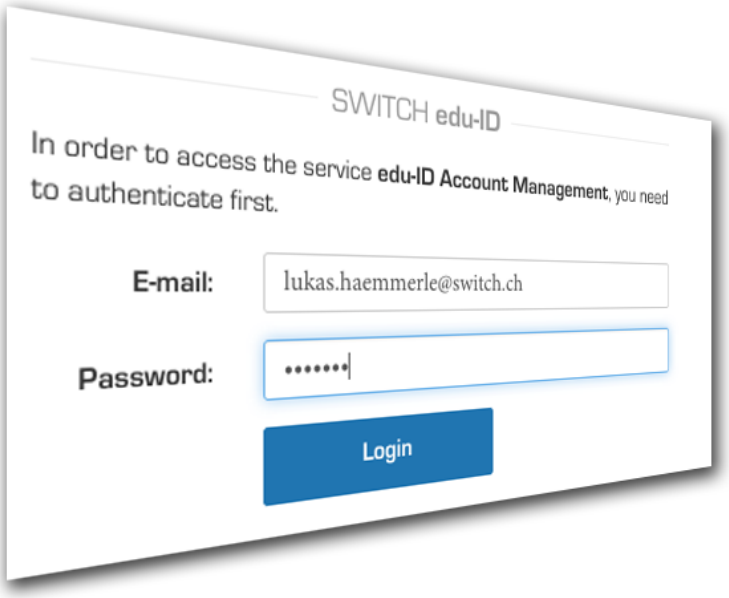
Secrets of the edu-ID Password



SWITCH

Lukas Hämmerle
lukas.haemmerle@switch.ch

Trust & Identity WG Meeting
14. March 2018, Bern

Setting a Good Password

- **System:** "Sorry, your password is too old and has expired – choose a new one."

  User types: `roses`
- **System:** "Sorry, too few characters."

  User types: `pretty roses`
- **System:** "Sorry, you must use at least one numerical character."

  User types: `1 pretty rose`
- **System:** "Sorry, you cannot use blank spaces."

  User types: `1prettyrose`
- **System:** "Sorry, you must use at least one upper case character."

  User types: `1FUCKINGprettyrose`
- **System:** "Sorry, you cannot use more than one upper case character consecutively."

  User types: `1FuckingPrettyRose`
- **System:** "Sorry, you must use no fewer than 20 total characters."

  User types: `1FuckingPrettyRoseShovedUpYourAssIfYouDon'tGiveMeAccessRightNow!`
- **System:** "Sorry, you cannot use punctuation."

  User types: `1FuckingPrettyRoseShovedUpYourAssIfYouDon'tGiveMeAccessRightNow`
- **System:** "Sorry, that password is already in use."

Modified version from: https://www.reddit.com/r/Jokes/comments/1v4bpa/passwords/

Design Goals (back in 2014)

- Pragmatic password selection process
  - No enforced renewal of passwords
  - Reasonable protection against brute-force cracking
  - Ease-of-use for user (e.g. no autocomplete="off")

- State of the art password hashing algorithm
  - When passwords hashes stolen, it should be hard to to crack them
  - Hashing algorithm widely accepted and standard
  - Pragmatic balance between security and compatibility

- **Today: >50'000 accounts and no user complaints since 2014 regarding difficulty to choose a password**

Coming Up

1. Password Hashing

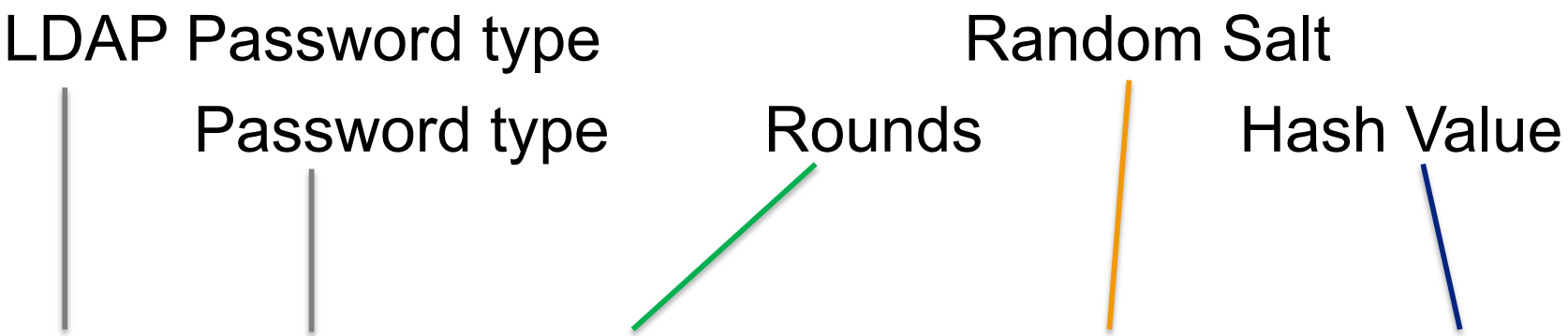
2. Choosing a Password

3. NIST Password Recommendations

Password Hashing

Passwords are stored as Salted SHA 512 with 5’000 rounds.

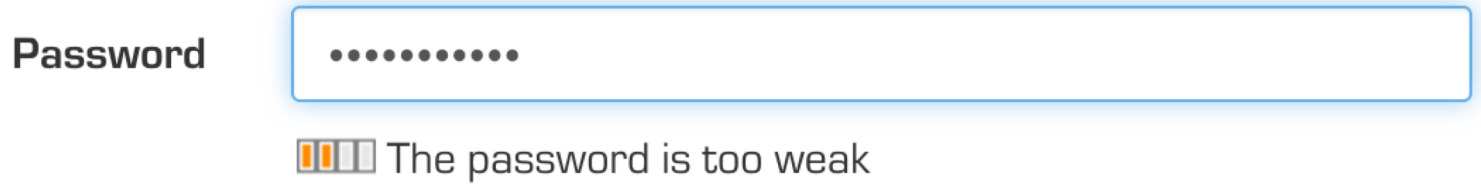
SHA-512(”None0fYourBusine55” + ”c004b603fecbb45b”)^{5000}



{CRYPT}6rounds=5000$c004b603fecbb45b$oO7tIG04nk
DlUTQ0BPTZSF.UpGjjAoh0ZnsmMuO4K4XMW6n48TfqHyH
E0YbhlmfBGbfDcYzO9a.34jHaC78ZF.

Choosing a Password

- Users choose their passwords, edu-ID provides guidelines



- Not all passwords are accepted. Depends on password score:
  - Length, Uppercase, Lowercase, Numbers, Symbols
  - Score must exceed a certain threshold

- Must not be in database with leaked passwords
  - **Since July 2016:** Local check (search as you type) against list of 10 million “most used“ password (only 41’000 of them exceed threshold)
  - **Since Feb. 2018**: When submitted, check against Troy Hunt’s 501M leaked password hashes (password/full hash are not sent to service)

Accepted and Rejected Passwords

424242424242 - ✓ **ok**

Thisisalongpassword - ✓ **ok**

this is also long - ✓ **ok**

This1$Shrt - ✓ **ok**

jesuis1pilote - **X not accepted**

Weihnachtsbaum - **X not accepted**

123456789qwertyuiop - **X not accepted**

Q1w2e3r4t5y6u7i8o9p0 - **X not accepted**

Most Used and Leaked passwords

NIST Password Recommendations

- NIST = National Institute of Standards and Technology
- NIST Special Publication 800-63B:
  Digital Identity Guidelines
  - https://pages.nist.gov/800-63-3/sp800-63b.html#memsecret
  - Released June 2017
  - Chapter about Memorized Secrets (”Passwords”)

Interesting Changes:

- Removed **periodic password change** requirements
- Dropped **password composition requirements**
- Introduced check of passwords against lists of **commonly used or compromised passwords**

NIST Password Rules: **SHALL**

- Minimum 8 characters long ✓ (min. 10 chars)
- No hint/reset questions stored ✓
- Compare password against list of commonly-used password ✓ (Leaked passwords won't be accepted)
- Rate limiting **X** (failed logins are monitored/alerted though)
- Encrypted/authenticated channel to check password ✓
- Salted Password hashes ✓
- Salt length min. 32 bit ✓ (128 bit)
- Approved random number generator **?** (unclear, but used openssl is considered cryptographically secure ✓)
- No truncation ✓

NIST Password Rules: **SHOULD**

- No character type composition rules (✓) (see previous slides)
- Password up to 64 characters ✓ (tested with 256 chars)
- All printing ASCII and space characters accepted ✓
- Warning when unicode characters are used **X** (not needed)
- Password-strength meter ✓
- Allow pasting password ✓
- A memory-hard hash function ✓ (Salted SHA-512)
- Hash iteration as large as verification server performance will allow, typically at least 10,000 iterations ✓/ **X** (“only” 5000)
- Additional hashing operation with secret stored in hardware module **X** (would break interoperability with SWITCHdrive/SWITCHengine, considerable effort needed)

Conclusion

- **We care about good passwords!**

- SHA-512 with 5’000 rounds probably still sufficient
  - Protection good enough unless NSA/FSB/MOSA/ want our passwords

- Most NIST recommendations are followed
  - Rate limiting is yet to be implemented
  - Hardware module for securing password hashes to be considered (is this in use at any university for storing password hashes?)

- Two-Factor authentication to be introduced late 2018
  - First: SMS One Time Password
  - Then: Time-based One Time Password