Tryton Authentication

Who are you?

Before

Identification:

Unique login name

Authentication:

Password

Password

- single-factor (knowledge)
- hashed (sha1/bcrypt)
- salted

Hash method

User.hash_method()

default: bcrypt

Hash stored as

'$sha1$<hash>$salt'

'$bcrypt$<hash>'

Custom method

User.hash_<name>(password)

User.check_<name>(password, hash)


New

Customized Authentication

[session]
authentications = ldap,password

Try each method until one succeed

User._login_<auth>(login, parameters)

parameters: dictionary of
authentication factors

Require a factor

raise LoginException(name, msg, type)

type: password, char

Succeed:

return user ID

Use User._get_login(login)

Failed:

return False/None

Existing methods:

- password (1FA: knowledge)
- ldap (1FA: knowledge)
- sms (1FA: ownership)
- password_sms
  (2FA: knowledge + ownership)

LDAP

- uri: RFC2255
  ldap://localhost/dc=tryton,dc=org
- uid

SMS

- function: qualname to function
  func(text, to, from)
- from
- length
- ttl

Brute Force Attack

Each attempt counted per login name

Each login sleep for
2 ** count - 1 seconds
before answering