Hash-Based Passwords

Steve Bellovin

https://www.cs.columbia.edu/~smb
Problem Area

• Clients and servers frequently store plaintext passwords
  – Used for keying crypto protocols
  – Password recovery (a dubious idea in any event, compared with password reset)
  – Password transmission to server by client
• People frequently (almost always?) reuse passwords
• Phishing protection
Non-Problem Areas

• Strong versus weak passwords
  – Keystroke loggers and compromised servers don’t care about password strength
  – Phishers don’t, either
  – People can’t remember $\aleph_0$ different strong passwords

• Targeted attacks against a specific user
Goal: An IETF Metastandard

• Standard way of converting user-typed password into site- and service-specific password
• Guidance to protocol designers on how to incorporate and specify hpw in their documents
• Guidance to implementers how to write the necessary code
Hashed Password Exchange

• The *effective password* is
  \[ \text{HMAC(userpw,scheme://username@hostname)} \]
  iterated many times

• “Scheme” is the protocol name as defined by IANA

• The “message” obviously makes the effective pw
  service-, user-, and host-specific
Why This Instead of Unilateral Schemes?

• Many proposals for browser-based site-specific passwords – why won’t they suffice?
  – Not all the world is a browser/server pair
  – Enter a password in one service; use it in another
  – Site restrictions on password length, “strength”, etc.
  – Allow sites to convert existing plaintext password databases to HPW
  – Universality, as user code is deployed
Objections

• HMAC is overkill
  – HMAC’s properties are well-understood; why invent something new?

• Iteration doesn’t help against massively-parallel password crackers
  – By increasing the attacker’s work factor by $n$, you decrease the number of passwords attackable by $n$

• Add a salt
  – User-hostile;doesn’t add any strength unless a particular user is being targeted, which is out of scope
Open Issues

• <Site,Portnum> pairs with multiple hostnames
  – Send hostname in the clear, similar to Host: HTTP header line?

• Multiple sites legitimately trying to share accounts/passwrds, e.g., amazon.com and amazon.fr
  – Altname in the certificate? Does this create phishing risk? Probably….
Discussion