HEXA

Hash Exchange Authentication

Alexey Melnikov <alexey.melnikov@isode.com>
Dave Cridland <dave.cridland@isode.com>

draft-cridland-sasl-hexa-00.txt

<http://dave.cridland.net/slides/>

Why?

- A Better DIGEST:
  - Deployable Security
  - Easy to Implement
  - Good for SysAdmins
- Probably to be merged with SCRAM-MD5

How?

- “Hi, I'm Alice, and I support MD5, SHA-1, and TLS-based channel binding!”
  - “Hi Alice! Here's a magic number! Use MD5 8 times, and do that funky channel binding thang.”
- “Okay. Here's my secret XORed with some ephemeral junk of equal length we can both make.”
  - “Cool, when I hash your secret I get mine! To prove it, here's some weird gunk!”

How?

- “Authcid:Alice\r\nClient-Nonce:abc[...]efg\r\nHashes:MD5 SHA1\r\nChannel-Bindings:TLS\r\n”
  - “Realm:server.example.net\r\nSalt:asd*[...]*ljfv\r\nHash:MD5\r\nHash-Cycles:8\r\nChannel-Binding:TLS\r\nServer-Nonce:qwe*[...]*rty\r\n”
- “Hash-Exchange:a1b2c3*[...]*f8\r\n”
  - “Server-Auth:1a2b3c*[...]*8f\r\n”

The Maths

- Alice's secret is a hash of the password salted with the realm.
  - Close to DIGEST-MD5 on client.
- Server's secret is a salted hash of Alice's secret – doesn't have Alice's secret.
  - Close to /etc/shadow on server.
- By hash, we really mean repeated HMAC based on an agreed hash algorithm.

Security Goals

- No plaintext on the wire or the server.
- No reliance on external channel for mutual auth - we do mutual auth and channel binding.
    - Allows ADH or leap-of-faith cert verification.
- Real-world hash agility.
- All options used for hash input – no MITM.

Security Non-Goals

- Security Layers
  - Nobody does these in DIGEST.
  - TLS, IPSec, et al do a better job here.
- Fast Reauthentication.
  - Nobody does this either.
  - Maybe piggyback onto TLS Session resumption for this anyway.

SysAdmin Goals

- Roughly similar to /etc/shadow in concept.
  - Could actually use /etc/shadow, more or less.
- Need to know when to upgrade hashes.
  - Practical hash agility – Alice says when she supports new hashes. Mad Hatter can upgrade on next password change.