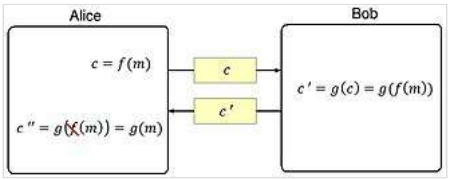
WIKIPEDIA
The Free Encyclopedia

Blind signature

In cryptography a **blind signature**, as introduced by David Chaum,[1] is a form of digital signature in which the content of a message is disguised (blinded) before it is signed. The resulting blind signature can be publicly verified against the original, unblinded message in the manner of a regular digital signature. Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties. Examples include cryptographic election systems and digital cash schemes.

An often-used analogy to the cryptographic blind signature is the physical act of a voter enclosing a completed anonymous ballot in a special carbon paper lined envelope that has the voter's credentials pre-printed on the outside. An official verifies the credentials and signs the envelope, thereby transferring his signature to the ballot inside via the carbon paper. Once signed, the package is given back to the voter, who transfers the now signed ballot to a new unmarked normal envelope. Thus, the signer does not view the message content, but a third party can later verify the signature and know that the signature is valid within the limitations of the underlying signature scheme.

Blind signatures can also be used to provide *unlinkability*, which prevents the signer from linking the blinded message it signs to a later un-blinded version that it may be called upon to verify. In this case, the signer's response is first "un-blinded" prior to verification in such a way that the signature remains valid for the un-blinded message. This can be useful in schemes where anonymity is required.



An example of blind signature in action

Blind signature schemes can be implemented using a number of common public key signing schemes, for instance RSA and DSA. To perform such a signature, the message is first "blinded", typically by combining it in some way with a random "blinding factor". The blinded message is passed to a signer, who then signs it using a standard signing algorithm. The resulting message, along with the blinding factor, can be later verified against the signer's public key. In some blind signature schemes, such as RSA, it is even possible to remove the blinding factor from the signature before it is verified. In these schemes, the final output (message/signature) of the blind signature scheme is identical to that of the normal signing protocol.

Uses

Blind signature schemes see a great deal of use in applications where sender privacy is important. This includes various "digital cash" schemes and voting protocols.

For example, the integrity of some electronic voting system may require that each ballot be certified by an election authority before it can be accepted for counting; this allows the authority to check the credentials of the voter to ensure that they are allowed to vote, and that they are not submitting more than one ballot. Simultaneously, it is important that this authority does not learn the voter's

selections. An unlinkable blind signature provides this guarantee, as the authority will not see the contents of any ballot it signs, and will be unable to link the blinded ballots it signs back to the un-blinded ballots it receives for counting.

Blind signature schemes

Blind signature schemes exist for many public key signing protocols. More formally a blind signature scheme is a cryptographic protocol that involves two parties, a user Alice that wants to obtain signatures on her messages, and a signer Bob that is in possession of his secret signing key. At the end of the protocol Alice obtains Bob's signature on m without Bob learning anything about the message. This intuition of not learning anything is hard to capture in mathematical terms. The usual approach is to show that for every (adversarial) signer, there exists a simulator that can output the same information as the signer. This is similar to the way zero-knowledge is defined in zero-knowledge proof systems.

Blind RSA signatures

[2]:235

One of the simplest blind signature schemes is based on RSA signing. A traditional RSA signature is computed by raising the message m to the secret exponent d modulo the public modulus N. The blind version uses a random value r, such that r is relatively prime to N (i.e. $gcd(r, N) = 1$). r is raised to the public exponent e modulo N, and the resulting value $r^e \bmod N$ is used as a blinding factor. The author of the message computes the product of the message and blinding factor, i.e.:

$$m' \equiv mr^e \pmod{N}$$

and sends the resulting value m' to the signing authority. Because r is a random value and the mapping $r \mapsto r^e \bmod N$ is a permutation it follows that $r^e \bmod N$ is random too. This implies that m' does not leak any information about m. The signing authority then calculates the blinded signature s' as:

$$s' \equiv (m')^d \pmod{N}.$$

s' is sent back to the author of the message, who can then remove the blinding factor to reveal s, the valid RSA signature of m:

$$s \equiv s' \cdot r^{-1} \pmod{N}$$

This works because RSA keys satisfy the equation $r^{ed} \equiv r \pmod{N}$ and thus

$$s \equiv s' \cdot r^{-1} \equiv (m')^d r^{-1} \equiv m^d r^{ed} r^{-1} \equiv m^d r r^{-1} \equiv m^d \pmod{N},$$

hence s is indeed the signature of m.

In practice, the property that signing one blinded message produces at most one valid signed messages is usually desired. This means one vote per signed ballot in elections, for example. This property does not hold for the simple scheme described above: the original message and the

unblinded signature is valid, but so is the blinded message and the blind signature, and possibly other combinations given a clever attacker. A solution to this is to blind sign a cryptographic hash of the message, not the message itself.[3]

Dangers of RSA blind signing

RSA is subject to the RSA blinding attack through which it is possible to be tricked into decrypting a message by blind signing another message. Since the signing process is equivalent to decrypting with the signer's secret key, an attacker can provide a blinded version of a message m encrypted with the signer's public key, m' for them to sign. The encrypted message would usually be some secret information which the attacker observed being sent encrypted under the signer's public key which the attacker wants to learn more about. When the attacker removes the blindness the signed version will have the clear text:

$$\begin{aligned} m'' &= m'r^e \pmod{n} \\ &= (m^e \pmod{n} \cdot r^e) \pmod{n} \\ &= (mr)^e \pmod{n} \end{aligned}$$

where m' is the encrypted version of the message. When the message is signed, the cleartext m is easily extracted:

$$\begin{aligned} s' &= m''^d \pmod{n} \\ &= ((mr)^e \pmod{n})^d \pmod{n} \\ &= (mr)^{ed} \pmod{n} \\ &= m \cdot r \pmod{n}, \text{since } ed \equiv 1 \pmod{\phi(n)} \end{aligned}$$

Note that $\phi(n)$ refers to Euler's totient function. The message is now easily obtained.

$$m = s' \cdot r^{-1} \pmod{n}$$

This attack works because in this blind signature scheme the signer signs the message directly. By contrast, in an unblinded signature scheme the signer would typically use a padding scheme (e.g. by instead signing the result of a cryptographic hash function applied to the message, instead of signing the message itself), however since the signer does not know the actual message, any padding scheme would produce an incorrect value when unblinded. Due to this multiplicative property of RSA, the same key should never be used for both encryption and signing purposes.

See also

- Dining cryptographers protocol
- Electronic money

References

1. Chaum, David (1983). "Blind Signatures for Untraceable Payments" (http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF) (PDF). *Advances in*

Cryptology. Vol. 82. pp. 199–203. doi:10.1007/978-1-4757-0602-4_18 (https://doi.org/10.1007%2F978-1-4757-0602-4_18). ISBN 978-1-4757-0604-8.

2. Goldwasser, S. and Bellare, M. "Lecture Notes on Cryptography" (http://cseweb.ucsd.edu/~mihir/papers/gb.html) Archived (https://web.archive.org/web/20120421084751/http://cseweb.ucsd.edu/~mihir/papers/gb.html) 2012-04-21 at the Wayback Machine. Summer course on cryptography, MIT, 1996–2001
3. The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme (http://eprint.iacr.org/2001/002.pdf)

External links

- EP application 1571777 (https://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=EP1571777), Canard, S., Gaud, M., Traore, J., "Electronic voting process using fair blind signatures", published 2005-09-07, assigned to France Telecom
- Security of Blind Signatures Under Aborts (https://web.archive.org/web/20110718231432/http://www.dominique-schroeder.de/data/publications/conference/security-blind-signature-abort.pdf)
- Implementation of Blind Signature in Java (https://github.com/arisath/Blind-RSA)