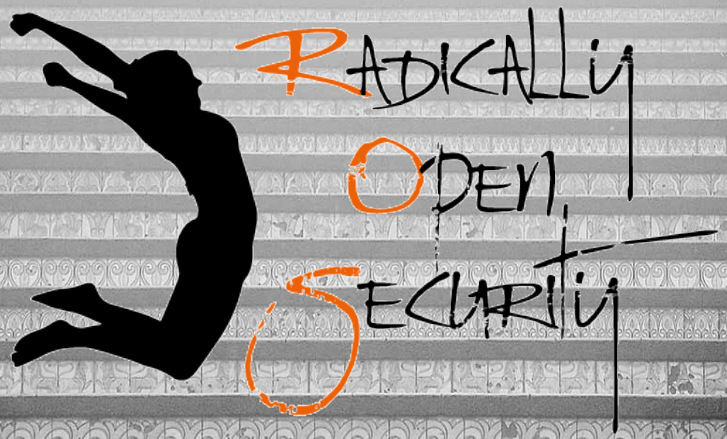
Password Management and Cracking Training

Developed by: Melanie Rieback, Rais Mense, Nathan Stern, Murtuja Bharmal, Fernando Quintero



Agenda

- Part I – Password Creation
  - Intro: what are Passwords? Hashes?
  - Weak passwords (guessability, recon, default Pws)
  - Attacks against passwords (brute force, dictionary attacks)
  - DEMO: PW cracking (Online vs. Offline, Rainbow Tables)
  - Solutions (salt, passphrases, PW policies)
- Part II – Password Usage
  - Passwords on the Wire
  - DEMO: ssl-strip
  - Worst Password Management techniques
- Part III – Password Storage
  - Intro to PW Storage (text files, DBs, memory, Linux)
  - Password caching, pros vs. cons
  - DEMO: DumpIt + Volatility
  - Solutions (PW vaults, encryption in DBs/filesystems)

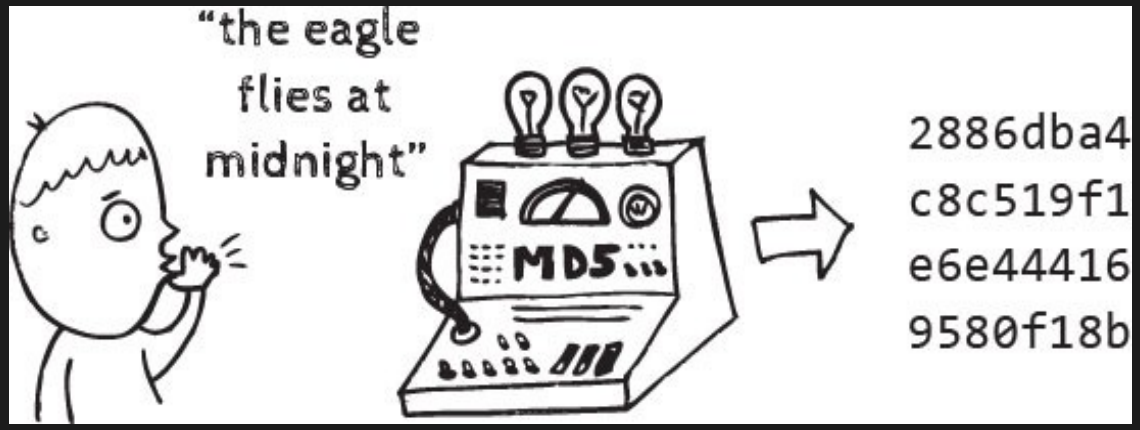
Part I - Password Creation

What is a Password?

- A secret word/string of characters used to authenticate a user into a system
- Authentication trilogy
  - What you have
  - Who you are
  - **What you know**

Hash Functions

- Cryptographic one-way functions, that convert a string into fixed number of character.
- Example algorithms: NT Hash, LM Hash, MD4, MD5, SHA1, SHA2, SHA256, SHA512



Hashing Vs Encryption

	Hashing	Encryption
Definition	Hashing involves the conversion of plaintext into a hash or digest. A digest cannot be reversed into the original message.	Encryption is the process of converting plain text into cipher by using an algorithm. The encrypted message can only be read by knowing the encryption key.
Protection of	Integrity	Confidentiality
Unlocking	No key can be used for unlocking	Requires key for unlocking

Courtesy:http://www.differencebetween.info/difference-between-hashing-and-encryption

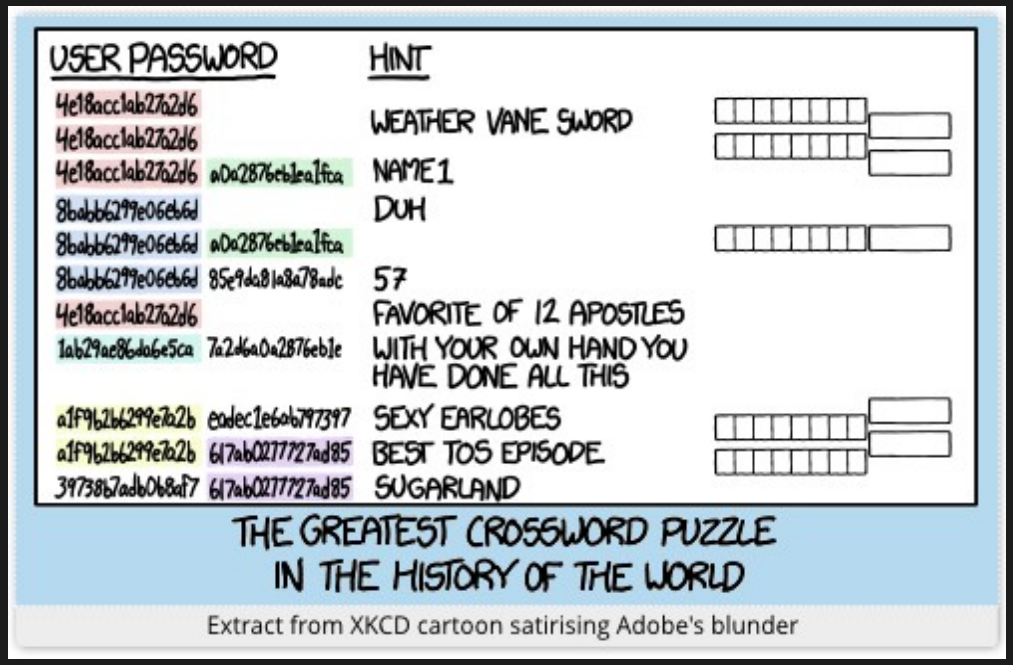
Worst Passwords of 2015

- Top 15: 123456, password, 12345678, qwerty, 12345, 123456789, football, 1234, 1234567, baseball, welcome, 1234567890, abc123, 111111

- All 11,000,000 passwords of Ashley Madison were hacked

What makes passwords weak?

- Guessability
  - Predictability and low entropy
- Relevance
  - Studying corporate literature, website sales materials and competitors, build custom word list



Extract from XKCD cartoon satirising Adobe's blunder

Default Passwords

RouterPasswords.com

Select Router Make: LINKSYS

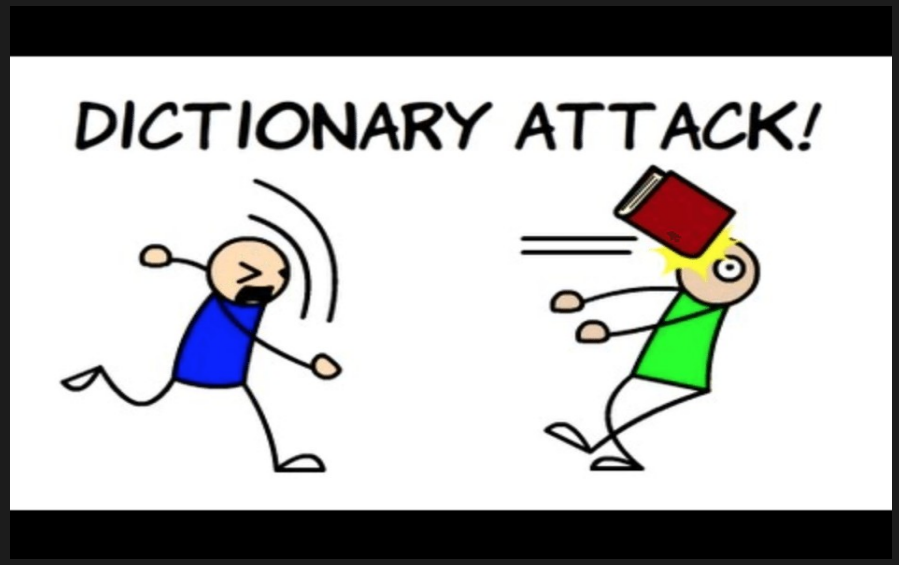
Find Password

Manufacturer	Model	Protocol	Username	Password
LINKSYS	WAP11	MULTI	n/a	(none)
LINKSYS	DSL	TELNET	n/a	admin
LINKSYS	ETHERFAST CABLE/DSL ROUTER	MULTI	Administrator	admin
LINKSYS	LINKSYS ROUTER DSL/CABLE	HTTP	(none)	admin
LINKSYS	BEFW11S4 *Rev. 1*	HTTP	admin	(none)
LINKSYS	BEFSR41 *Rev. 2*	HTTP	(none)	admin
LINKSYS	WRT54G	HTTP	admin	admin
LINKSYS	WAG54G	HTTP	admin	admin
LINKSYS	LINKSYS DSL		n/a	admin
LINKSYS	WAP54G *Rev. 2.0*	HTTP	(none)	admin
LINKSYS	WRT54G *Rev. ALL REVISIONS*	HTTP	(none)	admin
LINKSYS	MODEL WRT54GC COMPACT WIRELESS-G BROADBAND ROUTER	MULTI	(none)	admin

Courtesy:http://www.howtogeek.com/131338/how-to-access-your-router-if-you-forget-the-password/

Attacks Against Passwords

- Dictionary Attack
  - Systematically entering every word in a dictionary(wordlist) as a password
- Brute force attack
  - Decoding encrypted/hashed data through exhaustive effort (using brute force) rather than employing intellectual strategies.



Courtesy:http://searchsecurity.techtarget.com/

Types of Password Cracking

- Online
  - Trying different passwords interactively
  - Usually slow and noisy
  - You might be allowed only a few guesses
- Offline
  - Processing password files/hashes locally
  - Limited by computing speed

Rainbow Tables

- Rainbow Tables
  - A rainbow table is a list of pre-computed hashes
  - The hash to test gets compare against the other pre-computed hashes
  - Space/time tradeoff

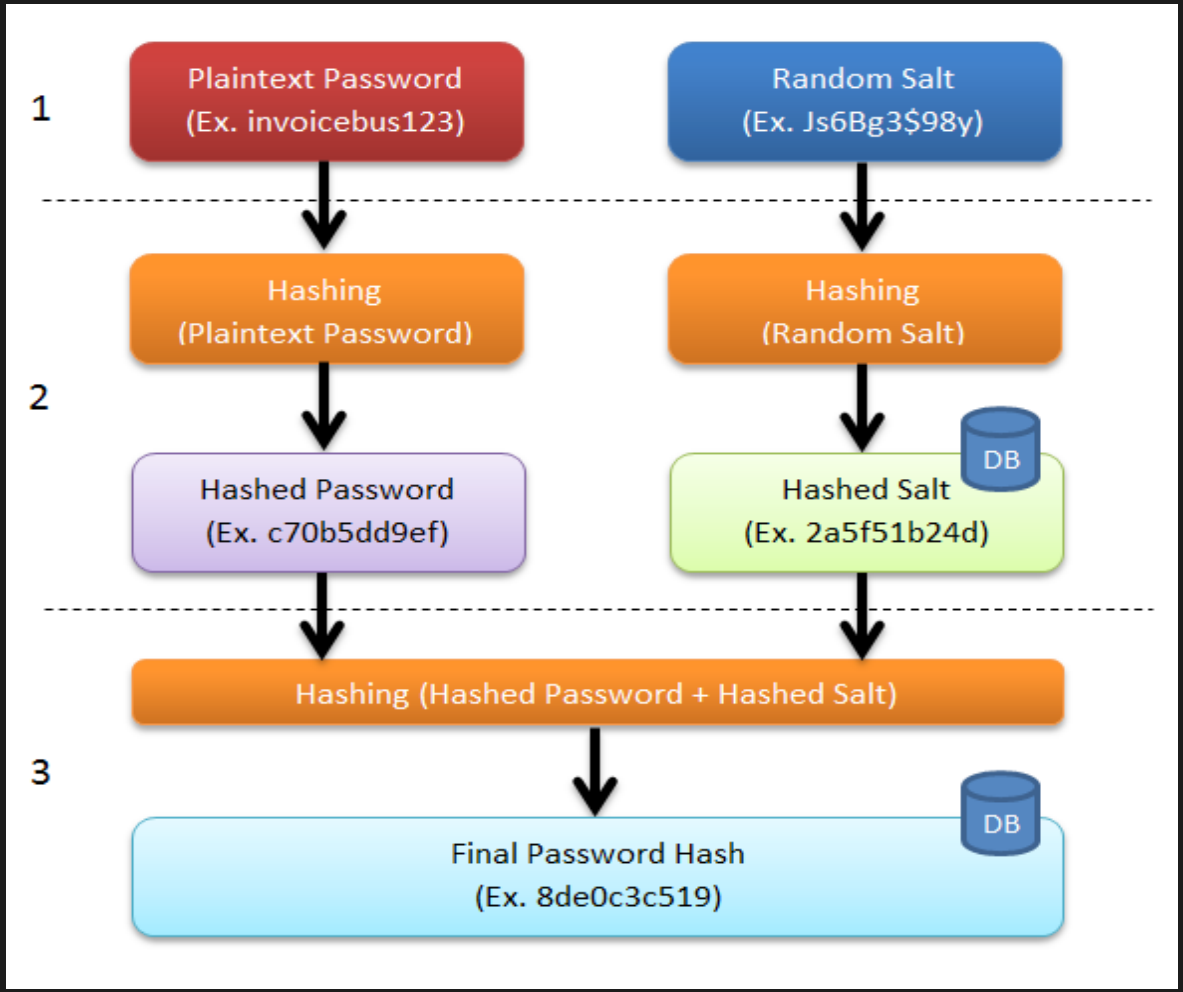
DEMO TIME!!!

- Estimator
- Generator
- Offline cracking
- Rainbow tables

Solutions: Salt

- Random data used as additional input to a one-way hash function.
- Salt can defend against dictionary attacks or pre-computed rainbow table attacks

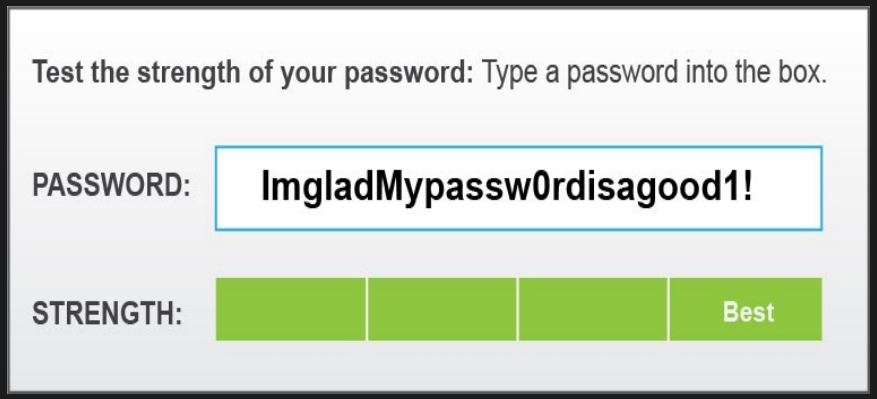
Example: Password Salt



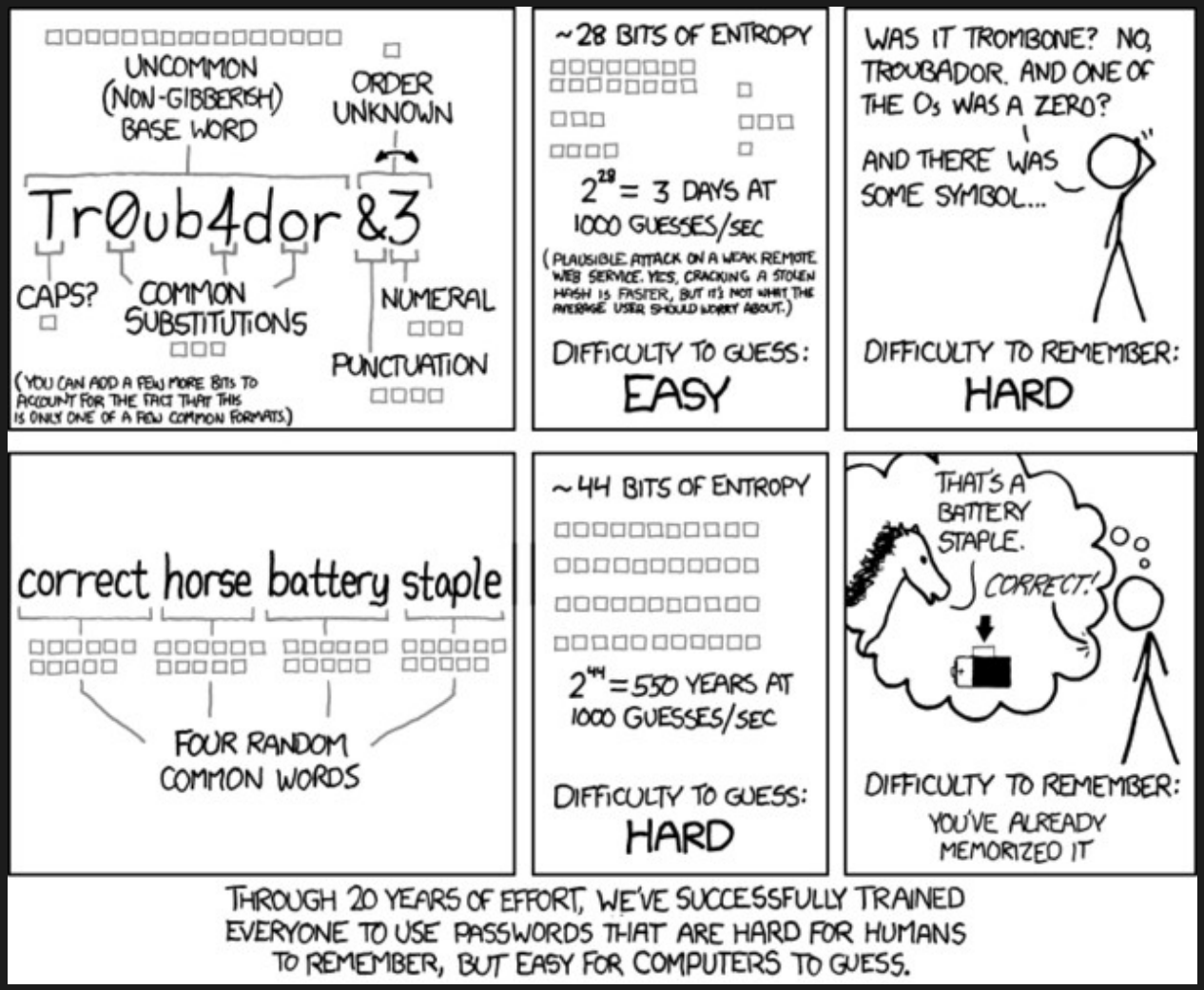
Courtesy:http://sladigitalforensics.blogspot.in/2013/12/salted-hash-future-for-passwords.html

Passphrases vs Passwords

- Passwords usually 10-12 letters / numbers / symbols
- Passphrase is long sentence which contains spaces. Can also contain symbols.
- Passphrases have more entropy



xkcd on Passphrases <3



Password Policy

Enforce password requirements				
Change <90 days	12+ characters	All character types	Prohibit re-use	Pattern checks?
Support				
Crack your own passwords			Awareness of phishing and re-use	

Courtesy: https://www.rsaconference.com/writable/presentations/file_upload/pdac-w05_the_state_of_modern_password_cracking_final.ppt.pdf

Part II - Password Usage

Password Pitfalls

- Writing them down on sticky notes
- Maintain a text file with user credentials
- Using same credentials at multiple places*
- *Specially the insecure ones ... (leaks)

Data on the Wire

- Password sniffing
  - Sniffing with tcpdump, tshark, Wireshark

    i.e. HSRP passwords in Cisco routers, VoIP passwords
  - MITM using sslsniff/sslstrip/bettercap

DEMO TIME!!!

- Password Sniffing with the WiFi Pineapple!
  - Ssl-split

Stuff That Can Help

- Different passwords everywhere
  - Twitter, Facebook, Google
  - Government logins
  - Banks
- Protect your access with additional controls. *i.e. 2FA*

Part III - Password Storage

Where Do Passwords Live?

- In plain-text files
  - .htpasswd, /etc/ppp/chap-secrets, browser/application cache file
- In databases
  - Mysql, MS-SQL, sqlite
- In memory
  - Temporary storage

Where Do Passwords Live?

- Windows
  - SAM database, Active Director
- Linux
  - /etc/shadow, OpenLDAP
- Application Servers
  - Files and DBs

Saving Passwords on the HD

- Password Hardcoding
  - Software (and filesystems) sometimes contain cleartext passwords, which are used for inbound authentication or outbound communication
  - This is useful for users / sysadmins.. and for attackers!

Saving Passwords in Caches

- Browser/application caches are handy!
  - Login credentials stored locally for later use.
  - Web browsers, applications, etc..
  - Password recovery tools/malware can recover and decrypt stored passwords

Chrome Password Decryptor

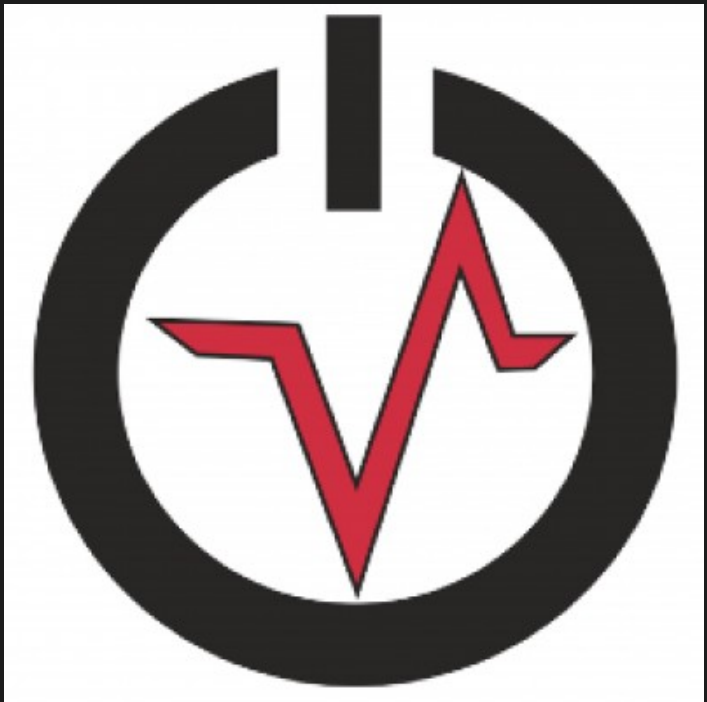
Courtesy: http://securityxploded.com/chromepassworddecryptor.php

Retrieving Password from Memory

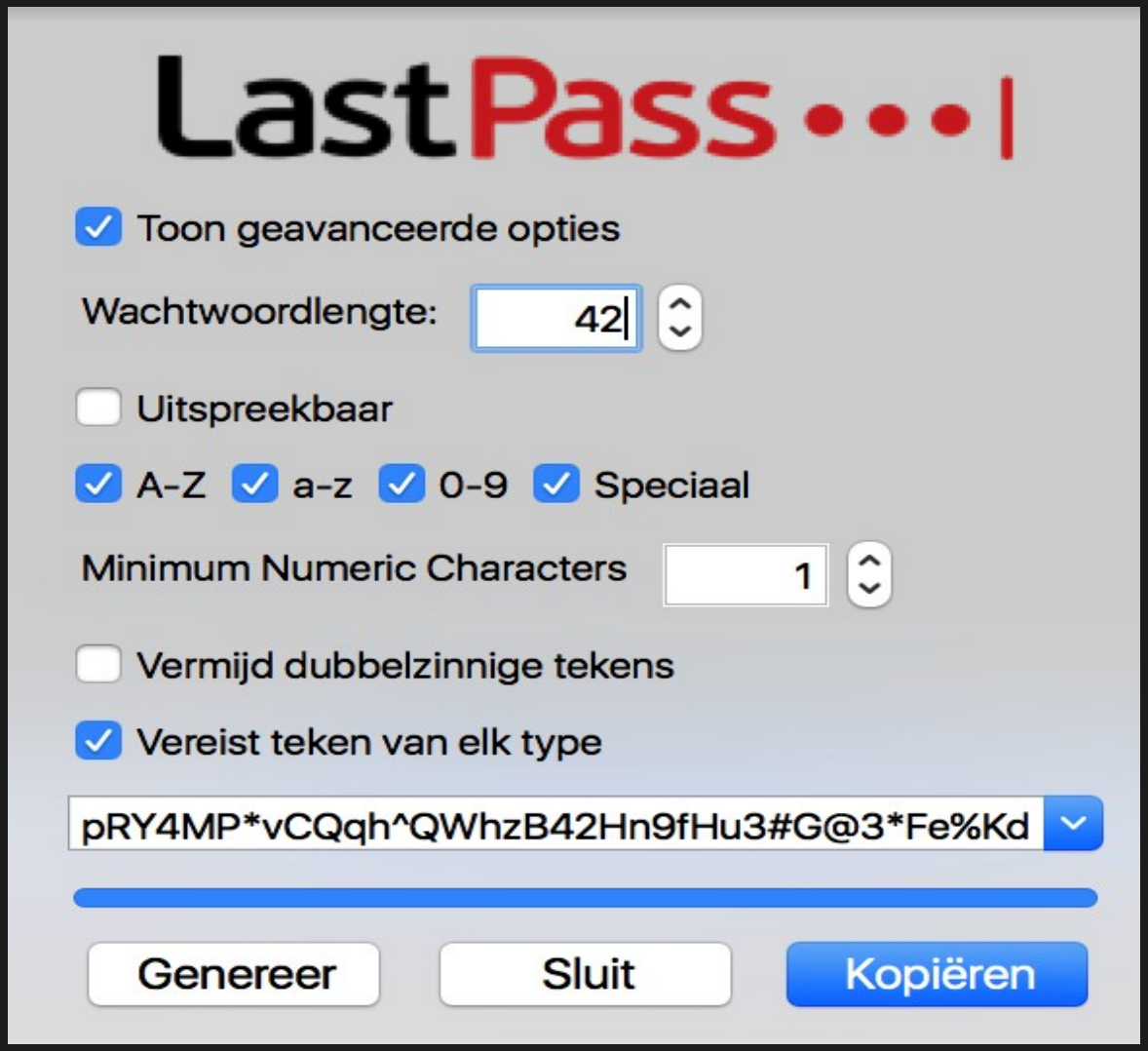
- Passwords are sometimes stored cleartext in memory
  - Attacker compromises a desktop or server + dumps the RAM memory
  - Plain-text or hashed passwords can be extracted from the memory dump
  - i.e. Process Memory Dumper, Volatility, Mimikatz

DEMO TIME!!!

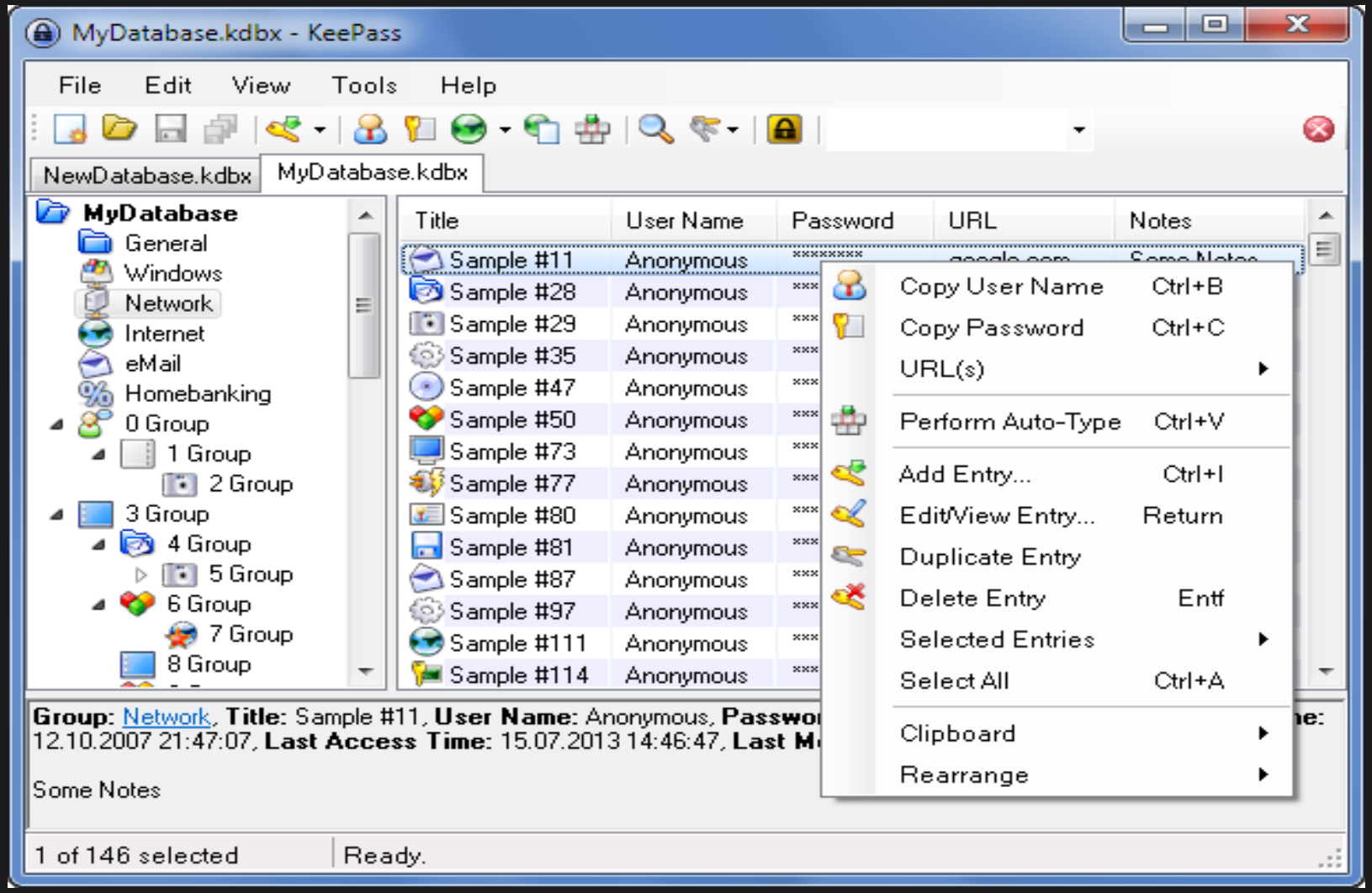
- Retrieving password hashes from memory
  - Dumpit
  - Volatility



Solution: Password Vaults

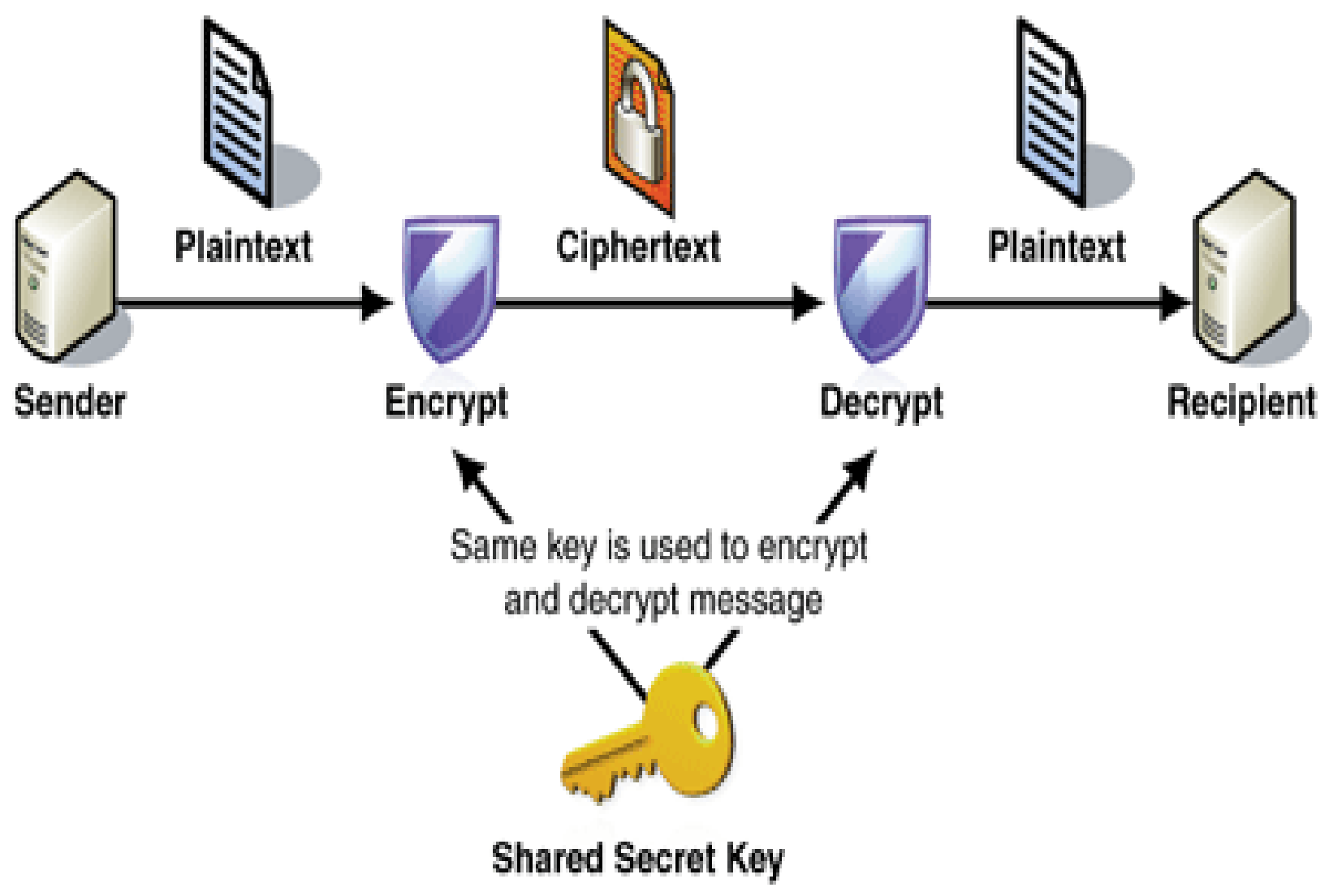


Solution: Password Vaults



Courtesy:http://keepass.info/

Solution: Encrypt Data at Rest



Courtesy:
http://www.kadix.ca/

Questions?