CS458: Introduction to Information Security

Notes 6: Digital Signatures

Yousef M. Elmehdwi

Department of Computer Science

Illinois Institute of Technology

yelmehdwi@iit.edu

October 4, 2018

Slides: Modified from Christof Paar and Jan Pelzl

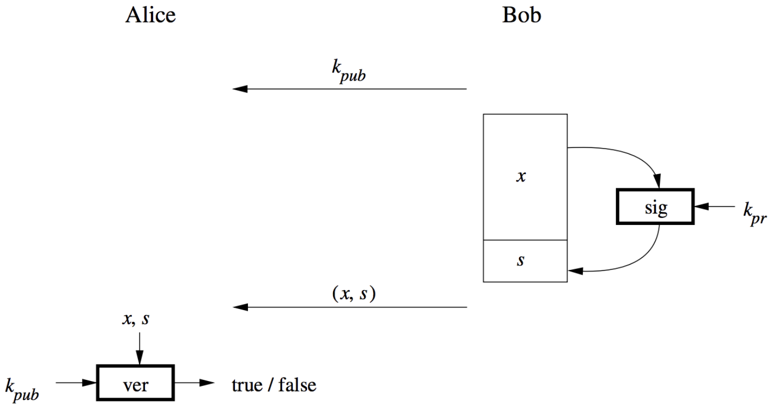
Outline

- The principle of digital signatures
- Security services
- The RSA digital signature scheme

Motivation

- Odd Colors for Cars, or: Why Symmetric Cryptography Is Not Sufficient
- Discuss a setting in which symmetric cryptography fails to provide a desirable security function
  - Bob orders a pink car from the car dealer Alice
  - After seeing the pink car, Bob states that he has never ordered it
  - How can Alice prove towards a judge that Bob has ordered a pink car? (And that she did not fabricate the order herself)
    $\Rightarrow$ Symmetric cryptography fails because both Alice and Bob can be malicious
    $\Rightarrow$ Can be achieved with public-key cryptography

Basic Principle of Digital Signatures



- The person who signs the message uses a private key, and the receiving party uses the matching public key

Main Idea

- For a given message x, a digital signature is appended to the message (just like a conventional signature).
- Only the person with the private key should be able to generate the signature.
- The signature must change for every document.

  $\Rightarrow$ The **signature** is realized as a function with the message x and the private key as input.

  $\Rightarrow$ The public key and the message x are the inputs to the **verification function**.

Core Security Services

- The objectives of a security systems are called security services.
  1. Confidentiality: Information is kept secret from all but authorized parties
  2. Integrity: Ensures that a message has not been modified in transit.
  3. Message Authentication: Ensures that the sender of a message is authentic. An alternative term is data origin authentication
  4. Non-repudiation: Ensures that the sender of a message can not deny the creation of the message. (e.g., order of a pink car)
     - But **who** is the sender?
- Confidentiality is provided by using primarily symmetric ciphers and less frequently asymmetric encryption.
- Integrity and message authentication are provided by digital signatures and message authentication codes.
- Non-repudiation can be achieved with digital signatures.

Additional Security Services[1]

5. Identification/entity authentication: Establishing and verification of the identity of an entity, e.g. a person, a computer, or a credit card.
   - **who are you**?
6. Access control/Authorization: Restricting access to the resources to privileged entities. (decide **who can do what**?)
7. Auditing: Provides evidences about security-relevant activities, e.g., by keeping logs about certain events. (provide a proof **who did what**?)
7. Availability: The electronic system is reliably available.
8. Auditing: Provides evidences about security-relevant activities, e.g., by keeping logs about certain events.
9. Physical security: Providing protection against physical tampering and/or responses to physical tampering attempts
10. Anonymity/privacy: Providing protection against discovery and misuse of identity. (what if we don't want to be identified?)

[1] Slide partial credit: Jia Wang, Department of Electrical and Computer Engineering Illinois Institute of Technology

Main idea of the RSA signature scheme

- To generate the private and public key
  - Use the same key generation as RSA encryption.
- To generate the signature
  - **"encrypt"** the message x with the private key.
    $s = sig_{K_{pr}}(x) \equiv x^d \; mod \; n$
  - Append s to message x
- To verify the signature
  - **"decrypt"** the signature with the public key
  - $ver_{K_{pub}}(x, s)$
    - $x' \equiv s^e \; mod \; n$
    - If $x \equiv x'$, the signature is valid
    - If $x \not\equiv x'$, the signature is invalid

The RSA signature Protocol

Alice		**Bob**
		$k_{pr} = d,\ k_{pub} = (n,e)$
	$\xleftarrow{(n,e)}$	
		compute signature: $s = \mathrm{sig}_{k_{pr}}(x) \equiv x^d \bmod n$
	$\xleftarrow{(x,s)}$	

verify: $\mathrm{ver}_{k_{pub}}(x,s)$

$x' \equiv s^e \bmod n$

$$x' \begin{cases} \equiv x \bmod n & \Longrightarrow \text{valid signature} \\ \not\equiv x \bmod n & \Longrightarrow \text{invalid signature} \end{cases}$$

- Alice can conclude from the valid signature that Bob generated the message and that it was not altered in transit,
    - i.e., message authentication and message integrity are given.
- If this security service is required, the message x and signature s can be encrypted, e.g., using AES.
- Signature verification is very efficient as a small number can be chosen for the public key

The RSA signature Protocol: Example

Alice		**Bob**
		1. choose $p = 3$ and $q = 11$
		2. $n = p \cdot q = 33$
		3. $\Phi(n) = (3-1)(11-1) = 20$
		4. choose $e = 3$
		5. $d \equiv e^{-1} \equiv 7 \bmod 20$
	$\xleftarrow{(n,e)=(33,3)}$	
		compute signature for message $x = 4$:
		$s = x^d \equiv 4^7 \equiv 16 \bmod 33$
	$\xleftarrow{(x,s)=(4,16)}$	
verify:		
$x' = s^e \equiv 16^3 \equiv 4 \bmod 33$		
$x' \equiv x \bmod 33 \Longrightarrow$ valid signature		

Existential Forgery Attack Against RSA Digital Signature

Alice		**Oscar**		**Bob**
				$k_{pr} = d$
				$k_{pub} = (n, e)$
	$\xleftarrow{(n,e)}$		$\xleftarrow{(n,e)}$	
		1. choose signature: $s \in \mathbb{Z}_n$		
		2. compute message: $x \equiv s^e \bmod n$		
	$\xleftarrow{(x,s)}$			
verification: $s^e \equiv x' \bmod n$				
since $x' = x$				
$\Longrightarrow$ valid signature!				

Existential Forgery and Padding

- An attacker can generate valid message-signature pairs (x, s)
- But attacker can only choose signature s and NOT the message x
  $\Rightarrow$ Attacker cannot generate messages like "Transfer \$1000 into Eve's account"

- Formatting the message x according to a padding scheme can be used to make sure that an attacker cannot generate valid (x, s) pairs.
- A messages x generated by an attacker during an Existential Forgery Attack will not coincide with the padding scheme.

Lessons Learned

- Digital signatures provide message integrity, message authentication and nonrepudiation.
- RSA is currently the most widely used digital signature algorithm.
- Competitors are the Digital Signature Standard (DSA) and the Elliptic Curve Digital Signature Standard (ECDSA).
- RSA verification can be done with short public keys e. Hence, in practice, RSA verification is usually faster than signing.
- In order to prevent certain attacks, RSA should be used with padding. The modulus of the RSA signature schemes should be at least $1024-bits$ long. For true long-term security, a modulus of length $3072\ bits$ should be chosen. .