Foundations of Computer Security

Lecture 53: Digital Signatures

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Digital Signatures

Suppose you write a (physical) check. *What would you like to be true?*

- A check is a *tangible object* authorizing the transaction.
- The signature on the check *confirms authenticity*.
- In the case of an alleged forgery, a third party may be called to *judge authenticity*.
- The check is *not alterable* or alterations can be easily detected.
- The signature is part of the check, so cannot be easily removed and re-used.

Can we define a mechanism for signing a document digitally that has analogous characteristics?

Digital Signatures Properties

Suppose S sends a message M to R with signature $f(S, M)$: We'd like the signature to have certain properties:

unforgeable: it should be difficult for anyone but S to produce $f(S, M)$;

authentic: R can verify that S signed the document M;

no repudiation: S cannot deny producing the signature;

tamperproof: after being transmitted, M cannot be modified;

not reusable: the signature cannot be detached and reused for another message.

Digital Signatures (Cont.)

Public key systems are well-suited for digital signatures. Recall that some algorithms, RSA in particular, have the following characteristic:

$$\{\{M\}_K\}_{K^{-1}} = M = \{\{M\}_{K^{-1}}\}_K.$$

So, if S wishes to send message M to R in a way that has some of the characteristics of a digitally signed message, S could send

$$\{\{M\}_{K_S^{-1}}\}_{K_R}.$$

Most often, it's not the M but a hash of M that is signed. *Why?*

What assurance does R gain from this interchange?

Digital Signatures Properties

S sends to R the following message:

$$\{\{M\}_{K_S^{-1}}\}_{K_R}.$$

This scheme has the desired properties:

unforgeable: only S can use K_S^{-1};

authentic: a third party can verify the signature with K_S;

no repudiation: only S can use K_S^{-1};

tamperproof: only R can remove the outer layer of encryption;

not reusable: the signature is tightly bound to the message M.

Lessons

- Digital signatures function much as physical signatures.
- Ideally a signature should be: unforgeable, authentic, tamperproof, non-reusable, and allow no repudiation.
- Public key cryptosystems facilitate creating digital signatures.

Next lecture: Certificates