How to (not) Store Your Passwords

https://github.com/rlindsgaard/presentations/tree/master/2017-03-18-how-to-not-store-your-passwords

Ronni Elken Lindsgaard
rel@zx.dk
@rlindsgaard

2017-03-18

- Analysis
- Methodology
  - Generating Secure Passwords
- Security discussion
  - Attack vectors
- Introducing RndPhrase Improved

Analysis

General Password Security

- Don't store in plain-text
- Don't re-use passwords
- Make secure passwords

Secure passwords

- High entropy (e.g. NIST[1])
- Passphrases: a sentence that is not too long to remember
- Schneier Scheme: ASSt's!2_2r [2]
- Troy Hunt: Should be too complex to remember! [3]

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

[2] 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

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

Online password managers

Strengths	**Weaknesses**	**Attack vectors**
Portability	Availability	Database compromise
Organisational sharing	One key to the kingdom	Meta-data leakage
Recoverable		3rd party
Strong passwords		Keylogging
Known secrets		

Offline password managers

Strengths	**Weaknesses**	**Attack vectors**
Trusted storage	Backup	Data-loss
Strong passwords	User interface	Computer/data compromise
No 3rd party		Keylogging
No meta-data		
Known secrets		

Bottom line

Data are susceptible to being either lost or stolen.

Let’s make things better

- Secure domain specific passwords
- Portable
- Configurable to website rules
- No storage needed!

Methodology

Deterministic Pseudo Random Number

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

Generating the password

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

password = a
```

Generating the password

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

password = aA
```

Generating the password

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

password = aA"
```

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("1234", "opensourcedays.org")
// puK5hbxzwjsEOs#pNO6sR&TcFn4<;x"q
g("1234", "github.com")
// &D8s1zM_rHAe$uuRysn>JO#Rv|oZ%j/d
```

Master key

- Salt
- Mitigate shoulder surfing
- Partial compromise on typing

Master Key use

```
function g(str salt, str password, str context) {
  echo hash(salt, password + context)
}
g("correct horse battery staple", "1234",
  "opensourcedays.org")
// L>nZQ]/Xb-Q$^i[cU1h@!4.mt+UGheV,
g("correct horse battery staple", "1234",
  "github.com")
// ‘mD*u,!.}u’Xklr _hNZCd5!SQ6clFGz
```

Security discussion

Attack vectors

- Keylogging
- Shoulder surfing
- Brute force

Bruteforcing

- PwdHash
- David Llewellyn-Jones and Graham Rymer
- Cracking PwdHash: A Bruteforce Attack on Client-side Password Hashing

Findings

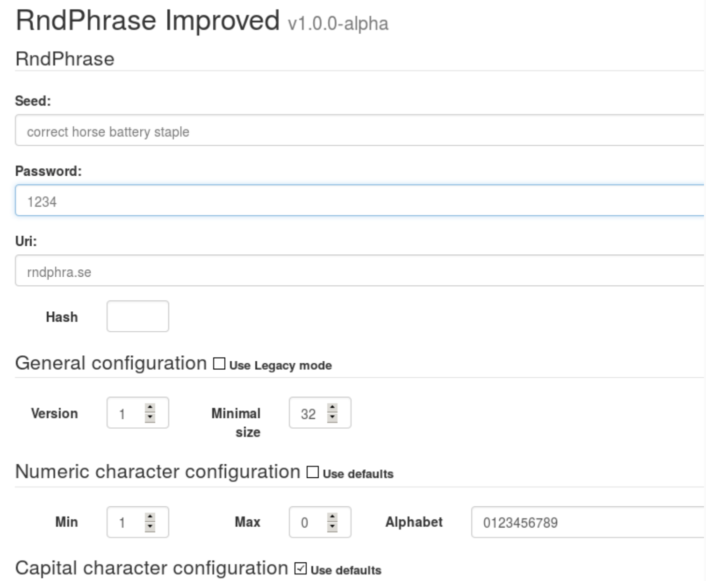
- TL;DR: Generated password entropy O(password)
- Master key (salt) + Group key
- Memory heavy hash function (PBKDF2)

Deterministic Manager Analysis

Strengths	**Weaknesses**	**Attack vectors**
Portable	Backups	Keylogging
No meta-data	Known secrets	Brute-force
No 3rd party		

Introducing RndPhrase Improved

User interface example



RndPhrase Improved v1.0.0-alpha

RndPhrase

Seed: correct horse battery staple

Password: 1234

Uri: rndphra.se

Hash:

General configuration □ Use Legacy mode

Version: 1

Minimal size: 32

Numeric character configuration □ Use defaults

Min: 1

Max: 0

Alphabet: 0123456789

Capital character configuration ☑ Use defaults

Introducing RndPhrase Improved

- 1.0.0-alpha2
- PBKDF2 for hashing (WebCrypto)
- Configurable alphabet
- Character occurence constraints
- Configurable size
- Re-use credentials (versions)

Roadmap

Beta

- At least 1 more peer review
- WebExtensions plugin

Stable

- Waiting for Candidate Recommendations: WebCrypto, Encoding

Would You Like To Learn More?

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

Bonus Slides

Another Piece to the Puzzle

Questions?