Questions to which the answer is NO (passwords edition)

Joseph Bonneau

jcb82@cl.cam.ac.uk

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

FC RUMP SESSION

Kralendijk, Bonaire, Netherlands

Feb 28, 2012

Questions to which the answer is NO

Is your shampoo making you FAT? The truth about 'chemical calories' in beauty products

By PETA BEE

Last updated at 9:21 AM on 11th July 2011

When it comes to losing weight, most of us are aware of the three factors at play: genetics, the number of calories we consume and the energy we are prepared to expend sweating our way into shape.

We can't choose our parents but, according to the dieting mantra, eat healthily, exercise regularly and the pounds will eventually drop off.

But what if your body stubbornly refuses to remove excess fat, despite concerted efforts to shift it?

Questions to which the answer is NO

Mail Online News

Home | News | U.S. | Sport | TV&Showbiz | Femail | Health | Science | Money | RightMinds | Coffee Break | Travel | Columnists

News Home | Arts | Headlines | Pictures | Most read | News Board | Login

Are U.S. government microwave mind-control tests causing TV presenters' brains to melt down?

By TOM LEONARD
Created 10:18 PM on 1st April 2011

Comments (217) | Share 1 Tweet 2,521 Like 10k

A bizarre spate of television presenters dissolving into on-air gibberish has sparked claims that the U.S. military could be to blame.

In four high-profile cases, the latest involving fast-talking Judge Judy, the presenters have started off speaking properly but have then descended into undecipherable nonsense - looking confused and unstable.

The frequency of the 'attacks' - and the fact that recorded examples of the mental meltdowns have been popular on websites - has led to conspiracy theorists pointing the finger at shadowy government experiments.

Site Web bing

FEMAIL TODAY

Oscars 2012: And the award for best breakout star goes to... Angie's right leg: Jolie's limb attracts attention, mocking and 10,000 Twitter followers

Oscars 2012: Is that really your best angle? Irina Shayk's metallic gown is a little too revealing
Shimmering gown dazzled onlookers

Danielle Lloyd's weight plummets to 8st after emergency blood transfusion
Gaunt WAG has lost 7lbs in just a week

Oscars 2012: Sir Elton John and David Furnish's son Zachary is entranced with a Pomeranian dog
Preferred Esther to Katy Perry...

Questions to which the answer is NO

theguardian

Your search

News | Sport | Comment | Culture | Business | Money | Life & style | Travel | Environment

Comment is free › Cif belief

Should we clone Neanderthals?

Given reliable technology, could it ever be ethical to bring our prehistoric relatives back from the dead?

Andrew Brown
guardian.co.uk, Thursday 23 June 2011 10.00 BST

Tweet this
Share
reddit this
Comments (…)

A larger | smaller

Science
Neanderthal man · Cloning · Genetics · Anthropology

World news
Ethics · Religion

More from Comment is free on

Science
Neanderthal man · Cloning · Genetics · Anthropology

World news
Ethics · Religion

Questions to which the answer is NO

Did the Romans leave London because of the miserable British weather?

- **Forensic tests on skeletons show settlers suffered from malnourishment and poor health due to lack of sunlight**

By GRAHAM SMITH

Last updated at 12:59 PM on 5th November 2011

Their huge empire stretched all the way from northern Britain to the Egyptian desert.

But it seems the all-conquering Romans had an unexpected Achilles' Heel in the grim British weather.

Settlers suffered from poor health due to a lack of sunlight and a poor diet after they established Londinium in the 1st century AD, according to scientists.

Will guessing entropy solve my problems?

$$G(\mathcal{X}) = E\left[\#_{\text{guesses}}(X \xleftarrow{R} \mathcal{X})\right] = \sum_{i=1}^{N} p_i \cdot i$$

Intepretation: Expected number of queries "Is $X = x_i$?" for $i = 1, 2, \ldots, N$ (optimal sequential guessing)

Will guessing entropy solve my problems?

```
ed65e09b98bdc70576d6c5f5e2ee38a9
e54d409c55499851aeb25713c1358484
dee489981220f2646eb8b3f412c456d9
c4df8d8e225232227c84d0ed8439428a
bd9059497b4af2bb913a8522747af2de
b25d6118ffc44b12b014feb81ea68e49
aac71eb7307f4c54b12c92d9bd45575f
9475d62e1f8b13676deab3824492367a
92965710534a9ec4b30f27b1e7f6062a
80f5a0267920942a73693596fe181fb7
76882fb85a1a8c6a83486aba03c031c9
6a60e0e51a3eb2e9fed6a546705de1bf
6843b9efec36f428deabce22c0fc1805
5dfbcd6390b77d06df9027c8d7d4fe84
4374968e935a9a0f8d56785ea682eb5f
075392900129109111258011109199 1a
0410412e7194adc1b419a87a47979c36
...
```

Random 128-bit passwords in the wild at RockYou ($\sim 2^{-20}$)

Will guessing entropy solve my problems?

Lemma: For a mixture distribution

$$\mathcal{Z} = p \cdot \mathcal{X} + q \cdot \mathcal{Y}$$

we have

$$G(\mathcal{Z}) \geq p \cdot G(\mathcal{X}) + q \cdot G(\mathcal{Y})$$

Will guessing entropy solve my problems?

Lemma: For a mixture distribution

$$\mathcal{Z} = p \cdot \mathcal{X} + q \cdot \mathcal{Y}$$

we have

$$G(\mathcal{Z}) \geq p \cdot G(\mathcal{X}) + q \cdot G(\mathcal{Y})$$

Therefore, for real passwords $\mathcal{P}$, we have:

$$G(\mathcal{P}) \geq p \cdot G(?) + 2^{-20} \cdot G(\mathcal{U}_{2^{128}})$$

$$\boxed{G(\mathcal{P}) > 2^{107}}$$

Should I use non-ASCII characters in my password?

пароль

Should I use non-ASCII characters in my password?

пароль

=

пароль

Should I use non-ASCII characters in my password?

пароль

=

пароль

=

%26%231087%3B%26%231072%3B%26%231088%3B
%26%231086%3B%26%231083%3B%26%231100%3B

Should I use non-ASCII characters in my password?

пароль

=

пароль

=

%26%231087%3B%26%231072%3B%26%231088%3B
%26%231086%3B%26%231083%3B%26%231100%3B

$6 \rightarrow 42 \rightarrow 78$

Should I use non-ASCII characters in my password?

пароль

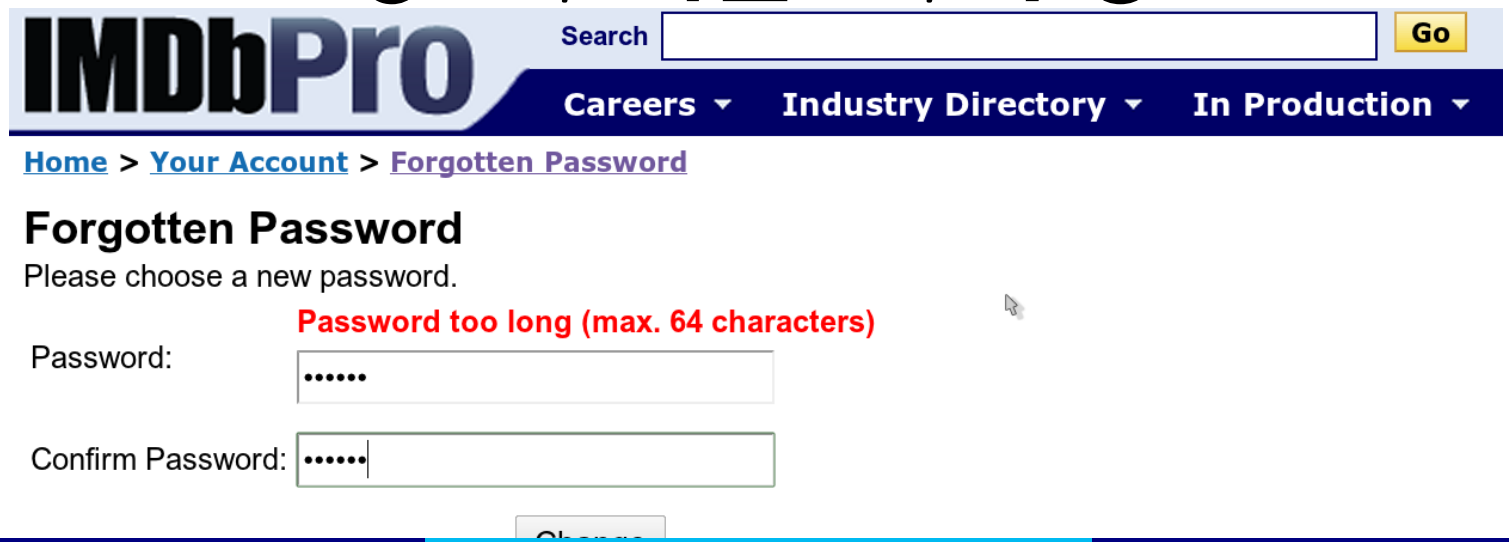
=

пароль

=

%26%231087%3B%26%231072%3B%26%231088%3B
%26%231086%3B%26%231083%3B%26%231100%3B

$6 \rightarrow 42 \rightarrow 78$



Is this table legible?

Category	Scheme	Described in section	Reference	*Memory-wise-Effortless*	*Scalable-for-users*	*Nothing-to-Carry*	*Manually-Effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*	*Accessible*	*Negligible-Cost-per-User*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-Observ*	*Resilient-to-Targeted-Impers*	*Resilient-to-Throttled-Guessi*	*Resilient-to-Unthrottled-Gues*	*Resilient-to-Internal-Observa*	*Resilient-to-Leaks-from-Othe*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]	○	●	○	●	●	○	●	●	●	●	●	●	●	●	○	○	○	○	○	○	○	●	●	●	●
Password managers	Firefox	IV-A1		◎	◎	◎	◎	●	●	◎	○	●	●	●	○	●	●	◎	○	○	○	○	○	○	◎	●	●	●	●
	LastPass	IV-A2		◎	◎	◎	◎	●	●	◎	○	●	◎	●	○	●	○	◎	○	○	◎	◎	○	◎	◎	●	○	●	●
Proxy	URRSA	IV-B1	[5]	◎	○	○	○	●	○	◎	○	◎	●	◎	●	○	○	○	○	○	○	○	○	◎	◎	○	○	●	●
	Impostor	??	[21]	○	◎	●	○	●	○	○	●	○	○	●	●	○	●	◎	○	○	○	○	○	◎	◎	●	○	○	●
Federated	OpenID	IV-C1	[25]	◎	◎	●	◎	○	●	●	●	●	●	○	●	●	●	◎	○	◎	◎	○	●	○	●	◎	●	○	○
	MS Passport	IV-C2	[29]	◎	◎	●	◎	●	●	●	●	●	○	○	●	●	○	◎	○	◎	◎	○	●	○	●	○	●	○	○
	FBConnect	IV-C3	[31]	◎	◎	●	◎	●	●	●	●	●	●	○	●	●	○	◎	○	◎	◎	○	●	○	●	○	○	○	○
	BrowserID	IV-C4	[33]	◎	◎	●	◎	●	●	●	●	●	●	○	◎	●	●	◎	○	◎	◎	○	●	○	●	○	●	○	○
	OTP over email	IV-C5	[37]	◎	◎	●	○	●	○	●	●	●	●	○	●	●	●	◎	○	○	◎	◎	○	●	●	●	○	●	○
Graphical	PCCP	IV-D1	[7]	○	○	●	○	●	◎	○	●	◎	●	○	●	●	●	○	●	◎	○	○	●	●	●	●	●	●	●
	PassGo	IV-D2	[93]	○	○	●	○	●	◎	○	●	◎	●	○	●	●	◎	○	●	○	○	○	○	○	●	●	●	●	●
Cognitive	GridSure	IV-E1	[51]	○	○	●	○	●	◎	○	●	◎	●	○	●	○	○	○	●	○	○	○	○	○	○	●	●	●	●
	Weinshall	??	[47]	○	○	●	○	○	○	○	○	○	●	○	●	○	●	◎	○	○	○	○	●	●	●	●	●	●	●
	Hopper Blum	??	[48]	○	○	●	○	○	○	○	○	○	●	○	●	○	●	◎	○	○	○	○	●	●	●	●	●	●	●
	Word Association	??	[50]	○	○	●	○	●	●	○	●	●	●	○	●	◎	●	○	○	○	○	○	○	○	●	●	●	●	●
Paper tokens	OTPW	IV-F1	[54]	○	○	○	○	●	○	○	●	◎	●	○	○	●	●	○	●	●	●	●	●	●	●	●	●	●	●
	S/KEY	IV-F2	[53]	●	○	○	○	●	○	○	●	◎	●	○	○	●	●	○	●	●	●	●	●	◎	○	●	●	●	●
	PIN+TAN	IV-F3	[56]	○	○	○	○	●	○	○	●	◎	◎	○	○	●	●	○	●	●	●	●	●	●	●	●	●	●	●
Visual crypto	PassWindow	IV-G1	[61]	●	○	○	○	○	○	○	○	○	◎	○	○	●	●	◎	●	●	●	●	●	●	○	●	●	●	●
Hardware tokens	RSA SecurID	IV-H1	[63]	◎	◎	○	○	●	◎	○	○	◎	○	○	○	●	●	●	●	●	●	●	●	●	●	◎	○	●	○
	Yubikey	IV-H2	[65]	○	○	○	○	●	●	○	○	●	○	○	○	●	◎	●	●	●	●	●	●	●	●	○	○	●	●
	Ironkey	IV-H3	[67]	◎	◎	○	◎	◎	◎	○	◎	●	○	●	○	●	○	●	○	○	○	◎	○	●	●	●	●	●	●
	CAP reader	IV-H4	[68]	○	○	○	○	○	◎	○	○	◎	○	○	○	●	○	●	●	●	●	●	●	●	●	●	●	●	●
	Pico	IV-H5	[8]	●	●	○	●	○	●	●	●	○	○	○	○	○	●	●	●	●	●	●	●	●	●	●	●	●	●
Phone-based	Phoolproof	IV-I1	[70]	○	○	◎	○	●	●	○	○	●	◎	◎	○	○	●	●	●	●	●	●	●	●	●	●	●	●	●
	Cronto	IV-I2		○	○	◎	○	●	●	○	◎	●	●	○	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●
	MP-Auth	IV-I3	[6]	◎	◎	◎	○	●	○	○	●	◎	◎	○	○	○	●	●	○	○	○	○	○	○	●	●	●	●	○
	OTP over SMS	IV-I4		●	●	◎	○	●	○	○	○	◎	○	○	●	●	●	●	○	●	●	●	●	●	●	●	○	●	●
	Google 2-Step	IV-I5	[73]	○	○	○	◎	●	◎	○	◎	◎	◎	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Biometric	Fingerprint	IV-J1	[75]	●	●	◎	◎	●	◎	○	○	◎	◎	○	○	○	◎	●	○	●	●	○	○	○	○	○	●	●	○
	Iris	IV-J2	[76]	●	●	●	◎	●	◎	○	○	◎	◎	○	○	○	◎	●	○	●	●	○	○	○	○	○	●	◎	○
	Voice	IV-J3	[77]	●	●	●	◎	●	◎	○	○	◎	○	●	○	◎	◎	●	○	●	◎	○	○	○	○	○	●	●	○
Recovery	Personal knowledge	IV-K1	[83]	◎	○	●	○	●	●	○	●	◎	●	○	●	●	●	○	○	○	○	○	○	○	●	●	●	●	●
	Preference-based	IV-K2	[91]	◎	○	●	○	●	◎	●	●	◎	●	○	●	○	○	○	○	○	○	○	○	○	●	●	●	●	●
	Social re-auth.	??	[94]	○	○	●	○	●	○	●	○	●	●	○	●	●	●	◎	○	○	○	○	◎	●	●	●	○	●	◎

Was this talk funny enough?

jcb82@cl.cam.ac.uk