Current Status of PAKE

HTTP Basic/Digest Authentication?!

PAKE

- Password-Authenticated Key Exchange
- Using human-memorable passwords only
  - Convenient in use
  - Widely deployed in practice
- Two dictionary attacks
  - On-line dictionary attacks
  - Off-line dictionary attacks
    - Should be prevented

Standards of PAKE

- IEEE 1363.2
- ISO/IEC 11770-4
- IETF [RFC2945, RFC5054, RFC5683]
- ITU-T Recommendation [X.1035]
- …

[RFC2945] “The SRP Authentication and Key Exchange System”, RFC 2945, Standard, 2000

[RFC5054] “Using the Secure Remote Password (SRP) Protocol for TLS Authentication”, RFC 5054, Informational, 2007

[RFC5683] “Password-Authenticated Key (PAK) Diffie-Hellman Exchange”, RFC 5683, Informational, 2010

[X.1035] “Password-Authenticated Key Exchange (PAK) Protocol”, 2007

Classification of PAKE

	Balanced PAKE	Augmented PAKE
Security requirements	Security against off-line dictionary attacks	Security against off-line dictionary attacks + Security against server compromise impersonation attacks
Protocols	EKE SPEKE PAK Dragonfly …	A-EKE (insecure), AuthA, VB-EKE B-SPEKE PAK-X/Y/Z/Z+ AMP [IEEE 1363.2, ISO/IEC 11770-4] SRP [IEEE 1363.2, ISO/IEC 11770-4, RFC2945, RFC5054] AugPAKE …

AMP and SRP

- AMP [IEEE 1363.2, ISO/IEC 11770-4]
  - AMP2 in IEEE 1363.2 and AMP+ in ISO/IEC 11770-4
  - Several AMP (e.g., AMP3, TP-AMP, AMP) turned out to be insecure
  - No provable security
  - Patent-free
- SRP [IEEE 1363.2, ISO/IEC 11770-4, RFC2945, RFC5054]
  - SRP6
  - SRP3 turned out to be insecure
  - EC conversion needs much care
  - No provable security
  - Not patent-free

Some RFCs in IETF

- RFC 5931 (Informational), 2010
  - EAP-PWD
- RFC 5683 (Informational), 2010
  - PAK
- RFC 6124 (Informational), 2011
  - EAP authentication method based on EKE
- RFC 6617 (Experimental), 2012
  - PSK (PWD) for IKE
- RFC 6631 (Experimental), 2012
  - PACE for IKEv2
- RFC 6628 (Experimental), 2012
  - AugPAKE for IKEv2

Current IETF Activity (1/2)

- TLS-PWD in TLS WG
  - https://datatracker.ietf.org/doc/draft-ietf-tls-pwd/
  - Based on Dragonfly
    - https://datatracker.ietf.org/doc/draft-irtf-cfrg-dragonfly/
    - Dragonfly has been reviewed by IRTF CFRG
  - Towards standard RFC
  - TLS-PWD LC ended on Dec. 12, 2013, but failed to move further (Parked WG Document)
    - No provable security, side-channel attacks on the loop
      - Some attacks found and fixed
    - Inefficiency (hunt-and-peck for-loop where k=40)
    - Cursory review by CFRG
    - Unclear IPR issue of SPEKE (redundancy added to SPEKE)
    - Nothing better than other (augmented) PAKE protocols (e.g., SRP, AugPAKE)

Current IETF Activity (2/2)

- Some opinions regarding TLS-PWD
  - Provable security + IP < neither both
  - Prefer augmented PAKE to balanced one
  - Prefer provable security