

Passwords in the Wild



Who am I...?



proud to be a vegan



My blog...

SkullSecurity.org

Random research, rants, etc.

Nmap dev news

Password database

I post updates to Twitter

<https://twitter.com/iagox86>



My job...

Tenable Network Security

Makers of the Nessus vulnerability scanner

I do research, reverse engineering

Giving talks

Plugins:

ms10-070 remote

ms10-075 remote

Padding oracle checks

ActiveSync audit (not yet released)



My other job...

Dash9Security.com

Vulnerability
assessment

Penetration testing

Training

Etc.

Local to Winnipeg. for
now



(C) Skull Security

And finally...

Developer for Nmap

Wrote smb-* scripts

Lots of http-*

Conficker detection

dhcp, ftp, etc etc.



Next projects...

IPv6?

Other ideas?

Outline

Overview of password cracking

John the ripper

Dictionaries

Password breaches

How people choose passwords

Cracking strategies



Password cracking

Hashing

One-way conversion of password → hash

Eg. md5, sha1, sha256, etc

md5:

Password: '123456'

md5: e10adc3949ba59abbe56e057f20f883e



Password cracking

Salting

Add something random to each password before cracking

Eg: the username

md5('123456') => md5('ron123456')

Prevents pre-computation attacks

Significantly slows down cracking:

Algorithm	c/s vs 1 hash	c/s vs 90.000 hashes
md5 (unsalted)	5.625.000	499.036.000.000
sha1 (unsalted)	2.613.000	107.168.000.000
sha1 (salted)	2.447.000	2.472.000
blowfish (x32)	753	754



Why crack passwords?

twitter

Login Join Twitter!

Just used Metasploit Pro to pass the hash. 1 shell becomes 89.

6:56 AM Nov 4th via Twiterrific
Retweeted by 2 people



n00bznet
n00bz.net



(C) Skull Security

Password cracking

Cracking a hash

Essentially, a bruteforce

Try every possible password for a hash, see what works

eg. hash = **e10adc3949ba59abbe56e057f20f883e**

md5('password') = 5f4dcc3b5aa765d61d8327deb882cf99

md5('qwerty') = d8578edf8458ce06fbc5bb76a58c5ca4

md5('123456') = **e10adc3949ba59abbe56e057f20f883e**

→ Found it!



Password cracking

Standard tool: john the ripper

- Free / opensource

- Created / maintained by Solar Designer (in Russia)

- Fast. customizable, etc

- Supports about 50 hash types

 - Lanman

 - NTLM

 - MD5 with all kinds of salting

 - SHA1 with all kinds of salting

 - Linux. Unix. BSD password files

 - SQL Server. Oracle



John the Ripper

--wordlist

Use your own base list

Default list is ~3100 entries

--rules

Used for mangling

Each password becomes ~50

Easily extensible in john's config

--stdin

Write you own mangler. etc

Not compatible with --rules

--stdout

Output the candidates instead of checking

password

Password

passwords

password1

Password1

drowssap

1password

PASSWORD

password2

password!

password3

password7

password9

password5

password4

password8

password6

password0

password.

password?

psswrđ

drowssaP

Drowssap

password

Dictionaries

Use your own --wordlist

Easiest/fastest way to crack passwords

Can be general or specific to the breach

List of general dictionaries:

<http://skullsecurity.org/wiki/index.php/Passwords>



Dictionaries

Examples of general dictionaries

English words

German words

Cities

Names

IMDB

Facebook



Quick aside – story!

29 July 2010 Last updated at 07:40 ET

Facebook data harvester speaks out

By Daniel Emery

Technology reporter, BBC News

Facebook directory - personal details for 100 million users

Type: [Other > Other](#)
Files: [11](#)
Size: 2.79 GiB (2991052604 Bytes)
Tag(s): [facebook](#) [directory](#) [100 million details](#) [personal security](#) [skull](#) [access](#) [bowes](#)
Quality: +0 / -0 (0)
Uploaded: 2010-07-28 16:58:11 GMT
By: [phatwarez](#) 
Seeders: 255
Leechers: 679
Comments: 3



Download

Enjoy Movies, TV Shows, Music and Games on your browser!

 [DOWNLOAD THIS TORRENT](#)  [MAGNET LINK](#)  [PIRATE CHAT](#)

The torrent is attracting hundreds of downloads

The man who harvested and published the personal details of 100m Facebook users has spoken out about his motives.

Dictionaries

General dictionaries (continued)

- Words from the holy bible

- Words from various wikis

 - Star Trek

 - The Muppets (yes, the muppets)

 - Wikis on Wikia (including Wikipedia) can be downloaded in .XML format



Dictionaries

General dictionaries (continued)

Other breaches

Nmap, john the ripper, Hydra, Cain&Abel, etc

All have built-in dictionaries based on common passwords

Among the most efficient for their size

Available on my wiki

<http://skullsecurity.org/wiki/index.php/Passwords>



Dictionaries

Site-specific dictionaries

Let's say a Star Trek fansite was breached
(okay. any geek site)

First thing to try is Star Trek passwords

The site itself

wget -r

The site's database

carders.cc, phpbb

I don't distribute these, generally



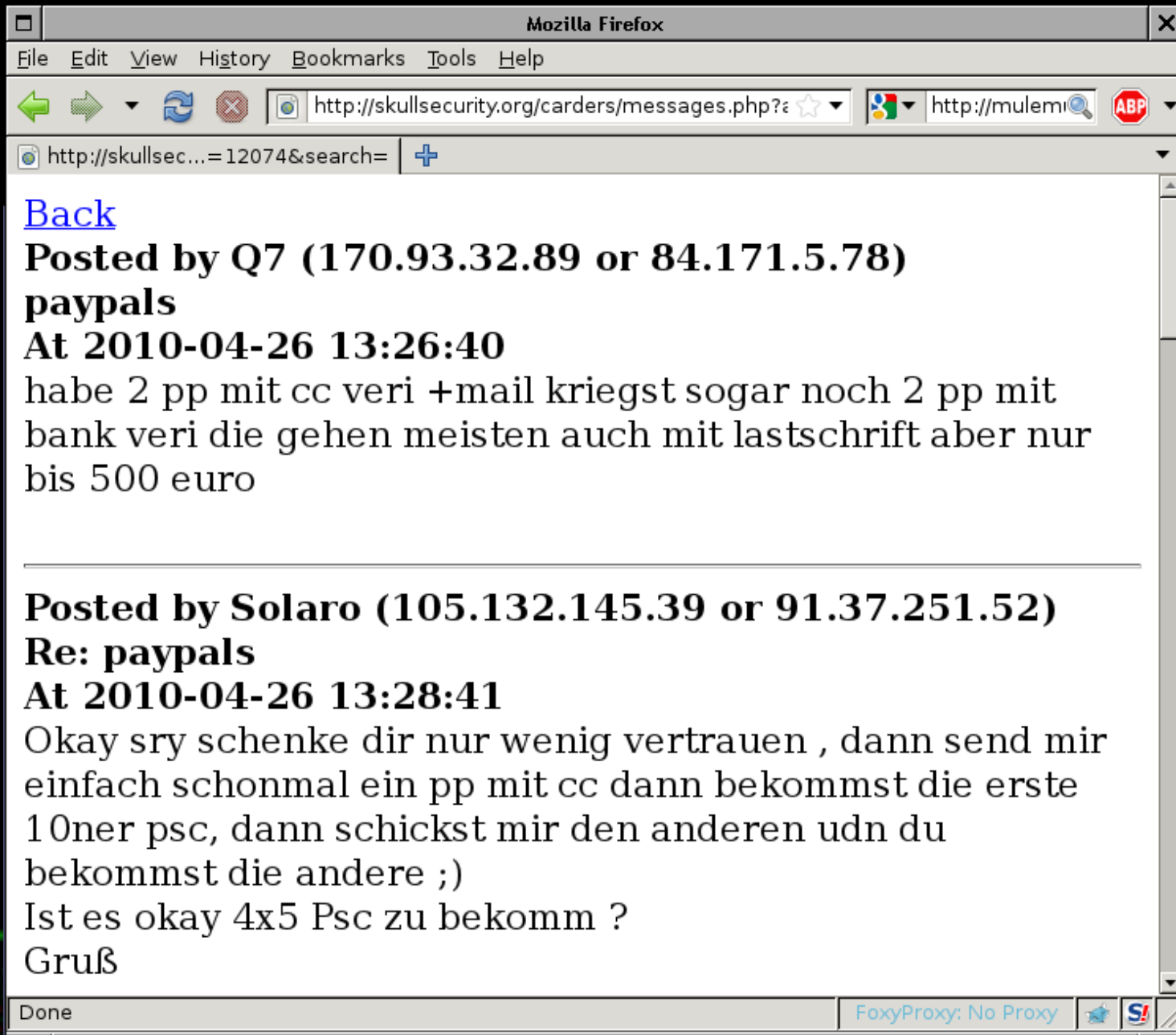
Dictionaries

Simplest command to build dictionary

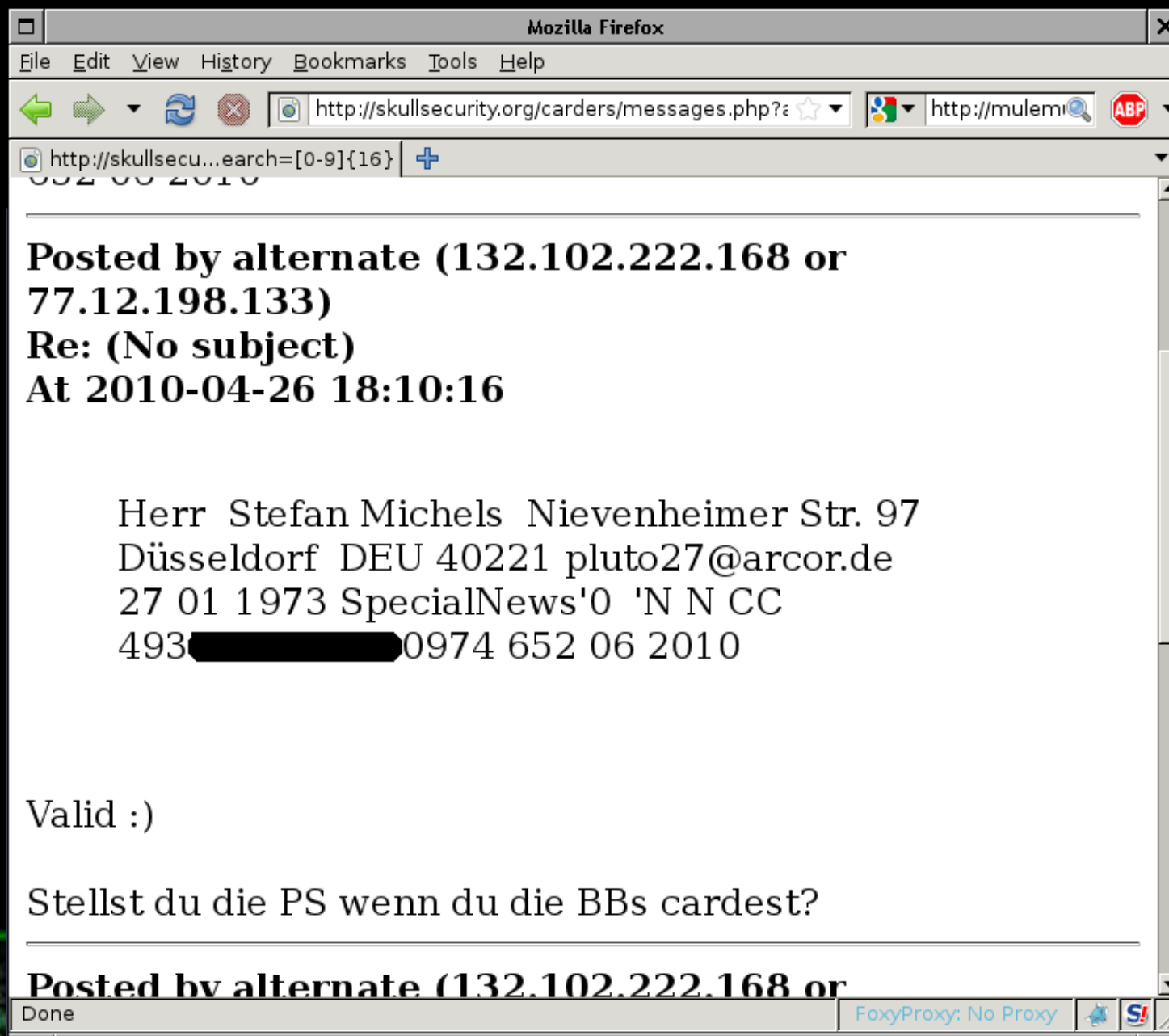
```
cat input.txt |  
  tr 'A-Z' 'a-z' |  
  sed -r "s/[^a-zA-Z0-9%_+-]/ /g" |  
  tr ' ' '\n' |  
  egrep -v '$^' |  
  sort -S2048M |  
  uniq -c |  
  sort -S2048M -n -r >  
  output-withcount.txt
```

```
cat output-withcount.txt |  
  cut -b9- >  
  output.txt
```

Aside: Carders.cc



Aside: Carders.cc



Breaches

Will cover 10 different breached sites

Normal sites: myspace, phpbb, rockyou

Finnish sites: älypää, finnish-unknown

Religious sites: faithwriters, singles.org

Adult sites: tuscl, porn-unknown

Hacking sites: carders.cc

The incident, statistics, other details

All breaches can be found on my wiki

<http://skullsecurity.org/wiki/index.php/Passwords>



MySpace

	Unique	Total
myspace	37.144	41.545
phpbb	184.389	255.421
rockyou	14.344.391	32.603.387
älypää	1.384	9.135
Finnish-unknown	36.323	50.795
faithwriters	8.348	9.755
singles.org	12.234	16.250
tuscl	38.820	50.028
Porn-unknown	8.089	10.000
carders.cc	1.904	5.062



MySpace

Exposed by a phishing attack

Poor quality

- Targeted “phishable” users

- Some users knew they were being phished

One of the first major breaches – 2006

- Target of significant research



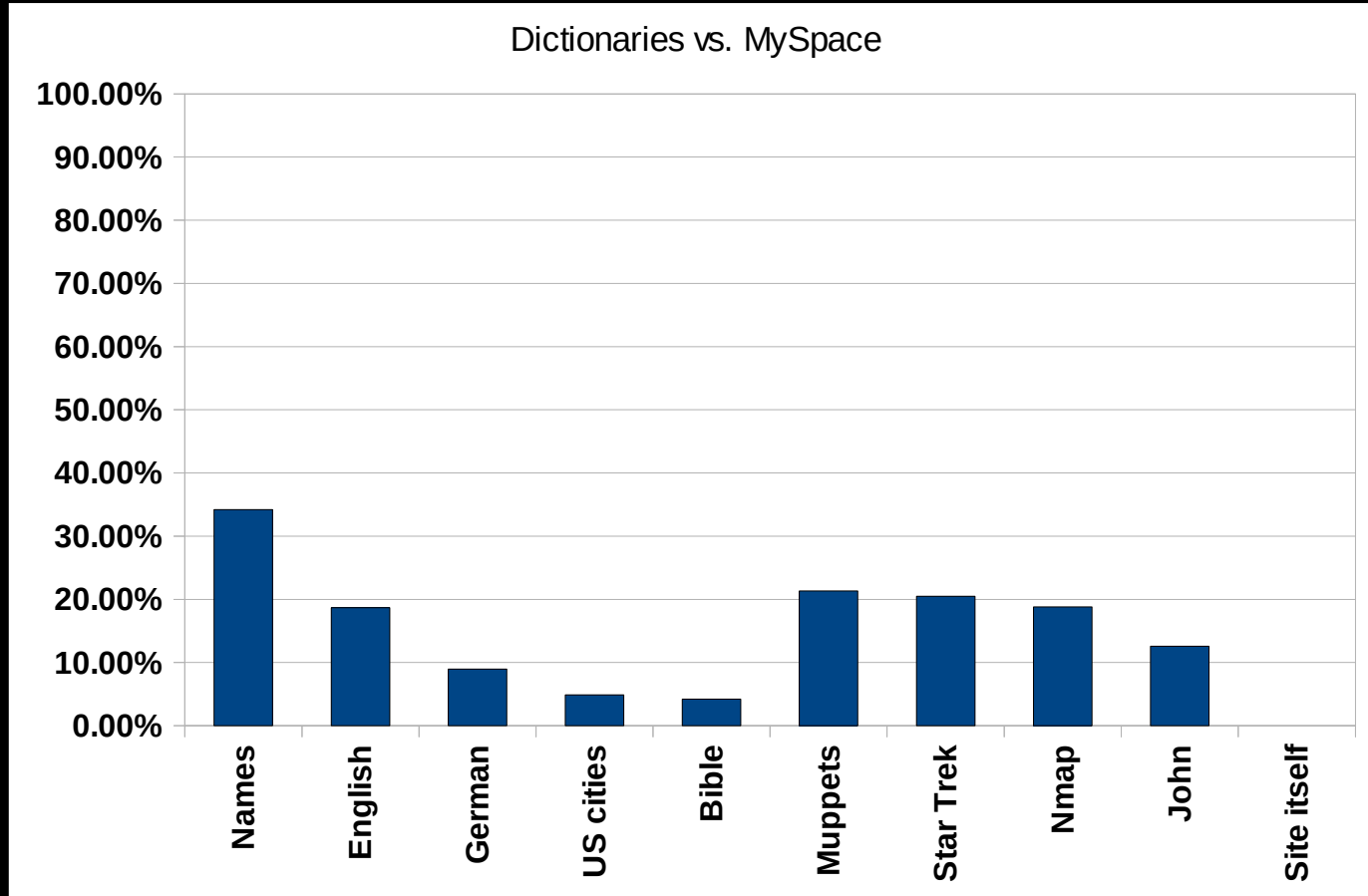
MySpace

Top-10 passwords:

<i>Password</i>	<i>Count</i>
password1	75
abc123	56
fuckyou	34
monkey1	29
iloveyou1	28
myspace1	24
fuckyou1	24
number1	18
football1	18
nicole1	17



MySpace



PHPBB

	Unique	Total
myspace	37.144	41.545
phpbb	184.389	255.421
rockyou	14.344.391	32.603.387
älypää	1.384	9.135
Finnish-unknown	36.323	50.795
faithwriters	8.348	9.755
singles.org	12.234	16.250
tuscl	38.820	50.028
Porn-unknown	8.089	10.000
carders.cc	1.904	5.062



PHPBB

Exposed by SQL Injection

Biggest breach at the time – January/09

Second biggest (public) breach of all time

Passwords were MD5 hashed

Currently. 184.389 out of 189.667 are cracked

That's **97,2%**

(And that's why plain hashing *sucks*)



(C) Skull Security

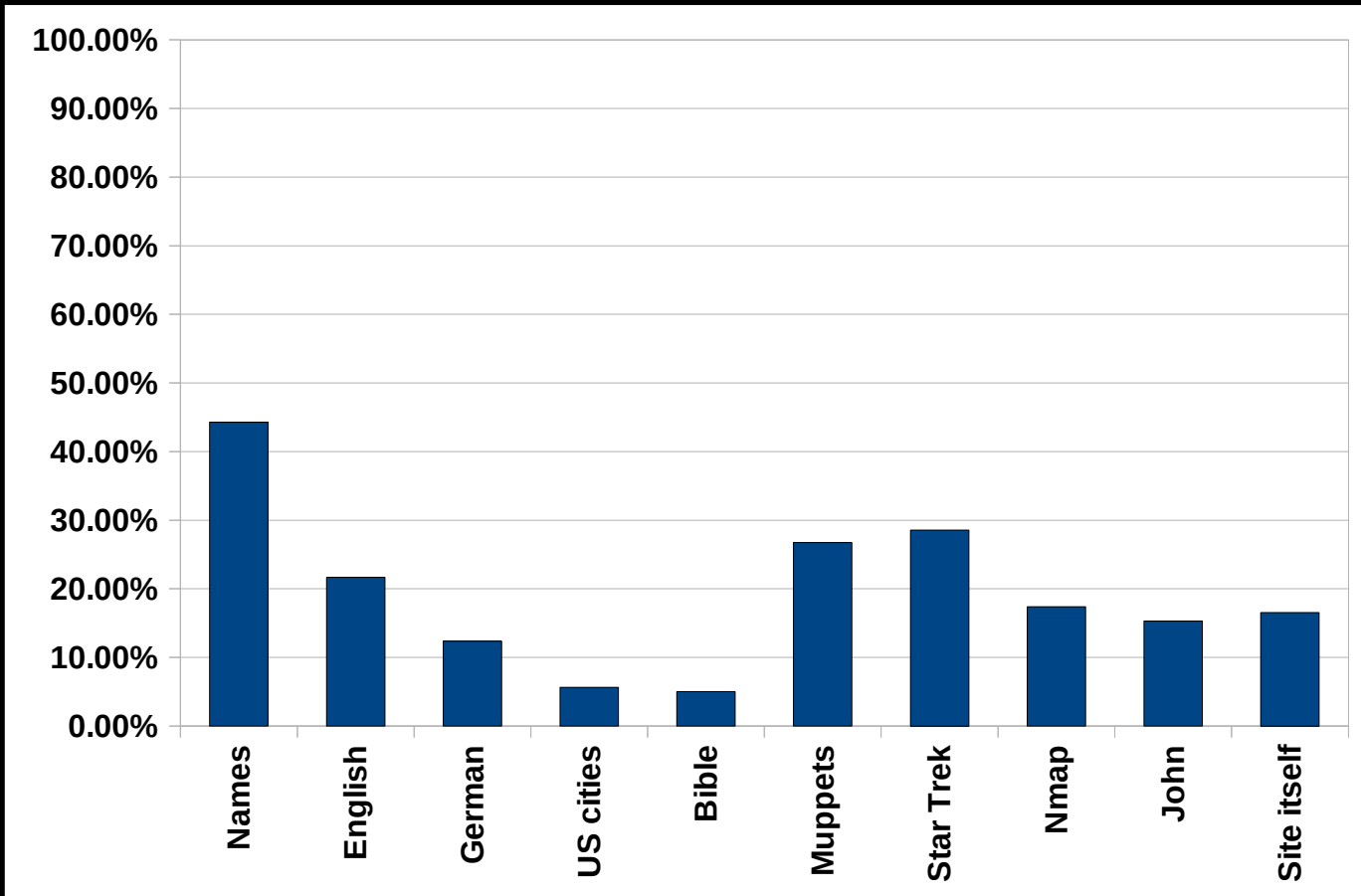
PHPBB

Top-10 passwords

Password	Count
123456	2.650
password	1.244
phpbb	708
qwerty	562
12345	418
12345678	371
letmein	343
111111	313
1234	273
123456789	253



PHPBB



Rockyou

	Unique	Total
myspace	37.144	41.545
phpbb	184.389	255.421
rockyou	14.344.391	32.603.387
älypää	1.384	9.135
Finnish-unknown	36.323	50.795
faithwriters	8.348	9.755
singles.org	12.234	16.250
tuscl	38.820	50.028
Porn-unknown	8.089	10.000
carders.cc	1.904	5.062



Rockyou

Exposed by SQL injection

Largest breach of all time, by far

Passwords were plaintext

Best sample ever released

Statistics are exceptionally useful



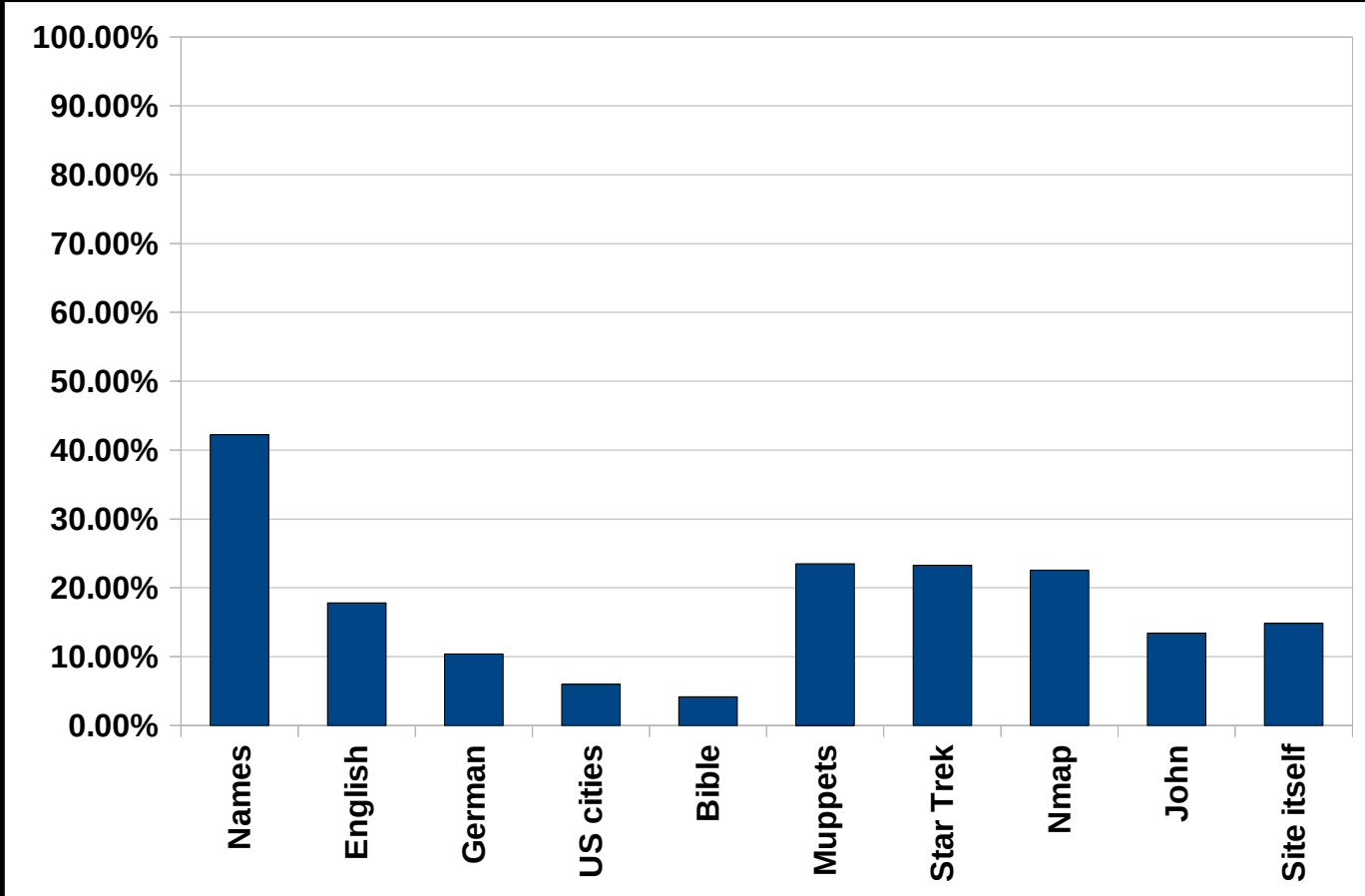
Rockyou

Top-10 passwords

Password	Count
123456	290.729
12345	79.076
123456789	76.789
password	59.462
iloveyou	49.952
princess	33.291
1234567	21.725
rockyou	20.901
12345678	20.553
abc123	16.648



Rockyou



Älypää

	Unique	Total
myspace	37.144	41.545
phpbb	184.389	255.421
rockyou	14.344.391	32.603.387
älypää	1.384	9.135
Finnish-unknown	36.323	50.795
faithwriters	8.348	9.755
singles.org	12.234	16.250
tuscl	38.820	50.028
Porn-unknown	8.089	10.000
carders.cc	1.904	5.062



Älypää

“Smart Aleck”

One of the better non-English breaches

Not clear how the breach happened

Likely SQL injection again

Passwords were plaintext

One of the smaller breaches, but useful

älypää!



Älypää

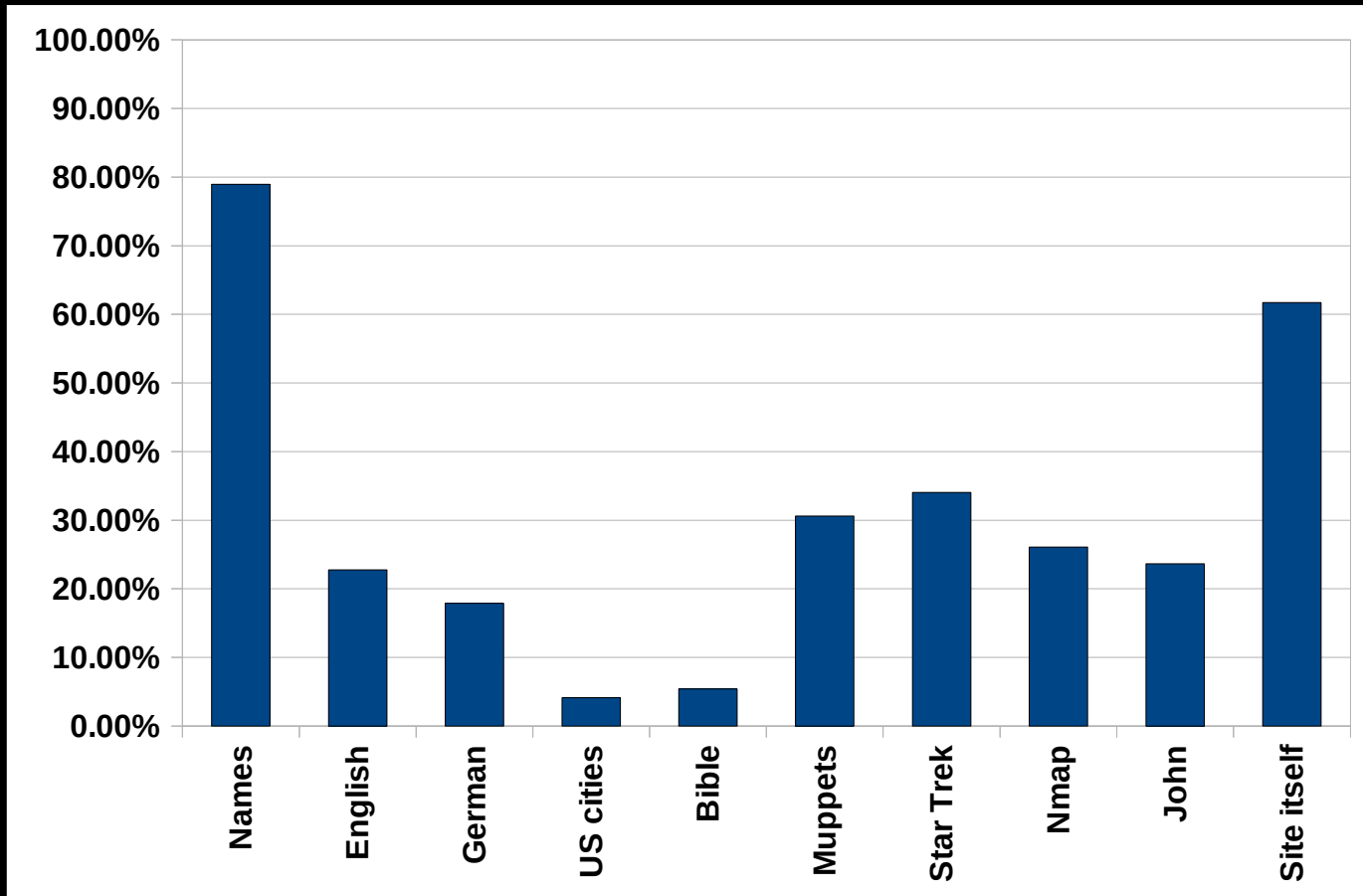
Top-10 passwords

Password	Count	
salasana	210	(password)
123456	176	
perkele	119	(devil)
12345	86	
qwerty	74	
514007	65	
kakka	63	(poo)
moikka	50	(bye)
paska	47	(crap)
koira	46	(dog)

Google translations.
Use your
imagination about
what they might
actually mean



Älypää



Finnish-Unknown

	Unique	Total
myspace	37.144	41.545
phpbb	184.389	255.421
rockyou	14.344.391	32.603.387
älypää	1.384	9.135
Finnish-unknown	36.323	50.795
faithwriters	8.348	9.755
singles.org	12.234	16.250
tuscl	38.820	50.028
Porn-unknown	8.089	10.000
carders.cc	1.904	5.062



Finnish-Unknown

Found by accident

Passwords were stored in four ways:

- Plaintext

- md5

- sha1

- Salted sha1

Cracked ~75% of unsalted, ~50% of salted

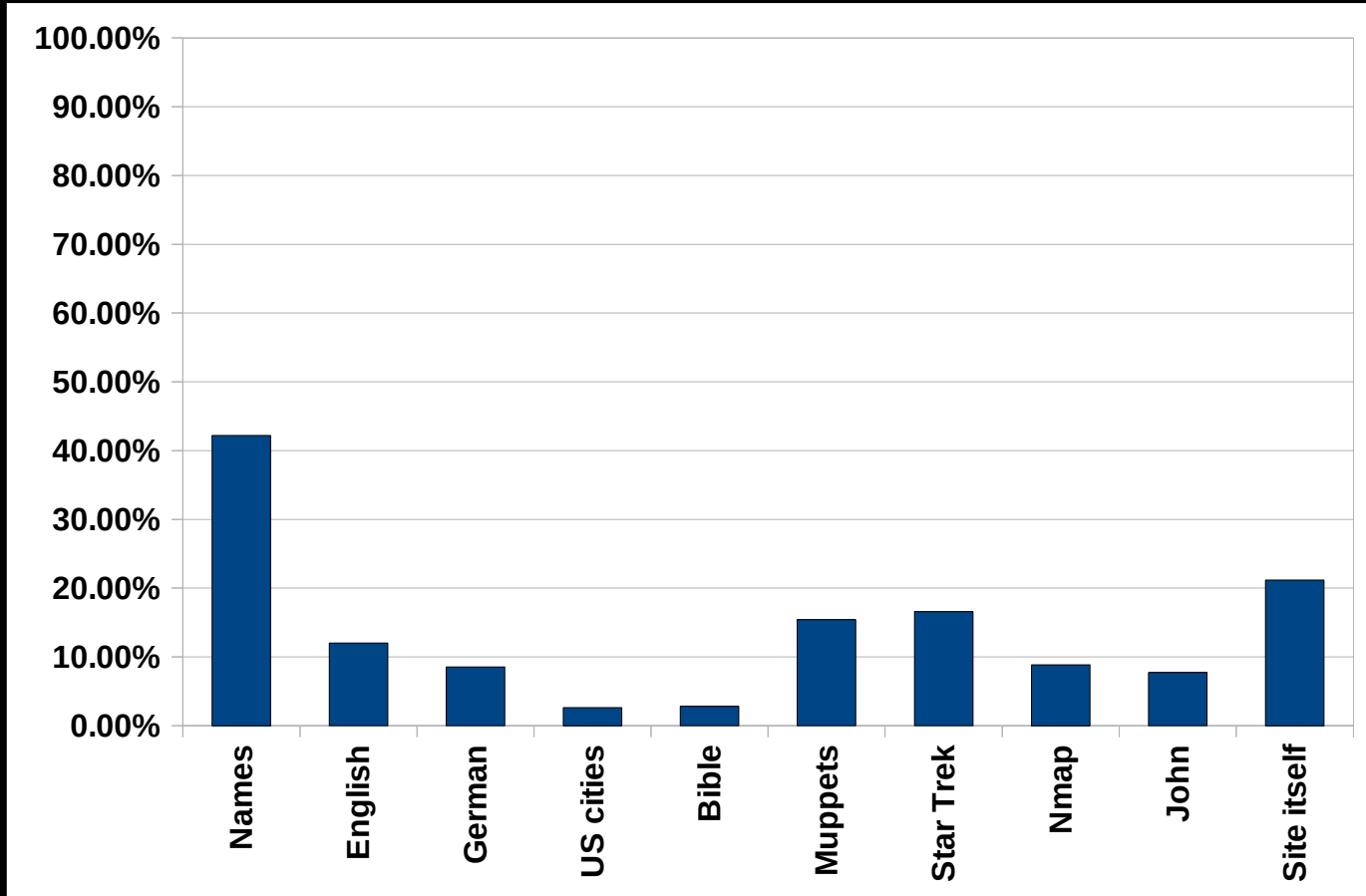


Finnish-Unknown

Password	Count	
salasana	216	(password)
123456	192	
perkele	119	(devil)
12345	87	
qwerty	78	
VQsaBLPzLa	75	(spammer)
514007	67	
kakka	66	(poo)
moikka	52	(bye)
paska	49	(crap)



Finnish-Unknown



Faithwriters

	Unique	Total
myspace	37.144	41.545
phpbb	184.389	255.421
rockyou	14.344.391	32.603.387
älypää	1.384	9.135
Finnish-unknown	36.323	50.795
faithwriters	8.348	9.755
singles.org	12.234	16.250
tuscl	38.820	50.028
Porn-unknown	8.089	10.000
carders.cc	1.904	5.062



Faithwriters

Religious book site

Allegedly breached by access problems

(ie. changing user.php?id=3 to ?id=4)

Admins deny the compromise happened. no information

Passwords were plaintext

The logo for FaithWriters features a blue pen icon above the text. The word "Faith" is in blue, and "Writers" is in black, followed by a registered trademark symbol (®).

FaithWriters®

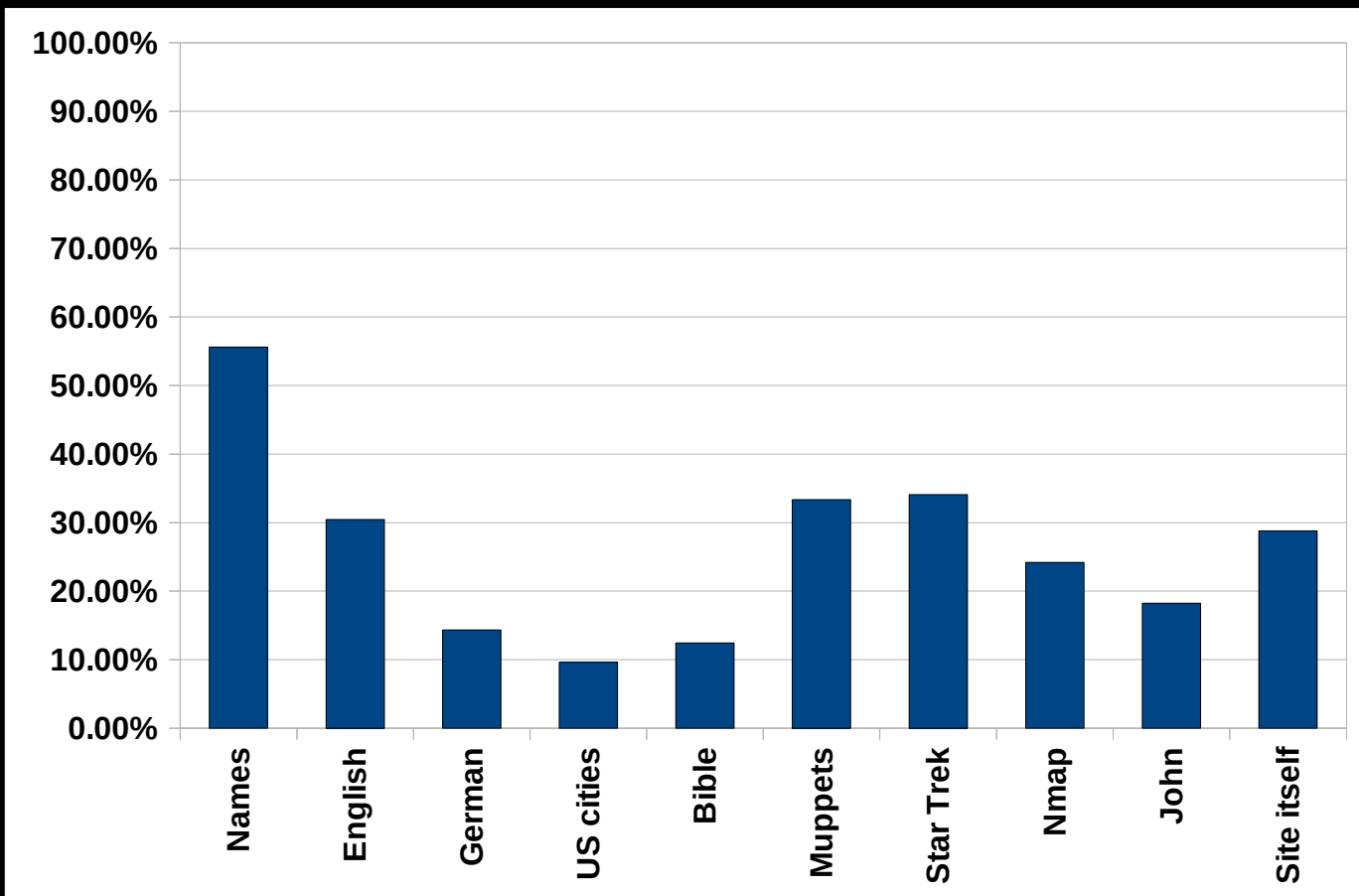
Faithwriters

Top-10 password

Password	Count
123456	53
	46
writer	25
jesus1	22
christ	18
blessed	18
john316	17
jesuschrist	16
password	15
heaven	15



Faithwriters



Singles.org

	Unique	Total
myspace	37.144	41.545
phpbb	184.389	255.421
rockyou	14.344.391	32.603.387
älypää	1.384	9.135
Finnish-unknown	36.323	50.795
faithwriters	8.348	9.755
singles.org	12.234	16.250
tuscl	38.820	50.028
Porn-unknown	8.089	10.000
carders.cc	1.904	5.062



Singles.org

Religious dating site

Compromised by access problems

If you knew 6-digit account number, you could access profile

Passwords were displayed on profile



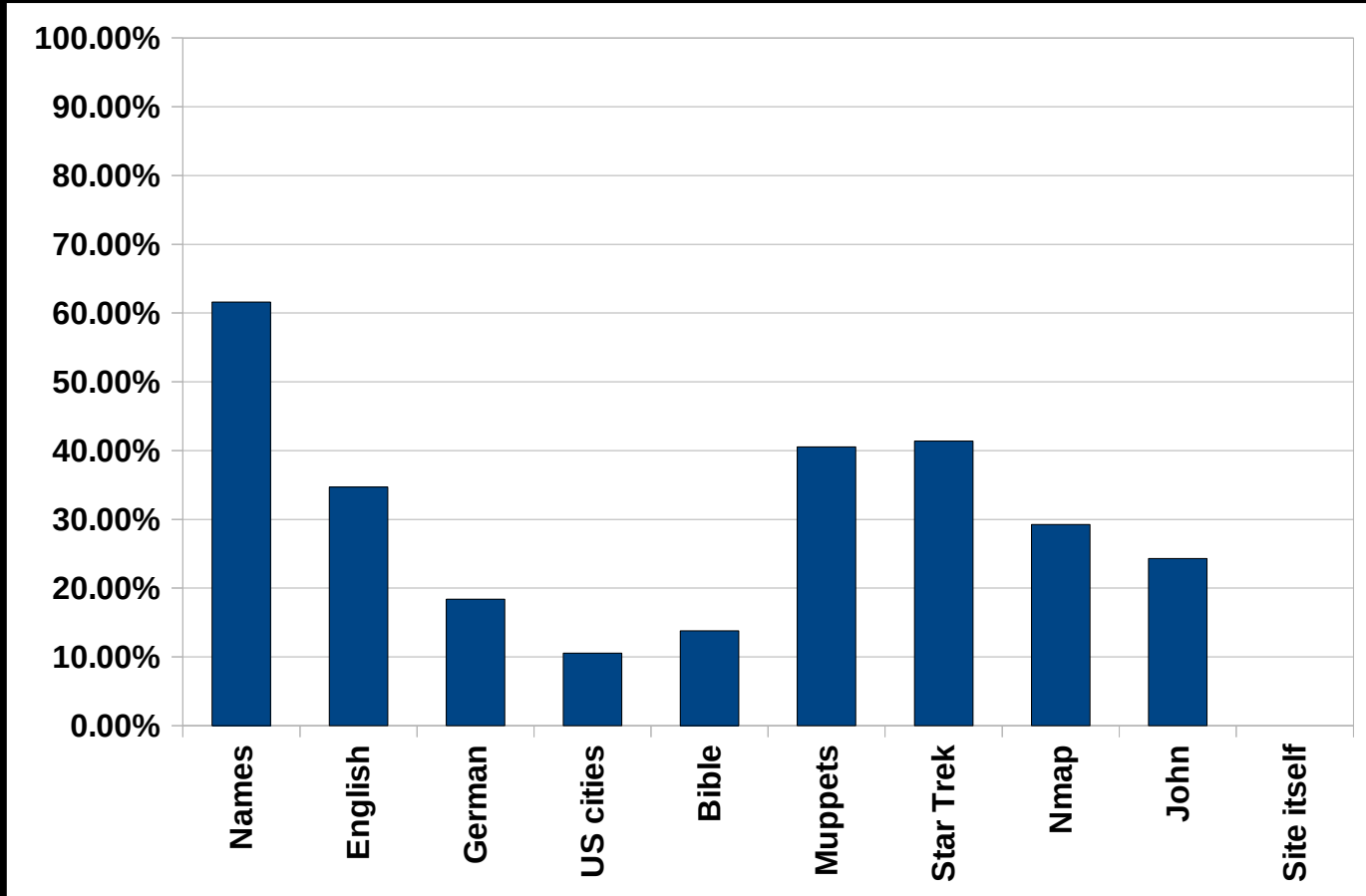
Singles.org

Top-10 passwords

Password	Count
123456	221
jesus	63
password	58
12345678	46
christ	36
love	29
princess	27
jesus1	25
sunshine	24
1234567	23



Singles.org



Tuscl

	Unique	Total
myspace	37.144	41.545
phpbb	184.389	255.421
rockyou	14.344.391	32.603.387
älypää	1.384	9.135
Finnish-unknown	36.323	50.795
faithwriters	8.348	9.755
singles.org	12.234	16.250
tuscl	38.820	50.028
Porn-unknown	8.089	10.000
carders.cc	1.904	5.062



Tuscl

“The Ultimate Strip Club List”
Compromised by SQL injection
September, 2010
Passwords were plaintext



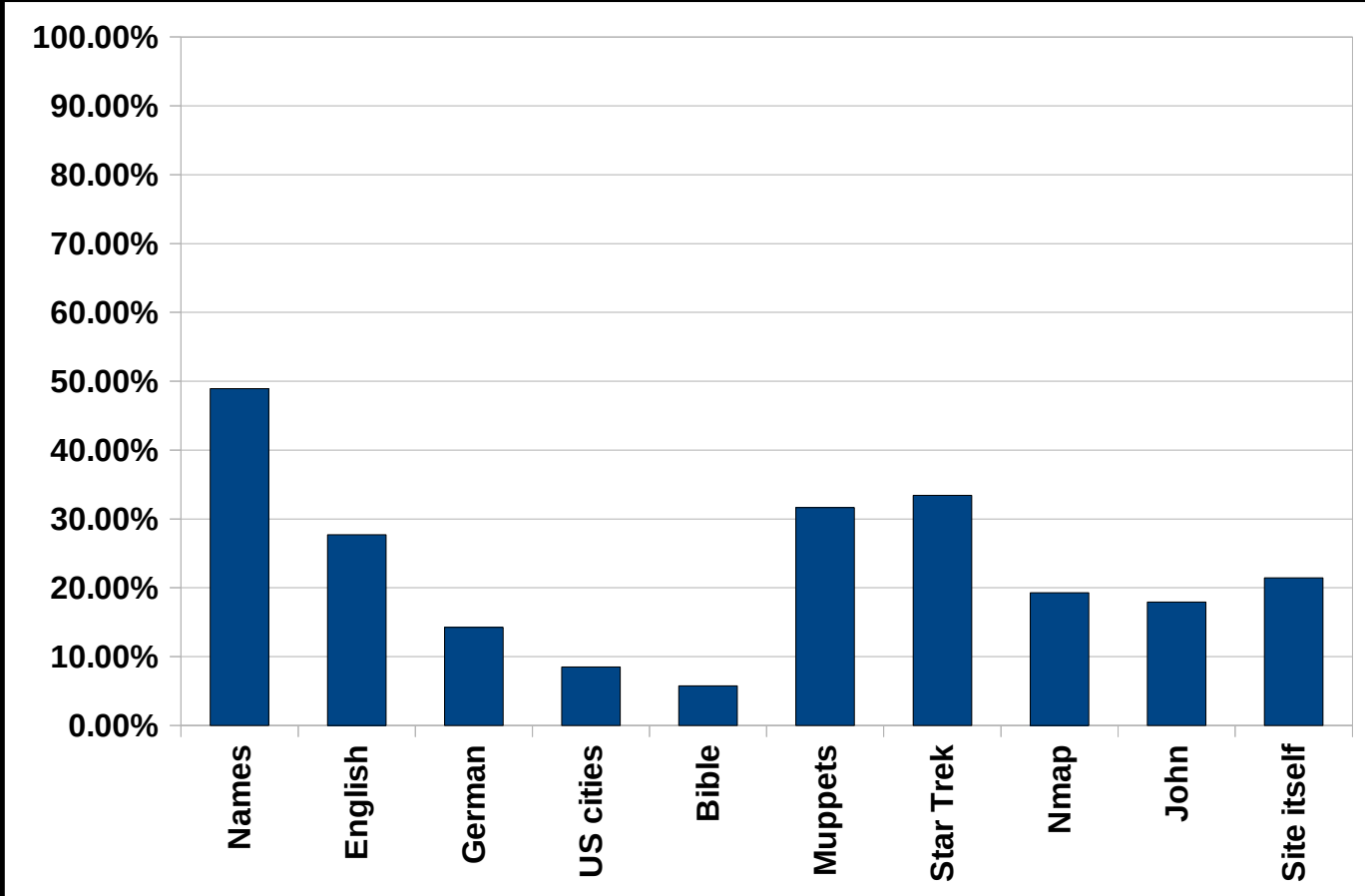
Tuscl

Top-10 passwords

Password	Count
password	266
123456	173
tuscl	83
stripper	66
qwerty	61
12345	49
12345678	47
1234	42
baseball	36
monkey	35



Tuscl



Porn-unknown

	Unique	Total
myspace	37.144	41.545
phpbb	184.389	255.421
rockyou	14.344.391	32.603.387
älypää	1.384	9.135
Finnish-unknown	36.323	50.795
faithwriters	8.348	9.755
singles.org	12.234	16.250
tuscl	38.820	50.028
Porn-unknown	8.089	10.000
carders.cc	1.904	5.062



Porn-unknown

Found by accident

Couldn't determine the source



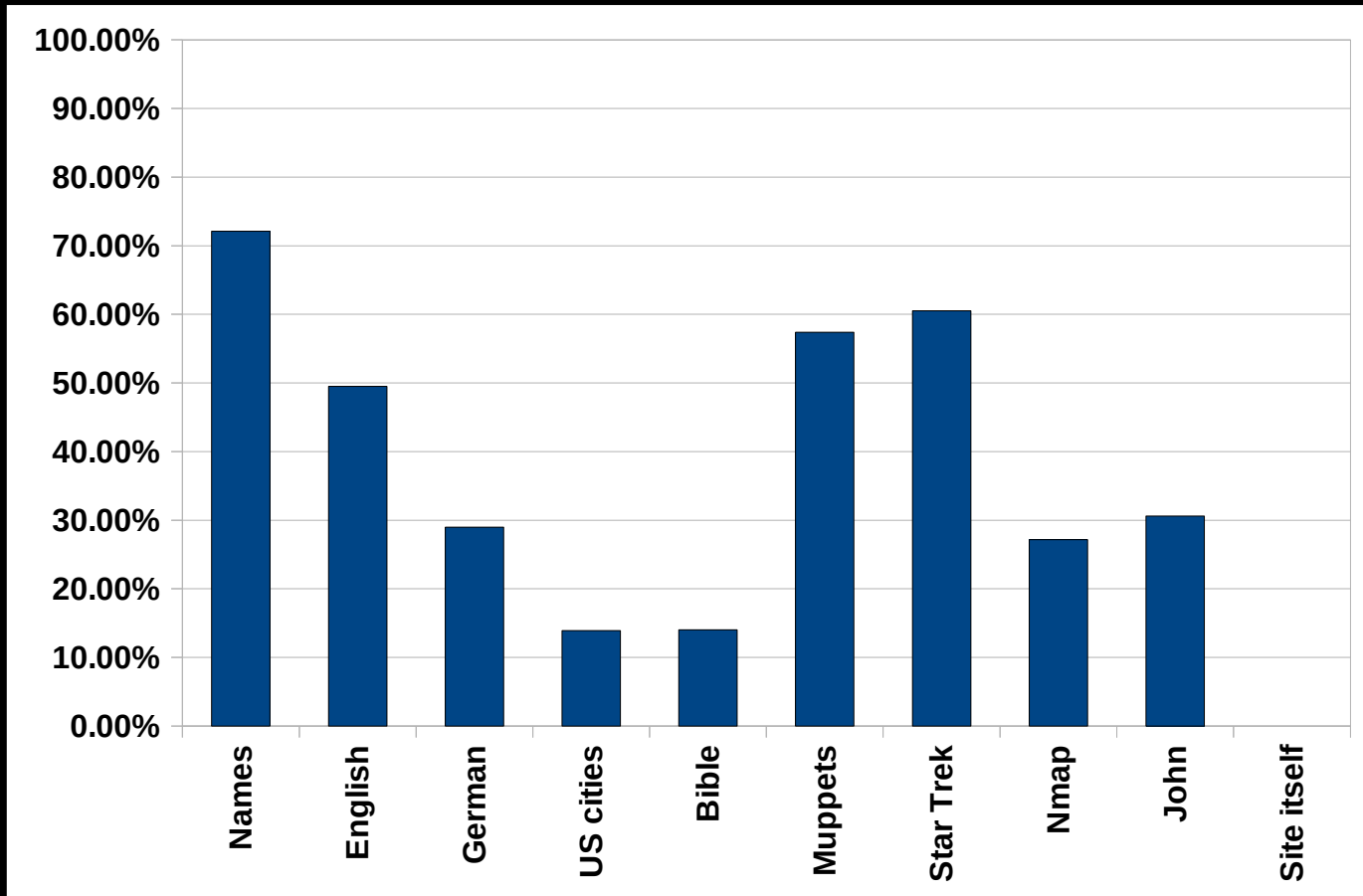
Porn-unknown

Top-10 passwords

Password	Count
1234	28
123456	25
password	20
pussy	19
12345	18
6969	15
mustang	14
love	14
michael	13
dick	13



Porn-unknown



Carders.cc

	Unique	Total
myspace	37.144	41.545
phpbb	184.389	255.421
rockyou	14.344.391	32.603.387
älypää	1.384	9.135
Finnish-unknown	36.323	50.795
faithwriters	8.348	9.755
singles.org	12.234	16.250
tuscl	38.820	50.028
Porn-unknown	8.089	10.000
carders.cc	1.904	5.062



Carders.cc

Credit card hackers' site

Passwords were salted-sha1

8 months of cracking = ~60% cracked

Slow!

Full database was released

Includes a lot of “interesting” information about credit
card thieves
(in German)



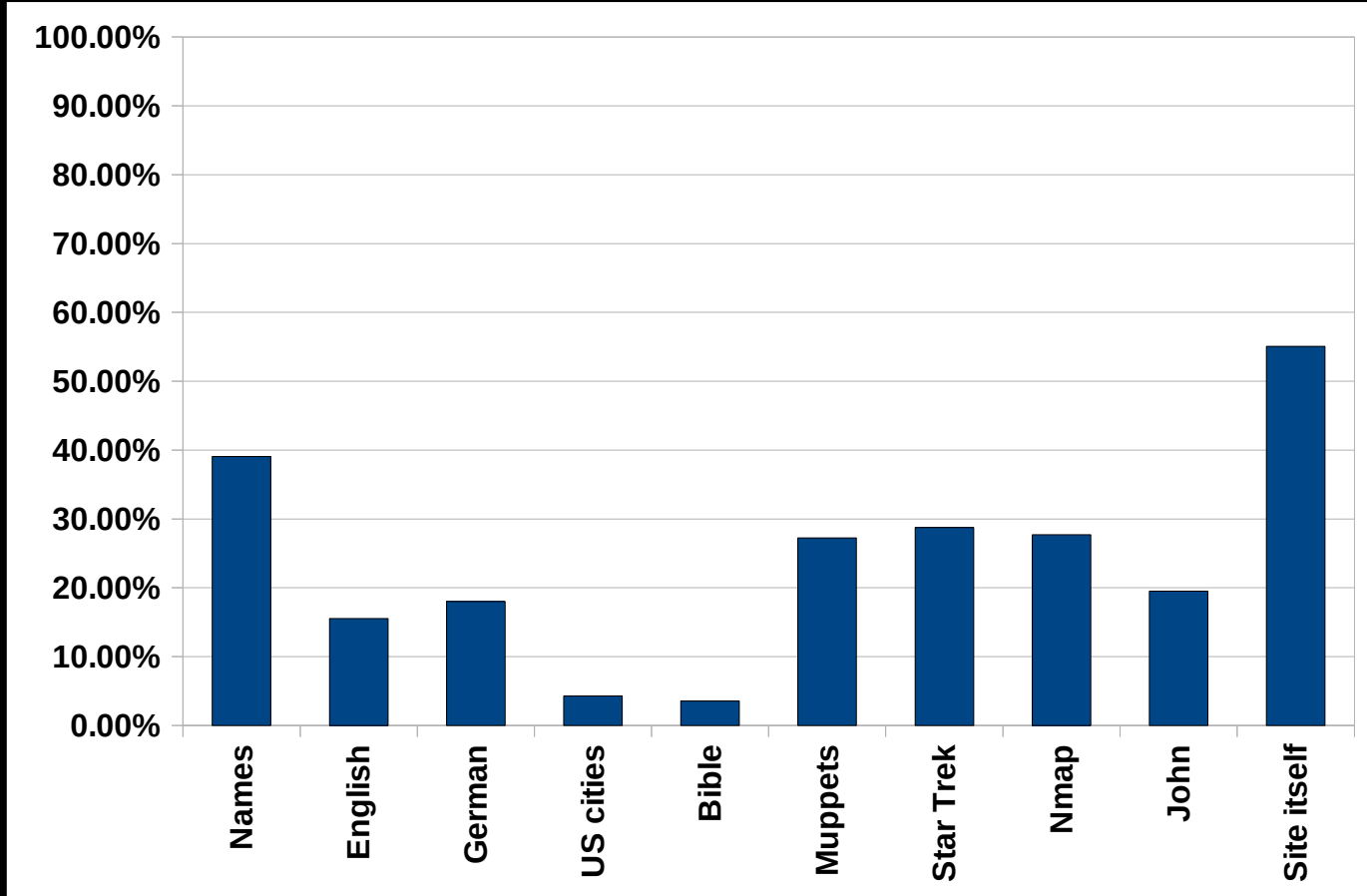
Carders.cc

Top-10 passwords

Password	Count
123456	218
12345678	71
123456789	68
hallo123	36
hurensohn	34
123123	32
121212	32
qwertz12	30
711681	28
13371337	22



Carders.cc

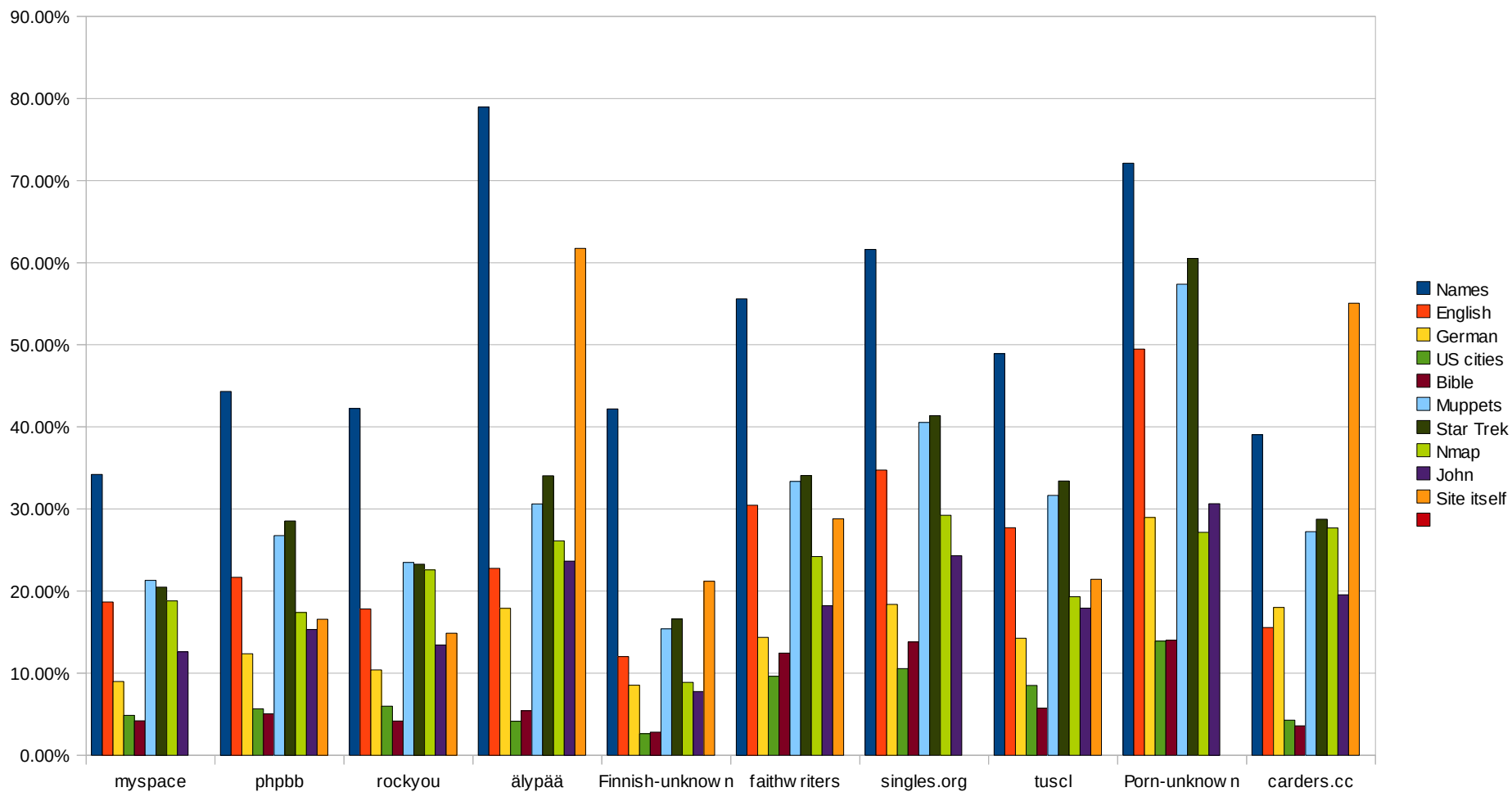


Summary

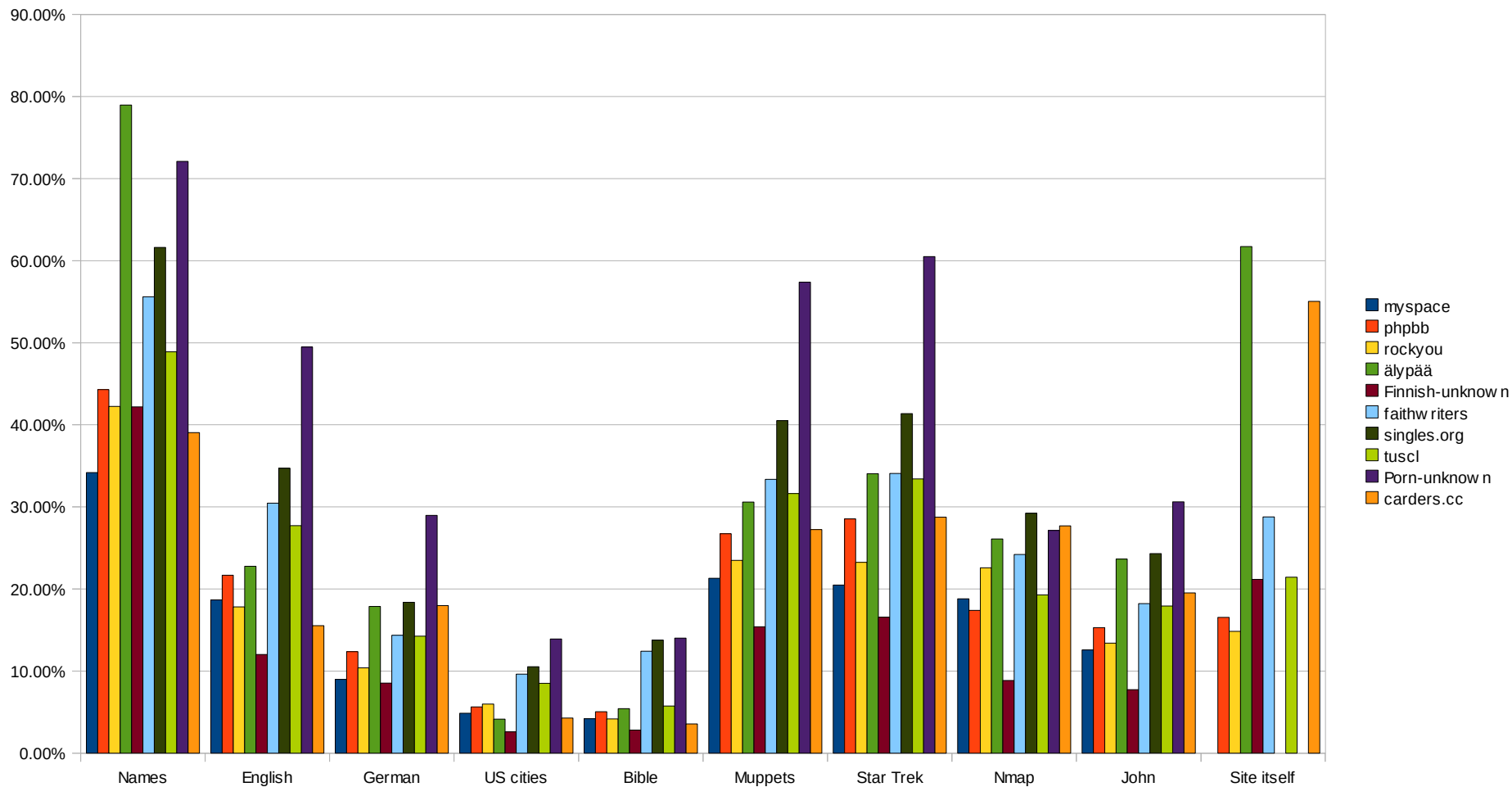
	Passwords	Algorithm	Success
myspace	41.545	n/a (phished)	
phpbb	255.421	md5	97%
rockyou	32.603.387	plaintext	
älypää	9.135	unknown	
Finnish-unknown	50.795	all of the above	60% - 75%
faithwriters	9.755	plaintext	
singles.org	16.250	plaintext	
tuscl	50.028	plaintext	
Porn-unknown	10.000	plaintext	
carders.cc	5.062	salted sha1	60%



Summary



Summary



Dictionary performance

Names did best overall, ranging from 34% to 78%

English words did well, ranging from 12% to 50%

Bible did poorly, but best against religious sites
(and a porn site)

Wikis (Star Trek and Muppets) did well, 16% to 60%

Due more to their size and English content than specific
passwords

Scraping sites varied greatly, from 15% to 62%

Best size/performance tradeoff. though

Cracking strategies

Let's talk about three...

John's mangling rules

Numeric

L33t passwords



John's mangling rules

Written in a specialized language

Found in john.conf

```
john.conf (~f/tools/john-1.7.6/run) - VIM
# Simple rules come first...
:
-s x**
-c (?a c Q
-c l Q
-s-c x** /?u l
# These were not included in crackers I've seen, but are pretty e
fficient,
# so I include them near the beginning
>6 '6
>7 '7 l
-c >6 '6 /?u l
>5 '5
# Weird order, eh? Can't do anything about it, the order is based
on the
# number of successful cracks...
<* d
r c
-c <* (?a d c
-c >5 '5 /?u l
```

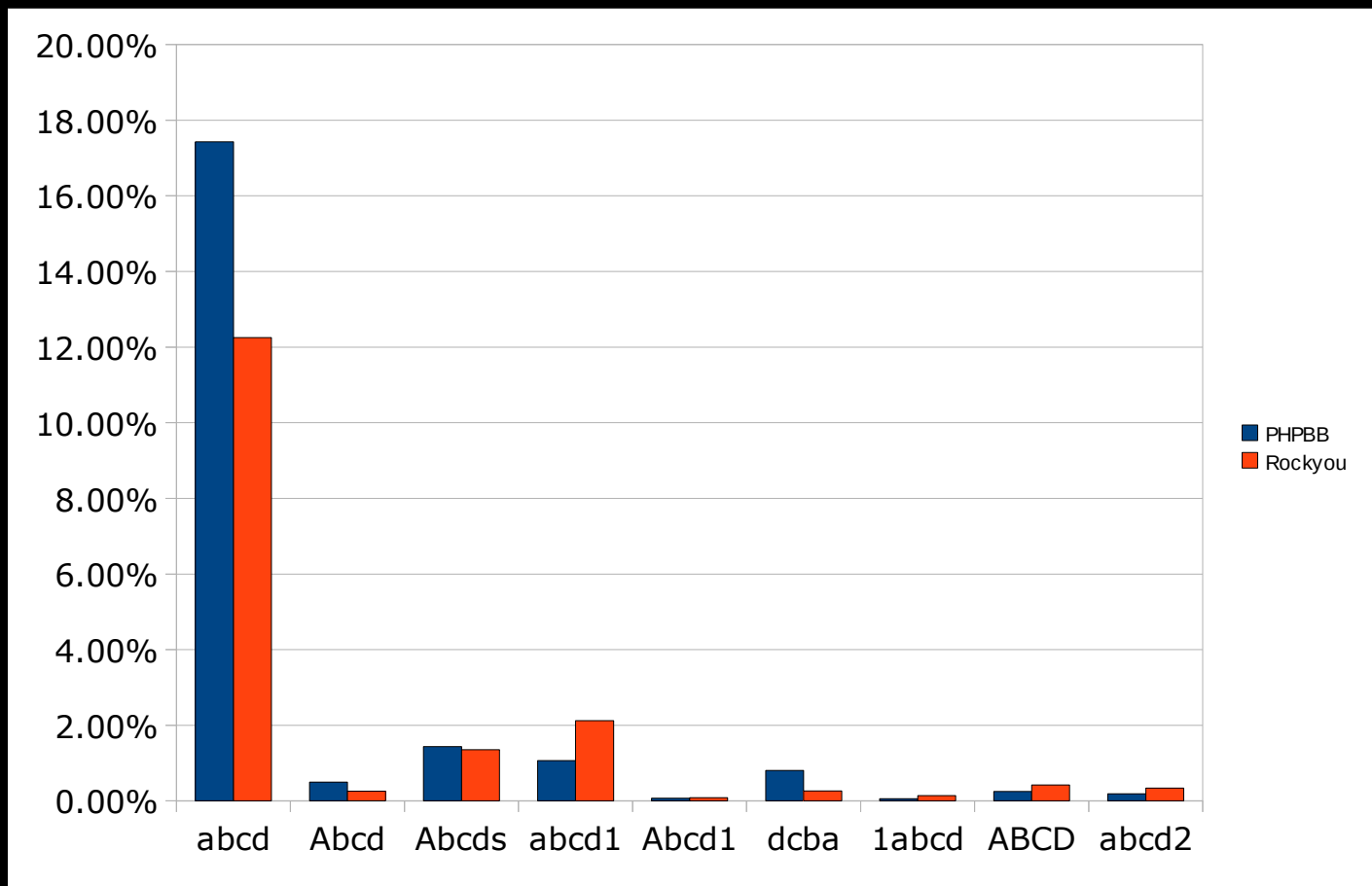
24.1 1%

John's mangling rules

Analysis of the first 9 against PHPBB and Rockyou

	PHPBB	Rockyou
abcd	44.522	3.993.000
Abcd	1270	83.661
Abcds	3.668	440.436
abcd1	2.722	691.146
Abcd1	177	26.039
dcba	2.058	85.339
1abcd	137	44.721
ABCD	639	137.016
abcd2	481	110.952

John's mangling rules



John's mangling rules

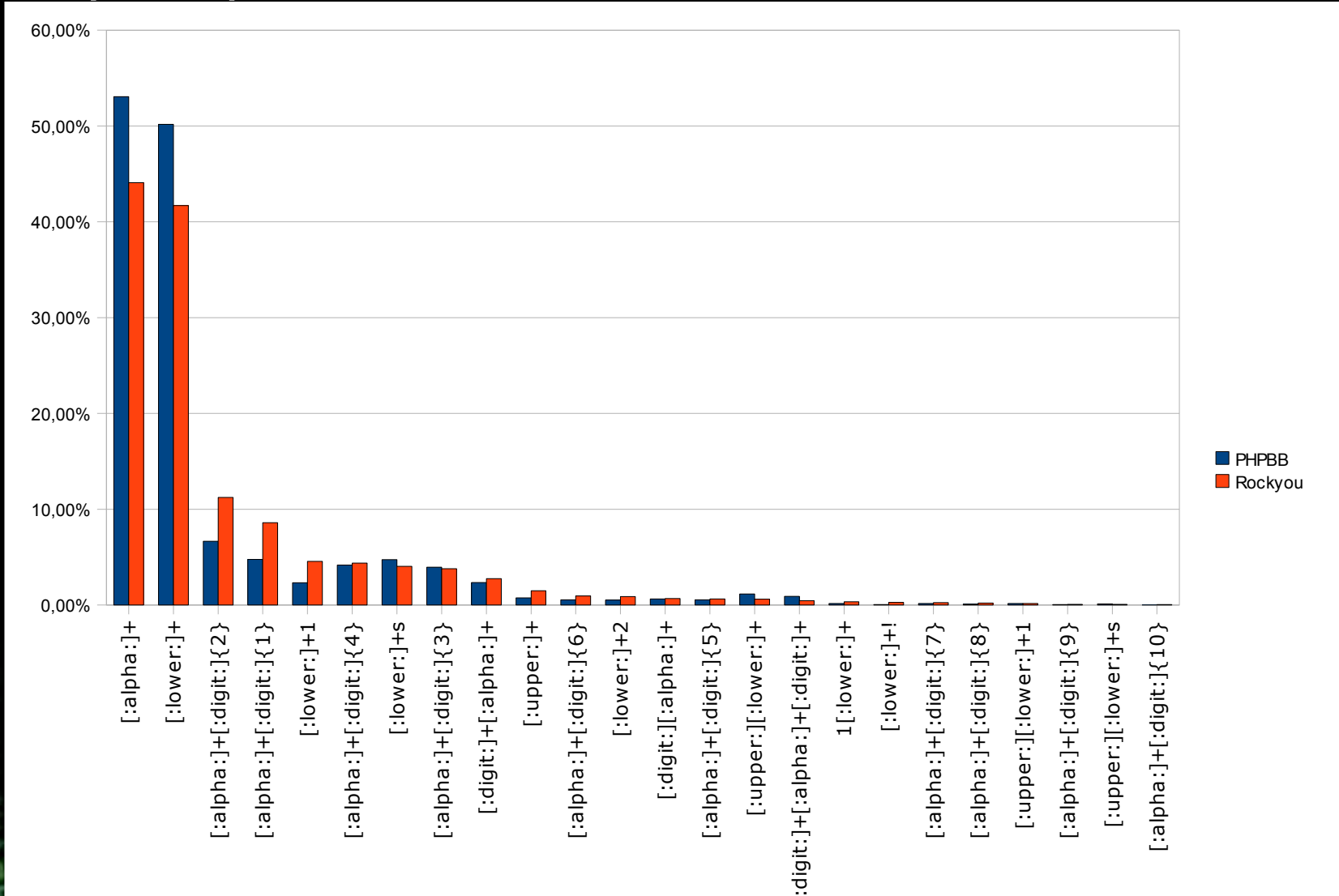
Top-10 password formats

Format	PHPBB	PHPBB%	Rockyou	Rockyou%
[alpha:]+	135.531	53,06%	14.369.769	44,07%
[lower:]+	128.157	50,17%	13.597.102	41,70%
[alpha:]+[digit:]{2}	16.979	6,65%	3.662.879	11,23%
[alpha:]+[digit:]{1}	12.158	4,76%	2.802.595	8,60%
[lower:]+1	5.946	2,33%	1.482.845	4,55%
[alpha:]+[digit:]{4}	10.643	4,17%	1.424.025	4,37%
[lower:]+s	12.123	4,75%	1.313.415	4,03%
[alpha:]+[digit:]{3}	10.095	3,95%	1.238.500	3,80%
[digit:]+[alpha:]+	5.995	2,35%	896.083	2,75%
[upper:]+	1.889	0,74%	488.622	1,50%



John's mangling rules

Top-10 password formats

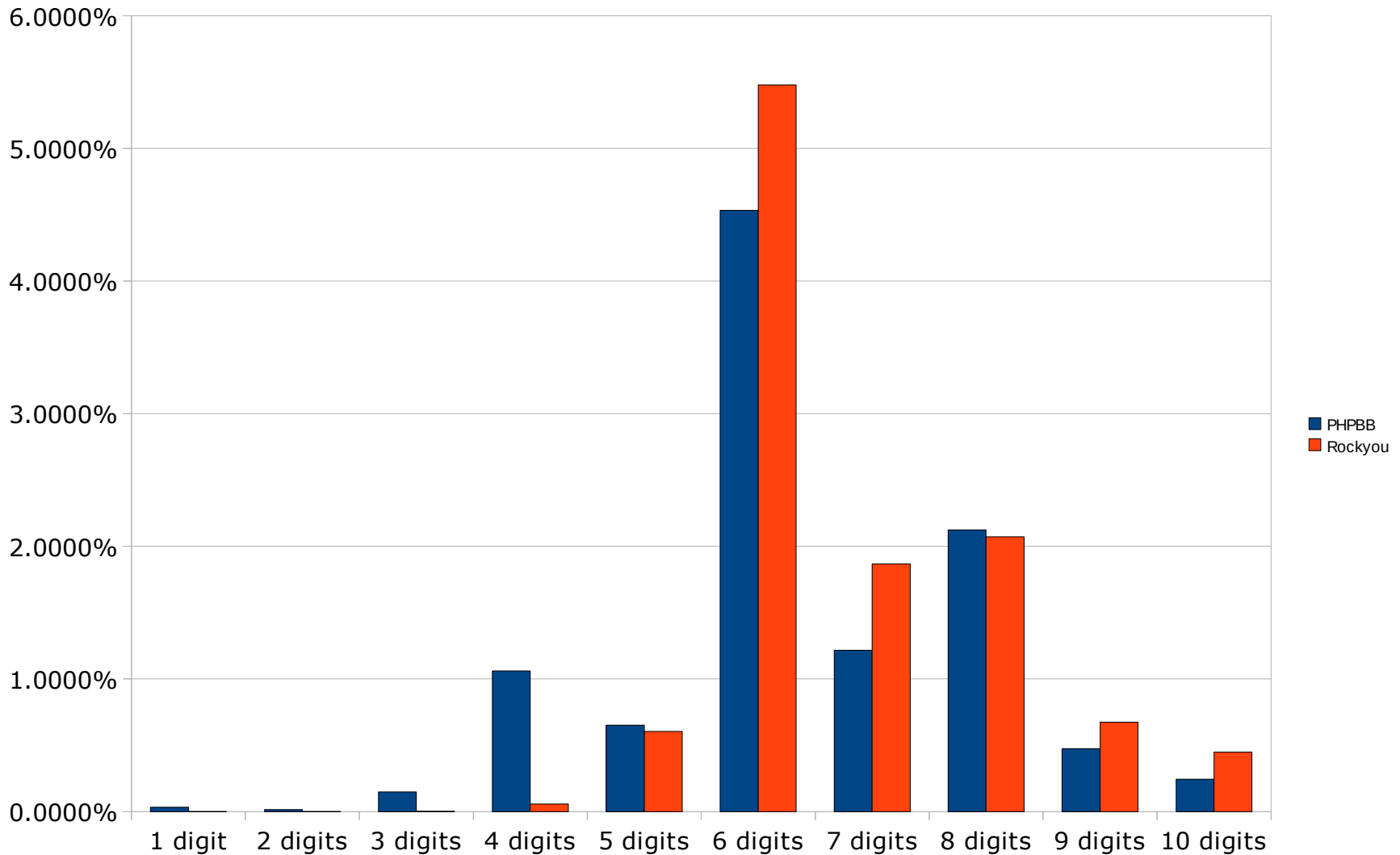


Numeric passwords

	PHBB	PHPBB%	Rockyou	Rockyou%
6 digits	11.575	4,5317%	1.785.924	5,4777%
8 digits	5.423	2,1232%	675.556	2,0720%
7 digits	3.108	1,2168%	608.959	1,8678%
9 digits	1.214	0,4753%	220.144	0,6752%
5 digits	1.665	0,6519%	197.030	0,6043%
10 digits	625	0,2447%	146.508	0,4494%
4 digits	2.710	1,0610%	18.522	0,0568%
3 digits	379	0,1484%	992	0,0030%
2 digits	41	0,0161%	134	0,0004%
1 digit	84	0,0329%	57	0,0002%
1 – 1 billion	26.199	10,2572%	3.507.305	10,7575%



Numeric passwords

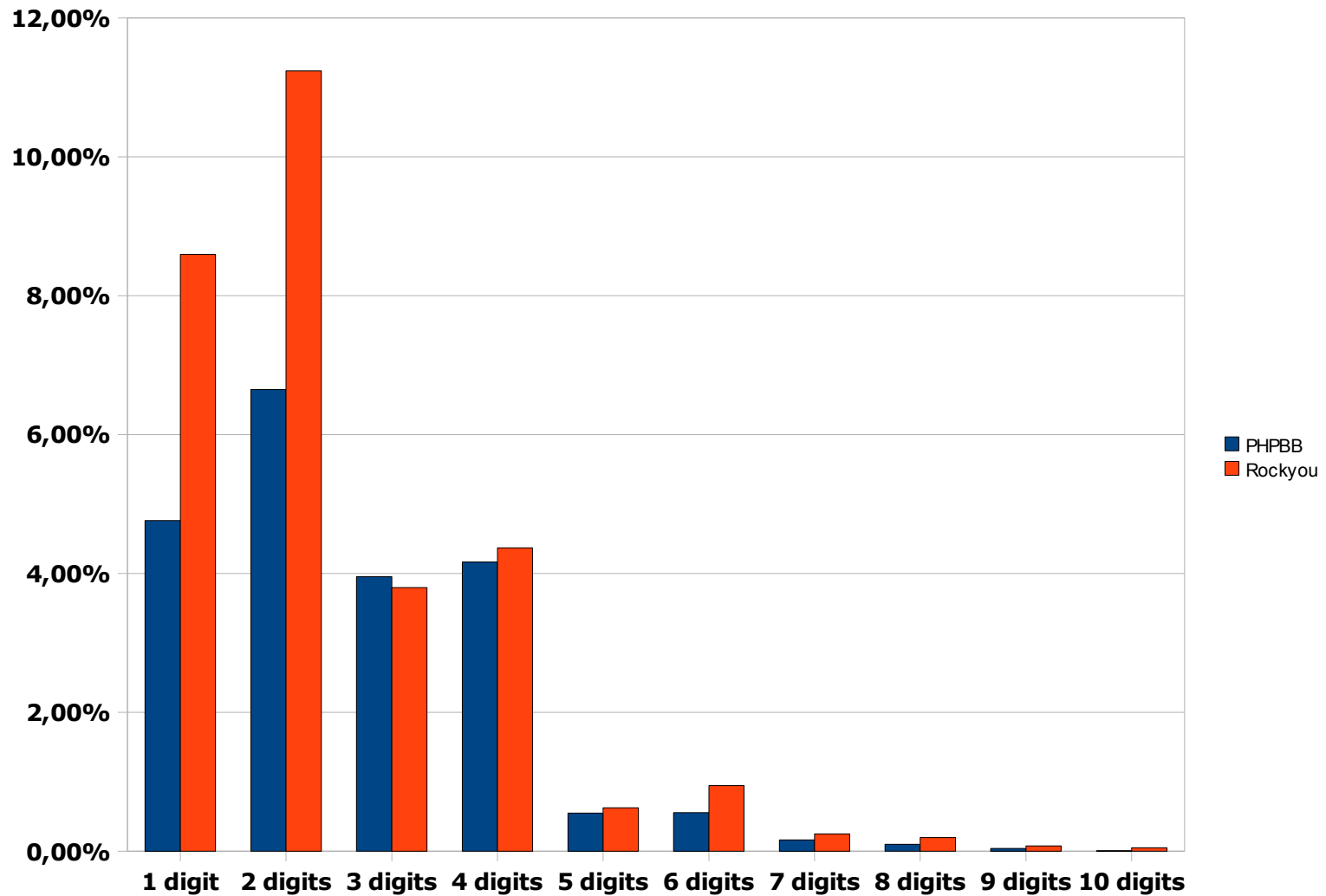


Numeric suffixes

	PHPBB	PHPBB%	Rockyou	Rockyou%
2 digits	16.979	6,65%	3.662.879	11,23%
1 digit	12.158	4,76%	2.802.595	8,60%
4 digits	10.643	4,17%	1.424.025	4,37%
3 digits	10.095	3,95%	1.238.500	3,80%
6 digits	1.418	0,56%	308.778	0,95%
5 digits	1.400	0,55%	204.479	0,63%
7 digits	416	0,16%	81.376	0,25%
8 digits	256	0,10%	63.771	0,20%
9 digits	99	0,04%	24.986	0,08%
10 digits	17	0,01%	16.664	0,05%

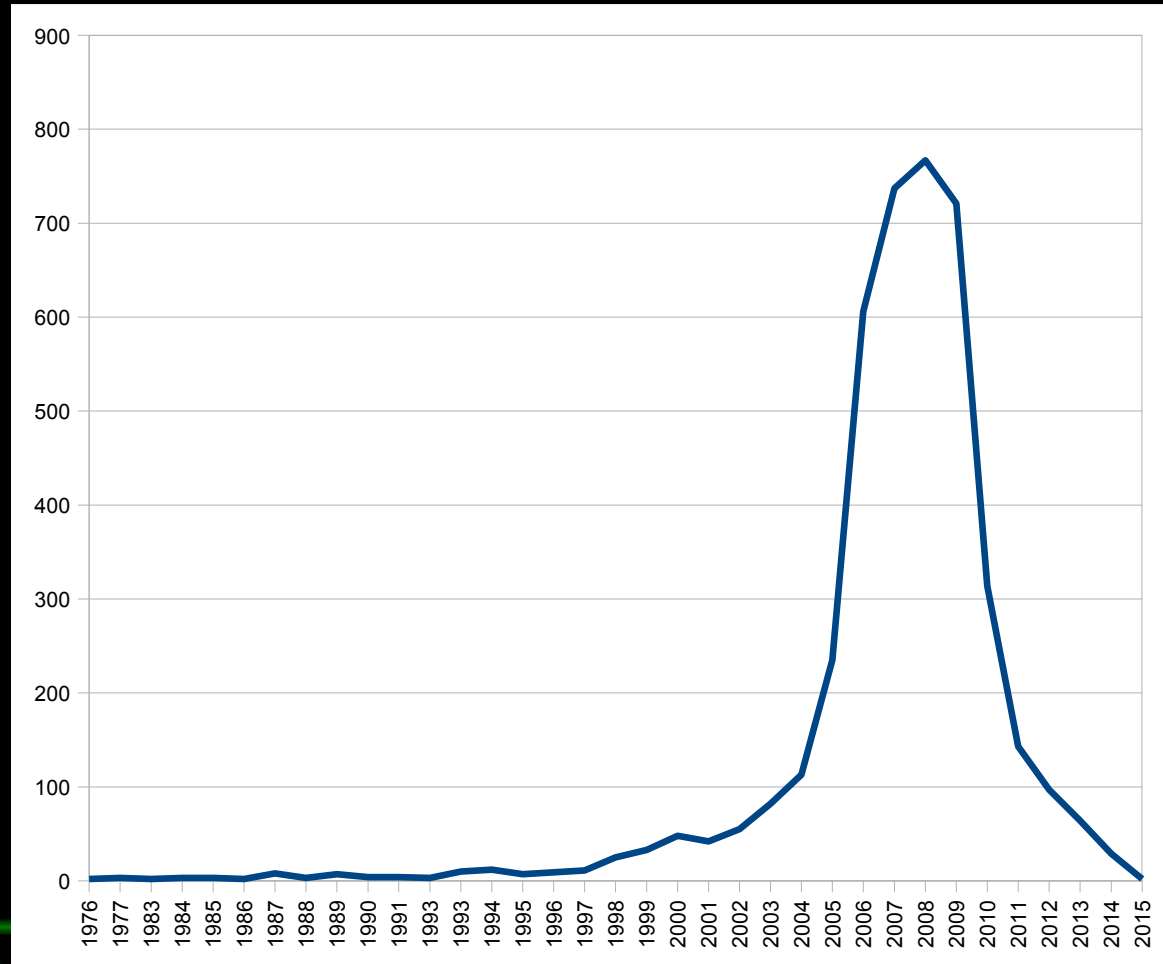


Numeric suffixes



Numeric suffixes

'classofXX' passwords on Rockyou



L33t passwords

Started with English dictionary

Following transformations:

A => 8	O => 0
B => 8	R => 12
C => (	S => \$
D => !	U => 5
E => 3	T => +
G => 6	V => \
I => 1	X => <
L => 1	Y => /

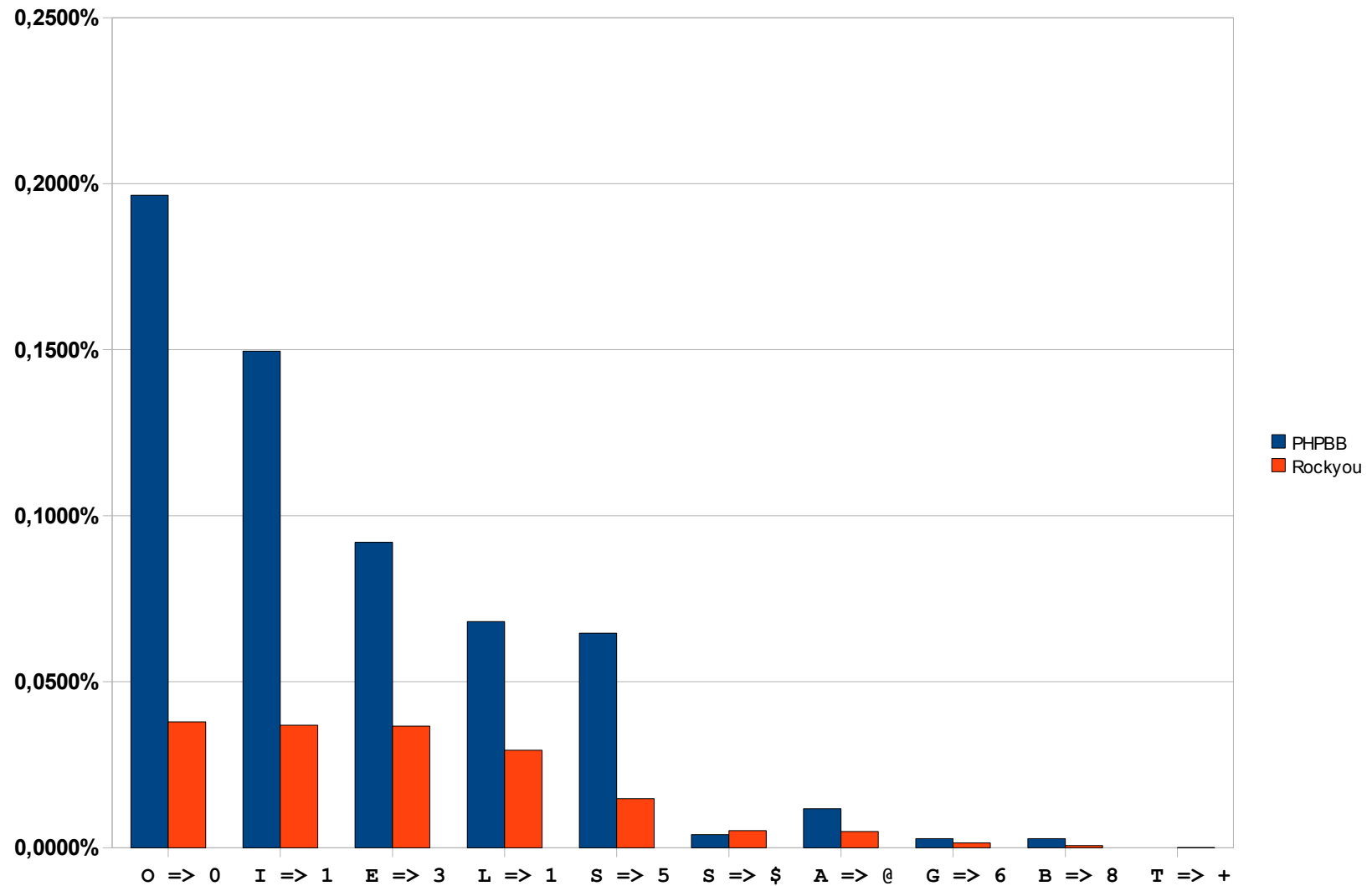


L33t passwords

133t	PHPBB	Rockyou
O => 0	502	12.363
I => 1	382	12.039
E => 3	235	11.940
L => 1	174	9.567
S => 5	165	4.817
S => \$	10	1.677
A => @	30	1.600
G => 6	7	471
B => 8	7	212
T => +	0	12



L33t passwords



L33t passwords

All of the above. in every permutation...

PHPBB: 2000 (0.78%)

Rockyou: 91.252 (0.28%)

Some of my favourites...

m0n0ph0nic

m0t0r0l@

gr33n3ry

h311f1r3

n3m3s1s

@br@c@d@br@

@rs3n@l

aw3s0m3n355

ch@m3130n5

ch0p50t1cks

d3g3n3rat3d

d15k3tt35



L33t passwords

```
go.rb (~/.svn/security/20...eepsec/research/mangling) - VIM
#!/usr/bin/env ruby

@replacements = {
  "e"=>"3", "l"=>"1", "o"=>"0", "s"=>"$",
  "x"=>"><", "a"=>"@", "v"=>"\/", "t"=>"+",
  "b"=>"8", "c"=>"(", "d"=>"|)", "g"=>"6",
  "i"=>"1", "r"=>"l2", "s"=>"5", "y"=>"`/",
}

def l33t(str, start)
  start.upto(str.length) { |i|
    c = str[i..i]
    @replacements.each { |from, to|
      if(c == from)
        new_str = String.new(str)
        new_str[i] = to
        puts(new_str)
        l33t(new_str, i)
      end
    }
  }
end

STDIN.read.split("\n").each do |a|
  l33t(a, 0)
end
```



What worked best?

John rules

Plain English: 12,3%

Plain English with 'l' appended: 2,1%

Plain English with a capital and a 's' appended: 1,4%

L33t

O → 0: 0,04%

l → 1: 0,04%

E → 3: 0,04%

L → 1: 0,03%

Numeric

6 digits: 5,5%

8 digits: 2,1%

7 digits: 1,9%

9 digits: 0,7%



What worked best?

Common password formats:

All alphabetic: 44,1%

All lowercase: 41,7%

All lowercase followed by 2 digits: 11,2%

All lowercase followed by 1 digit: 4,6%

All lowercase followed by 4 digits: 4,4%

All lowercase followed by 's': 4,0%

Password followed by 'x' digits:

Followed by 2 digits: 11,2%

Followed by 1 digit: 8,6%

Followed by 4 digits: 4,4%

Followed by 3 digits: 3,8%



Other methods

Misspelled words (anti-spellchecker)

Other languages

Chinese/Japanese symbols, phonetic versions

Unicode symbols

o => ò

e => é

Etc

Keyboard patterns

'qwerty', 'qawsedrft', 'qetuo['



Conclusion

Sites are always being breached

People choose poor passwords

Most passwords are alphabetic, or alpha followed by one or two numbers

'L33t' passwords don't crack as many

But crack very obscure ones

With good techniques, 97%+ coverage is possible



Questions

Ron Bowes

Email: ron@dash9security.com

Company site: <http://www.dash9security.com>

Blog: <http://www.skullsecurity.org>

