How to (not) Store Your Password

https://github.com/rlindsgaard/presentations/tree/master/2016-09-01-how-to-not-store-your-password

---

Ronni Elken Lindsgaard
rel@zx.dk
@rlindsgaard

2016-09-01

Analysis

Online password managers

Benefits:

- Portable
- Organisational sharing
- Not on your machine
- Strong passwords

Problems:

- Not on your machine [1]

Attack vectors:

- Keylogging
- Phishing
- Database compromise

[1] http://www.martinvigo.com/even-the-lastpass-will-be-stolen-deal-with-it/

Offline password managers

Benefits:

- Stored on your machine
- Encrypted password storage
- Strong passwords

Problems:

- One key to the kingdom
- Not portable
- It's still stored (CVE-2015-8378)

Attack vectors:

- Keylogging attacks
- Computer/storage compromise

Let's make things better

- Secure passwords.
- Configurable.
- Easy to use and manage.
- Shareable.
- No storage!

Methodology

Secure passwords

- High entropy (e.g. NIST[2])
- Passphrases: a sentence that is not too long to remember
- Schneier Scheme: ASSt's!2_2r [3]
- Troy Hunt: Should be too complex to remember! [4]

---

[2] http://wayback.archive.org/web/20040712152833/http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

[3] https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html, https://www.schneier.com/essays/archives/2008/11/passwords_are_not_br.html

[4] https://www.troyhunt.com/only-secure-password-is-one-you-cant/, http://robinmessage.com/2014/03/why-bruce-schneier-is-wrong-about-passwords/

Deterministic Pseudo Random Number

Example

```
% echo "naturalbornhacker" | md5sum -
04d1530d764932ccbff01c185a283c8e  -
```

Generating the password

```
hash = 04d1530d764932ccbff
alphabet = abcdABCD1234!"#_

password = aA"bBda"DCA2dc!!__
```

Domain specific passwords

```
function g(str password, str context) {
  echo hash(password + context)
}
g(naturalbornhacker, bornhack.dk)
// 1Fvcck'XE%j_cD%7oHV'AO_COrl"fK}}S,:'
g(naturalbornhacker, github.com)
// ;YR|_>(sJXgQK2S%KvSS"zH_43b6z_yN
```

Session key

- Hash function seed
- Synchronously encrypt configuration
- Mitigate shoulder surfing

Implementations

PwdHash

- https://pwdhash.com/
- Stanford Paper 2004 [5]
- Browser plugin
- Outdated security (DOM)
- No special characters

[5] https://crypto.stanford.edu/PwdHash/

RndPhrase

- `https://rndphrase.appspot.com/`
- `http://brinchj.blogspot.dk/2010/02/rndphrase.html`
- Johan Brinch 2009
- Small letters and numbers only
- Cubehash
- Browser plugin

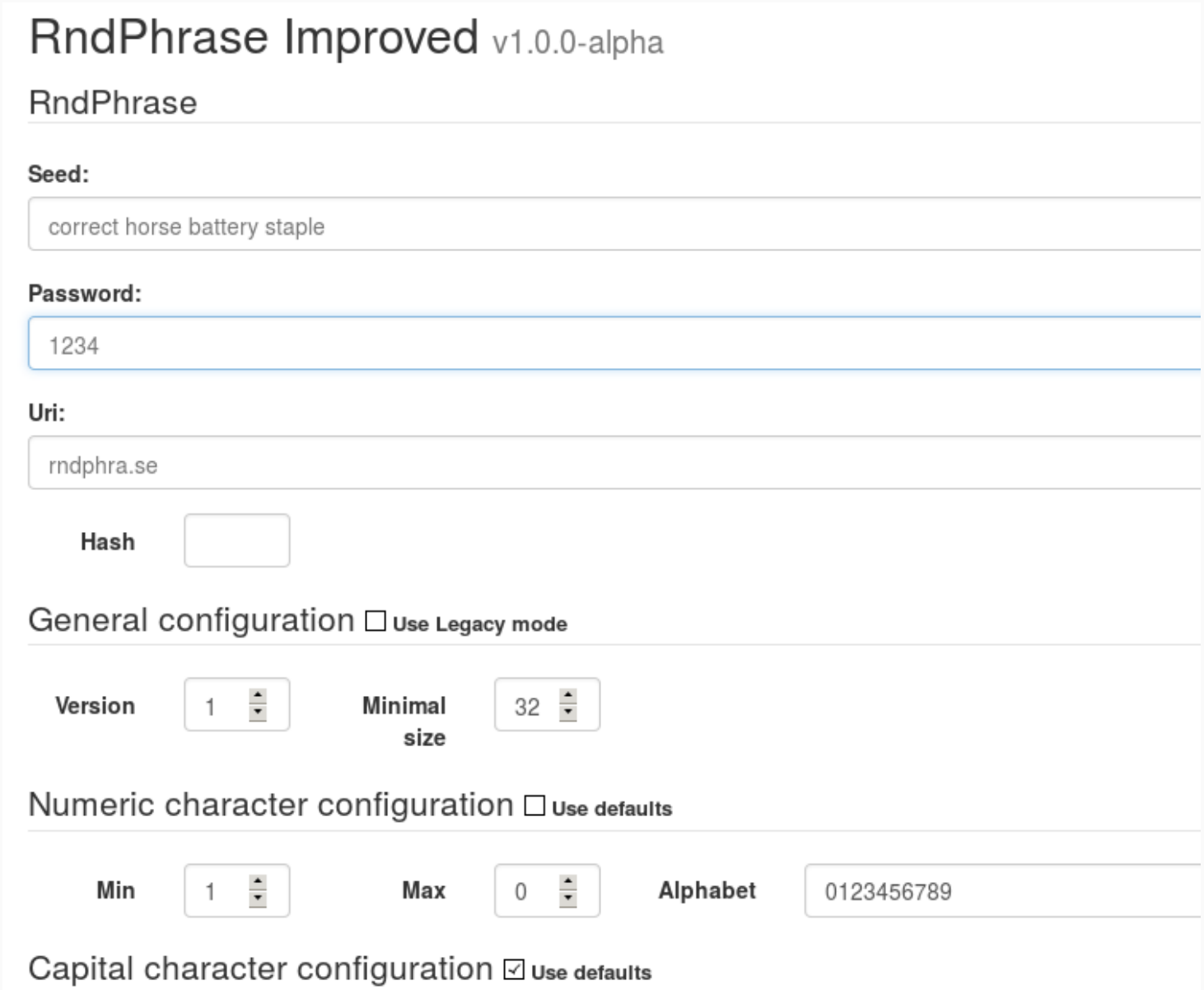
One Shall Pass

- `https://oneshallpass.com/`
- Maxwell Krohn
- Up to date
- Similar solution
- PBKDF2

Introducing RndPhrase Improved

- 1.0.0a1
- PBKDF2 for hashing (WebCrypto)
- Configurable alphabet
- Character occurence constraints
- Configurable size
- Re-use credentials (versions)

User interface example



Security Analysis

- Keylogging and other active attacks still a problem
- No necessary storage though

Summary

Let's make things better

- Secure passwords.
- Configurable.
- Easy to use and manage.
- Shareable.
- No storage!

Moar?

- https://rndphra.se
- https://github.com/RndPhrase
- http://rlindsgaard.github.io/2016/01/29/rndphrase-roadmap.html