

Cyber Security



How can we keep our data secure?

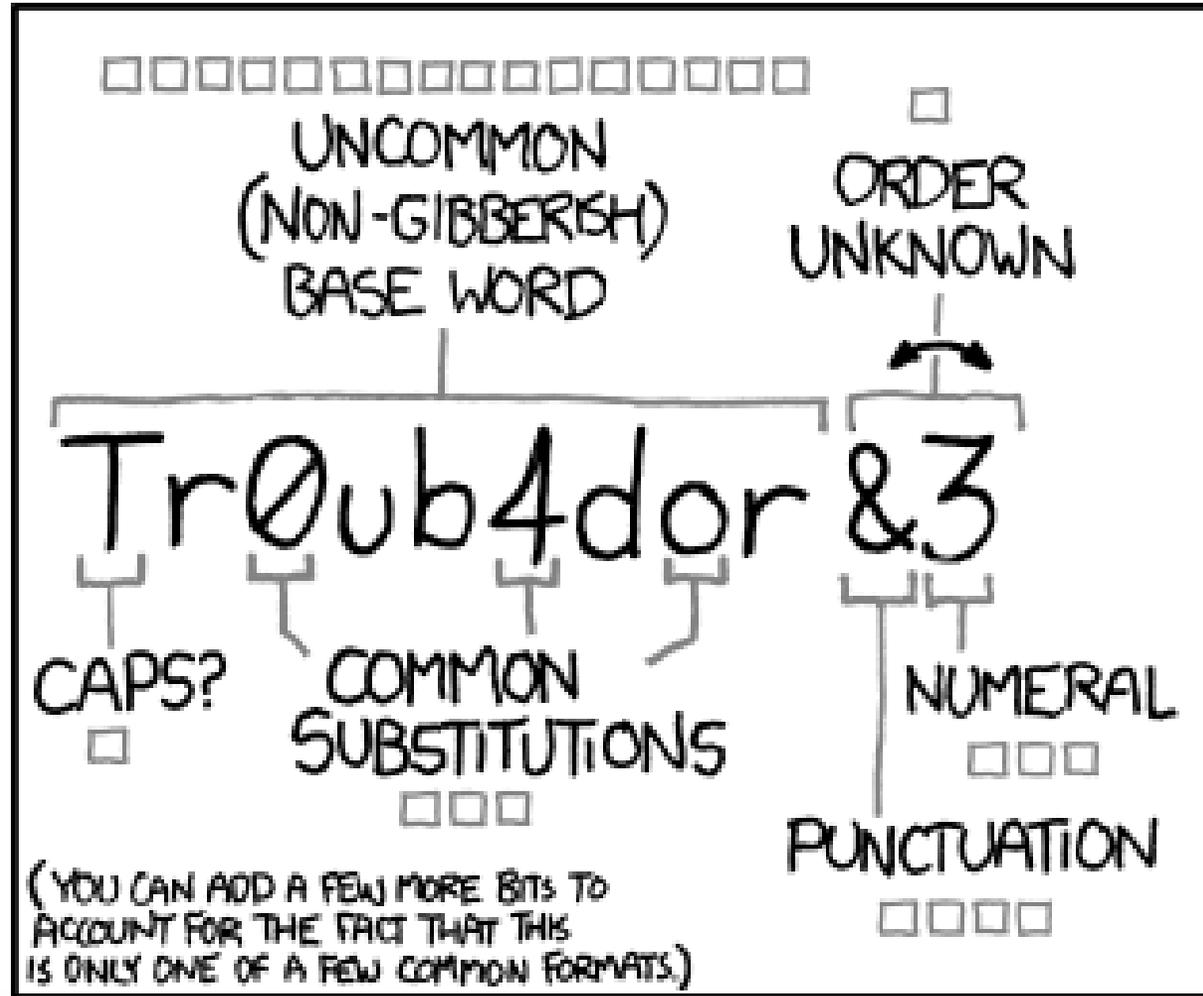


Put your white hat on

Authentication

- **Ownership** Factors - something the user *has*
- **Knowledge** Factors - something the user *knows*
- **Inherence** Factors - something the user *is*

Passwords



Cracking Passwords – Brute Force

- aaaaaa
- aaaaab
- aaaaac
- aaaaad
- aaaaae
- aaaaaf
- aaaaag

- aaaaah
- aaaaai
- aaaaaj
- aaaaak
- aaaaal
- aaaaam
- aaaaan

- aaaaao
- aaaaap
- aaaaaq
- aaaaar
- aaaaas
- aaaaat
- aaaaau

Rainbow Tables

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou
11. princess
12. admin
13. welcome
14. 666666
15. abc123
16. football
17. 123123
18. monkey
19. 654321
20. !@#\$%^&*
21. charlie
22. aa123456
23. donald
24. password1
25. qwerty123

Password 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

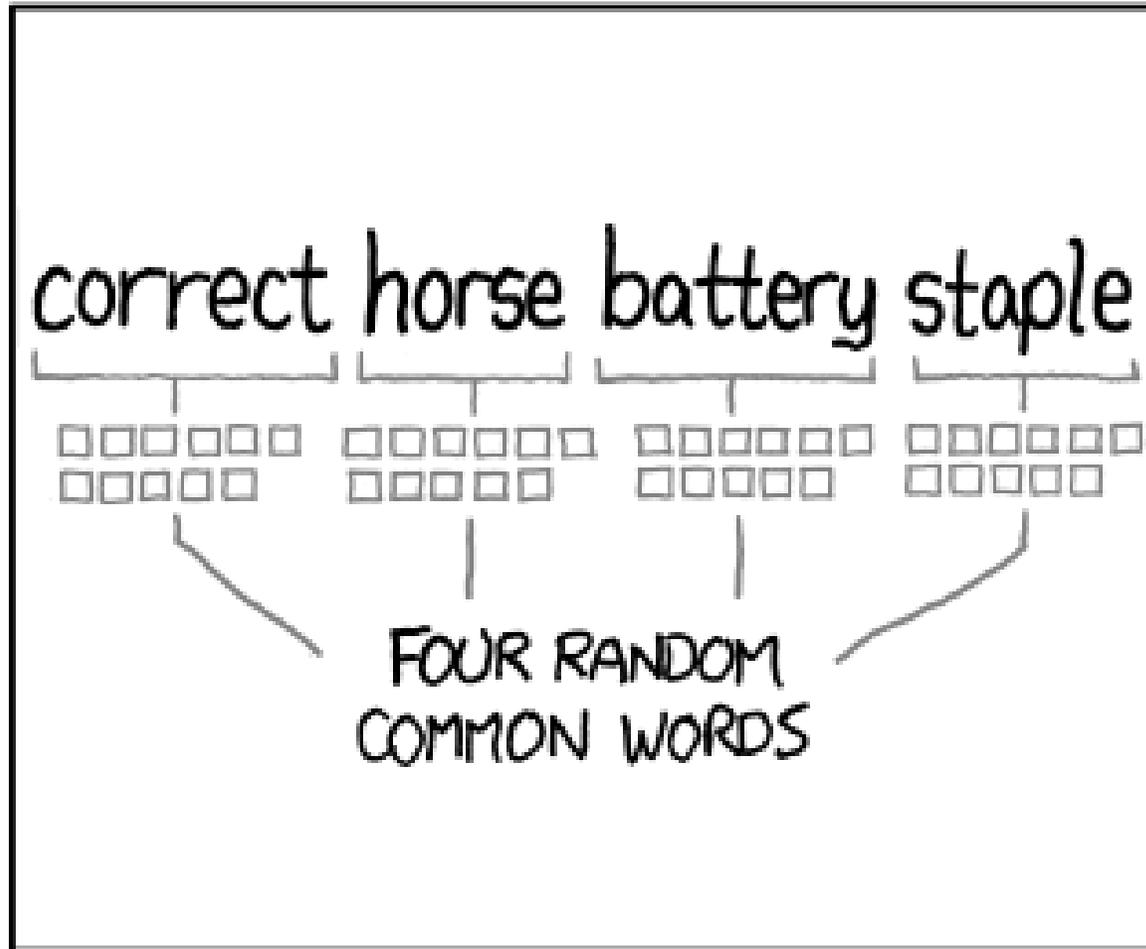
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O's WAS A ZERO?

AND THERE WAS SOME SYMBOL...



DIFFICULTY TO REMEMBER:
HARD

Password Entropy



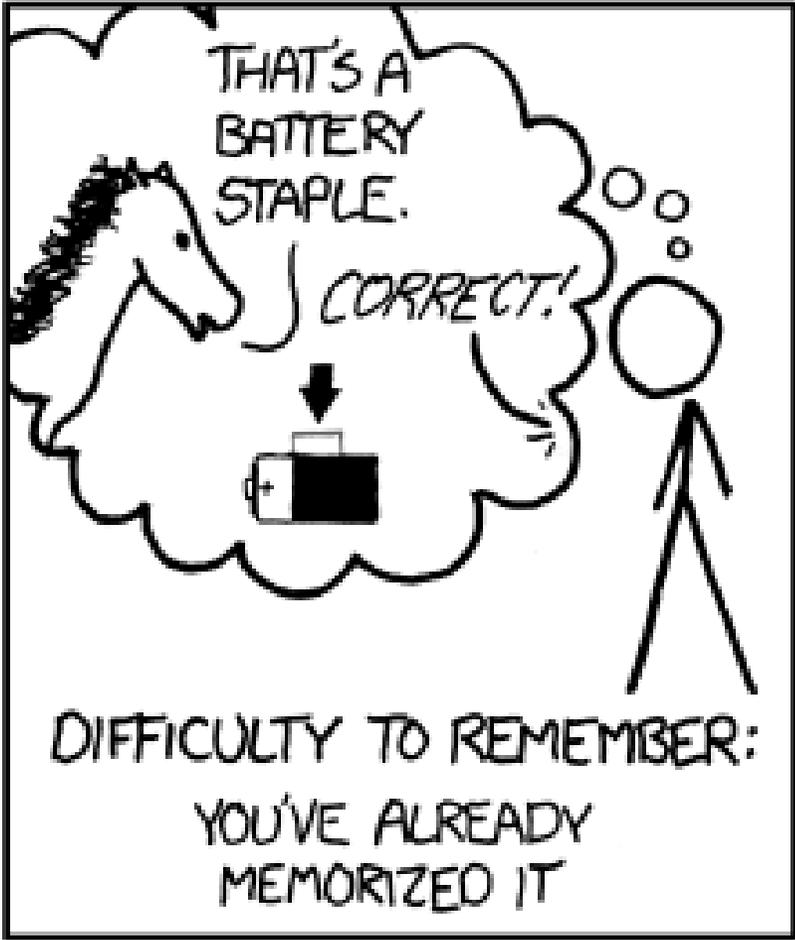
Password Entropy

~ 44 BITS OF ENTROPY

□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□

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

DIFFICULTY TO GUESS:
HARD



THAT'S A
BATTERY
STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER:
YOU'VE ALREADY
MEMORIZED IT

Storing Passwords Securely

Store the password itself

- Needed to compromise: database access
- Accounts compromised: all
- Relative ease: simple

Storing Passwords Securely

Encrypt all passwords with a key

- Needed to compromise: database & key (or lookup table)
- Accounts compromised: all
- Relative ease: medium

Password Salt

- Random data added to a password before hashing
- Protects against dictionary and rainbow table attacks
- Ensures the password is long enough to be hard to crack

Storing Passwords Securely

Encrypt all passwords with a global salt value

- Needed to compromise: database, encryption key & salt value
- Accounts compromised: all
- Relative ease: harder

Storing Passwords Securely

Encrypt all passwords with a unique salt value

- Needed to compromise: database, encryption key & salt value
- Accounts compromised: one at a time
- Relative ease: really hard

[MD5 Hash](#)

HACKERS RECENTLY LEAKED 153 MILLION ADOBE USER EMAILS, ENCRYPTED PASSWORDS, AND PASSWORD HINTS.

ADOBE ENCRYPTED THE PASSWORDS IMPROPERLY, MISUSING BLOCK-MODE 3DES. THE RESULT IS SOMETHING WONDERFUL:

USER	PASSWORD	HINT	
4e18acc1ab27a2d6		WEATHER VANE SWORD	<input type="text"/>
4e18acc1ab27a2d6			<input type="text"/>
4e18acc1ab27a2d6	a0a2876eb1ea1fca	NAME 1	<input type="text"/>
8babbb6299e06eb6d		DUH	<input type="text"/>
8babbb6299e06eb6d	a0a2876eb1ea1fca		<input type="text"/>
8babbb6299e06eb6d	85e9da81a8a78adc	57	
4e18acc1ab27a2d6		FAVORITE OF 12 APOSTLES	
1ab29ae86dabe5ca	7a2d6a0a2876eb1e	WITH YOUR OWN HAND YOU HAVE DONE ALL THIS	
a1f9b2b6299e7a2b	e0dec1e6ab797397	SEXY EARLOBES	<input type="text"/>
a1f9b2b6299e7a2b	617ab027727ad85	BEST TOS EPISODE	<input type="text"/>
39738b7adb0b8af7	617ab027727ad85	SUGARLAND	
1ab29ae86dabe5ca		NAME + JERSEY #	
877ab7889d3862b1		ALPHA	<input type="text"/>
877ab7889d3862b1			<input type="text"/>
877ab7889d3862b1			<input type="text"/>
877ab7889d3862b1		OBVIOUS	<input type="text"/>
877ab7889d3862b1		MICHAEL JACKSON	<input type="text"/>
38a7c9279c0deb44	9dca1d79d4dec6d5		<input type="text"/>
38a7c9279c0deb44	9dca1d79d4dec6d5	HE DID THE MASH, HE DID THE	<input type="text"/>
38a7c9279c0deb44		PURLAINED	<input type="text"/>
a8ae5745a7b7af7a	9dca1d79d4dec6d5	FAV. LATER-3 POKEMON	<input type="text"/>

THE GREATEST CROSSWORD PUZZLE
IN THE HISTORY OF THE WORLD

How Secure is your Password?

<https://howsecureismypassword.net/>

Social Engineering

Using techniques to compromise a system by exploiting the users directly instead of the system's security



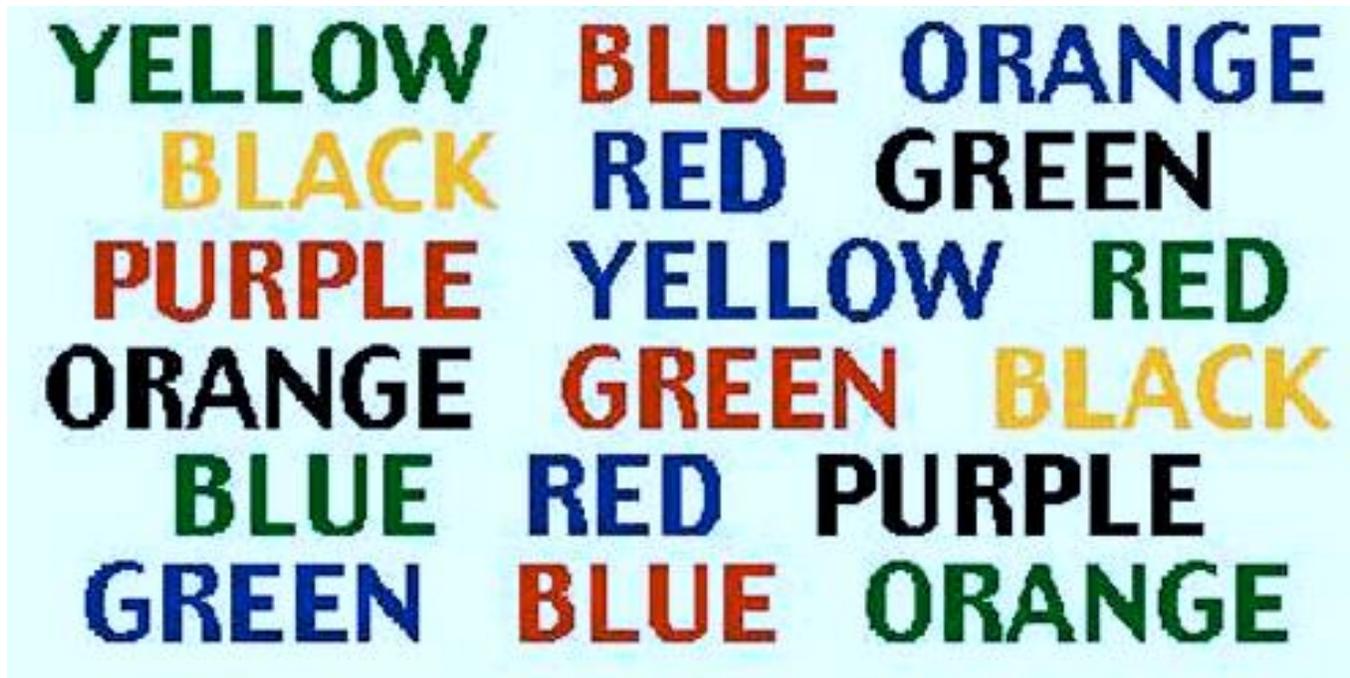
Pretexting



Impersonation



Human Buffer Overflow



YELLOW	BLUE	ORANGE
BLACK	RED	GREEN
PURPLE	YELLOW	RED
ORANGE	GREEN	BLACK
BLUE	RED	PURPLE
GREEN	BLUE	ORANGE

QUIDPROQUO

This for that.

Phishing

KSU.EDU WEBMAIL TEAM SUPPORT UPDATE/MAINTENANCE OF USER ACCOUNT

© Kansas State University WEBMAIL TEAM <accountupgrade@ksu.edu>

Extra line breaks in this message were removed.

Sent: Thu 4/4/2013 12:51 AM

To: undisclosed-recipients:

DEAR KSU.EDU USER,

Due to the congestion in all ksu.edu users and removal of all ksu.edu Accounts, © Kansas State University will be shutting down all unused Accounts.

We will be conducting our regularly scheduled maintenance, to ensure that we provide the highest connectivity and services to customers. Your connectivity and services with us may be interrupted for a short period of time during this maintenance window. We will also ensure minimal disruption to services where possible.

In order to enable us perform quality maintenance on your Internet access and e-mail service, please reply to this mail message confirming your ksu.edu account details with us.

Do confirm your account details below.

-
1. First Name & Last Name:
 2. Full Login Email Address:
 3. Username:
 4. Password:
 5. Retype Password:
 6. eID :
-

419 Scams

Hello Dear,

My name is Mrs Simone Gbagbo the wife of Laurent Gbagbo. the president of Cote d'Ivoire. I decided to contact you because of the prevailing financial report of war in our country Cote d'Ivoire in Abidjan which have kill many people in our country and the intense nature of politics in Africa.

This is to inform you that i realized some reasonable amount of money from various deals that I successfully executed. Well i secretly put in a box the sum of \$7,000,000 million US dollars (Seven million United states dollars) and deposit it in a security company abroad.

I am contacting you because I want you to help me in securing the money for the future of my children. I hope to trust you as who will not sit on this money when you claim it. i will give you 25% of the total money for your assistance. if you are willing to help me.

All you need to do now is to send to me:

1. Name in full:.
2. Address:.....
3. Nationality:..
4. Age/Sex :.....
5. Occupation:...
6. Phone/Cell:....
7. Country:.....

Note: The security company does not know the real contents of the box, the content was declared to be Sensitive Photographic Film Materials. If you are interested please reply me through this my private email address (mrs.gbagbo37@yahoo.com) for more details.

Best Regards,
Mrs.Simone Gbogbo

Baiting



Threats



Combat Social Engineering

- User Training
- Security Protocols and Audits
- Always Questioning Everything
- Penetration Testing
- Properly Disposing of Garbage

Social Engineering in Practice

- "Capture the Flag" style contest
- Contestant try to gain information about companies via the internet
- Using that information, they call the company and attempt to gain more information flags for points

[Read the Report](#)