DNS security

Karst Koymans & Niels Sijm

Informatics Institute

University of Amsterdam

Friday, September 14, 2012

1. DNS: what to secure?
2. The long (and winding) road to the DNSSEC specification
3. On locks and seals

Outline

How is DNS insecure?

- How is DNS insecure?
  - Does it give you papercuts?
  - Will your Internet break down?
  - Computer says no?

How is DNS insecure?

- DNS data can be subject to forgery
  - www.facebook.com –> CNAME for my.evil.com
- DNS data traverses the network in clear text
  - People can eavesdrop on your DNS traffic

What DNSSEC has to offer

- Protects against forgery
  - Uses public key cryptography
  - Cryptographically signs answers
  - Builds a chain of trust
- Does NOT prevent eavesdropping
  - Data still traverses the network in clear text

Outline

DNSSEC specification

- Original specification from January 1997
  - RFC 2065
- Revised specification from March 1999
  - RFC 2535
  - Incorporated feedback from early users
  - Had deployment problems, especially scaling issues
- "Final" specification from March 2005
  - DNSSEC-bis (RFC 4033, 4034 and 4035)
- "Final" addition from February 2008
  - NSEC3 (RFC 5155)

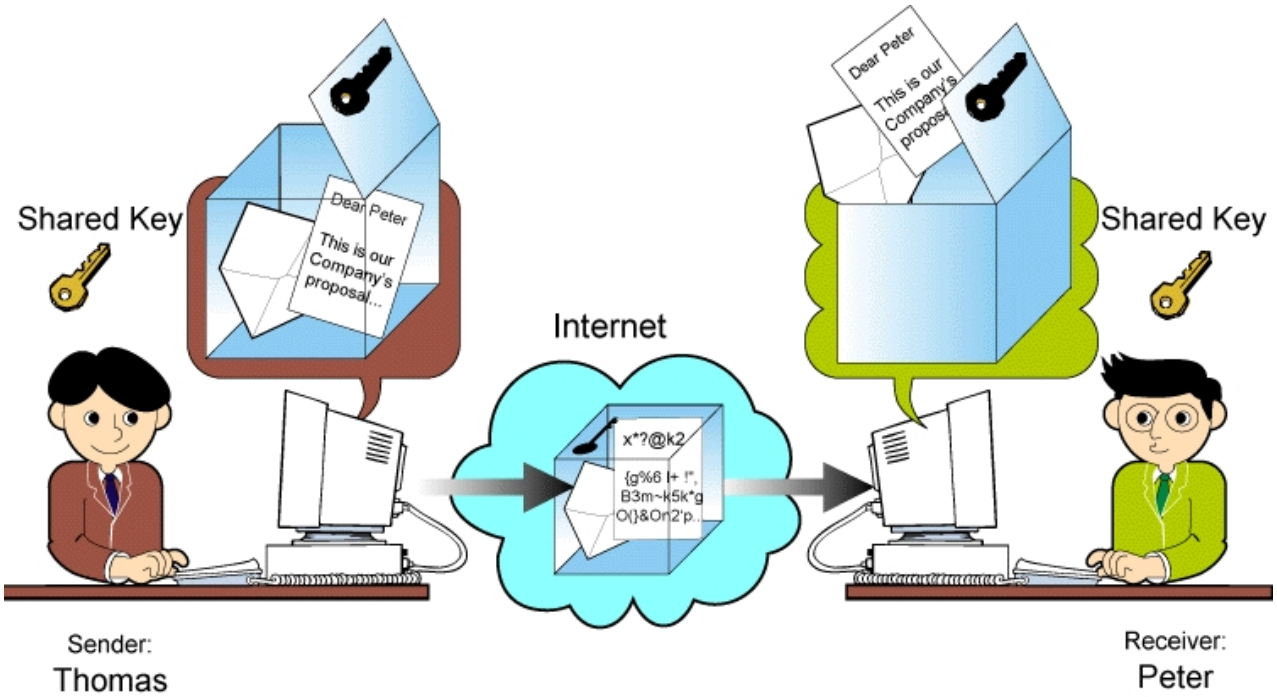
Alternative DNS security mechanism

- DNSCurve
  - Idea by Dan Bernstein
  - Proposed in August 2008 (after NSEC3 spec)
  - Encrypts and authenticates on the link level
  - Signs communication packets, not resource records
  - Uses labels of name servers to distribute public keys
  - Uses state of the art elliptic curve cryptography for speed
  - Worth a read at `http://dnscurve.org/`
    - Also see `http://curvecp.org/`

Outline

Secret key cryptography

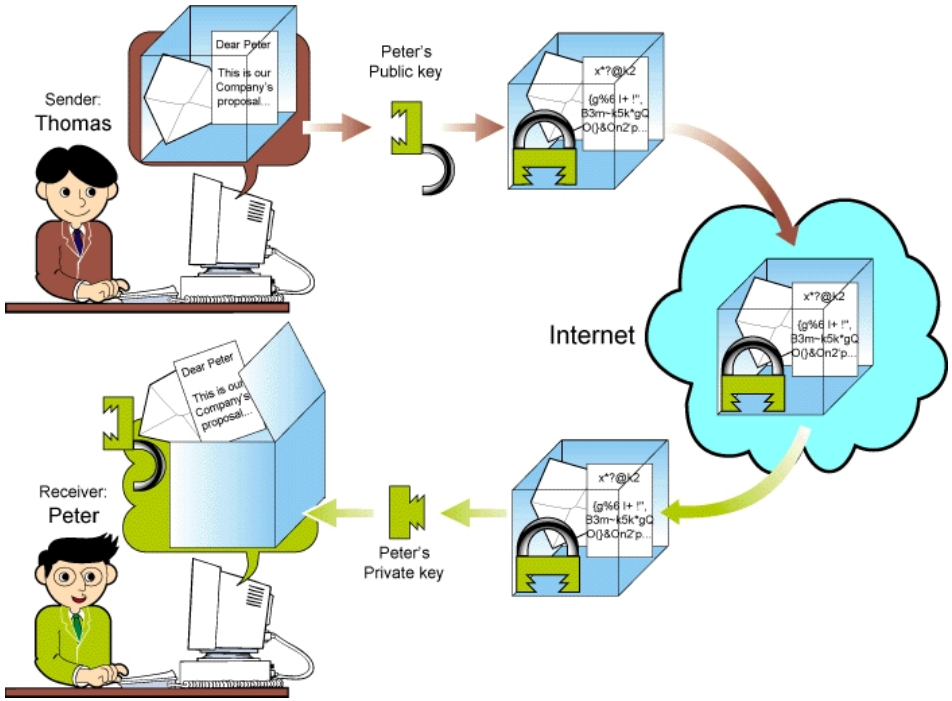
- Use one lock and two identical keys



(Source: Cisc, University of Hong Kong)

Public key cryptography – encryption

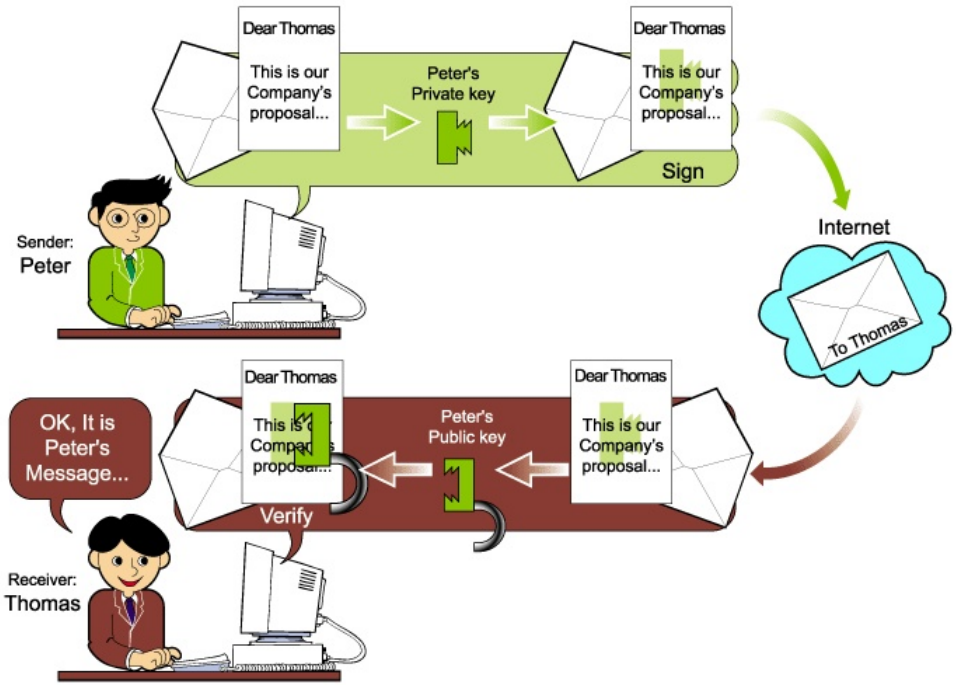
- Use a lock, which closes without key, and one key to open



(Source: Cisc, University of Hong Kong)

Public key cryptography – signing

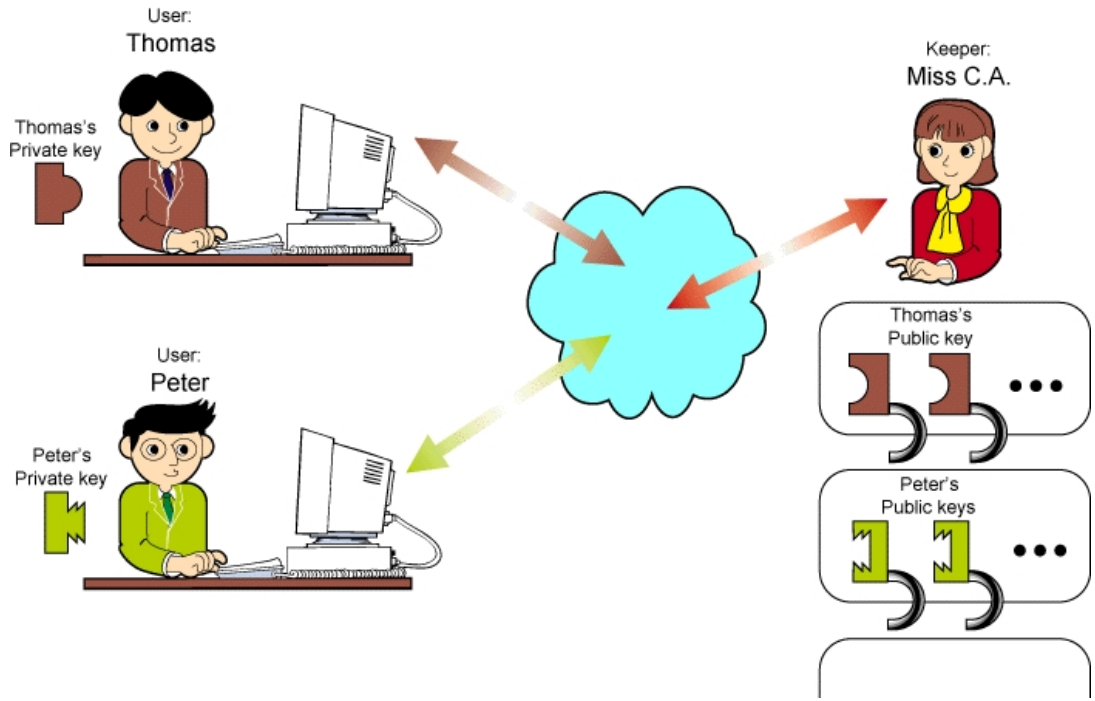
- Use an unforgeable seal and check the characterisitics



(Source: Cisc, University of Hong Kong)

Trusted party and/or certificate authority

- Use a trusted repository or party
- Create a chain of trust by signing public keys



(Source: Cisc, University of Hong Kong)