Simplifying Public Key Management

By Peter Gutmann

IEEE, Computer, Volume: 37, Issue: 2 ,February 2004

Present by Cheung Ling Kelly Yu

Summary

- The Universal PKI (Public Key Infrastructure) is not really successful and there are alternative approaches to public key management.
  - A single authority to manage PKI
  - Reason for alternative approaches
    - Many security protocols in use today were designed under the assumption that some form of global distributed PKI
- Discussion of two alternative approaches to the public key management.
  - Key continuity
  - Certificate approaches
    - Hard-coded certificate-authority certificates
    - Self-issued certificates

Critical comment

- Gutmann said that "1990s, when a universal PKI was thought to be just around the corner. Ten years later, it's still just around the corner, and it probably always will be."
  - But why " it probably always will be"? He didn't discuss the reason!
  - Any proof about this assumption?

Appreciative comment (1)

- The author have mention a very good security analysis in this article "The real test of a security mechanism's effectiveness is its user acceptability."
  - This comment is good because it tells us what is the true story of a security mechanism's effectiveness.
  - This comment remind us that human issue is also very important for security mechanism.

Appreciative comment (2)

- Discuss the alternative approaches comprehensively
  - The discussion is pleasing because he shows readers the full picture of those approaches
    - Mechanism of those approaches
    - Disadvantages of those approaches
    - Advantages of those approaches

Appreciative comment (2)

- Mechanism of those approaches
  - The way Key continuity deployed in SSH (security shell)
    - Know-host mechanism
      - In SSH (security shell) protocol a user initially connects to a SSH server the client will receive a new public key. If the client application repeatedly receives the same key, the source as most likely the same server.
  - How does certificate approaches works
    - Hard-coded certificate-authority certificates
      - In SSL/TLS(SSL/transport layer security), the Web browser contain more than 100 hard-coded certificate-authority certificates that in turn are trusted to issue SSL server certificates.
    - Self-issued certificates
      - Both SSL/TLS(SSL/transport layer security) and IPsec can act as their own certificate authorities, issuing themselves certificates for installation on client/peer machines.

Appreciative comment (2)

- Advantages of those approaches
  - Ease of use
  - Transparency to end users
  - Low unit cost
- Disadvantage of those approaches
  - Vulnerabilities of Key continuity
    - E.g MITM (Man In The Middle) attack
      - Someone in between the two communicating parties. A weak tie between a key and its owner invites MITI attacks.
  - Vulnerabilities of Certificate approaches
    - E.g many hard-coded CAs (certification Authority) are completely unknown and using weak 512-bit keys or with 40 years lifetime

Question

- Do you think universal PKI will implement successfully in the future and why do you think that?
  - At the moment I don't think it will be done in the future!
  - Reason:
    - Now a day people are reasonably satisfy with the alternative approaches of the public key management.
    - Organisational, economical and political
      - Who would issue/ store/ administer certificates and how much such service would cost.

THANK YOU!!