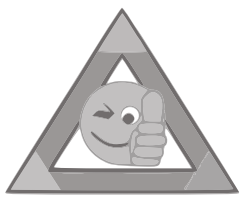
Extended HTTP Digest Access Authentication

Henning Klevjer, Kent Are Varmedal and Audun Jøsang
{hennikl, kentav, josang}@ifi.uio.no

Department of Informatics, University of Oslo



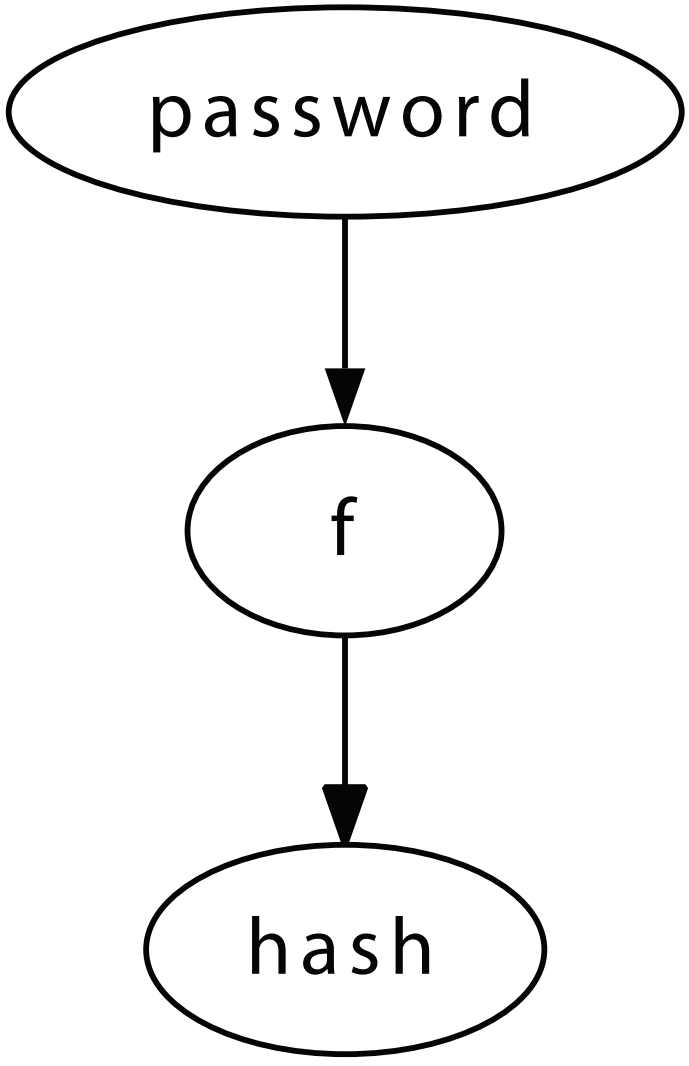
March 27, 2013

Agenda

- The status quo
- The problem of clear text entering of passwords
- Digest Authentication and its shortcomings
- What is Extended Digest Authentication?

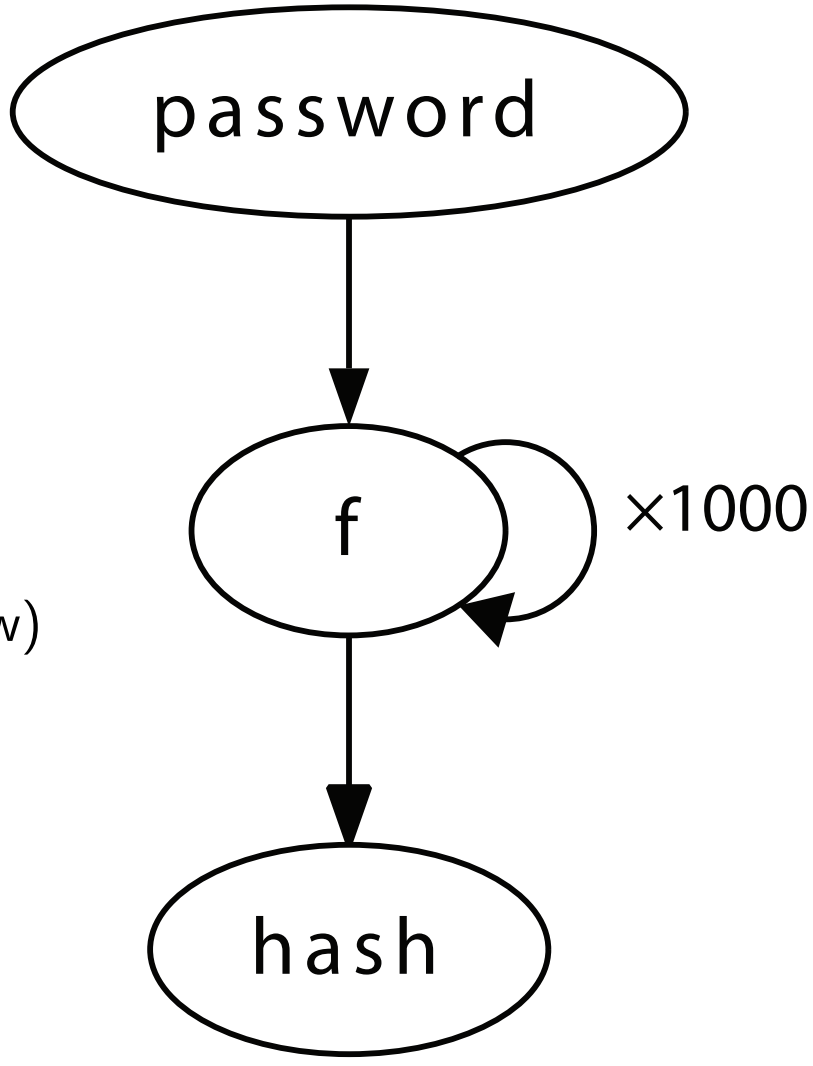
Status quo

- We have:
  - **Hash functions**
  - Key derivation functions (slow)
    - bcrypt and scrypt



Status quo

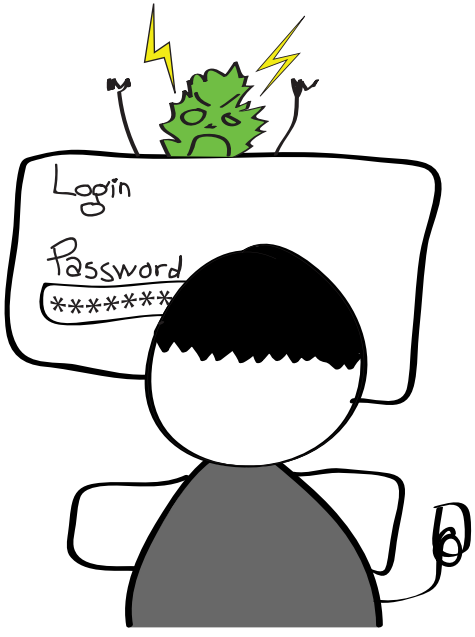
- We have:
  - Hash functions
  - **Key derivation functions** (slow)
    - bcrypt and scrypt

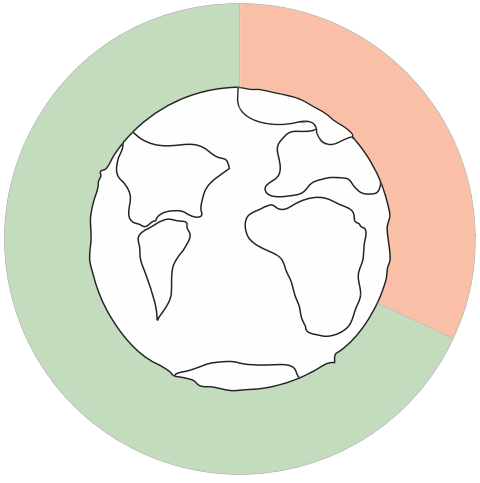


Sufficiently protected passwords are difficult to recover from server-side breaches.

However, on a compromised client, passwords are sitting ducks.

Status quo

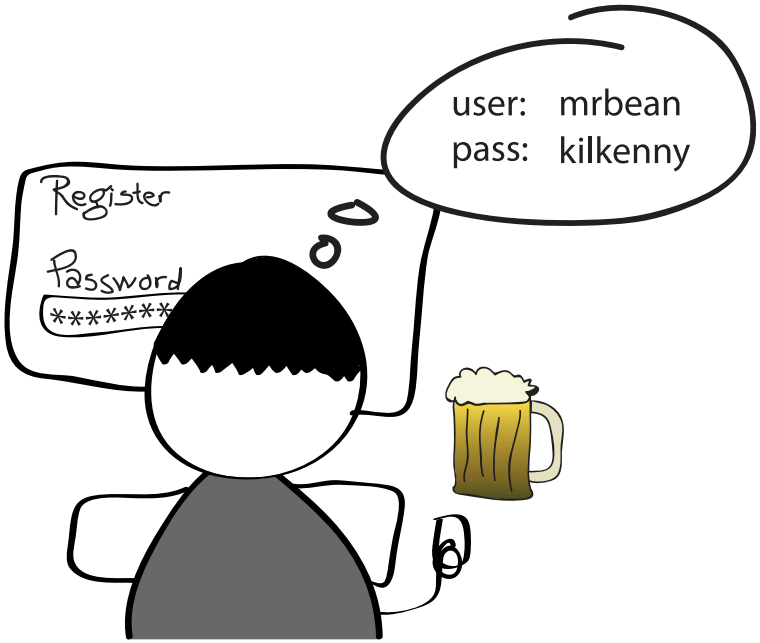


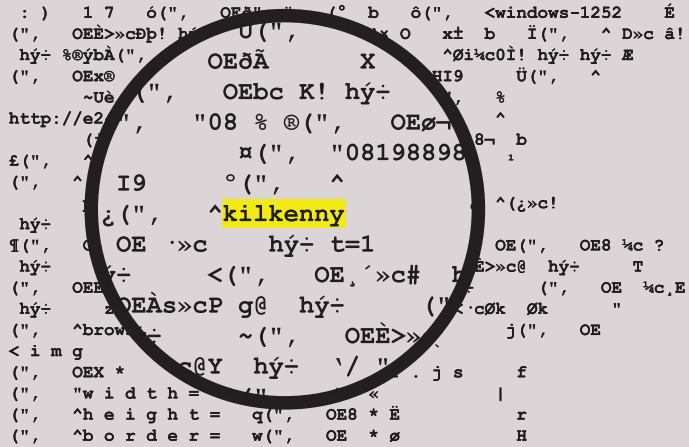


32 % of PC's are infected with malware

[PandaLabs 2012]

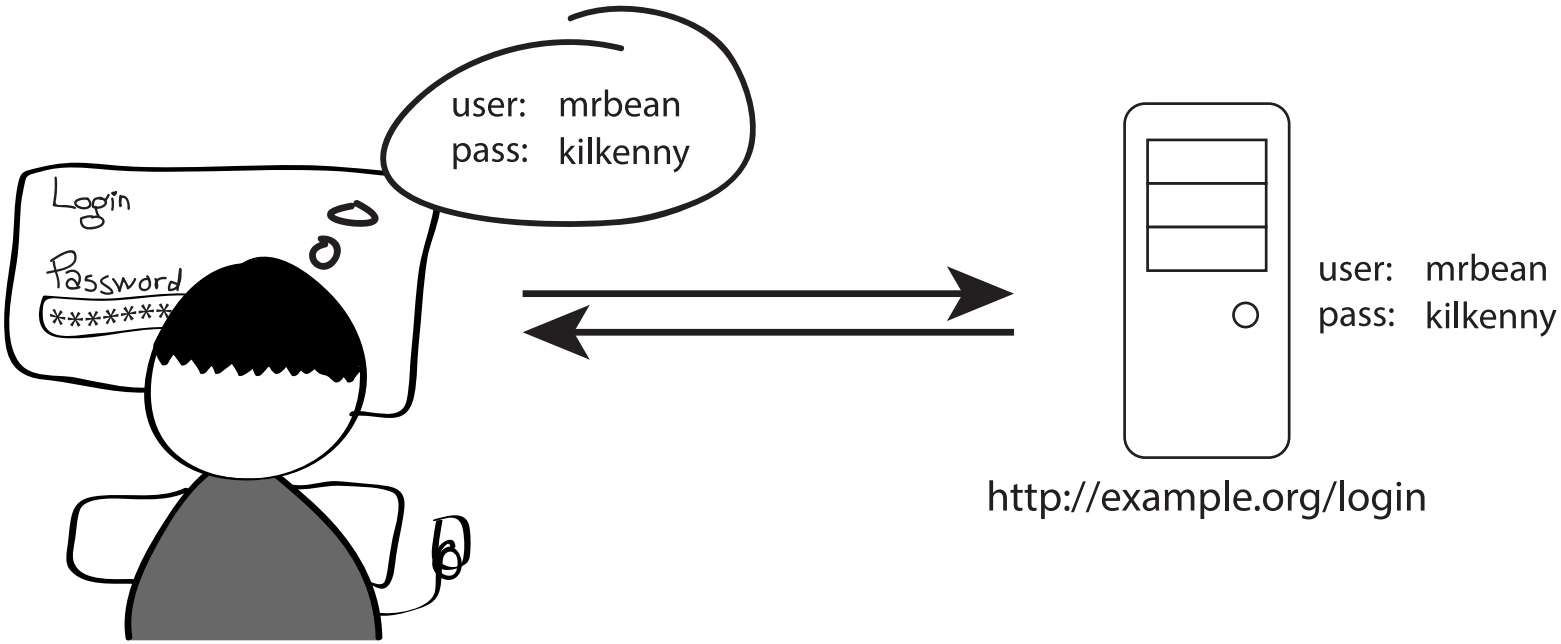
Creating a password



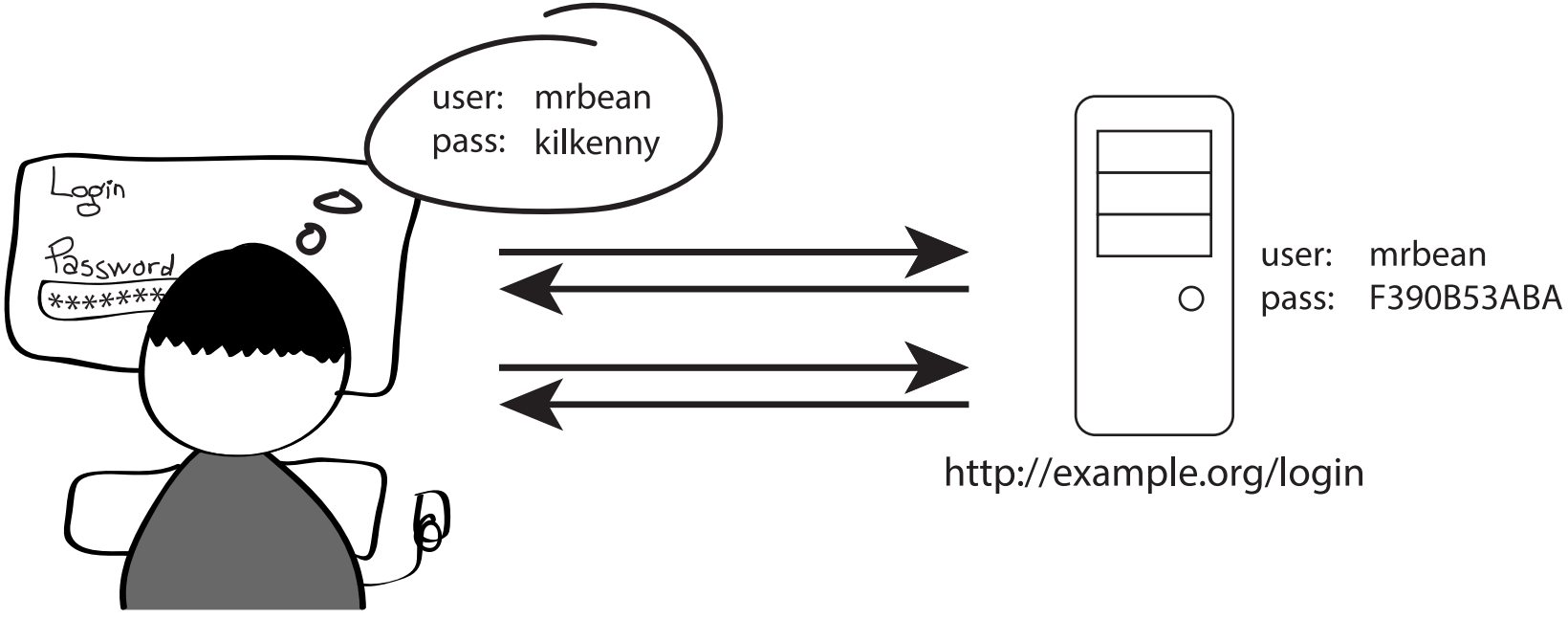


Password exposed in memory

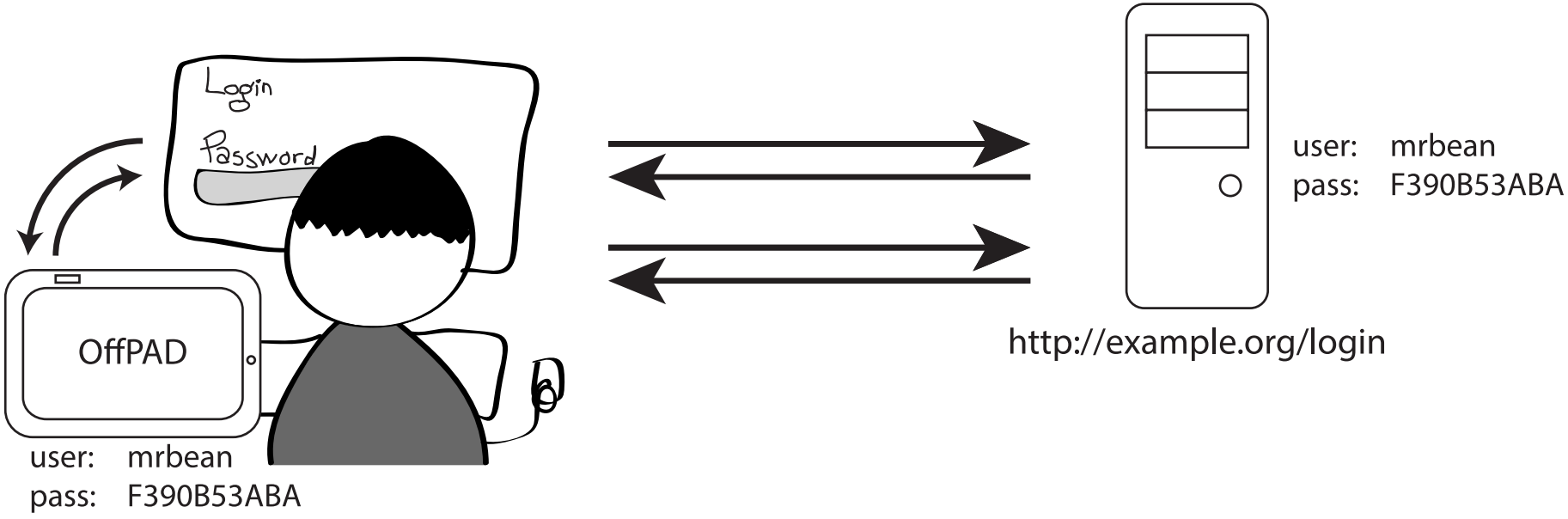
Clear text authentication



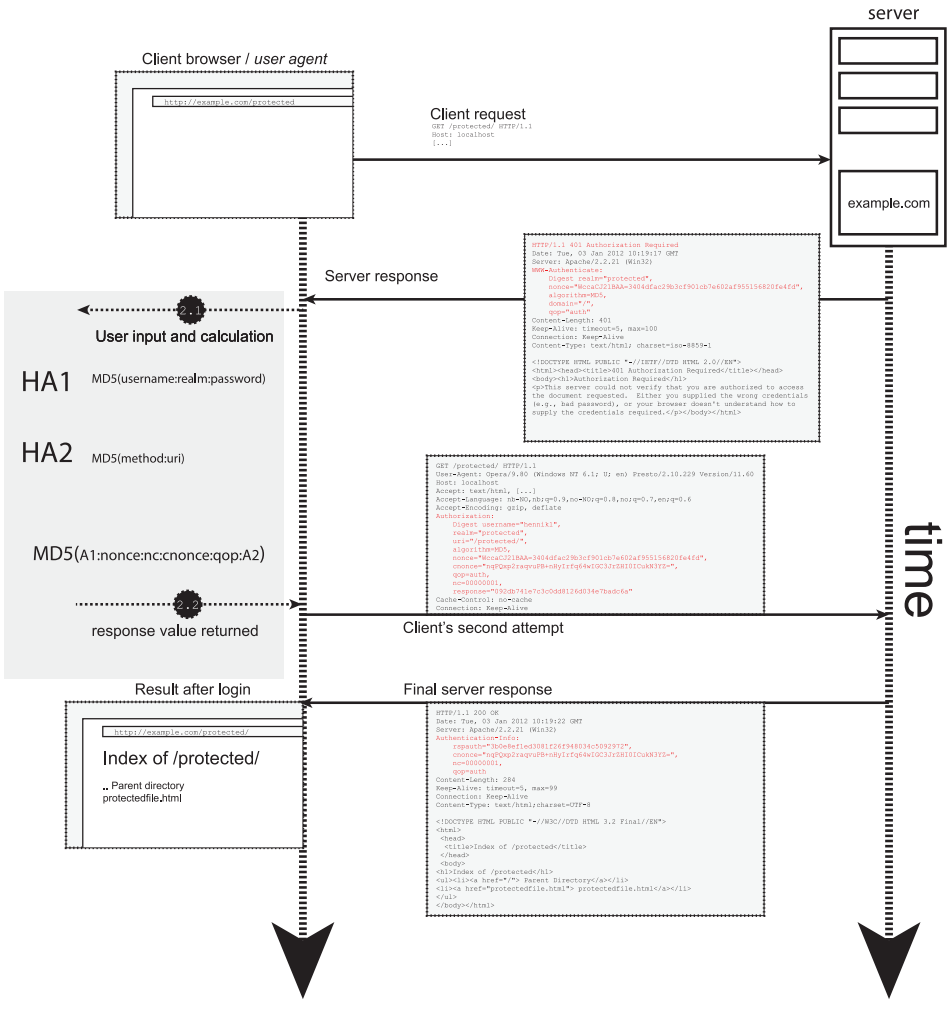
Challenge-response authentication



OffPAD authentication



HTTP Digest Access Authentication

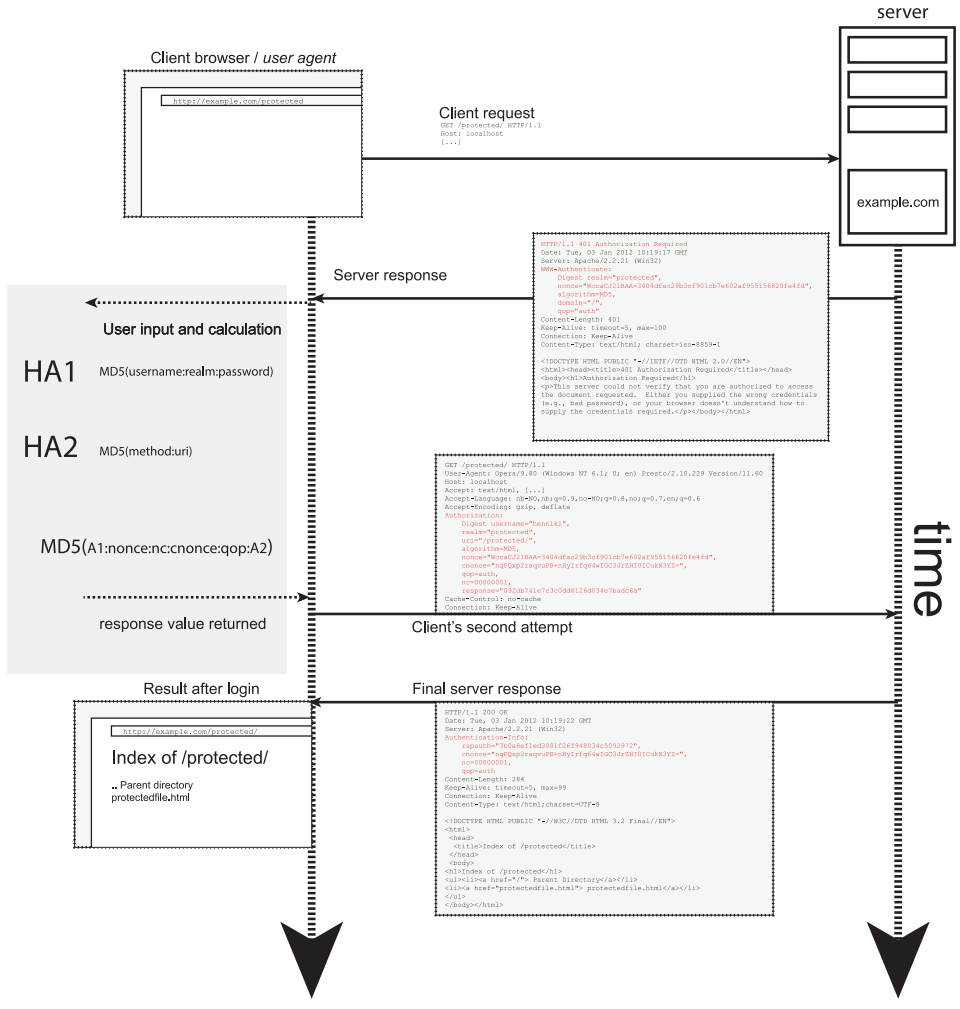


HTTP Digest Access Authentication

```
username:realm:MD5(username:realm:password)
```

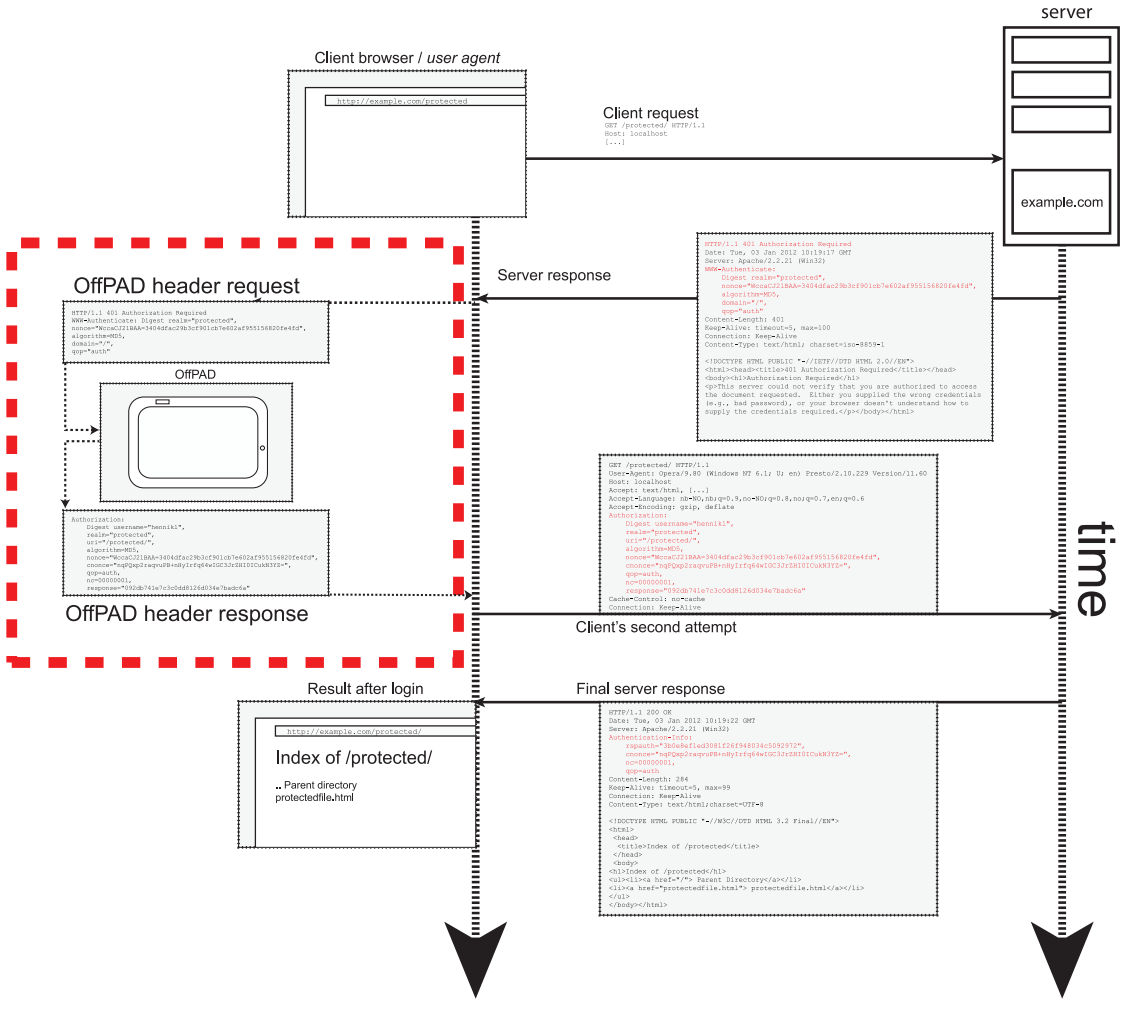
```
alan:accounting:c7565f0746b8d0e7ce76f278b9da068d
george:accounting:783303868cfdef45f66cc0d8566c7464
superman:hr:2d25f0afddc6d2f8baef94db1d64d904
bossman:adm:ada528cecf8f813abe57e30049700c31
```

Our proposal



Relocate the entering of credentials to a hardened device.

Our proposal



Relocate the entering of credentials to a hardened device.

Our proposal

- Our "mostly **Off**line" **P**ersonal **A**uthentication **D**evice is
  - Mostly offline through physical activation
  - A PAD storing unlimited credentials for several users
  - Potentially enabled for several authentication schemes

Our proposal

- Our Extended HTTP Digest Access Authentication scheme provides
  - Stronger confidentiality - for both process and transmission
  - Privacy - The clear text password is visible only to the OffPAD
  - Better usability - Forget your password, remember your device

User input and calculation

HA1 MD5(username:realm:password)

HA2 MD5(method:uri)

MD5(A1:nonce:nc:cnonce:qop:A2)

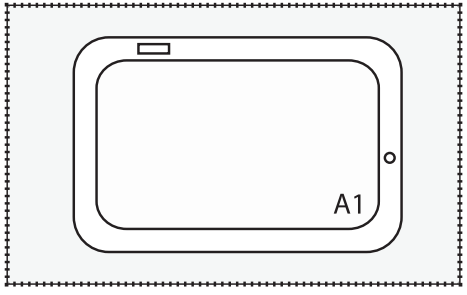
response value returned

Original HTTP Digest Access Authentication

OffPAD header request

```
HTTP/1.1 401 Authorization Required
WWW-Authenticate: Digest realm="protected",
nonce="WccaCJ21BAA=3404dfac29b3cf901cb7e602af955156820fe4fd",
algorithm=MD5,
domain="/",
qop="auth"
```

OffPAD

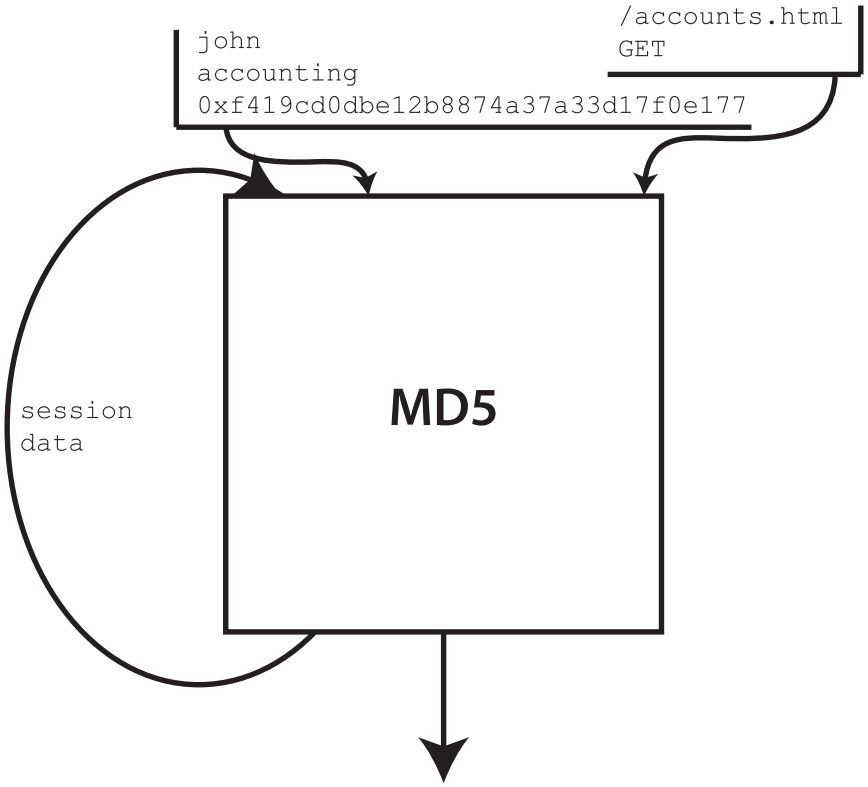



```
Authorization:
    Digest username="hennikl",
    realm="protected",
    uri="/protected/",
    algorithm=MD5,
    nonce="WccaCJ21BAA=3404dfac29b3cf901cb7e602af955156820fe4fd",
    cnonce="nqPQxp2raqvuPB+nHyIrfq64wIGC3JrZHI0ICukN3YZ=",
    qop=auth,
    nc=00000001,
    response="092db741e7c3c0dd8126d034e7badc6a"
```

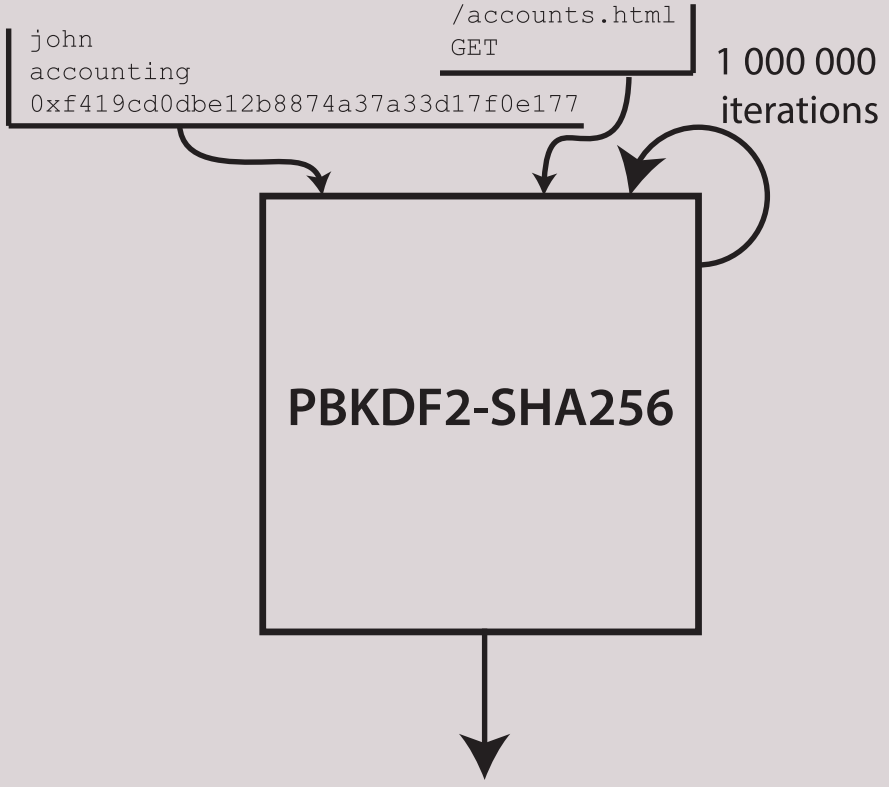
OffPAD header response

Automatic OffPAD authentication

Sticking with MD5



Trying out KDF



Secret = AES(`DERIVED_KEY`, salt) : salt

Benefits

- No requirement of user interaction
  - Dramatically reduces time penalty of login
- No need to remember passwords
  - Password can be a long random character sequence or a hash
- No need to store passwords
  - HTTP Digest authentication: credentials can be stored in hashed format
- Simple one-step setup
  - Identity creation can be done synchronously at both server and OffPAD

Drawbacks

- Deployment and learning curve
  - Credential synchronization between OffPAD and server.
- Security considerations
  - Must make sure the OffPAD is sufficiently protected.
  - The static credential value must be regarded as the new password.
- That bloody device
  - Someone must pay for it
  - Someone must teach you how to use it
- Digest authentication is vulnerable to MITM
  - Requires server authentication

Questions?

? Thank you.