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

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

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

Three possible phishing attacks:
1. Steal user’s password
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)

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.
  \[ \pi = H(\text{password}, \text{host}) \]
- Computational cost similar to TLS
  - Single public- key op. for 1st access
  - A few hash ops. 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
- Field test in a part of Yahoo! Japan
- Distribution of open-source modules

Future Plans
- Internet- Draft in preparation

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

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