PAKE-based mutual HTTP authentication for preventing phishing attacks

Yutaka Oiwa, Hiromitsu Takagi, Hajime Watanabe - RCIS, AIST / Hirofumi Suzuki - Yahoo! Japan

Our proposal
new mutual authentication protocol for Web systems which is

Secure
- detecting phishing websites reliably
- Both users and servers are authenticated
- no password information leaks for false websites
- offline dictionary attack impossible
  (→DIGEST auth., PwdHash:
  >20 chars required for password secrecy)

Easy to use
- using human-memorable passwords only
- no need for personal secret storage
  (↔TLS client auth., password reminders)

Generic
- no whitelist (↔EV SSL)
- no blacklist (↔IE/Firefox phishing warnings)
- not site-specific

★ Aiming for long-term solution:
  future replacement for form-based auth.

Technology
- Adopting PAKE for Web authentication
- Mutual auth. with weak secret (password)
- Password information is not leaked at all
  - Offline dictionary attack impossible
- Naturally extending RFC2617
- Drop-in replacement for BASIC/DIGEST
- Replacement for form-based authentication in web applications
- Relying on TLS for secrecy of payload
  - Assume transport/DNS security
- Host-name based detection of phishing
  - avoiding man-in-the-middle phishing

Protocol details
- Based on ISO-defined variant of PAKE protocol (ISO 11770-4 KAM3)
  - Password is combined with hostname as “weak secret” to prevent MITM attack.
    \[ \pi = H(\text{password}, \text{host}, \ldots) \]
  - Computational cost similar to TLS
- Single public-key op. for 1st access
- A few hash op. for 2nd access & more

UI consideration
- Entry field must be protected from image-based forgeries
  - no popup dialog (↔BASIC/DIGEST auth.)
  - e.g. use the chrome area (see above)
- Auth. status must be indicated
  - to prevent imitated auth. success

Current status
- Plugin for Apache server implemented
- Firefox-based browser implemented
  - Both available as open-source software
  - Internet-Draft submitted to IETF
    - “draft-oiwa-http-mutualauth-04.txt”
- Field trials
  - Our project website (see below)
  - Yahoo! Japan Auction Trial site (in 2008)
- Distribution of open-source modules

Future Work
- Standardization of the protocol
- Propose an integration to Mozilla etc.

Four possible phishing attacks:
1. steal user’s password sent
2. imitate successful login
   - to steal user’s privacy data afterwards
3. check password’s validity
   by forwarding it to the genuine site
   (man-in-the-middle attack)
4. hijack user’s sessions

Project URL: https://www.rcis.aist.go.jp/special/MutualAuth/