Research Center for Information Security (RCIS)
National Institute of Advanced Industrial Science and Technology (AIST)

PAKE-based mutual HTTP authentication for preventing phishing attacks

Yutaka Oiwa, Hiromitsu Takagi, Hajime Watanabe --- ***Joint work with Auction Dept., Yahoo Japan Corp.***

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.*

Three 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)

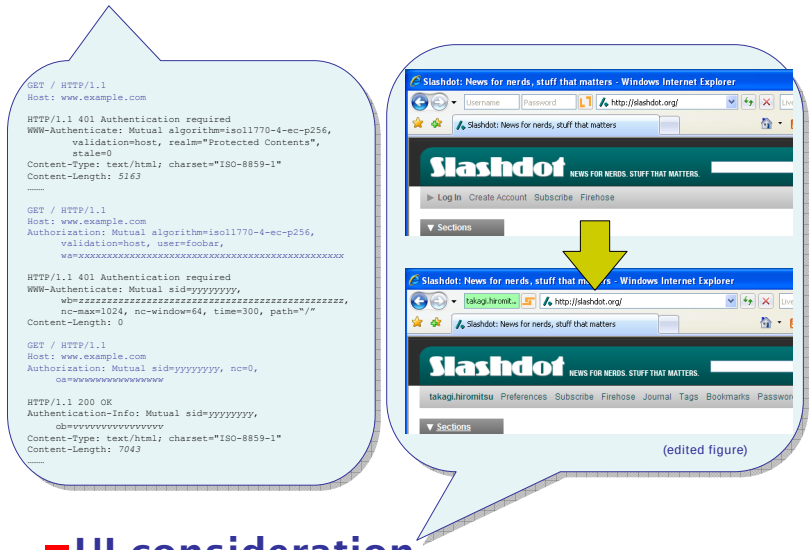
Technology

- 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 MIM attack.

    π = H (password, host)
- 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 toolbar area (see above)
- Auth. status must be indicated
  - to prevent imitated auth. success

Current status

- Plugin for Apache server implemented
- Test Firefox extension implemented
  - Full implementation is about to start
- Internet-Draft in preparation

Future Plans

- Field test in a part of Yahoo! Japan
- Distribution of open-source modules

Related Work

- EV-SSL … relies on central authorities
- Passpet … requires private key storage
- PwdHash
  - Similar hostname-based mangling
  - Weak against offline attacks