22 March 2006 6:21

To: shyaam@xxxxxxxx; security-basics@xxxxxxxxxxxxxxxxxxxx

Subject: RE: Signing before Encryption and Signing after Encryption

Signing requires a private key — therefore, it **must** be Asymmetric.

Asymmetric is typically much slower than Symmetric, so you get things like SSL that use Asymmetric to protect the

RE: Signing before Encryption and Signing after Encryption

exchange of the Symmetric key used for actual payload encryption.

Signing after encryption allows the signature to be verified before/without decrypting the payload. There are a variety of circumstances in which that could be useful, which are blocked if the signing is done first. I can't think of any where the opposite is true.

David Gillett, CISSP

Liability limited by a scheme approved under Professional Standards Legislation in respect of matters arising within those States and Territories of Australia where such legislation exists.

DISCLAIMER

The information contained in this email and any attachments is confidential. If you are not the intended recipient, you must not use or disclose the information. If you have received this email in error, please inform us promptly by reply email or by telephoning +61 2 9286 5555. Please delete the email and destroy any printed copy.

Any views expressed in this message are those of the individual sender. You may not rely on this message as advice unless it has been electronically signed by a Partner of BDO or it is subsequently confirmed by letter or fax signed by a Partner of BDO.

BDO accepts no liability for any damage caused by this email or its attachments due to viruses, interference, interception, corruption or unauthorised access.

EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE

The Norwich University program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience. Tailor your education to your own professional goals with degree customizations including Emergency Management, Business Continuity Planning, Computer Emergency Response Teams, and Digital Investigations.

<http://www.msia.norwich.edu/secfocus>
