Gestione di password e certificati

Indice

- Tecniche di autenticazione e multi-factor authentication
- Protocolli di autenticazione
- Gestione delle password e dei certificati.
- Modelli e tecniche per autorizzazione e controllo dell’accesso
- Privileged Identity and Access Management (PAM)
- Cenni sulla segregazione e segmentazione delle reti

Indice

- Tecniche di autenticazione e multi-factor authentication
- Protocolli di autenticazione
- Gestione delle password e dei certificati.
- Modelli e tecniche per autorizzazione e controllo dell'accesso
- Privileged Identity and Access Management (PAM)
- Cenni sulla segregazione e segmentazione delle reti

Gestione delle password

- Meccanismo più diffuso di autenticazione

- Deve essere resistente ad attacchi
  - *a forza bruta* (provare tutte le password possibili)
  - basati su dizionari
  - basati su *open source intelligence*

Scelta delle password

- Lunghezza della password
  - maggiore è la lunghezza, maggiore il numero di tentativi mediamente necessari
- Contenuto della password
  - sequenza di caratteri poco *prevedibile*
  - ad es. sequenza casuale

Scelta delle password

- Lunghezza della password
  - maggiore è la lunghezza, maggiore il numero di tentativi mediamente necessari
- Contenuto della password
  - sequenza di caratteri poco *prevedibile*
  - ad es. sequenza casuale

Scelta delle password

- Contenuto della password *casuale*
  - generata automaticamente
  - una *frase* relativamente lunga
    (NIST SP 800-63B – Giugno 2017)
- Verifica robustezza password
  - algoritmi che misurano la prevedibilità

Scelta delle password

- Se per uso da parte di persone
  - o facilmente *memorizzabile* MA non facilmente *indovinabile*
  - o sequenze casuali memorizzati in archivi software cifrati
    - occorre tenere a mente solo la password dell'archivio
- Requisito necessario: mai utilizzare la medesima password in servizi o dispositivi diversi

Creazione di parole d'ordine *sicure*

- Uso di software *password manager*
  - gestiscono un database di password personali
  - consentono di creare e memorizzare password contenenti sequenze casuali di caratteri
  - cifratura del database
  - protezione del database con una *master password*, unico segreto che l'utente deve ricordare

NIST 800-63 FAQ

Creazione di parole d'ordine *sicure*

- Uso di *passphrases*
  - concatenazione di più parole di senso compiuto
    - anche appartenenti a lingue o dialetti diversi
  - facilità di memorizzazione individuale
  - lunghezza elevata -> maggior difficoltà di essere individuata automaticamente

NIST blog

Scelta delle password

- Nel caso di comunicazioni fra dispositivi, l'analogo della password è una sequenza *casuale*
  - la *chiave*
- In questo caso si agisce prevalentemente sulla lunghezza
  - ipotizzando di usare un algoritmo robusto per la generazione di sequenze casuali

Generazione e distribuzione di password e chiavi

- Fondamentale **gestire** il processo di generazione e distribuzione di password e chiavi
- Preferibile comunicazione *out-of-band* se password o chiave devono essere comunicate *in chiaro*
  - SMS o documento cartaceo per password personali
  - dispositivi fisici removibili o reti non collegate a Internet in caso di *pre-shared key*

Conservazione di password e chiavi

- Memorizzate su dispositivi non direttamente accessibili da rete esterna, in formato cifrato
- Problema: conservazione della chiave di cifratura dell'archivio cifrato
- In contesti ad alta sicurezza, può essere un dispositivo hardware consegnato a persone fidate.

Certificati digitali

- Riconoscimento di una organizzazione (pubblica o privata) come terza parte fidata
- Si occupa di generare coppie di chiavi crittografiche asimmetriche (pubblica-privata)
- Garantisce sulla
  - univocità della chiave
  - segretezza della chiave

Distribuzione certificati digitali

- PKI – Public Key Infrastructure
  Insieme di strumenti hardware e software, protocolli di comunicazione e le regole per generazione e distribuzione di certificati
- Una organizzazione può rilasciare certificati su delega di una organizzazione di livello superiore

Certificati digitali e fiducia

- La sicurezza delle comunicazioni basate su certificati digitali si basa unicamente sulla fiducia nelle organizzazioni che li gestiscono
- L'autenticazione fra due soggetti (ad es. browser e sito di home banking) avviene perché entrambi si *fidano* della organizzazione che ha rilasciato i certificati

Approfondimento 1: Password *deboli*

- Sono password che possono essere facilmente scoperte
  - perché sono facili da ricordare come sequenze banali di numeri o lettere
  - legate a fatti noti del soggetto (esempio: nomi di parenti, animali domestici, date note, ecc.)
  - perché parole di uso comune legate e fatti di cronaca o personaggi famosi
  - perché parole di uso comune anche se con variazioni come sostituzioni di vocali con cifre, ecc.
- Verifica di robustezza di password con strumenti che generano automaticamente password attraverso dizionari e regole euristiche
  - John the Ripper password cracker
    http://www.openwall.com/john/
  - Hashcat
    https://hashcat.net/hashcat/
- Have I Been Pwned - https://haveibeenpwned.com
  consente di verificare se un indirizzo email è incluso all'interno di insiemi di dati relativi a *data breach* pubblici che hanno interessato gli *hash* delle password utilizzate insieme all'indirizzo email per autenticarsi a qualche servizio

Approfondimento 2:
Classifica delle password *deboli*

splashdata

The Top 50 Worst Passwords of 2019

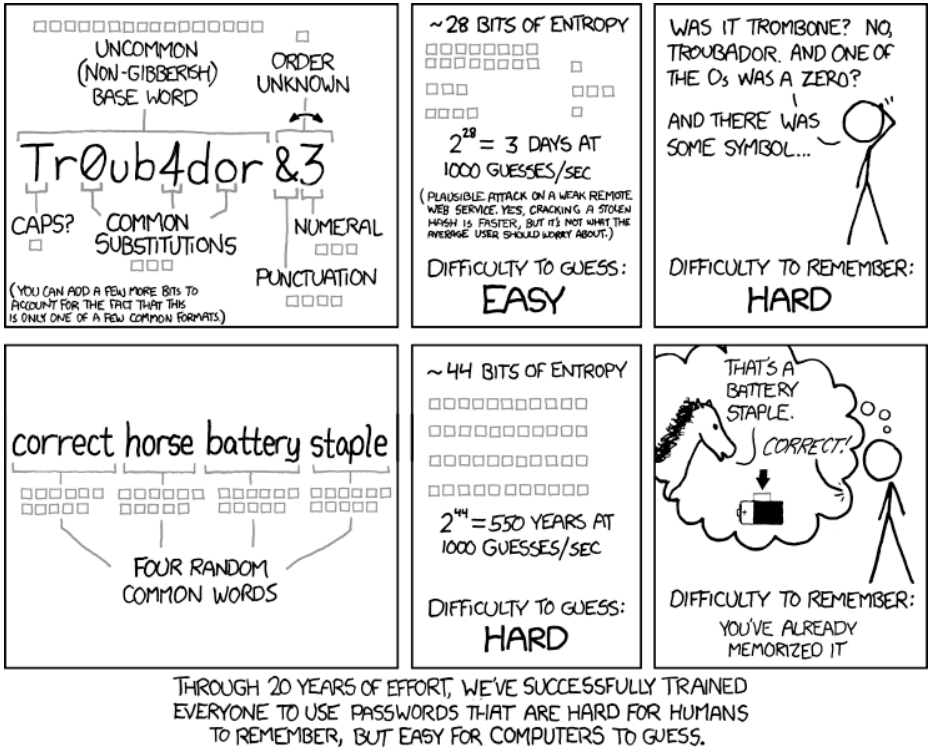
https://www.teamsid.com/1-50-worst-passwords-2019/

Approfondimento 3: NIST 800-63 FAQ

- **Password managers** offer greater security and convenience for the use of passwords to access online services. Greater security is achieved principally through the capability of most password manager applications to generate unique, long, complex, easily changed passwords for all online accounts and the secure encrypted storage of those passwords either through a local or cloud-based vault. Greater convenience is provided by the use of a single master password to access the password vault rather than attempting to memorize different passwords for all accounts. Most password manager applications offer additional capabilities that enhance both convenience and security such as storage of credit card and frequent flyer information and autofill functionality.
- The compromise of the master secret to a password vault would require all passwords in the vault to be recreated. However, many password managers today provide two-factor capability and are designed in a way that cloud password services are not able to access the vault, even if compromised. Password managers contain much information that is valuable to cyber criminals, making them high-value targets, so securing these vaults is essential.
- In SP 800-63B, NIST has not explicitly recommended the use of password managers, but recommends that verifiers permit the use of “paste” functionality so that the subscriber can use a password manager if desired. If using a password manager, subscribers should:
  - Choose a long passphrase for the master password to the password manager and protect it from being stolen. A passphrase can be made sufficiently long to protect against attacks while still allowing memorization.
  - Create unique passwords for all accounts or use the capability of most program managers to generate random, unique, complex passwords for each account.
  - Avoid password managers that allow recovery of the master password. Any compromise of the master password through account recovery tools can compromise the entire password vault.
  - Use multi-factor authentication for program manager applications that allow that capability.
  - Use the password generator capability in most password managers to generate complex, random text answers to online “security” questions for those sites still using them.

https://pages.nist.gov/800-63-FAQ/#q-b12

Approfondimento 4: Passphrases



Credit: Randall Munroe, xkcd.com, CC 2.5

Approfondimento 5: Crittografia e memorizzazione della password

"If you want, I can store the encrypted password." A Password-Storage Field Study with Freelance Developers

Alena Naiakshina
University of Bonn
naiakshi@cs.uni-bonn.de

Anastasia Danilova
University of Bonn
danilova@cs.uni-bonn.de

Eva Gerlitz
University of Bonn
gerlitz@uni-bonn.de

Emanuel von Zezschwitz
University of Bonn, Fraunhofer FKIE
zezschwitz@cs.uni-bonn.de

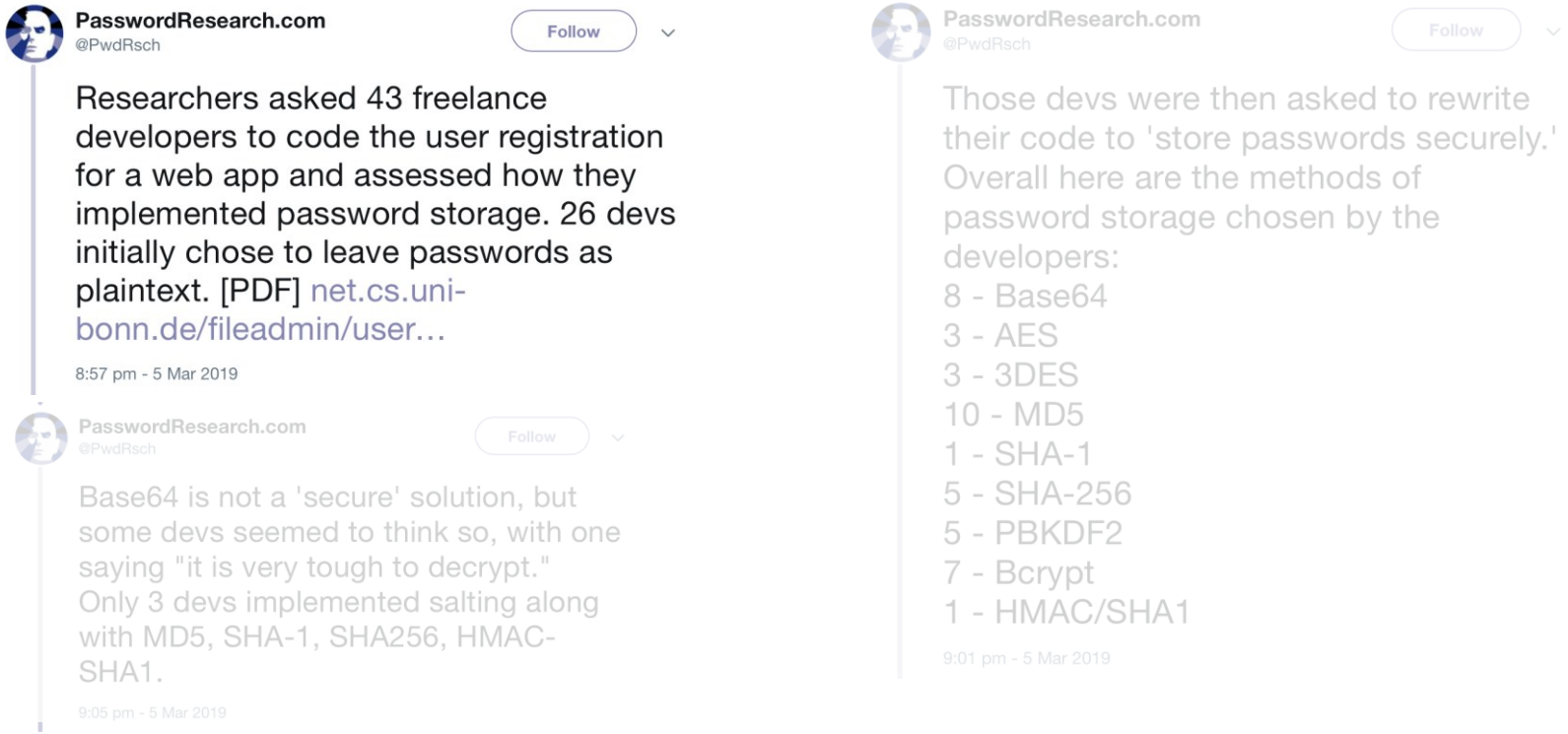
Matthew Smith
University of Bonn, Fraunhofer FKIE
smith@cs.uni-bonn.de

CHI 2019, May 4–9, 2019, Glasgow, Scotland UK

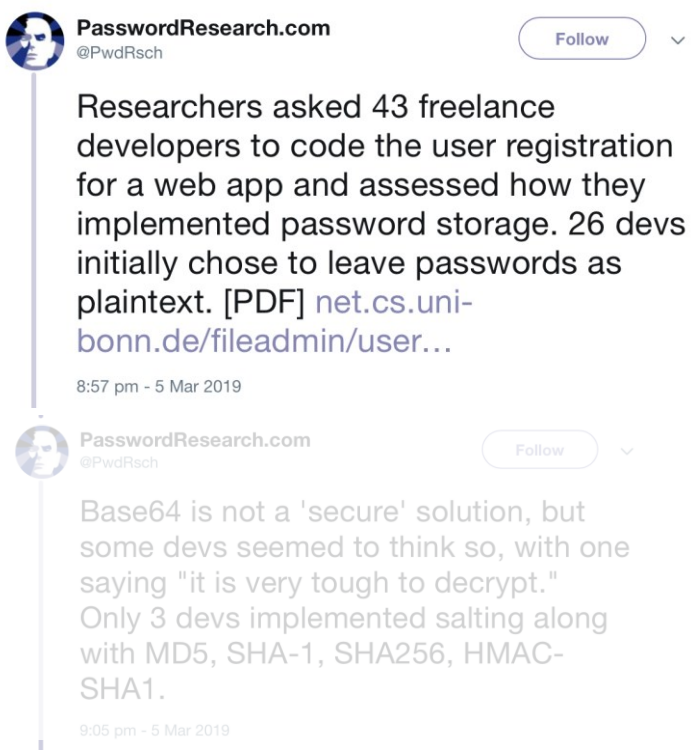
ACM ISBN 978-1-4503-5970-2/19/05.

https://net.cs.uni-bonn.de/fileadmin/user_upload/naiakshi/Naiakshina_Password_Study.pdf

Approfondimento 5: Crittografia e memorizzazione della password



Approfondimento 5: Crittografia e memorizzazione della password



PasswordResearch.com
@PwdRsch
Follow

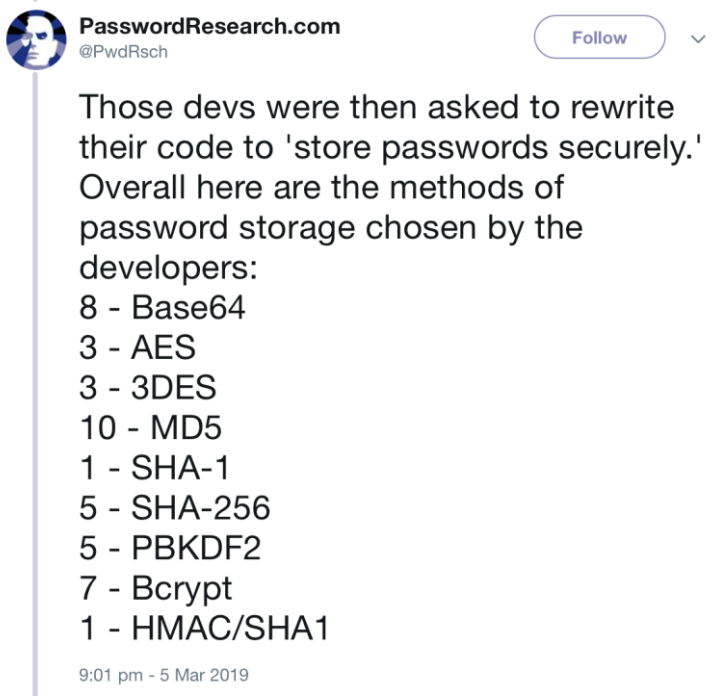
Researchers asked 43 freelance developers to code the user registration for a web app and assessed how they implemented password storage. 26 devs initially chose to leave passwords as plaintext. [PDF] net.cs.uni-bonn.de/fileadmin/user…

8:57 pm - 5 Mar 2019

PasswordResearch.com
@PwdRsch
Follow

Base64 is not a 'secure' solution, but some devs seemed to think so, with one saying "it is very tough to decrypt." Only 3 devs implemented salting along with MD5, SHA-1, SHA256, HMAC-SHA1.

9:05 pm - 5 Mar 2019



PasswordResearch.com
@PwdRsch
Follow

Those devs were then asked to rewrite their code to 'store passwords securely.' Overall here are the methods of password storage chosen by the developers:
8 - Base64
3 - AES
3 - 3DES
10 - MD5
1 - SHA-1
5 - SHA-256
5 - PBKDF2
7 - Bcrypt
1 - HMAC/SHA1

9:01 pm - 5 Mar 2019

Approfondimento 5: Crittografia e memorizzazione della password