Passwords
“The Death of '*Clever*'.”

A Press Review / news update

Bill Ricker (compiler/editor)

for BLU.org 2012-09-19

Sources

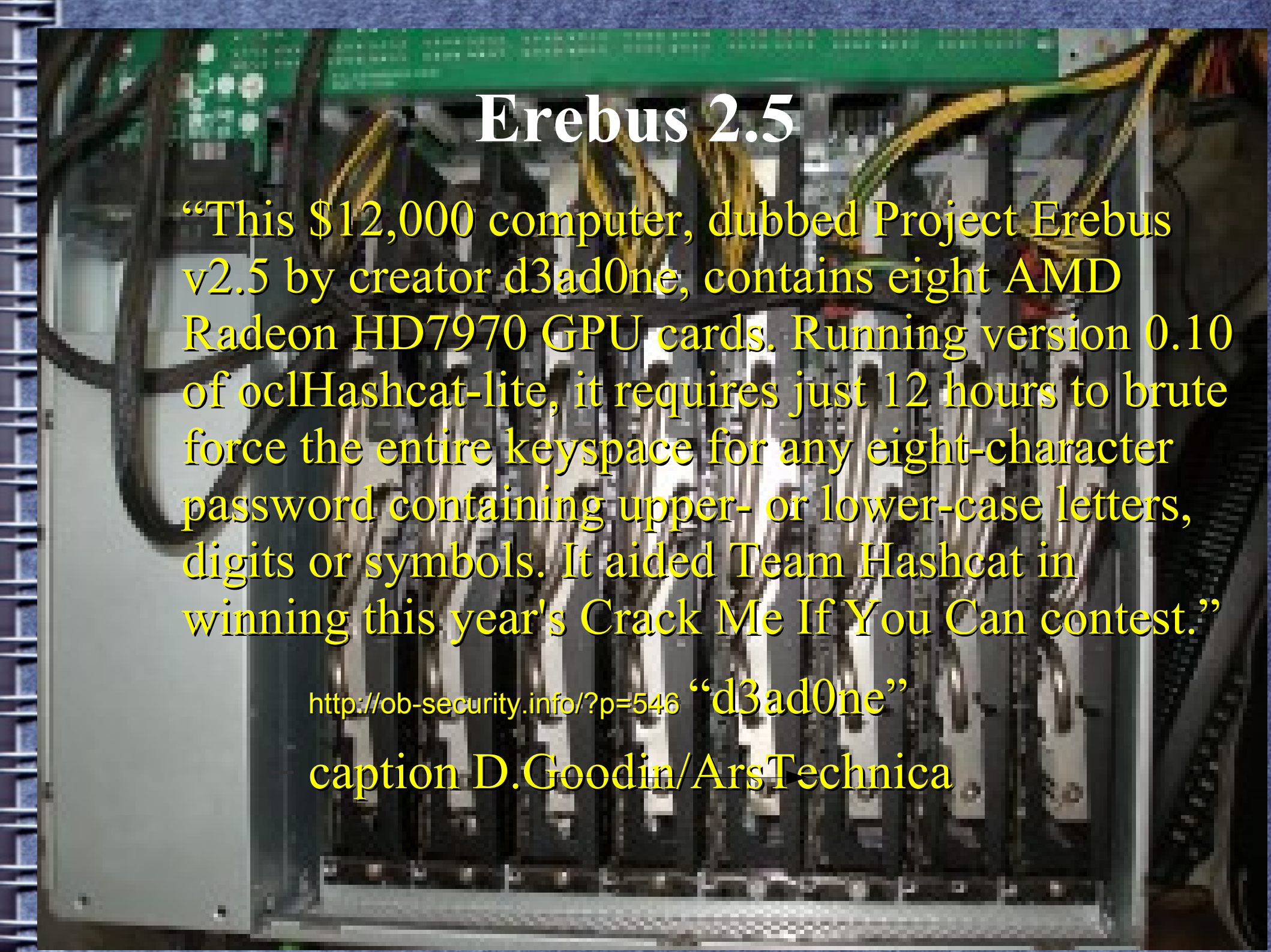
- Dan Goodin / Ars Technica “Passwords under assault”

  primary source unless cited otherwise

  - http://arstechnica.com/security/2012/08/passwords-under-assault/
- R.Graham, Errata Security
  - “The deal with passwords” http://erratasec.blogspot.com/2012/08/the-deal-with-passwords.html (source of an illo)
  - “Common misconceptions of password cracking” http://erratasec.blogspot.com/2012/08/common-misconceptions-of-password.html
- Cory Doctrow, BoingBoing
  - “Password cracking goes into hyperdrive” http://boingboing.net/2012/08/21/password-cracking-goes-into-hy.html (hyperdrive
- Steve Gibson, Security Now
  - #366: The Death of "Clever" (Yes, swiping his title) www.grc.com/securitynow.htm http://twit.tv/sn

Changed Threat Environment

- Brute force is getting easier
  - Hardware cracking – Parallel is now cheap: GPU
  - Bedroom crackers have speed previously NSA-grade, 10^{10} guesses/second offline
  - 100KK of real passwords in dumps – they have seen it all *and adapted*
- Rampant password re-use & use of email addresses as userids.
- Whole Dbs getting liberated
  - even if hash and salted, will cough up any easy ones fast and all memorable ones eventually.



Erebus 2.5

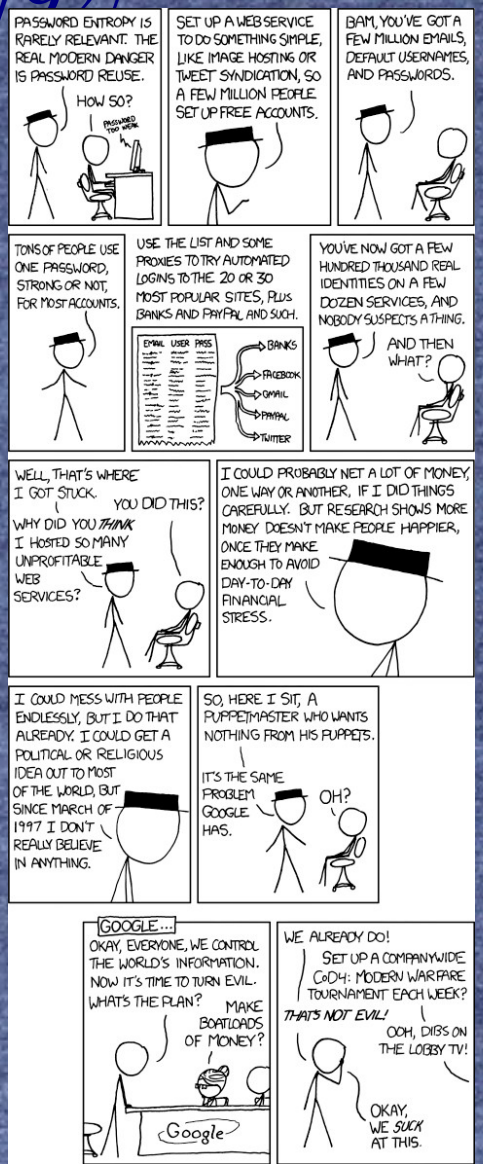
“This $12,000 computer, dubbed Project Erebus v2.5 by creator d3ad0ne, contains eight AMD Radeon HD7970 GPU cards. Running version 0.10 of oclHashcat-lite, it requires just 12 hours to brute force the entire keyspace for any eight-character password containing upper- or lower-case letters, digits or symbols. It aided Team Hashcat in winning this year's Crack Me If You Can contest.”

http://ob-security.info/?p=546 “d3ad0ne”

caption D.Goodin/ArsTechnica

XKCD 792: Password Reuse

- https://m.xkcd.com/792/
-



Iterated Game

- Crackers carry knowledge forward.
  - If it's in a previously cracked dump – as `Sup3rThinkers` is – it's now just a dictionary word, pick one of 100KK known plaintexts is only 27 bits entropy.
- In a new leak, 60% are found in prior lists.
  - Most of rest can be found by combining things in lists
  - or rule-based generation ($word.$digit , $name.$number, $word.reverse($word))
  - ("rainbow tables" – see the article for efficient huge dictionary)

Password Breaches & Dumps

year	Date Made Public	Name	Password	breach??
2005	June 4, 2005	Duke University Medical	yes	14,000
2006	April 7, 2006	DiscountDomainRegistry	yes	
	March 8, 2006	iBill [disputed]	yes	17,781,462
2007	August 9, 2007	Penson Worldwide	yes	11
2008	January 18, 2008	Colorado State Universit	yes	300
	March 21, 2008	Compass Bank	yes	1,000,000
2009	December 15, 2009	RockYou	yes	32,000,000
	February 5, 2009	phpBB.com	yes	400,000
	March 16, 2009	Comcast	yes	4,000
2010	December 12, 2010	Gawker	yes	1,300,000
	January 1, 2010	collective2.com	yes	25,000
2011	April 27, 2011	Sony, PlayStation Netwo	yes	101,600,000
	August 14, 2011	Bay Area Rapid Transit (	yes	2,450
	August 24, 2011	Allianceforbiz.com, Sho	yes	20,000
	December 12, 2011	Florida Family Associati	yes, encrypte	22
	December 25, 2011	Stratfor.com, Strategic F	yes	68,063
	July 12, 2011	Toshiba, Toshiba Americ	yes, plain	7,971
	July 8, 2011	Kiplinger Washington Ed	yes	142,000
	June 19, 2011	Sega	yes, encrypte	1,290,000
	June 4, 2011	Infragard	yes	180
	June 6, 2011	Ravelry.com	yes, encrypte	0
		Sony Pictures, Sony Co	yes	1,000,000
	November 10, 2011	Steam (The Valve Corpo	yes salt	0
	November 13, 2011	Providencenightlife.net	yes	50,000
Total Result				**156,705,459**

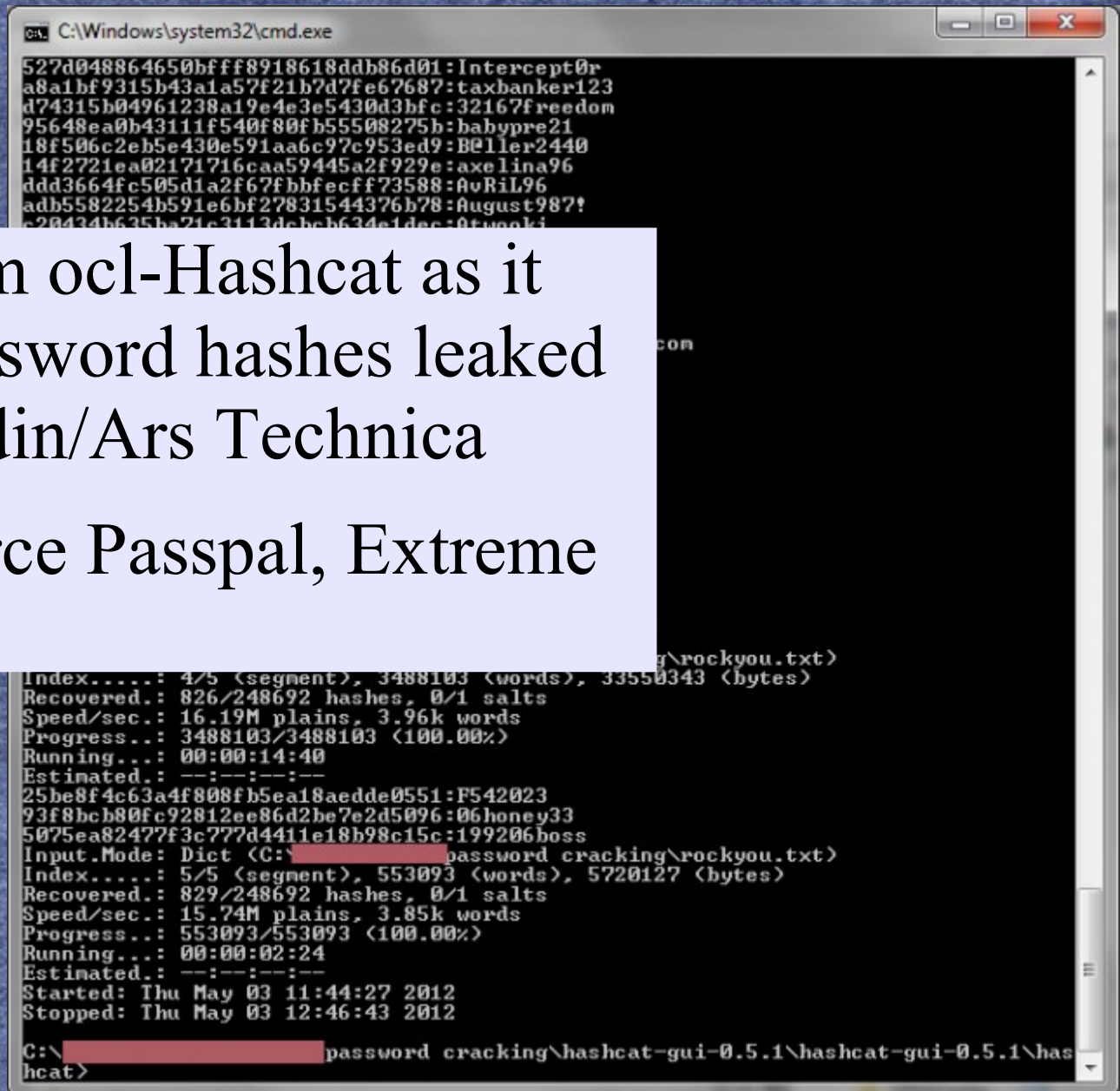
year	Date Made Public	Name	Password	breach??
2012	April 1, 2012	Bethesda Softworks, Be	yes	3,657
	April 27, 2012	Three Rivers Park Distri	yes	82,000
	April 6, 2012	Vote Sex!	yes	35,959
	February 11, 2012	Manwin Holding SARL (B	yes, encrypte	350,000
	February 13, 2012	Gossip Girl	yes hash	2,480
	February 20, 2012	Yamaha Commercial Au	yes, plain	1,755
	February 3, 2012	Salt Like City Police Dep	yes hash	1,073
	February 8, 2012	Internet Marketing Strate	yes, encrypte	5,860
	January 20, 2012	Arizona State University	yes	300,000
	July 11, 2012	Formspring	yes hash	420,000
	July 12, 2012	Yahoo! Voices	yes, plain	453,492
	July 13, 2012	Nvidia	yes hash	400,000
	July 18, 2012	ITWallStreet.ccom	yes hash	50,000
	July 19, 2012	Yale University	yes	1,200
	July 20, 2012	Oregonwine.com	yes	1,313
	July 23, 2012	Gamigo	yes, encrypte	3,000,000
	June 1, 2012	MOAB Training Internati	yes, encrypte	1,442
	June 6, 2012	LinkedIn.com	yes, encrypte	6,458,020
	March 15, 2012	Iran Defense Forum, Iran	yes salt	3,212
		vBCoderz.com	yes salt	1,290
	March 16, 2012	Arizona Sports Fans, An	yes salt	8,855
	March 19, 2012	Adult Insider Network, A	yes salt	10,704
	March 25, 2012	MilitarySingles.com	yes	171,000
	March 30, 2012	Public Broadcasting Sys	yes, plain	1,871
		Savvyinsider.com	yes	2,457
	March 5, 2012	Digital Playground	yes, plain	72,794
	March 9, 2012	Gaming Perfection	yes salt	1,784
	May 26, 2012	Gridiron Strategies	yes	2,109
	May 9, 2012	InfoLink, ServerPronto, (	yes	1,926
Total Result				**11,846,253**

Omits breaches < 1000 in 2012
Eharmony not included?
Data from PRC https://www.privacyrights.org/data-breach

ocl-Hashcat in action

"A screenshot from ocl-Hashcat as it cracks a list of password hashes leaked online." Dan Goodin/Ars Technica

- Similar: open-source Passpal, Extreme GPU Bruteforcer



“Clever is not enough.”

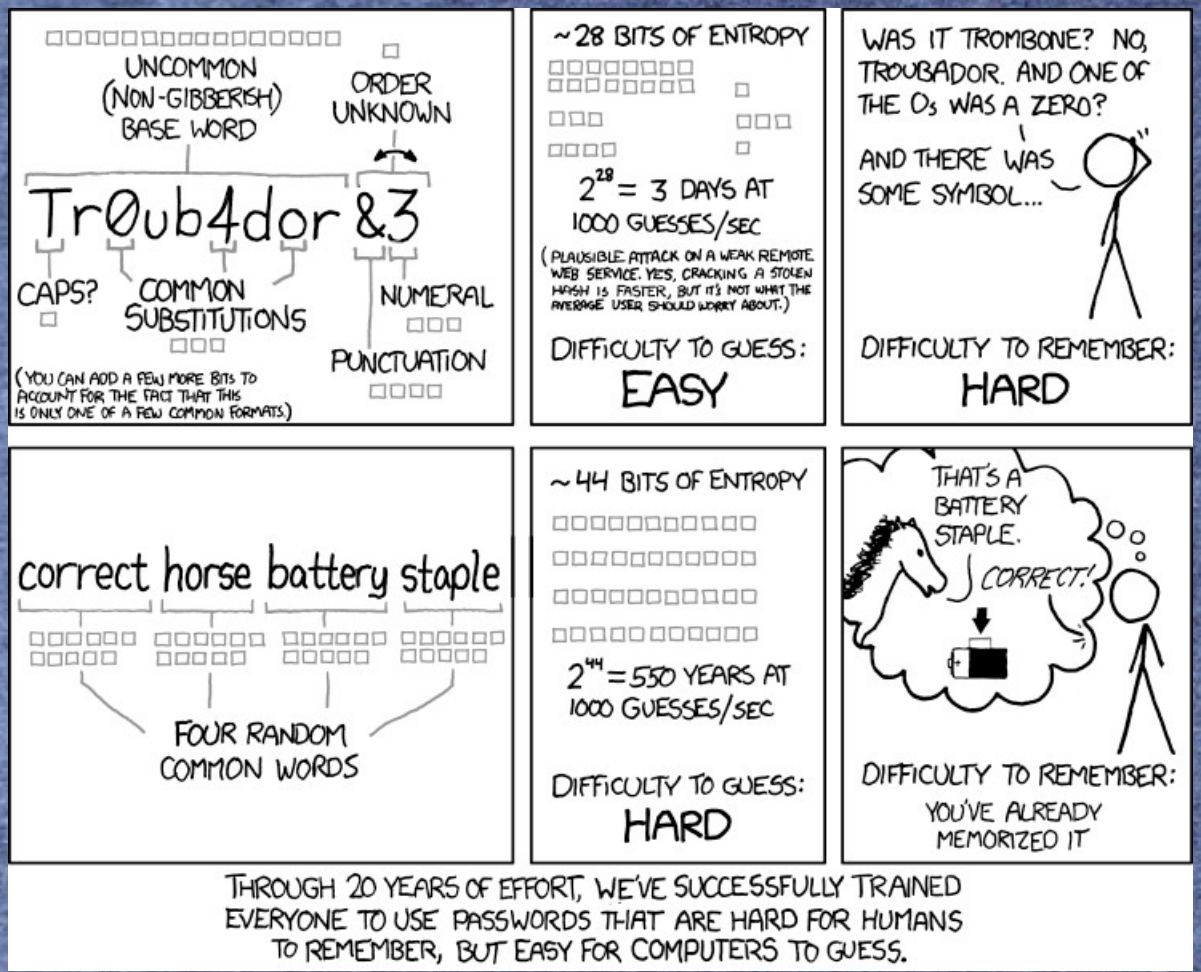
- Clever defeats the *prior* threat.
- Clever has an Entropy deficit today.
  - `Sup3rThinkers` is not selected from 96^{13} or 62^{13} (which would 85 or 77 bits entropy)
  - It's 2 words, a plural choice, 13 upper/lower choices, maybe 6 Leet/1337 choices, for around 44 to 50 bits total.
  - That is strong vs on-line guessing but not against modern offline cracking.

– Credit Steve Gibson for title.

XKCD 936: Password Strength

http://m.xkcd.com/936/ http://imgs.xkcd.com/comics/password_strength.png

Correct for on-line guessing (irrelevant, DOS)
but not parallel off-line cracking of dumps
GigaPw/s guessing $2^{44-30} = 2^{14}$s = 4 hours gets all similar ones too.



BUSTED!

Password Meters

BUSTED!

- “Many websites have some sort of "password meter" to show the "strength" of your password. While they certainly point out "weak" passwords, just because they claim your password is strong doesn't make it so. Don't believe them.”
- RDG/es-myths http://erratasec.blogspot.com/2012/08/common-misconceptions-of-password.html credits Pers Thorsheim https://twitter.com/thorsheim/status/238368167058096129 & security nirvanna http://securitynirvana.blogspot.com/2010/02/never-trust-password-meters.html http://securitynirvana.blogspot.com/2010/11/revisiting-password-meters.html
- (Because they don't have the rules derived from the dumps so don't see how little entropy `Sup3rThinkers` has. Meter reading for `NCC1701` depends on their dictionary.)
-

The Exponential Wall

- For random passwords 96^n or 62^n only, Not for "Jane1968"
- "Brute-force cracks work well against shorter passwords. The technique can take days or months for longer passcodes, even when using Amazon's cloud-based EC2 service." -DG/at.

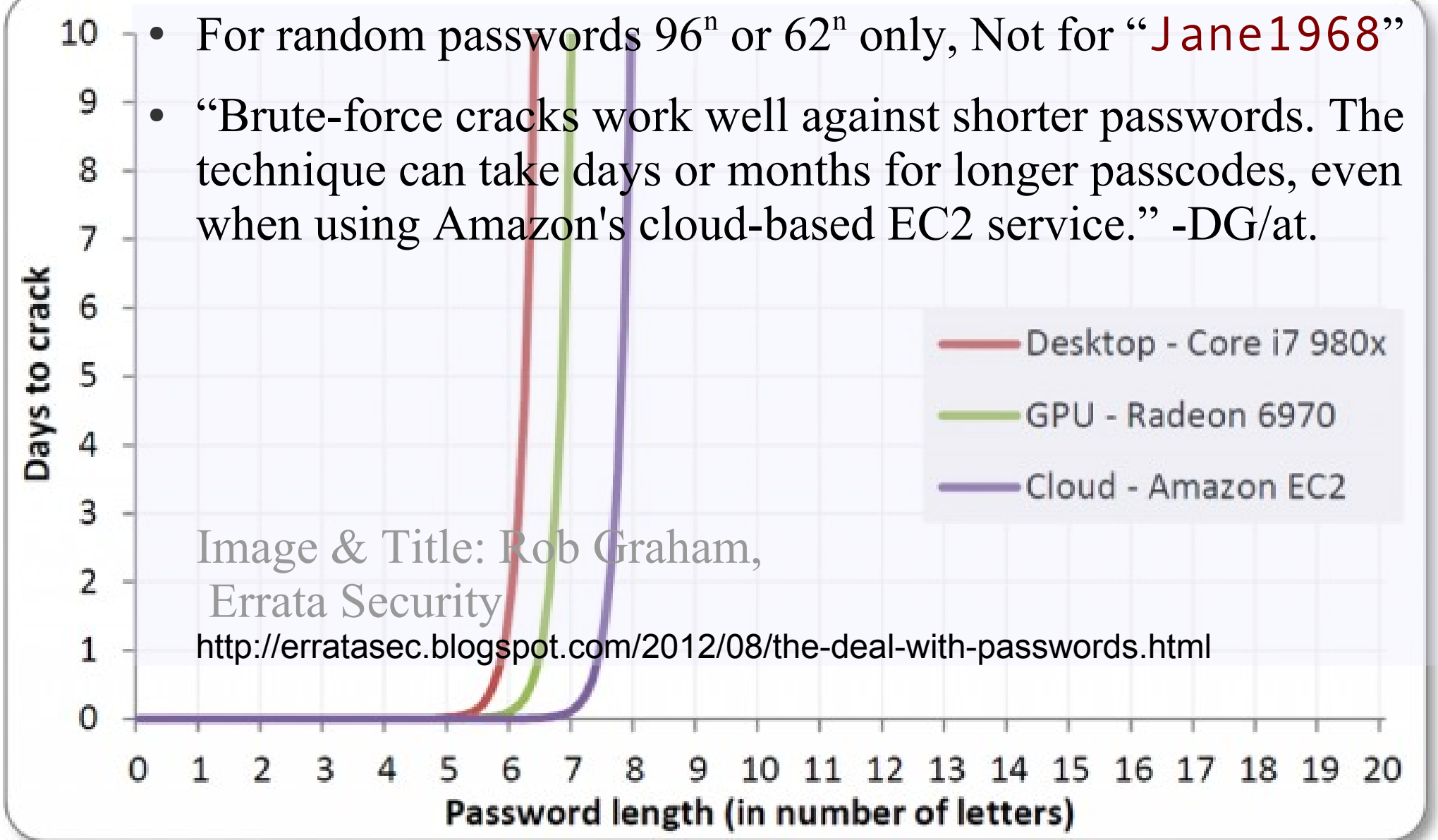


Image & Title: Rob Graham, Errata Security

http://erratasec.blogspot.com/2012/08/the-deal-with-passwords.html

Recommendations (User)

- Every password unique
  - Not just for you
  - Never used before or after, anywhere, by anyone
- Random characters to maximum char set, 13+ preferred, longer no symbols allowed
- Change regularly
- Login only over https:

Requires a password tool w/ master password that's truly strong, unique, and memorable.

- 1Password
- PasswordSafe
- KeePass (FLOSS https://en.wikipedia.org/wiki/KeePass)
- LastPass <SG recommends
- Not SuperGenPass

http://akibjorklund.com/2009/supergenpass-is-not-that-secure &
http://stackoverflow.com/questions/554224/is-the-bookmarklet-password-generator

LastPass

- Plug-ins (or apps)

IE v6 +
Firefox v2+
Google Chrome v4+
Safari v3+ OS X, v5+ Win
Opera (bookmarklets)
iPhone, iPod Touch, Apple's iOS
iPad (tabbed browser)
Android
RIM Blackberry
Windows Mobile
Symbian
Palm's webOS

Freemium (apps cost)
- Sync between devices
- Offline recovery and generates lockbox paper sheet if desired – guarantees recovery if they fold
- Trust No One (TNO)

your master key never leaves your device, they cache encrypted thunk for syncing, but only used on your device.

Steve Gibson, Security Now

#256 LASTPASS review & other eps
www.grc.com/securitynow.htm
http://twit.tv/sn

also in episodes 229 236 244 238 (256) 257 259 262 265 267 269 271 277 290 294 295 297 299 301 302 303 306 307 308 312 314 322 326 327 329 331 334 338 339 340 341 342 347 348 350 354 356 357 358 360 362 363 365 366

Assumptions (Hosts)

- Stored passwords are a necessary evil
  - Certs and identity servers don't work for most memberships
- Must Mitigate the evil on the host
  - Never store, transmit, or compare PW in clear.
  - Never store PW in reversible, symmetric encryption
    - Your password safe must do this … but should do whole blocks of file
  - Salt and iterate a crypto grade hash
  - Store hash and compare old vs offered hash
  - If they can mail you your **old** password as password recovery, they're doing it **wrong**.

Recommendations (Hosts) 1

- Salted Hashes are necessary but not sufficient to prevent dictionary attacks.
  - NTLM, LinkedIn, Yahoo, eHarmony did not salt.
- A secure hash designed for signature is not secure for passwords.
  - Faster hashing is faster cracking.
  - Slow hashing is better here.
  - A barely susceptible delay for login to succeed multiplies for crackers, soaking up their multi-GPU parallelism.

Best Practices (Hosts)

- Don't build, re-use a quality implementation.
  - Means you get Patches. Apply them.
- Iterate.
  - SHA512crypt (5k iter)
  - Bcrypt (iterates mod. Blowfish)
  - PBKDF2 (in .net)
- If you must use PHP, the new 5.5 is building in Bcrypt with DB store.

XKCD 538: Rubber Hose Cryptanalyis

https://xkcd.com/538/

No stronger than the weakest link.