Simplifying Public Key Management

by Peter Gutmann

Computer 37:2, 101-103, February 2004

Presented by Chris Mills

Summary

- There is a lack of a universal public key infrastructure (PKI).
- Public key management involves:
  - Public keys
  - The entity that uses them
- Alternative solutions for public key management provide ease of use, transparency, and low cost.

Critical: Key continuity can be security hazard

- Author gives an alternative to PKI, key continuity
  - Key continuity – perpetual key used to identify the same entity.
- Mentions that if key is kept in perpetuity, can lead to compromised data
  - Longer use means more data can be cracked.
- Needs to be explored or given more prominence in the article

Appreciative: Usability affects a security mechanism success

- Author makes a point that the usability of a security mechanism determines its acceptance
- This is true for key continuity and self issued certificates
  - Ease of use
  - Transparent
  - Low cost

Appreciative: Usability affects a security mechanism success

- Secure Shell
  - Uses key continuity
  - Client remembers known entities through it known hosts mechanism
- StartTLS
  - Uses certificates for authentication
  - Can use self-issued certificate

Appreciative: Server side certificate generation, client side key continuity

- Gutmann details an ideal setup for the StartTLS security mechanism
  - Automatic server-side certificate generation
  - Client-side key continuity management
- This could be extended to other applications, apart from StartTLS
  - e.g. Browsers

Question

- How do you think a universal PKI would be implemented and how successful do you think it would be?