

Passwords In The Internet Age

what, how, and why - a practical guide

Jim Salter

Mercenary Sysadmin,
Small Business Owner



Today's slides can be found at:

<http://openoid.net/presentations/>

Passwords are much, *much* older than the internet.



The password was originally
only a *layer* of security!



... and there were *severe* consequences for attackers.



We use passwords *very* differently these days.



There's little or no penalty for trying to “game” the password.

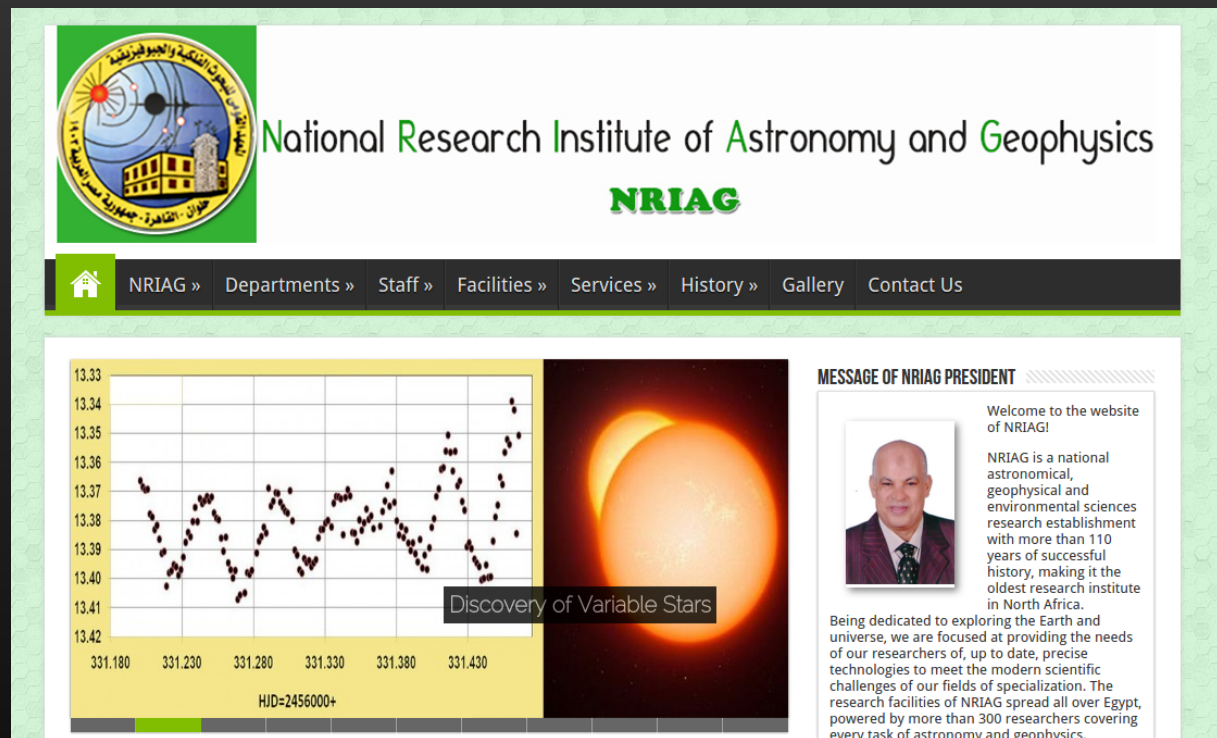
```
Oct 26 11:04:41 web sshd[1769]: Failed password for nagios
from 123.59.55.83 port 55046 ssh2
Oct 26 11:04:41 web sshd[1769]: Received disconnect from
123.59.55.83: 11: Bye Bye [preauth]
Oct 26 11:06:37 web sshd[1787]: Did not receive
identification string from 123.59.55.83
Oct 26 11:08:30 web sshd[1906]: pam_unix(sshd:auth):
authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=123.59.55.83 user=nagios
Oct 26 11:08:33 web sshd[1906]: Failed password for nagios
from 123.59.55.83 port 46835 ssh2
Oct 26 11:08:33 web sshd[1906]: Received disconnect from
123.59.55.83: 11: Bye Bye [preauth]
Oct 26 11:09:09 web sshd[1931]: Connection closed by
173.230.137.22 [preauth]
23189 total attempts since Oct 25 06:46:59
root@web:~#
```

There's not even much risk of *exposure* for the attacker.

```
Oct 26 04:53:09 web sshd[27794]: Failed password for invalid user david from
195.43.6.9 port 41981 ssh2
Oct 26 04:53:13 web sshd[27796]: Failed password for invalid user scanner from
195.43.6.9 port 44191 ssh2
Oct 26 04:53:17 web sshd[27798]: Failed password for invalid user webmaster from
195.43.6.9 port 46916 ssh2

root@web:~# host 195.43.6.9
9.6.43.195.in-addr.arpa domain name pointer mail.nriag.sci.eg.

root@web:~# dig +short mail.nriag.sci.eg
195.43.6.9
```



The screenshot displays the homepage of the National Research Institute of Astronomy and Geophysics (NRIAG). The header features the institute's logo on the left and the text "National Research Institute of Astronomy and Geophysics" and "NRIAG" in green. A navigation menu below the header includes links for Home, NRIAG, Departments, Staff, Facilities, Services, History, Gallery, and Contact Us.

The main content area is divided into two sections. On the left, a scatter plot titled "Discovery of Variable Stars" shows a fluctuating line graph with data points. The y-axis ranges from 13.33 to 13.42, and the x-axis shows star IDs: 331.180, 331.230, 331.280, 331.330, 331.380, and 331.430. Below the x-axis, it specifies "HJD=2456000+". To the right of the graph is a large, glowing orange and red image of a star or celestial body.

On the right side of the main content area, there is a section titled "MESSAGE OF NRIAG PRESIDENT". It includes a small portrait of a man in a suit and a welcome message: "Welcome to the website of NRIAG!". Below the portrait, the text reads: "NRIAG is a national astronomical, geophysical and environmental sciences research establishment with more than 110 years of successful history, making it the oldest research institute in North Africa." The final paragraph states: "Being dedicated to exploring the Earth and universe, we are focused at providing the needs of our researchers of, up to date, precise technologies to meet the modern scientific challenges of our fields of specialization. The research facilities of NRIAG spread all over Egypt, powered by more than 300 researchers covering every task of astronomy and geophysics."

The dialog we *all* dread

Microsoft Office Excel



The password supplied does not meet the minimum complexity requirements.
Please select another password that meets all of the following criteria:

Does not include your account name

contains at least three of the following four character groups:

Uppercase characters (A through Z)

Lowercase characters (a through z)

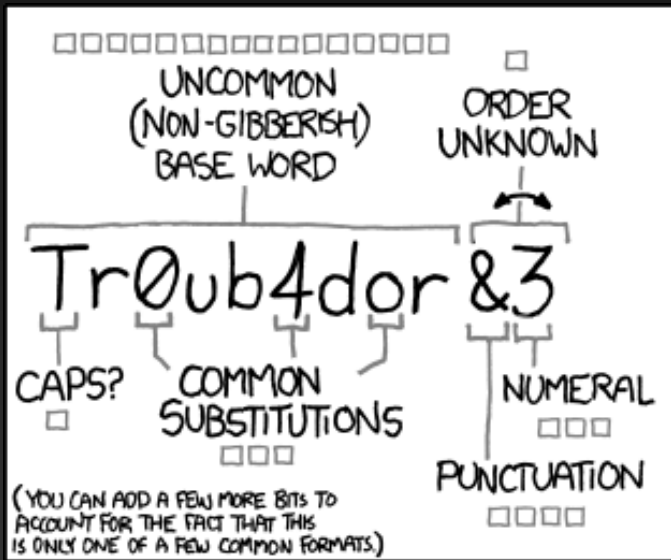
Numerals (0 through 9)

Non-alphabetic characters (such as !, \$, #, %)

OK

[Was this information helpful?](#)

Let's talk about entropy.



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

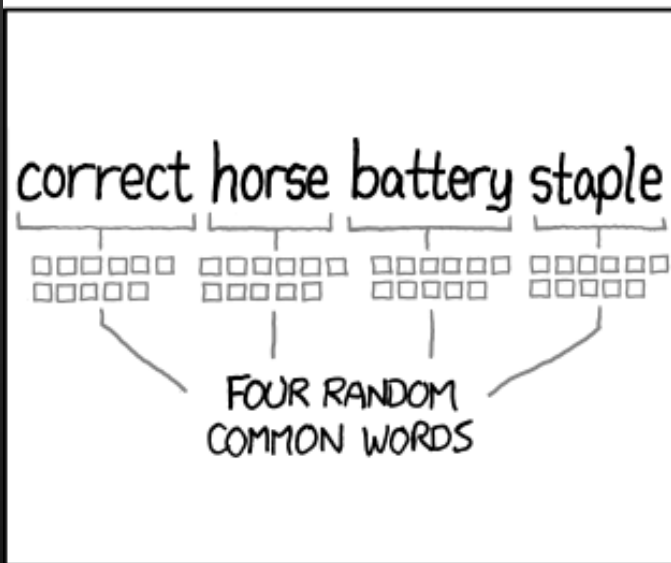
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS:
EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER:
HARD



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS:
HARD

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

So let's get back to entropy.

www.zdnet.com/article/25-gpus-devour-password-hashes-at-up-to-348-billion-per-second/

$3.65615844 \times 10^{15}$ possible four-word Diceware passphrases

~~ same entropy as 8 random chars using FULL typeable set

Offline brute force (SHA1) succeeds in 16 hours

Online brute force succeeds in 115,936 years
... at *1,000 tries/sec!*

**There's no WAY I can remember
so many different passwords!**

**Diceware makes it easier than you'd think, but
yes, you're going to need some backup.**

Browser-integrated password manager? **NO.**

Oldschool little black book? **OK, actually :)**

Offline, mobile-capable manager: **YES!**



KeepPass

But I LIKE my browser-integrated password manager!

What happens when you don't have it available?

What if the company goes out of business?

What if a malicious site tricks it into divulging passwords?

Keep it offline, keep it away from the web.



KeepPass

Securing your secure DB

What if you forget your *KeePass* passphrase?

Option 1: it's just one passphrase... so, you know, *don't forget it.*

Option 2: paper backup, preferably in an *extremely* safe place

Keep it offline, keep it away from the web.



KeePass

Thinking in “rings”

Ring 4: “one time” signups

Ring 3: “hobby/social” sites / services

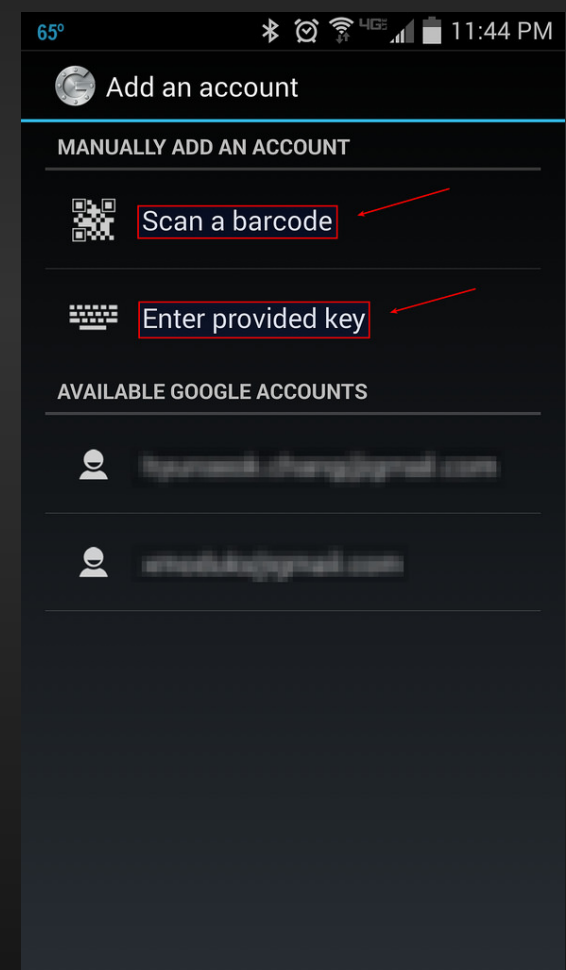
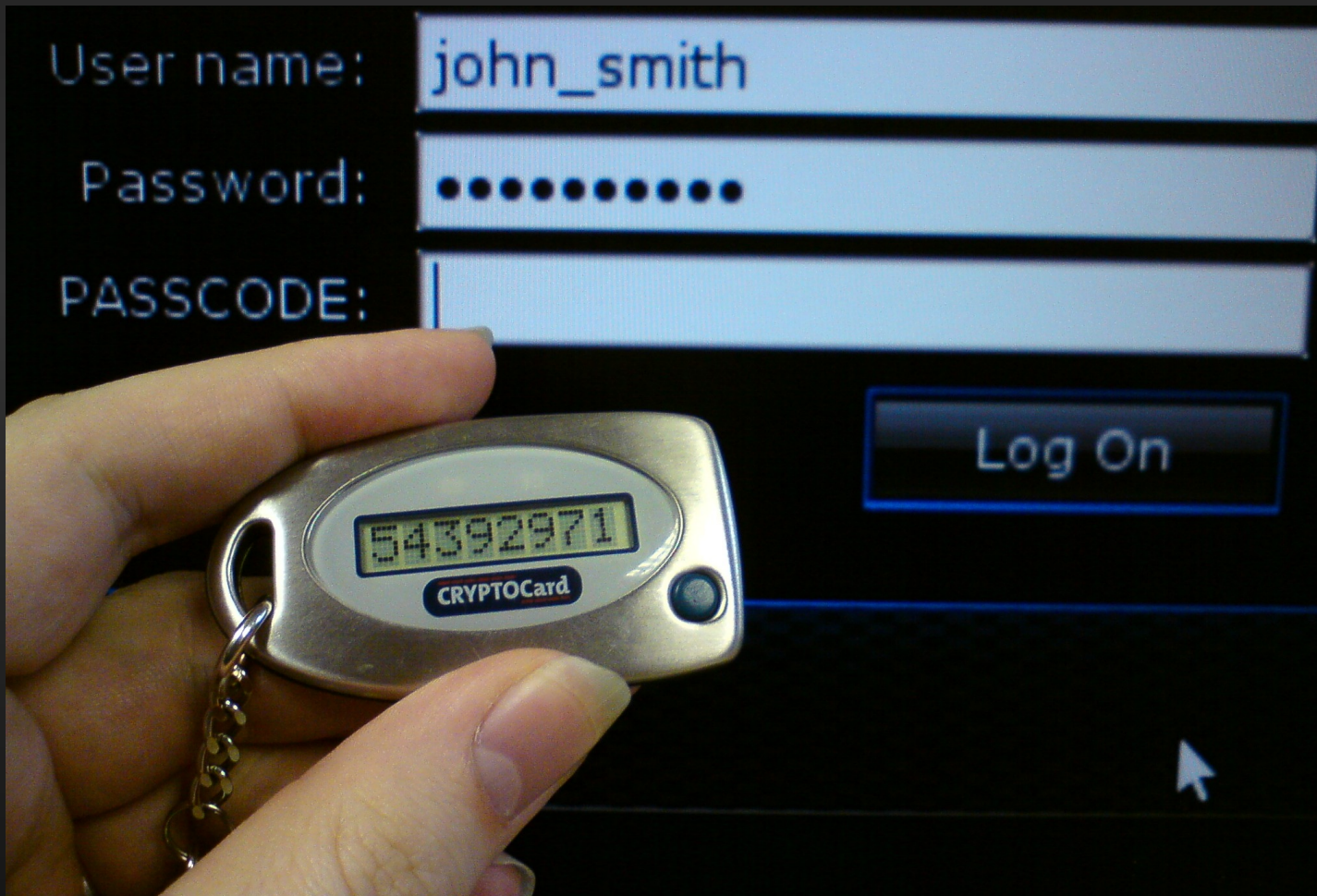
Ring 2: “professional” sites/services

Ring 1: “money” sites/services

Ring 0: **primary email account**

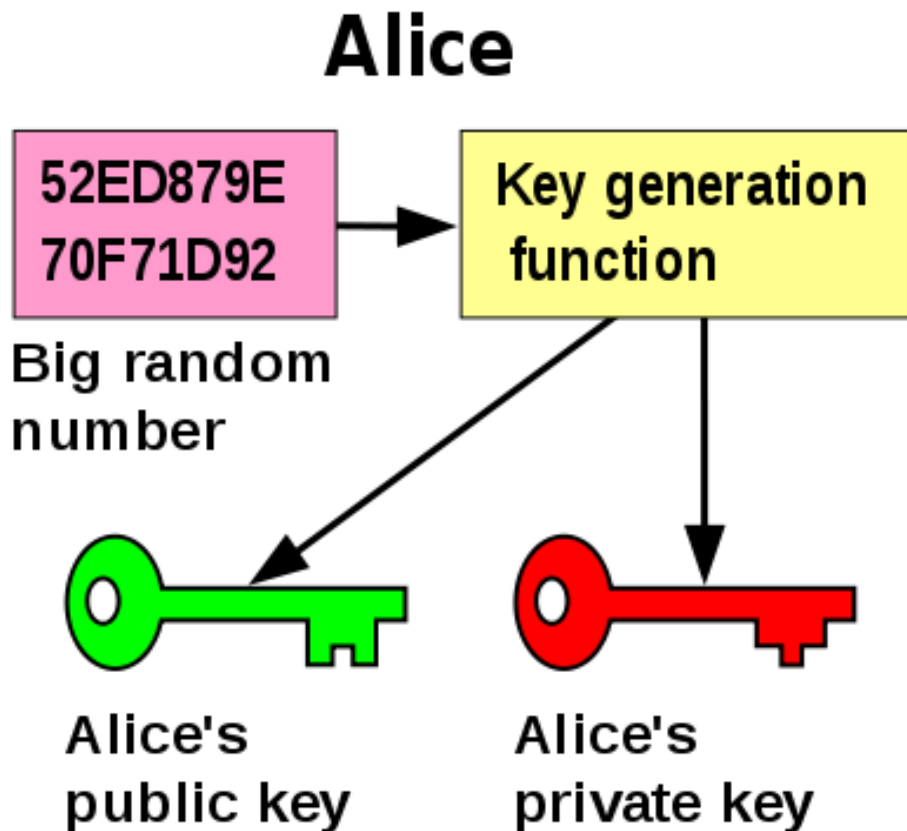
Adding Extra Layers

Two-factor authentication



Beyond Passwords

Public/Private Key Pair Encryption



Encrypt with public key
Decrypt with private key

Public key is **PUBLIC!**
Private key is **PRIVATE!**

Safely use same private key *everywhere*

In The Real World

Public/Private Key Pair Encryption



Each Estonian citizen is provided with a crypto keypair instead of an SSN.



The public key is printed on their government ID.



Questions?

Comments?

Angry denunciations?



OPENAI