Is it too late for PAKE?

John Engler  
(UC Berkeley)

Chris Karlof  
(Usable Security Systems)

Elaine Shi  
(PARC)

Dawn Song  
(UC Berkeley)
What is PAKE?

- Password Authenticated Key Exchange

1. Enter Password
2. Crypto Protocol
3. Generate Session Key
Why PAKE?

- Password not transmitted
- Mutual Authentication
Two Hurdles

- Secure password entry
- Branding and message
Problem: Mimicry Attacks

Using PAKE

Not using PAKE
Possible Solution: Secure UI

Rachna, et al. Dynamic Security Skin Login

Oiwa, et al. MAP-HTTP's In-chrome Login
Problem: Confusion Attacks
Problem: Branding and Messaging
Conclusion

• More issues remain:
  – User Training
  – Implementation
  – Deployment

• PAKE: Potential benefits but hurdles.

• Full Paper: Firefox implementation:
  http://webblaze.cs.berkeley.edu/2009/pake/