The HP (Hashed Password :-) Payment Protocol

- Design goals
- Protocol technical overview
- Commentary

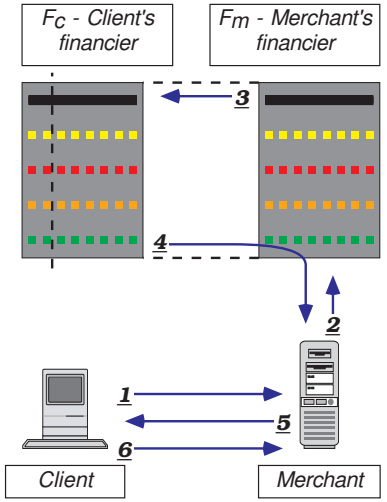
Design Goals

- Security
  - Authentication
  - Non-repudiability
  - Robust against known-to-be-feasible Internet attacks: snooping, replay, forgery, interception, non-delivery
- Scalability
  - Devolved responsibility for validation
  - Minimum number of parties
- Deployability
  - Smooth link to current payment procedures
  - Exportable, importable
  - Avoid legally unproven Certification Authorities

Protocol features

- Strong authentication, non-repudiation without general-purpose public keys and certification authorities
- Trusted third party/parties: acquirer = F_C = F_M in common, simple case
- Authentication by round-trip exchange of quantities only knowable and useful to authenticated parties
- Crypto technology used:
  - modular exponentiation like Diffie-Hellman
  - ticket generation like Kerberos / KryptoKnight (IBM)

Hashed Password Payment Protocol



1 Cleartext payment order, with signature bound to as-yet-unrevealed nonce
2 as **1** plus merchant's authentication nonce
3 as **2** plus merchant's hashed password
4 *Core step: payment-ticket generation*
Create single-use payment tickets which only client & merchant can use; also creates signature-verification info for merchant and client
5 Merchant unpacks merchant ticket; passes client ticket + payment nonce
6 Client unpacks client ticket, authenticating merchant; releases signature-nonce from **1** to merchant
7 *(off-line)* Merchant verifies above signature, and now holds redeemable, non-repudiable payment order. *(Redemption batched, off-line.)*

Rollout

- $F_m = F_c$ when acquirer takes full risk
- F_m acts for F_c but with side transaction over existing secure channel to Fm to authorise payment (like iKP)
- F_c on-line for
  - debit payments
  - greater distribution of load
  - closer involvement
- Browser, server support in WWW handy, but existing callouts can be used
- Smartcards strongly preferred for user (client & merchant) key storage and computation

Commentary 1

- Passwords hashed at financiers, so servers much cheaper than Kerberos and insider attacks less feasible
- Secure hardware at financiers thwarts insider forgery of payment tickets
- Asymmetric keys (like RSA), but client & merchant keys used only for payment with audit trail & non-repudiation: allows financiers to act as specialised CAs, with resistance to insider attack making this legally defensible

Commentary 2

- Financier(s) provide(s) information to client and merchant to allow them to authenticate: doesn't do authentication itself on-line, only in case of off-line dispute resolution
- Final redeemable payment order not issued by client until all round trips done: hence robust to comms failure (real or claimed!)