Challenge-Response New Authentication Scheme

Rifaat Shekh-Yusef

IETF 90, CFRG WG, Toronto, Canada

July 23, 2014

Overview

- **Goal**
  - Define a **new scheme** for the **challenge-response framework** to replace Basic/Digest.
- **How**
  - The proposals do **not** introduce any novel cryptographic algorithms.
  - The proposals use a combination of existing protocols and algorithms.

Challenge-Response Framework

```
Client                                                     Server
-------------------------------------------------------------------
   |                                                          |
   | Initial-Request                                          |
   |-------------------------------------------------------->|
   |                                                          |
   |                                      Challenge [Scheme] |
   |<--------------------------------------------------------|
   |                                                          |
   | Response [Scheme]                                        |
   |-------------------------------------------------------->|
   |                                                          |
   |                                            Confirmation |
   |<--------------------------------------------------------|
   |                                                          |
```

Usage

This framework is used by a variety of protocols; e.g. HTTP, SIP, OAuth, STUN,…

Basic/Digest Schemes Issues

- Weak protection of passwords at rest.
- Low entropy passwords.
- Password/password-hash sent on the wire.
- Optional support for mutual authentication.
- Susceptible to downgrade attack.
- Susceptible to replay attack (depends on qop)
- And more

PBKDF2-JPAKE-based Proposal

- **PBKDF2**
  - Derive a **key** from the shared password.
  - Store the **key** in the DB.

- **JPAKE**
  - Three-pass Variant
  - Key Confirmation

To fit the above into the **challenge-response** framework, the proposal:

- Uses the PBKDF2 **key** as an input to JPAKE.
- Utilizes the **Initial-Request**.
- Combines the **Key Confirmation** procedure with the **Three-pass Variant** procedure.

Key-Derivation Proposal

- **Scrypt-based scheme**:
  - Derive a **key** from the shared password.
  - Store the **key** in the DB.
  - Use the **key** to establish mutual authentication.
  - Never send the **password** or the **key** on the wire.
  - **Key**-derived data will be sent on the wire

Questions

- Can the WG agree on **one** or **more** PAKE protocols to consider?
- Should the **Key-Derivation** proposal be considered and discussed here?

References

- **PBKDF2**
  - "NIST Special Publication 800-132 - Recommendations for Password-Based Key Derivations", December 2010. http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf
- **SCRYPT**
  - Percival, C., Josefsson, S., "The scrypt Password-Based Key Derivation Function", "draft-josefsson-scrypt-kdf-01" (Work In Progress), September 2012.
- **JPAKE**
  - Hao, F., "J-PAKE: Password Authenticated Key Exchange by Juggling", draft-hao-jpake-01, (Work In Progress), December 2013.