



SIX-DIGIT ICT DISASTER

COME PREVENIRLI EVITANDO I CONSEGUENTI DANNI DI
BUSINESS A 6 ZERI

“SECURE CODING” & PASSWORD STORAGE TECNICHE DI
PREVENZIONE DEI RISCHI DI SICUREZZA



Whoami

David Calligaris

- Head of security consulting at Emaze
- **Contact:** david.calligaris@emaze.net

Introduction

Why bothering about password?

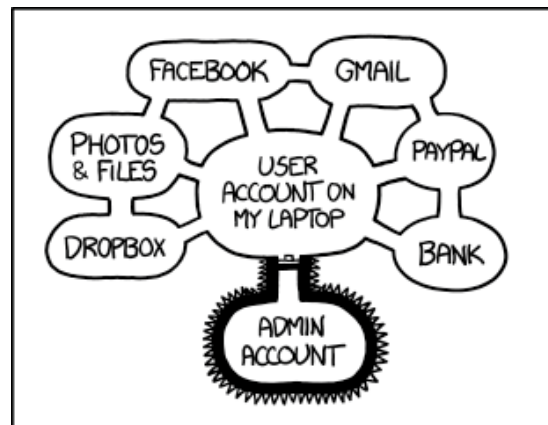


- Passwords (and authentication in general) are the main defense against **personification** attacks
 - Authentication is one the main building blocks of our “digital” lives, both personal and professional

Why bothering about password?

- Passwords (and authentication in general) are the main defense against **personification** attacks
 - Authentication is one the main building blocks of our “digital” lives, both personal and professional

What happens if someone steals your “favorite” password?



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS, BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

Why haven't we solved this yet?



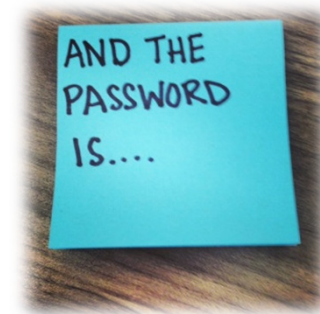
- In our professional experience, about 90% of the systems we exploit are accessed using **weak or default passwords**
 - What are the reasons behind this problem?

Why haven't we solved this yet?

- In our professional experience, about 90% of the systems we exploit are accessed using **weak or default passwords**
 - What are the reasons behind this problem?

People are **lazy**, and try to simplify their lives as much as possible

- Simple passwords are easy to remember

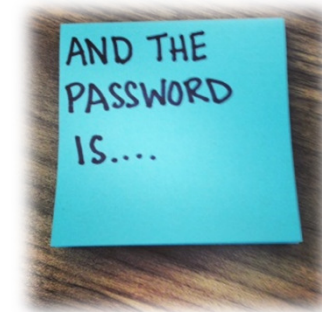


Why haven't we solved this yet?

- In our professional experience, about 90% of the systems we exploit are accessed using **weak or default passwords**
 - What are the reasons behind this problem?

People are **lazy**, and try to simplify their lives as much as possible

- Simple passwords are easy to remember



Systems are getting more and more **sophisticated**

- A single weak password is enough to compromise the whole infrastructure

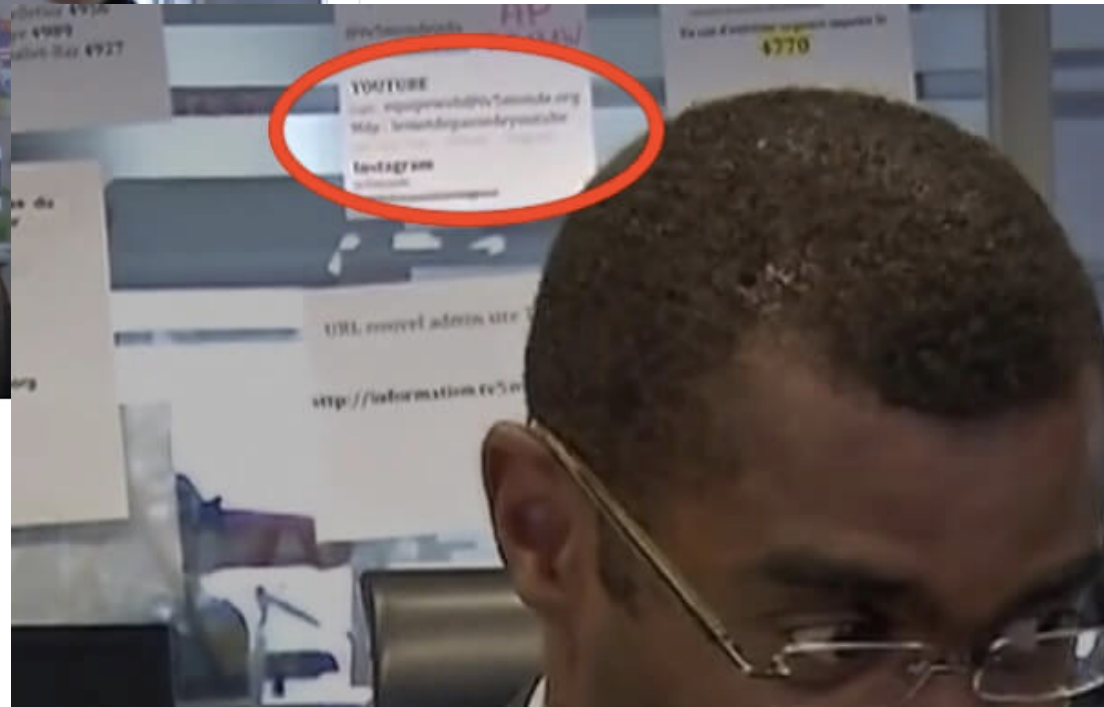
Case Study #1

Hacked French network exposed its own passwords during TV interview

Post-it note on wall revealed network's passwords for YouTube, Instagram.

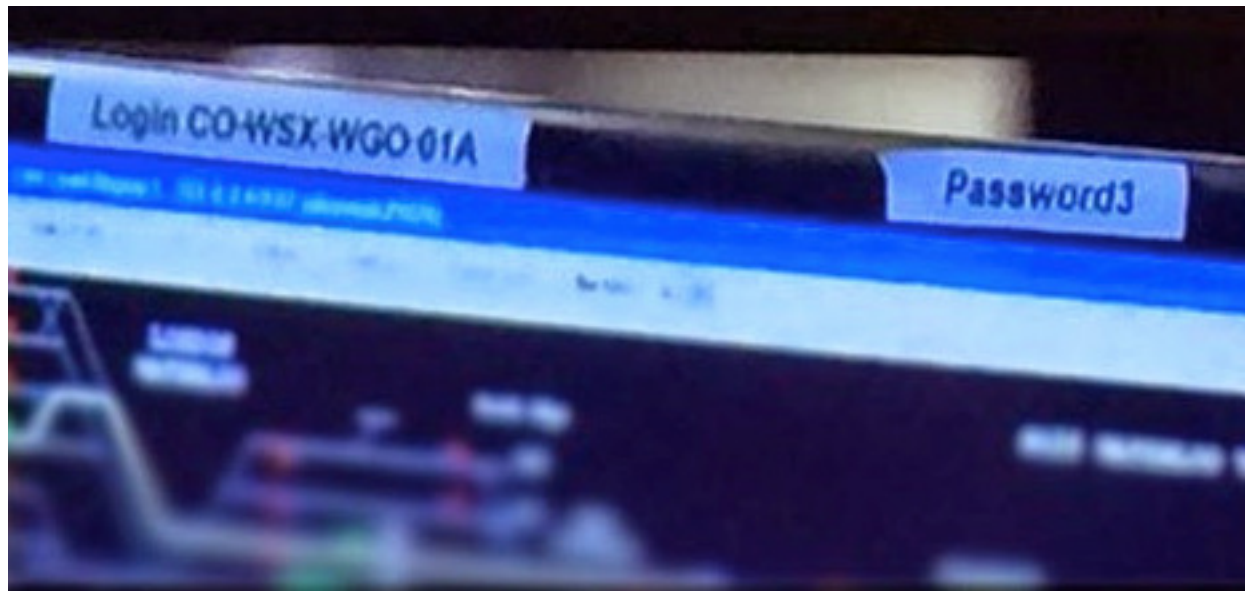
by Sam Machkovech - Apr 10, 2015 3:37am CEST

Share Tweet 110



Case Study #2

- London Railway System Password Exposed in TV Documentary



Other authentication mechanisms



A screenshot of a CNET news article. The header includes the CNET logo, a search bar, and navigation links for Reviews, News, and Video. The article title is "Gates predicts death of the password" by Munir Kotadia, dated February 25, 2004. A "Related Stories" box highlights a story about security at an RSA show, with a snippet of text: "SAN FRANCISCO—Microsoft Chairman Bill Gates predicted the demise of the traditional password because it cannot 'meet the challenge' of keeping critical information secure."

- Why don't we move to **other** authentication mechanisms?
 - Two-factor authentication is becoming quite common for key services
 - Other mechanisms (e.g., biometrics) are not so widespread
- ...in the meantime, passwords are anything but dead 😊

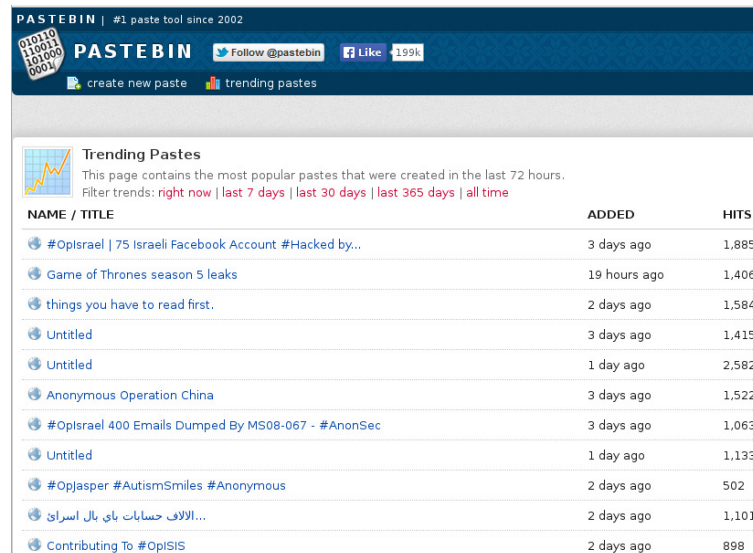
The rise of data leaks

- **Data leakages** are an (illicit) practice that is becoming more and more common
 - Someone (often “*hacktivists*”) compromises an Internet-facing server
 - Attacks typically rely on trivial vulnerabilities (e.g., Internet-wide scans)
 - Attackers dump accessible DBs and publish their contents on the Internet
- In 2014, several **big companies** were affected by data breaches
 - JPMorgan, ~80M personal accounts and 7M SME accounts
 - Apple, hundreds of “celebrity” accounts compromised
 - Target, 110M record exposed
 - eBay, 145M users affected
 - ...



The rise of data leaks

- **Data leakages** are an (illicit) practice that is becoming more and more common
 - Someone (often “*hacktivists*”) compromise an Internet-facing server
 - Attacks typically rely on trivial vulnerabilities (e.g., Internet-wide scans)
 - Attackers dump accessible DBs and publish their contents on the Internet

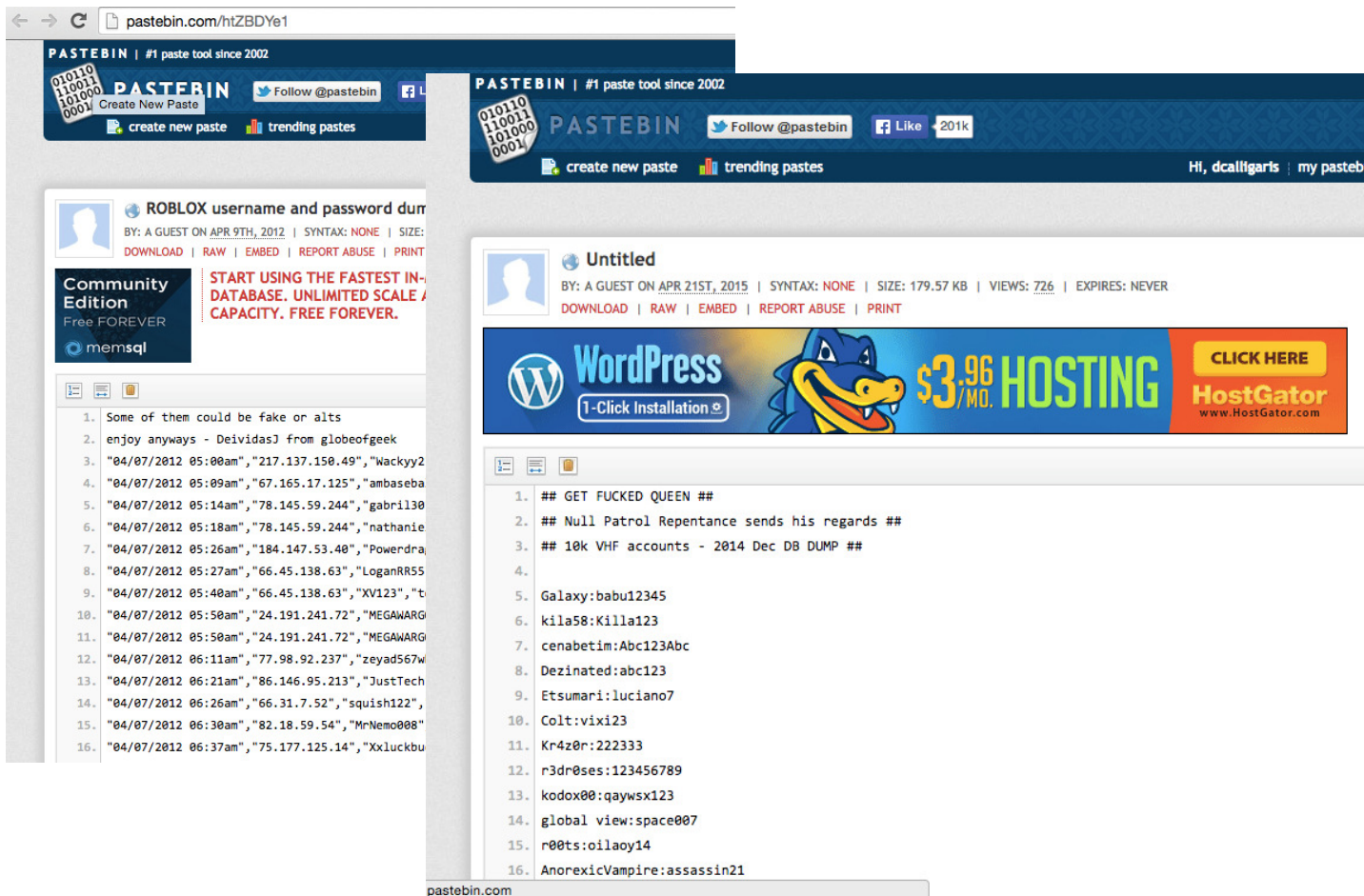


The screenshot shows the Pastebin website interface. At the top, it says 'PASTEBIN | #1 paste tool since 2002'. Below that, there are social media links for 'Follow @pastebin' and 'Like 199k'. The main content area is titled 'Trending Pastes' and includes a sub-header: 'This page contains the most popular pastes that were created in the last 72 hours. Filter trends: right now | last 7 days | last 30 days | last 365 days | all time'. Below this is a table with three columns: 'NAME / TITLE', 'ADDED', and 'HITS'.

NAME / TITLE	ADDED	HITS
#Opisrael 75 Israeli Facebook Account #Hacked by...	3 days ago	1,885
Game of Thrones season 5 leaks	19 hours ago	1,406
things you have to read first.	2 days ago	1,584
Untitled	3 days ago	1,415
Untitled	1 day ago	2,582
Anonymous Operation China	3 days ago	1,522
#Opisrael 400 Emails Dumped By MS08-067 - #AnonSec	3 days ago	1,063
Untitled	1 day ago	1,133
#Opjasper #AutismSmiles #Anonymous	2 days ago	502
الالاف حسابات باي بال اسرئ...	2 days ago	1,101
Contributing To #OpISIS	2 days ago	898

It is quite **difficult** to estimate the *real size* of this phenomenon

The rise of data leaks



PASTEBIN | #1 paste tool since 2002

ROBLOX username and password dump
BY: A GUEST ON APR 9TH, 2012 | SYNTAX: NONE | SIZE: [unreadable]
DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

Community Edition
Free FOREVER
memsql

START USING THE FASTEST IN-DATABASE. UNLIMITED SCALE & CAPACITY. FREE FOREVER.

1. Some of them could be fake or alts
2. enjoy anyways - DeividasJ from globeofgeek
3. "04/07/2012 05:00am", "217.137.150.49", "Wacky2
4. "04/07/2012 05:09am", "67.165.17.125", "ambaseba
5. "04/07/2012 05:14am", "78.145.59.244", "gabril130
6. "04/07/2012 05:18am", "78.145.59.244", "nathanie
7. "04/07/2012 05:26am", "184.147.53.40", "Powerdra
8. "04/07/2012 05:27am", "66.45.138.63", "LoganRR55
9. "04/07/2012 05:40am", "66.45.138.63", "XV123", "t
10. "04/07/2012 05:50am", "24.191.241.72", "MEGAWARG
11. "04/07/2012 05:50am", "24.191.241.72", "MEGAWARG
12. "04/07/2012 06:11am", "77.98.92.237", "zeyad567w
13. "04/07/2012 06:21am", "86.146.95.213", "JustTech
14. "04/07/2012 06:26am", "66.31.7.52", "squish122",
15. "04/07/2012 06:30am", "82.18.59.54", "MrNemo008"
16. "04/07/2012 06:37am", "75.177.125.14", "Xxluckbu

PASTEBIN | #1 paste tool since 2002

Untitled
BY: A GUEST ON APR 21ST, 2015 | SYNTAX: NONE | SIZE: 179.57 KB | VIEWS: 726 | EXPIRES: NEVER
DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

WordPress 1-Click Installation

\$3.96/MO. HOSTING HostGator www.HostGator.com

1. ## GET FUCKED QUEEN ##
2. ## Null Patrol Repentance sends his regards ##
3. ## 10k VHF accounts - 2014 Dec DB DUMP ##
- 4.
5. Galaxy:babu12345
6. kila58:Killa123
7. cenabetim:Abc123Abc
8. Dezinated:abc123
9. Etsumari:luciano7
10. Colt:vixi23
11. Kr4z0r:222333
12. r3dr0ses:123456789
13. kodox00:qaywsx123
14. global view:space007
15. r00ts:oilao14
16. AnorexicVampire:assassin21

Consequences of data leaks

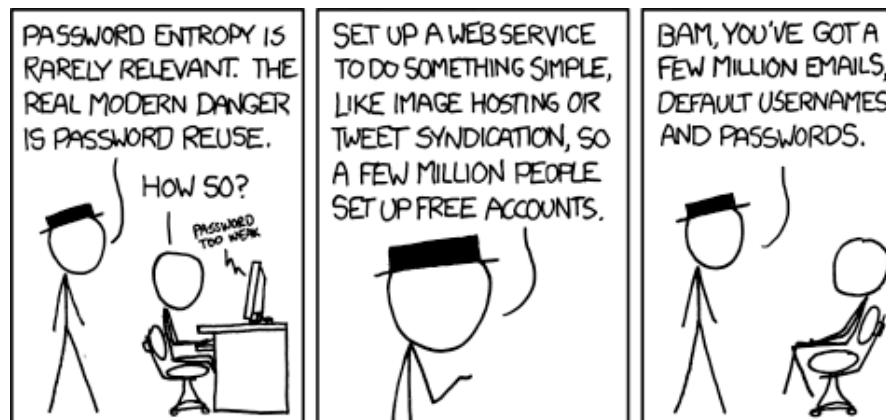
Do data leaks affect only the compromised companies?



Consequences of data leaks

Do data leaks affect only the compromised companies?

- Unfortunately not...
 - People love to **reuse** the very same password on multiple web sites
 - ...or just some simple **mutations**, to cheat password history policies





Password storage

Password storage

- Most important questions about implementing password-based authentication are related to **storage**
 - How to persistently store passwords?
- Password storage system should satisfy some obvious **requirements**
 1. The storage format should support the authentication procedure
 2. It should be difficult for attackers who access the storage system to
 - *Retrieve* the original passwords
 - *Reuse* the stored password to impersonate legitimate users



Password storage

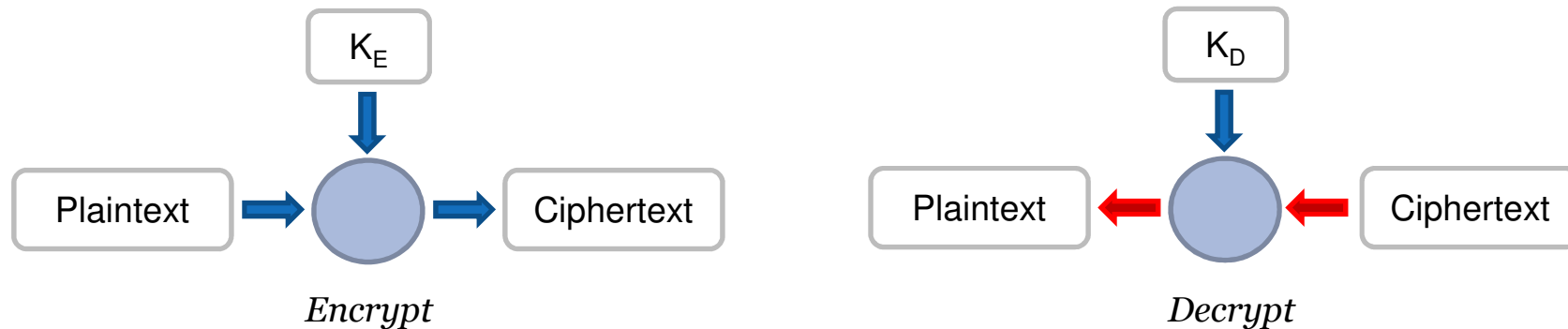
Clear-text passwords



- The simplest approach consists in storing passwords in clear-text form
 - Also the most **insecure** solution
 - Attackers with access to the database can instantly retrieve user passwords
- Consider that **obfuscation** is roughly equal to clear-text
 - Standard obfuscators are trivial to reverse (e.g., base64)
 - Custom methods require a little more effort, but offer no additional protection
- More secure solution consists in relying on **encryption** or **hashing**

Cryptography crash course

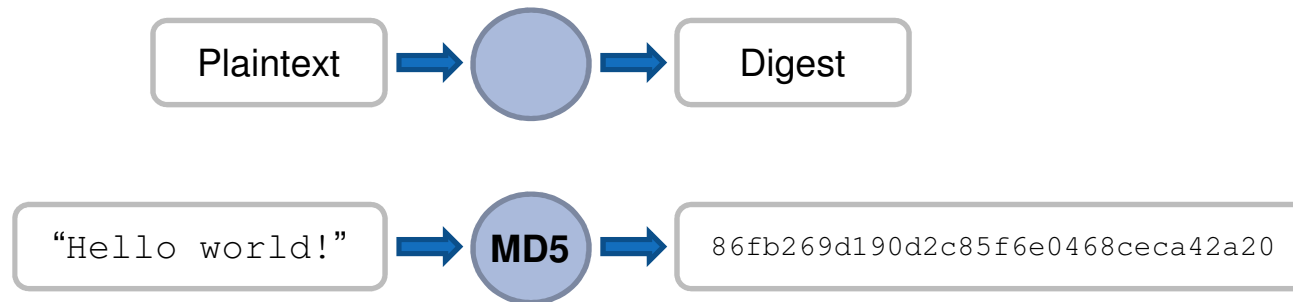
Encryption



- **Encryption** transforms a *plaintext* into a *ciphertext* using a **reversible** scheme
 - *Symmetric*, when encryption and decryption keys are the same (e.g., AES)
 - *Asymmetric*, when encryption and decryption keys are different (e.g., RSA)

Cryptography crash course

Hashing



- **Hashing** maps arbitrary data to a fixed-size digest value
 - Perfect hash functions are one-way (i.e., very difficult to invert)
 - Cryptographic hash functions have other useful properties (e.g., pre-image resistance, plus others)

Password Storage

Crypto is hard!

- Implementing proper cryptosystems is **really** difficult
 - A small mistake could have serious consequences
 - Even systems designed by professional cryptographers are sometimes found to be buggy (e.g., various padding oracle attacks)
- Probably the most important point you should take from this talk is:
Never re-invent crypto!



Password storage

Encrypted passwords



- The most obvious solution for storing password in a “secure” way consists in **encrypting** them
 - Does this approach bring any security benefit?

...but where should we keep the encryption keys?



Password storage

Encrypted passwords



- The most obvious solution for storing password in a “secure” way consists in **encrypting** them
 - Does this approach bring any security benefit?

...but where should we keep the encryption keys?

- **Locally**, on the same system where passwords are stored
 - How to prevent local attackers from accessing them?
 - In short, you can't
- Storing keys on a **remote** host won't help so much
 - There must be a way to transfer keys & passwords to/from the remote machine



Password storage

A case study



- On October 2013, records about 153M Adobe customers were **leaked** on the Internet, including
 - E-mail addresses
 - Passwords hashed/encrypted with an unknown algorithm
 - Password hints

```
103238704-|-|-jmyuncker@aol.com-|-r4Vp5iL2VbM=-|-maiden name|--
103238705-|-|-autumnsomer@yahoo.com-|-BB4e6X+b2xLioxG6CatHBw=-|-boyfriend|--
103238706-|-|-fernandograciliano@hotmail.com-|-Cm8mAzzAiwzioxG6CatHBw=-|-Flamengo|--
103238707-|-|-witold.sadowski@gmail.com-|-n+TZlu41zyHioxG6CatHBw=-|-|--
103238708-|-|-isolon08@gmail.com-|-FAniAwP+U13ioxG6CatHBw=-|-|--
103238709-|-|-ojaimayorga2@yahoo.com-|-kxiV+a47bSlf+E5Ulu/AzA=-|-newest|--
103238710-|-|-sancia@hotmail.com-|-UimSy9NunUU=-|-regl|--
103238711-|-|-hmgc@hotmail.com-|-sKZcDAyegNzioxG6CatHBw=-|-muacacias|--
103238712-|-|-jose_rb15@hotmail.com-|-7EdrqFiVnE8=-|-scream|--
103238713-|-|-roy_pol@yahoo.com-|-mv0h9x97N02evXXgSB9QHg=-|-mobile|--
103238714-|-|-mvgepte@yahoo.com-|-v0I0zz9q+SIjK53VtQ56Pw=-|-itim b|--
103238715-|-|-bigsid21@hotmail.com-|-TArgD00dEij9JL72Rf2Mg=-|-|--
103238716-|-|-stanley_nsh@hotmail.com-|-/MoTSWte948DDM5y6e6/lQ=-|-|--
103238717-|-|-volcomstone6667@aim.com-|-cytpqWtXupE=-|-|--
103238718-|-|-laura_elizondo@sbcglobal.net-|-05FHBhiMjSo=-|-cat|--
103238719-|-|-felt5.kt3@hotmail.co.uk-|-156uBx8IY+vX0cGWdawkEw=-|-none of the above|--
103238720-|-|-grazi_almeida16@ig.com.br-|-dgTRyrEzF5K5n2auThm2+Q=-|-Fisioterapial--
103238721-|-|-reeko48@aol.com-|-SMn46JjxdOU=-|-rear|--
103238722-|-|-mag_mimi78@hotmail.com-|-g7Z+Mtbg22aaSMtqJlIttPQ=-|-|--
103238723-|-|-chaparralinda@msn.com-|-VlTVSIHrn7sBAJNije+B8w=-|-my kitty|--
```



Password storage

A case study



- On October 2013, records about 153M Adobe customers were **leaked** on the Internet, including
 - E-mail addresses
 - Passwords hashed/encrypted with an unknown algorithm
 - Password hints

```
103238704-|--|-jmyuncker@aol.com-|-r4Vp5iL2VbM=-|-maiden name|--  
103238705-|--|-autumnsomer@yahoo.com-|-BB4e6X+b2xLioxG6CathBw=-|-boyfriend|--  
103238706-|--|-fernandograciliano@hotmail.com-|-Cm8mAzzAiwzioxG6CathBw=-|-Flamengo|--  
103238707-|--|-witold.sadowski@gmail.com-|-n+TZlu41zyHioxG6CathBw=-|-|--  
103238708-|--|-isolon08@gmail.com-|-FAniAwP+U13ioxG6CathBw=-|-|--  
103238709-|--|-ojaimayorga2@yahoo.com-|-kxiV+a47bSlf+E5Ulu/AzA=-|-newest|--  
103238710-|--|-sanscia@hotmail.com-|-UimSy9NunUU=-|-regl|--  
103238711-|--|-hmgc@hotmail.com-|-sKZcDAyegNzioxG6CathBw=-|-muacacias|--  
103238712-|--|-jose_rb15@hotmail.com-|-7EdrqFiVnE8=-|-scream|--  
103238713-|--|-  
103238714-|--|-  
103238715-|--|-  
103238716-|--|-stanley_nshenotmail.com-|-/Mo1SWte948UUMsy6eo/lQ=-|-|--  
103238717-|--|-volcomstone6667@aim.com-|-cytpqWtXupE=-|-|--  
103238718-|--|-laura_elizondo@sbcglobal.net-|-05FHBhiMj5o=-|-cat|--  
103238719-|--|-felt5.kt3@hotmail.co.uk-|-156uBx8IY+vX0cGWdawkEw=-|-none of the above|--  
103238720-|--|-grazi_almeida16@ig.com.br-|-dgTRyrEzF5K5n2auThm2+Q=-|-Fisioterapial--  
103238721-|--|-reeko48@aol.com-|-SMn46Jjxd0U=-|-rear|--  
103238722-|--|-mag_mimi78@hotmail.com-|-g7Z+Mtbg22aaSMtqJlittPQ=-|-|--  
103238723-|--|-chaparralinda@msn.com-|-VlTVSIHrn7sBAJNiJe+B8w=-|-my kitty|--
```

Do you see anything suspicious?



Password storage

A closer look at the Adobe leak



- Look at one of those encrypted passwords
 - Base64 encoded
 - Apparently password length is not a multiple of a known hash block size (→ encrypted)
 - Multiple occurrences, with different “hints”

A sample encrypted password

2aZl4Ouarwm52NYYI936YQ== → base64(d9a665e0eb9aaf09b9d8d61823ddfa61)

- **Multiple** hints associated to this password hash
 - Clear symptom of the lack of password salting
 - Sample hints include “*adobex2*”, “*adobe2*”, “*adobe twice*”, “*adobe2x*”
 - Can you guess the password?

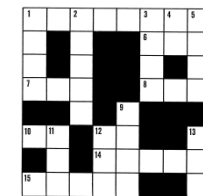
Password storage

A closer look at the Adobe leak

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
4e18acc1ab27a2d6		
4e18acc1ab27a2d6	a0a2876eb1ea1fca	NAME1
8bab6279e06eb6d		DUH
8bab6279e06eb6d	a0a2876eb1ea1fca	
8bab6279e06eb6d	85e9da81a2a78adc	57
4e18acc1ab27a2d6		FAVORITE OF 12 APOSTLES
1ab29ae86dabe5ca	7a246a0a2876eb1e	WITH YOUR OWN HAND YOU HAVE DONE ALL THIS
a1f9b2b6299e7a2b	e0dec1e6ab797397	SEXY EARLOBES
a1f9b2b6299e7a2b	617ab027727ad85	BEST TOS EPISODE
39738b7adb0b8af7	617ab027727ad85	SUGARLAND
1ab29ae86dabe5ca		NAME + JERSEY #
877ab7889d3862b1		ALPHA
877ab7889d3862b1		
877ab7889d3862b1		
877ab7889d3862b1		OBVIOUS
877ab7889d3862b1		MICHAEL JACKSON
38a7c9279c0deb44	9dca1d79d4dec6d5	
38a7c9279c0deb44	9dca1d79d4dec6d5	HE DID THE MASH, HE DID THE
38a7c9279c0deb44		PURLOINED
a8ae5745a2b7af7a	9dca1d79d4dec6d5	FAV LATER-3 POKEMON

THE GREATEST CROSSWORD PUZZLE IN THE HISTORY OF THE WORLD



Password storage

Hashed passwords

- A better approach consists in storing a **digest** of the password
 - Hashing is one-way, thus comparison of the plain-texts is not possible
 - Authentication is performed by computing the hash of the input password and comparing it with the stored value
- Attackers are forced to perform “**brute force**” attacks
 - More about this later
 - Other more efficient attacks are sometimes possible, e.g., “*pass the hash*”
- Not applicable when retrieving the plain-text password is required
 - Such cases should be very rare



Brutefo

Rainbow tak

- Humong
- If the tar



153b07b7757b8e43ce6f171eb76ccd0c

Cerca con Google Mi sento fortunato

Circa 84 risultati (0,52 secondi)

[153b07b7757b8e43ce6f171eb76ccd0c - md5cracker.org](#)
md5cracker.org/.../153b07b7757b8e43ce6f171eb... Traduci questa pagina
The decrypted value behind your md5 hash of "153b07b7757b8e43ce6f171eb76ccd0c"
can be a password or something else. In the most cases the value is a ...

mediate

Reverse a MD5 hash

MD5 sum to reverse

153b07b7757b8e43ce6f171eb76ccd0c

Reverse

You can generate the MD5 hash of the string which was just reversed to have the proof that it is the same as the MD5 hash you provided:

Convert a string to a MD5 hash

String to convert to MD5

armadillo

Convert

[.com - 153b07b7757b8e43ce6f171eb76...](#)
b30.com/153b07b7757b8e43ce6f171... Traduci
5: 153b07b7757b8e43ce6f171eb76ccd0c ntlm:
20ffd6a26ad91be226e8 sha1:
05a0cb86df52491fda34c4dcd5235 ...

MD5decoder.org

armadillo MD5: 153b07b7757b8e43ce6f171eb76ccd0c hashes

153b07b7757b8e43ce6f171eb76ccd0c

search

Put MD5 or a word

- Eurobuch
ch.com/.../153b07b7757b8e43ce6f17... Traduci
e Bücher von - Armadillo. Bei der Büchersuchmaschin
antiquarische und Neubücher VERGLEICHEN UND SOF

[armadillo - Hosted Weblate](#)
https://hosted.weblate.org/.../translate/?...153b07b7... Traduci questa pagina
Non è disponibile una descrizione per questo risultato a causa del file robots.txt del sito.

Result

MD5 Code
153b07b7757b8e43ce6f171eb76ccd0c

Decrypted String
Decrypted String Found

armadillo

[pt To MD5 | armadillo](#)
aduci questa pagina
illo. Encrypted String
her Encryption Algorithms. Algorithms.
8e43ce6f171eb76ccd0c
e43ce6f17... Traduci questa pagina



Improving password strength

Server side



- Eventually, it's in the users' hand to pick a strong password...
- ...is there something we can do **server-side**, to make users' passwords harder to crack? **Salting!**



```
hash = hash_f( salt + password )
```


Improving password strength

Server side

- Eventually, it's in the users' hand to pick a strong password...
- ...is there something we can do **server-side**, to make users' passwords harder to crack? **Salting!**



$$\text{hash} = \text{hash_f}(\text{salt} + \text{password})$$

- **Salting** consists in adding pseudo-random prefix to the password before hashing it
- The result is (usually) stored as:



What **very useful** features does salting grant? Any idea?

Improving password strength

Server side



- Eventually, it's in the users' hand to pick a strong password...
- ...is there something we can do **server-side**, to make users' passwords harder to crack? **Salting!**



`hash = hash_f(salt + password)`

- If two users have the same password, the stored hash is different
- Can an attacker use rainbow tables against **salted** passwords?

Detecting password issues

Static analyzer



- In order to statically identify issues related to password handling in software projects, there are a number of properties that can be checked
- For example a static analyzer could:
 1. Identify usage of weak encryption methods (es., md5)
 2. Assess the presence of known vulnerabilities in crypto libraries
 3. Identify unsafe use of cryptographic methods (es., static salt/IVs)
 4. Check code handling password file/DB



Conclusions

Conclusions

- So, how passwords should be stored?
 - Prefer **salt hash-based** schemes
 - Never rely on **custom** obfuscation schemes
 - Again: do **not** re-invent crypto!





Thank You!

DIREZIONE GENERALE

Viale Francesco Restelli, 3/1 - 20124 Milano (MI)
Tel. +39 02 89078400 Fax +39 02 36559773

SEDE LEGALE

Area Science Park ssl 14 km 163,5 Basovizza, 34149 Trieste (TS)
Tel +39 040 375 75 80 · fax +39 040 375 75 81

C.F. - P. I.V.A e Reg.
Imprese Trieste 00998050322
R.E.A 116618 Cap. Soc. € 100.000 i.v.
