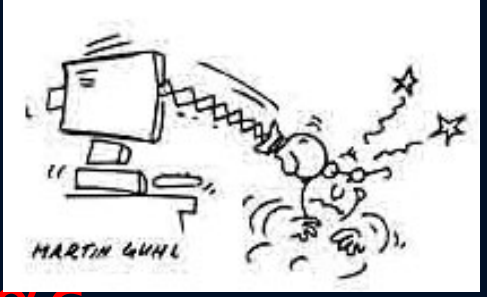
ΤΕΙ ΗΠΕΙΡΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε
ΜΕΤΑΠΤΙΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

Ασφάλεια

ΛΙΑΓΚΟΥ ΒΑΣΙΛΙΚΗ
ΔΙΑΛΕΞΗ-ΙΙ



Επιθέσεις σε συστήματα που βασίζονται σε κωδικούς ασφαλείας

A. Υποκλοπή κατά την εισαγωγή
   - π.χ. Spoofing, spyware, keylogger…
B. Υποκλοπή κατά τη μετάδοση
   - π.χ sending passwords "in the clear"
C. Online επιθέσεις (επιθέσεις «ωμής βίας» ή «επιθέσεις λεξικού»)
   - π.χ. δοκιμάζω κωδικούς για να συνδεθώ (log-in) στο σύστημα
D. Offline επιθέσεις (επιθέσεις «ωμής βίας» ή «επιθέσεις λεξικού»)
   - π.χ. υποκλοπή του αρχείου κωδικών (password file) και προσπάθεια ανάκτησης κωδικού (-κών)
E. Επιθέσεις Παραπλάνησης
   - π.χ. Phishing, spoofing, MITM attacks, Social Engineering

Fake Login (Spoofing) attack

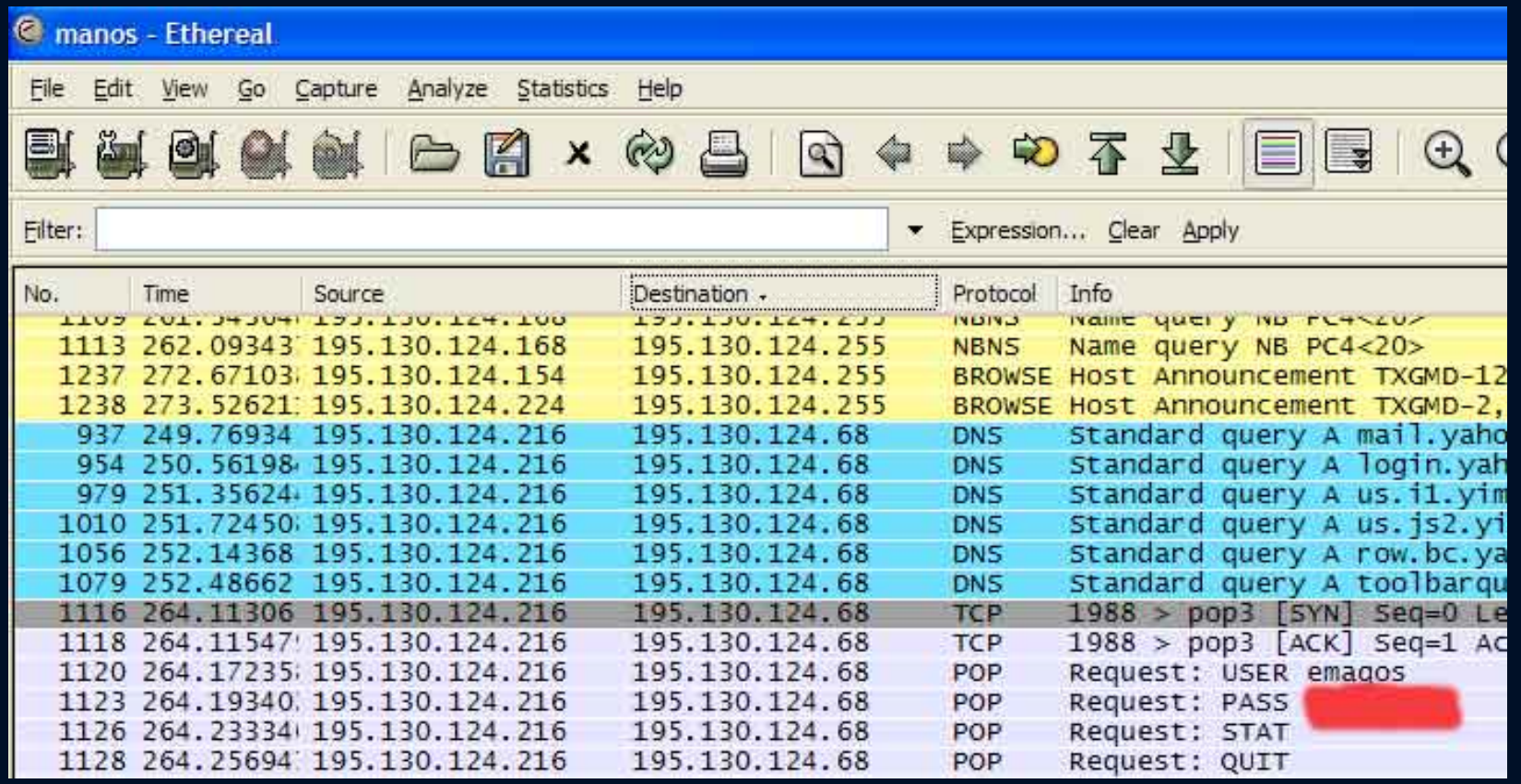
(Gollmann, 2010)

- Policies :
  - Show number of failed logins
  - Trusted path with OS
  - Mutual authentication
  - ...

Login spoofings είναι τεχνικές που χρησιμοποιούνται για να κλαπεί ο κωδικός πρόσβασης ενός χρήστη. Στον χρήστη παρουσιάζεται ένα συνηθισμένο παράθυρο για να γράψει ο χρήστης τα στοιχεία του για το όνομα χρήστη και τον κωδικό πρόσβασης, το οποίο είναι ένα κακόβουλο πρόγραμμα, π.χ δούρειος ίππος κάτω από τον έλεγχο του εισβολέα. Όταν συμπληρωθούν το όνομα χρήστη και ο κωδικός πρόσβασης, αυτή η πληροφορία καταγράφεται ή με κάποιο τρόπο διαβιβάζεται στον εισβολέα.

Για να αποφευχθεί αυτό, ορισμένα λειτουργικά συστήματα απαιτούν ένα ειδικό συνδυασμό πλήκτρων (ονομάζεται Secure κλειδί) που πρέπει να πατηθούν για να παρουσιαστεί ένα login παράθυρο, για παράδειγμα Control-Alt-Delete.

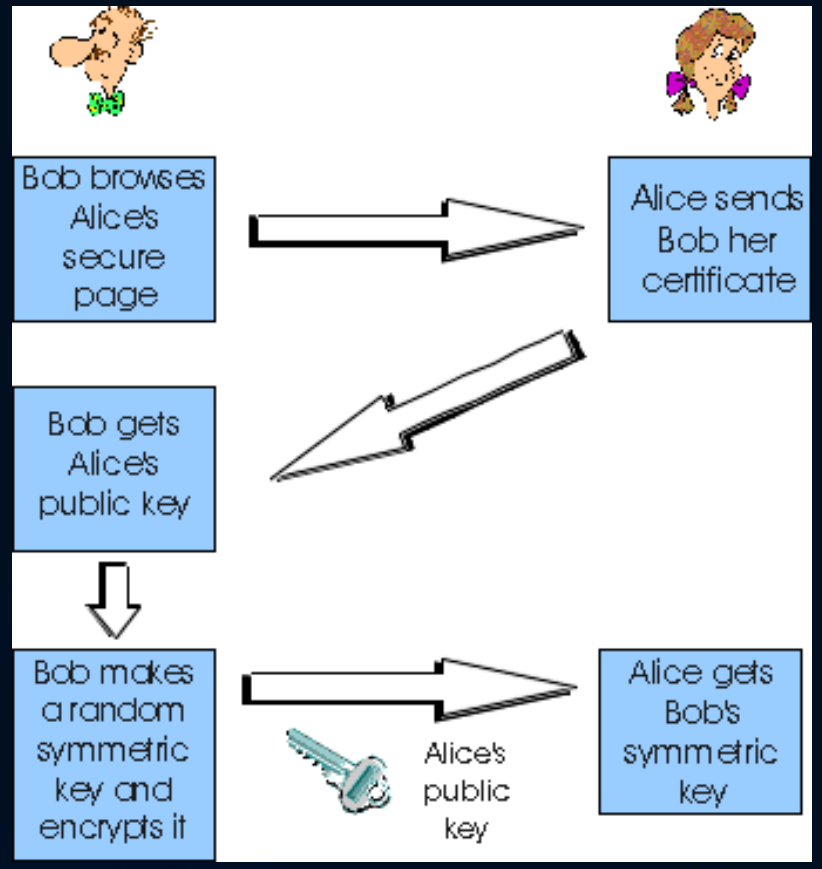
Υποκλοπή κατά τη μετάδοση
Περίπτωση: Ethereal



Υποκλοπή κατά την εισαγωγή & μετάδοση

Μηχανισμοί Ασφάλειας

- Αποστολή του κωδικού ασφάλειας μέσα από ένα κρυπτογραφημένο και αυθεντικοποιημένο κανάλι:
  - Προυποθέτει: ασφαλή εδραίωση συμμετρικού κλειδιού
    - π.χ. πρωτόκολλο Diffie-Hellman, κρυπτογράφηση κλειδιού με το RSA public key του παραλήπτη,…
- Συστήματα:
  - SSH, SSL/TLS, IPSEC, 802.11i, PGP, S/MIME, …



Τεχνική: Key transfer

Επιθέσεις Online (ενεργητικές)

Σημείωση: Η επίθεση δυσχερής όταν υπάρχουν μηχανισμοί κλειδώματος (lockout) μετά από έναν αριθμό αποτυχημένων προσπαθειών (π.χ. 3)

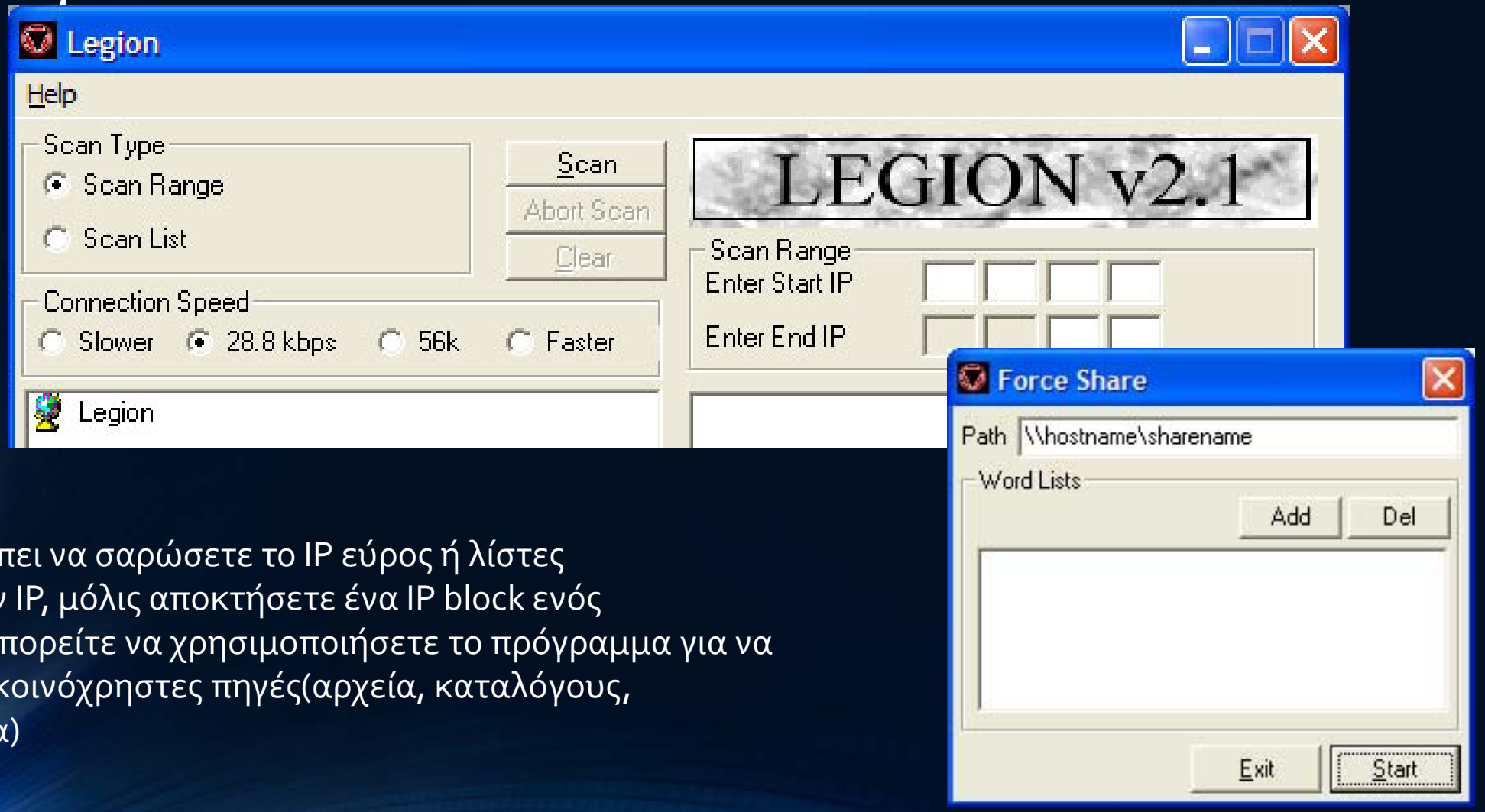
Επιθέσεις Online

- Ο Mallory προσπαθεί να συνδεθεί δοκιμάζοντας πιθανούς κωδικούς
  - Η επίθεση προϋποθέτει τη γνώση του username
  - π.χ. επιθέσεις σε συνδέσεις HTTP, Telnet, POP, FTP, SMB
  - περιπτώσεις: Brutus, ObiWan, pop.c, TeeNet, SNMPbrute, …

Brutus είναι μία από τις ταχύτερα, πιο ευέλικτα remote password crackers.
Το Brutus σαν εργαλείο μπορεί να εφαρμόσει επιθέσεις λεξικού και brute force επιθέσεις όπου τα passwords δημιουργούνται από έναν τυχαίο χαρακτήρα.

ObiWan είναι ένα password cracking εργαλείο που μπορεί να εφαρμοστεί σε έναν διακομιστή.
Το Obiwan χρησιμοποιεί λίστες λέξεων και εναλλαγές χαρακτήρων(αλφαβητικών και αριθμητικών) σαν πιθανά passwords

Legion

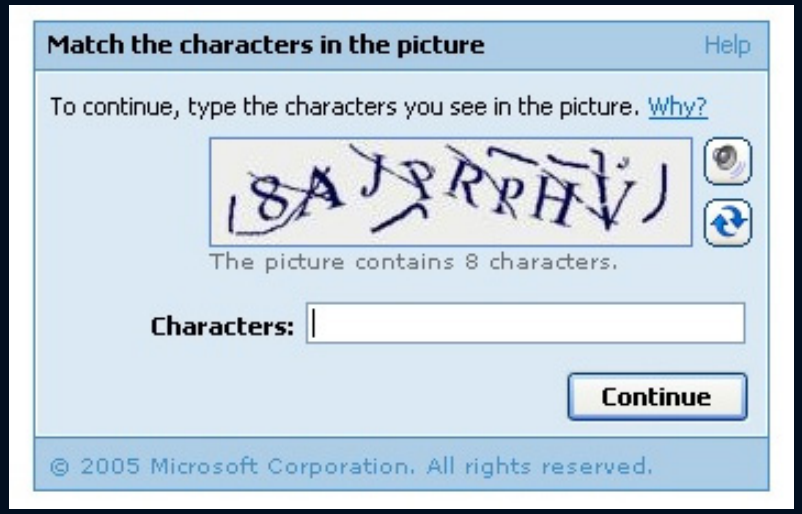


Legion επιτρέπει να σαρώσετε το IP εύρος ή λίστες κοινόχρηστων IP, μόλις αποκτήσετε ένα IP block ενός οργανισμού μπορείτε να χρησιμοποιήσετε το πρόγραμμα για να αναζητήσετε κοινόχρηστες πηγές(αρχεία, καταλόγους, εκτυπωτές κ.α)

Ασφάλεια έναντι online επιθέσεων: CAPTCHAs

Completely Automated Public Turing tests to tell Computers and Humans Apart

- Ποιος συνέλαβε την ιδέα; (Naor, 1996)
- Στόχοι (Motoyama et al, 2010)
  1. Να λύνεται εύκολα από άνθρωπο
  2. Να μη λύνεται εύκολα από Η/Υ
- Κατηγορίες
  - Visual challenges (αλφαριθμητικά με «θόρυβο») *
  - Audio challenges (ηχητικά μηνύματα) ♪
  - Image recognition
    - π.χ Microsoft Asirra *



L. von Ahn, M. Blum, N. Hopper, and J. Langford. CAPTCHA: Using hard AI problems for security. In *Proceedings of Eurocrypt, 2003*, 2003.

- Άλλες ωφέλειες CAPTCHAs
  - Spam σε blogs και forums
  - Μαζικές εγγραφές σε δωρεάν υπηρεσίες αλληλογραφίας,...
  - MISC ♪

CAPTCHAs – Ζητήματα

1. Security and Usability (Bursztein et al, 2010)
   - Πόσο εύκολα/αποδεκτά είναι τα CAPTCHAs από τους χρήστες;
2. "Arms race"
   - Από τη μία, βελτίωση εργαλείων αυτοματοποιημένης επίλυσης
   - Απάντηση κατασκευαστών CAPTCHA: Περισσότερος «θόρυβος»
3. Economics of CAPTCHAs
   - Περίπτωση: Human Solver Services

Koobface botnet

- Koobface είναι ένα hacking σκουλήκι που προσβάλλει τα Microsoft Windows, Mac OS X και Linux
- Στοχεύει στους χρηστες των ιστοσελίδων δικτύωσης όπως το Facebook, το Skype, Yahoo Messenger, και το ηλεκτρονικό ταχυδρομείο ιστοσελίδες όπως το Gmail , το Yahoo Mail, AOL και Mail. Απευθύνεται επίσης και σε άλλες ιστοσελίδες δικτύωσης, όπως το MySpace, Twitter και μπορεί να μολύνει άλλες συσκευές στο ίδιο τοπικό δίκτυο.
- Επιτρέπει σε έναν εισβολέα να έχει πρόσβαση στις προσωπικές πληροφορίες των χρηστών, όπως τραπεζικές πληροφορίες, κωδικούς πρόσβασης, ή προσωπική ταυτότητα (IP address).
- Το Koobface δεν εμποδίζεται από τα CAPTCHAs.
- Όταν χρειάζεται να λύσει ένα CAPTCHA να δημιουργήσετε ένα νέο λογαριασμό, στέλνει την εικόνα CAPTCHA σε έναν άλλο υπολογιστή στο botnet.
- Η CAPTCHA παρουσιάζεται στον χρήστη του άλλου υπολογιστή σε ένα ψευδές popup παράθυρο ασφαλείας.
- Αν απαντήσει εμπρόθεσμα, οι απαντήσεις στέλνονται πίσω και χρησιμοποιούνται από το Koobface ώστε να "αποδείξει" ότι θα μπορούσε να απαντήσει στην πρόκληση.

CAPTCHAs – Ζητήματα

- GYC-είναι ένας δημιουργός λογαριασμού Gmail, Yahoo! Hotmail κ.α. γεμίζει αυτόματαφόρμες εγγραφής. - αυτοματοποιεί τη διαδικασία δημιουργίας λογαριασμών - - Αλλαγή paswords
- Decaptcher λύνει τα captchers μέσω ενός API.
- Pixprofit είναι ένα captcha. Πληρώνουν $ 1 ανά 1000 x captcha.

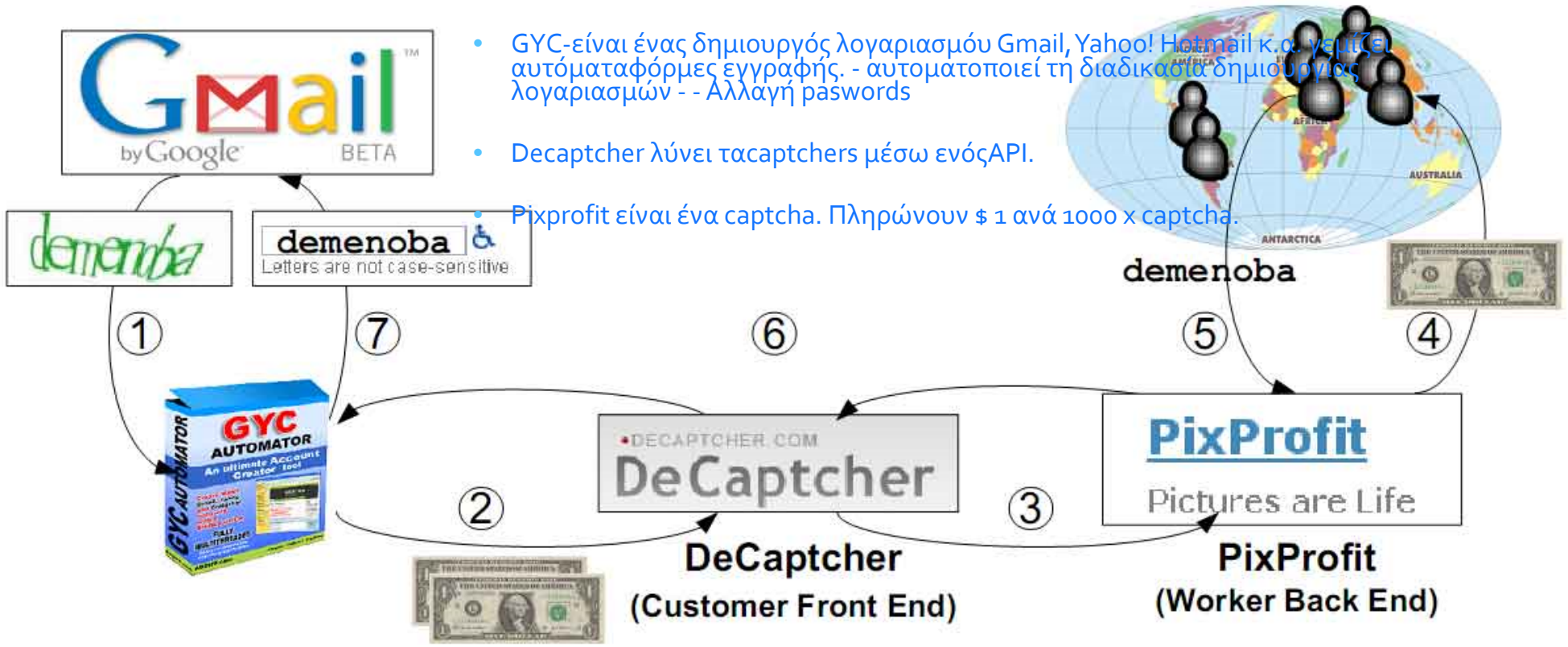


Figure 3: CAPTCHA-solving market workflow: ① GYC Automator attempts to register a Gmail account and is challenged with a Google CAPTCHA. ② GYC uses the DeCaptcher plug-in to solve the CAPTCHA at $2/1,000. ③ DeCaptcher queues the CAPTCHA for a worker on the affiliated PixProfit back end. ④ PixProfit selects a worker and pays at $1/1,000. ⑤ Worker enters a solution to PixProfit, which ⑥ returns it to the plug-in. ⑦ GYC then enters the solution for the CAPTCHA to Gmail to register the account.

Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

Προστασία Αρχείου Κωδικών

Κρυπτογραφικές Τεχνικές

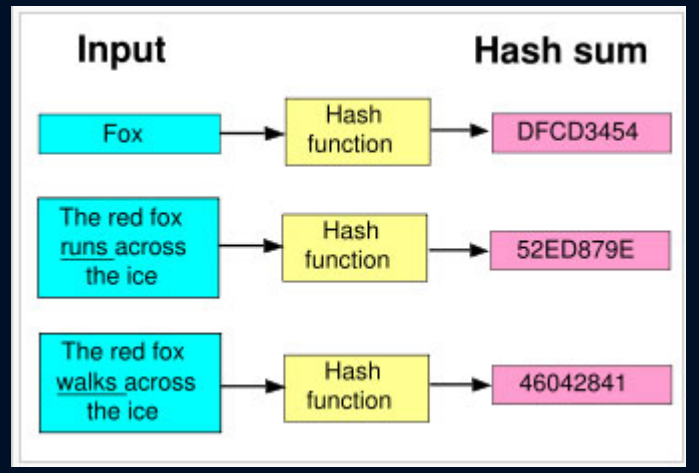
Χρήστες	Κωδικοί
Alice (ID_A)	P_A
Carol (ID_C)	P_C
Dave (ID_D)	P_D
Frank (ID_F)	P_F

- Προβλήματα:

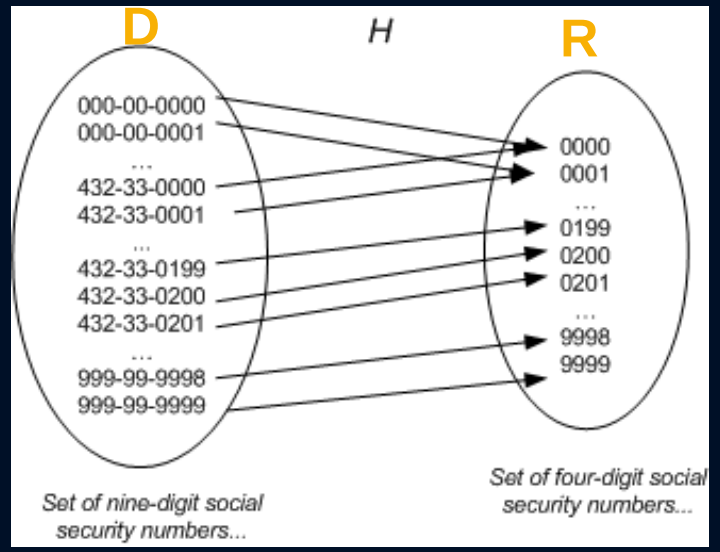
Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Παρένθεση
Συναρτήσεις Hash

- Ιδιότητες Συναρτήσεων Hash
  1. Compression
  - Είσοδος (pre image): Αλφαριθμητικό κάθε μεγέθους.
  - Έξοδος: αλφαριθμητικό μεγέθους X (τιμή hash)
  2. Ευκολία στον υπολογισμό
  - Δεδομένης μιας τιμής x και της συνάρτησης H, είναι εύκολο να βρείς το H(x)

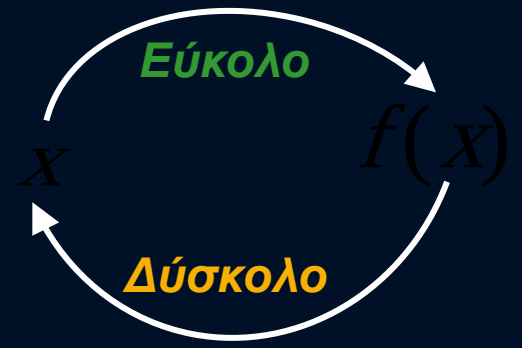


http://en.wikipedia.org/wiki/Hash_algorithm



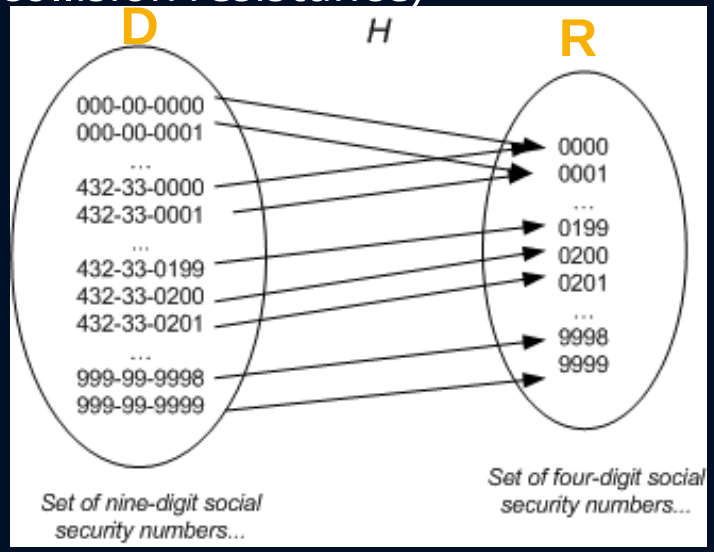
http://msdn.microsoft.com/library/en-us/dnvs05/html/datastructures_guide2-fig09.gif

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001



Κρυπτογραφικές Συναρτήσεις Hash

- Κρυπτογραφικές Συναρτήσεις Hash
  - Μονόδρομες Συναρτήσεις Hash με επιπλέον προστασία από συγκρούσεις (collision resistance)



http://msdn.microsoft.com/library/en-us/dnvs05/html/datastructures_guide2-fig09.gif

Σημείωση: Αν |D| > |R| τότε οι συγκρούσεις είναι αναπόφευκτες, ωστόσο, σε μια κρυπτογραφική συνάρτηση hash είναι δύσκολο να βρεθούν

- Ιδιότητες Κρυπτογραφικών Συναρτήσεων Hash

1. One way: Εύκολο να υπολογίσεις την τιμή hash δεδομένου του αρχικού μηνύματος, δύσκολο να υπολογίσεις το αρχικό μήνυμα δεδομένης της τιμής hash.
2. Collision-Resistance: Δύσκολο να βρεθεί σύγκρουση
   - Σύγκρουση: δύο μηνύματα που δίνουν την ίδια τιμή hash

Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

Προστασία Αρχείου Κωδικών

Κρυπτογραφικές Τεχνικές – Το πρωτόκολλο του Needham

Protocol 11.3: Needham's Password Authentication Protocol

PREMISE:	User U and Host H have setup U's password entry $(ID_U, f(P_U))$ where f is a one-way function; U memorizes password P_U;
GOAL:	U logs in H using her/his password.

1. $U \longrightarrow H$: ID_U;
2. $H \longrightarrow U$: "Input Password:";
3. $U \longrightarrow H$: P_U;
4. H applies f on P_U, finds entry $(ID_U, f(P_U))$ form its archive; Access is granted if the computed $f(P_U P)$ matches the archived.

Needham-Schroeder

Alice

KDC

Bob

N1, Alice θέλει να μιλήσει στον Bob

Κοινό κλειδί της Alice και Bob

E_{Ka}(N1, "Bob", Kab, ticket)

N1 authenticates KDC to Alice

ticket = E_{Kb}(Kab, "Alice")

E_{Kab}(N2), ticket

Bob αποκρυπτογραφεί το εισιτήριο και κατέχει το Kab

E_{Kab}(N2 - 1, N3)

E_{Kab}(N3 - 1)

Nonces χρησιμοποιούνται για την πιστοποίηση κάθε μέρους που κατέχει Kab

- N1, N2, N3 are nonces («αριθμοί που χρησιμοποιούνται μια φορά")

Προστασία Αρχείου Κωδικών

Κρυπτογραφικές Τεχνικές – Το πρωτόκολλο του Needham

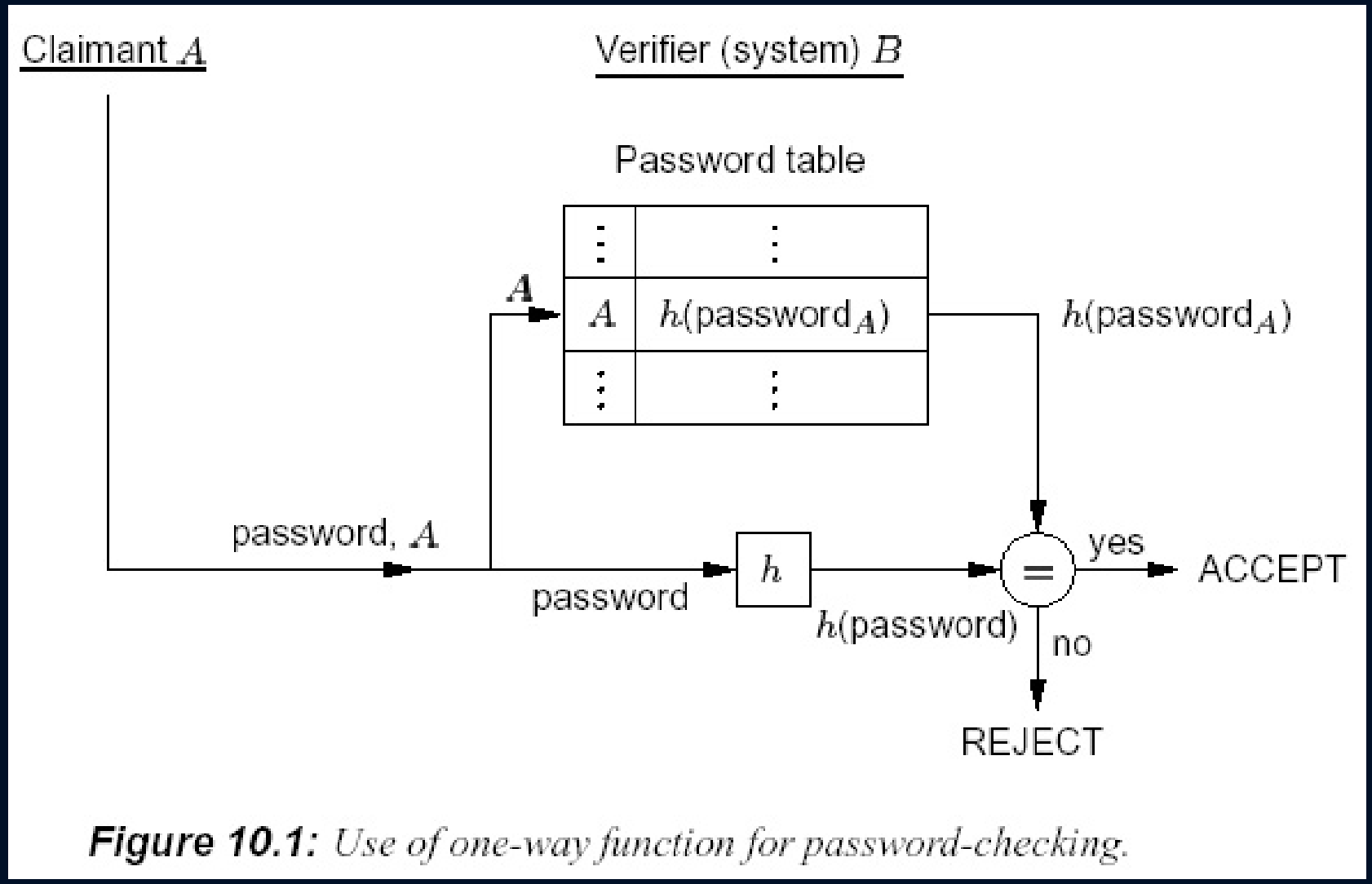
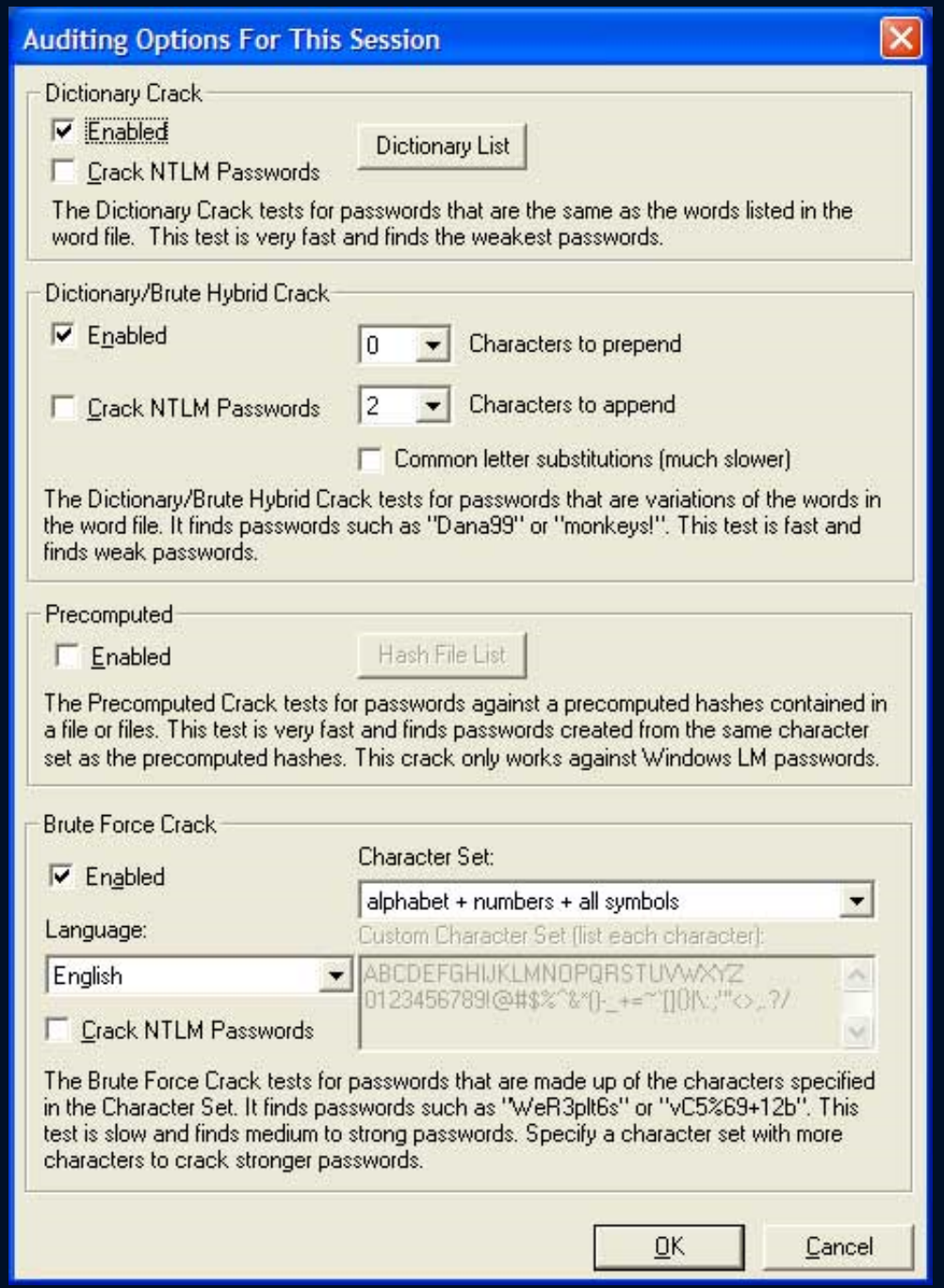


Figure 10.1: *Use of one-way function for password-checking.*

LAN hash Manager Είναι μια γνωστή συνάρτηση κατακερματισμού, που ήταν η κύρια συνάρτηση που ο π Microsoft LAN Manager Χρησιμοποιούσε Microsoft Windows στις εκδόσεις πριν από τα Windows NT για την αποθήκευση των κωδικών πρόσβασης των χρηστών.
NT LAN Manager (NTLM) είναι μια σουίτα πρωτοκόλλων ασφαλείας της Microsoft που παρέχει έλεγχο ταυτότητας, την ακεραιότητα και την εμπιστευτικότητα των χρηστών.
pwdump μας δίνει την έξοδο από τις LM και NTLM hash συναρτήσεις των κωδικών του τοπικού λογαριασμού χρηστή από τον Security Account Manager (SAM).Μπορεί κάποιος να το τρέξει σαν administrator και να έχει πρόσβαση στις τιμές των χρηστών

Επιθέσεις Offline (Παθητικές)

- Ο Mallory αποκτά πρόσβαση στο αρχείο («κρυπτογραφημένων») κωδικών του συστήματος (π.χ. /etc/passwd, SAM file)
- σ.σ. ο Mallory έχει ήδη συνδεθεί στο σύστημα, ως απλός χρήστης (ή administrator)
- Στη συνέχεια ο Mallory εκτελεί ένα πρόγραμμα ανάκτησης κωδικών
- Εργαλεία: pwdump, LophtCrack, John the Ripper, Crack …
- Brute force ή Dictionary attacks



Επιθέσεις Offline Περίπτωση: Lophtcrack

LophtCrack είναι ένα λογιστικό για την αποθήκευση και ανάκτηση του κωδικού πρόσβασης. χρησιμοποιείται για τη δοκιμή της αντοχής του κωδικού και για την ανάκτηση κωδικού πρόσβασης, χρησιμοποιώντας επιθέσεις λεξικού,brute-force επιθέσεις, υβριδικές επιθέσεις, και οι πίνακες ουράνιου τόξου Αποτέλεσε την πιο δημοφιλή επιλογή των κράκερ

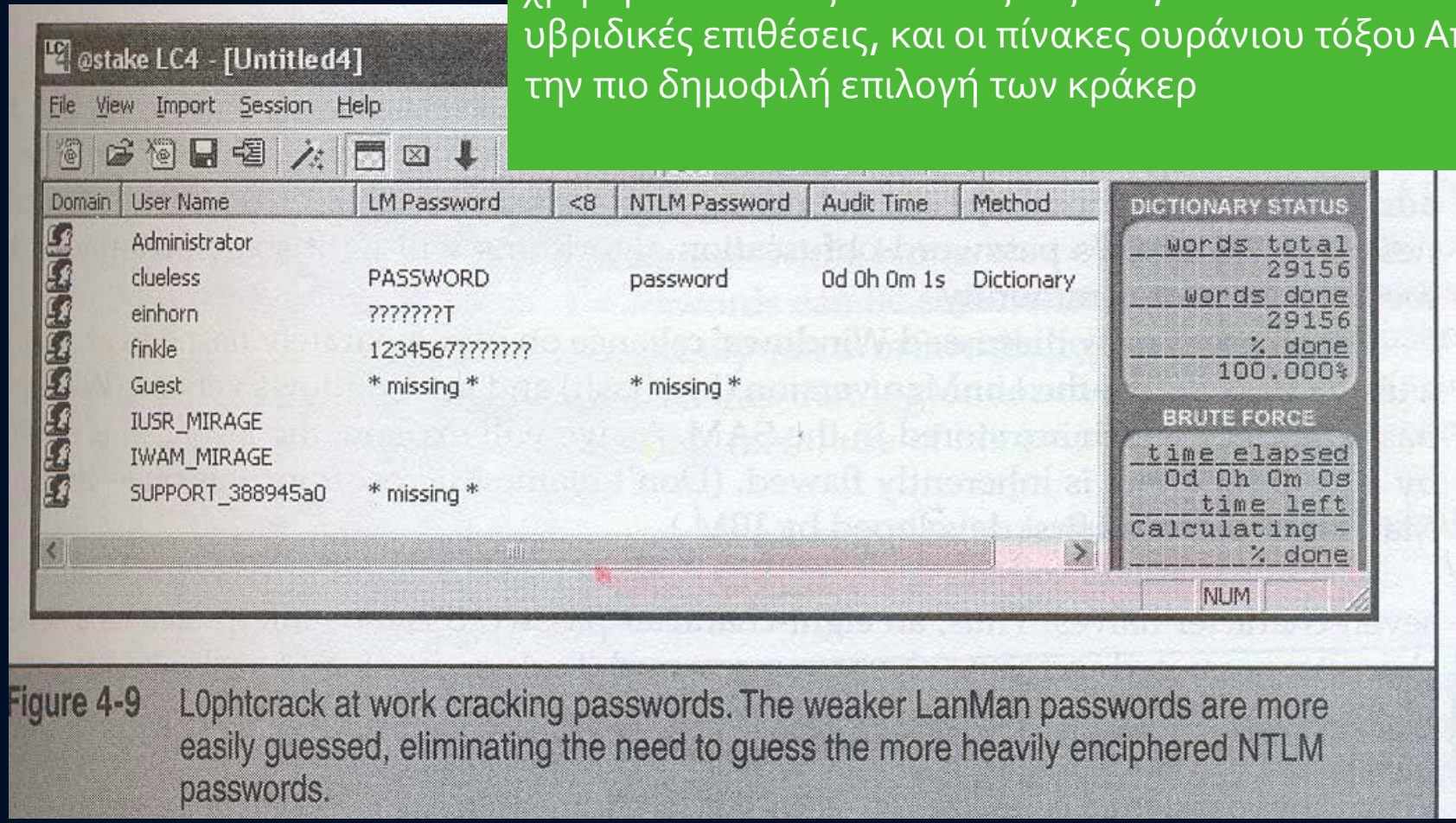
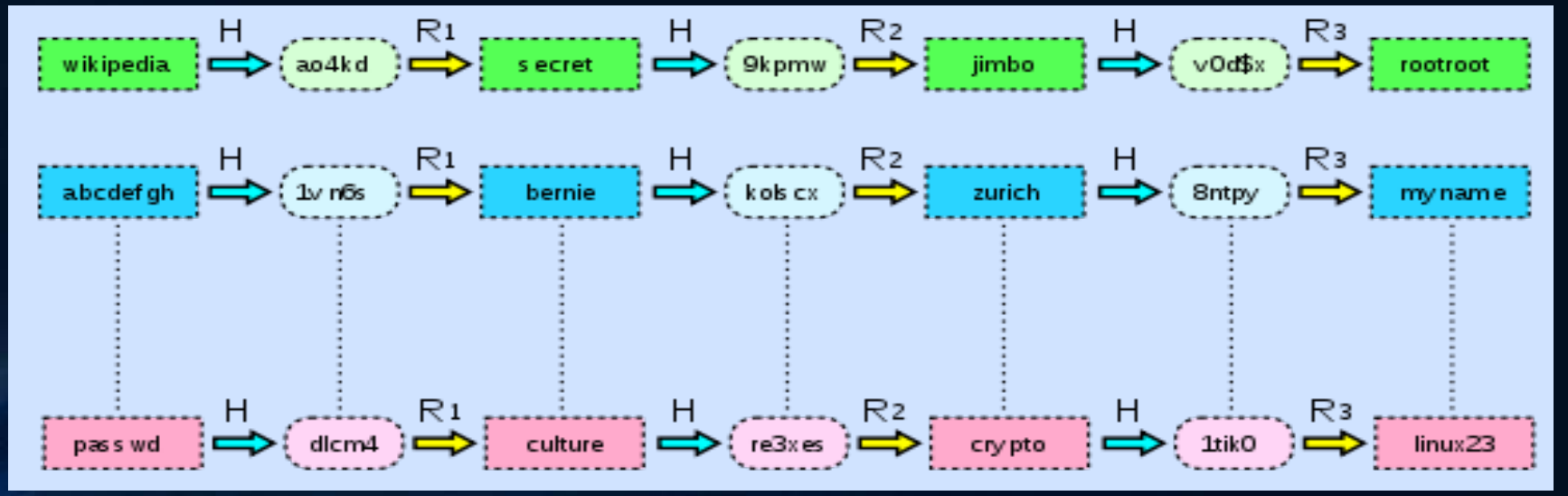


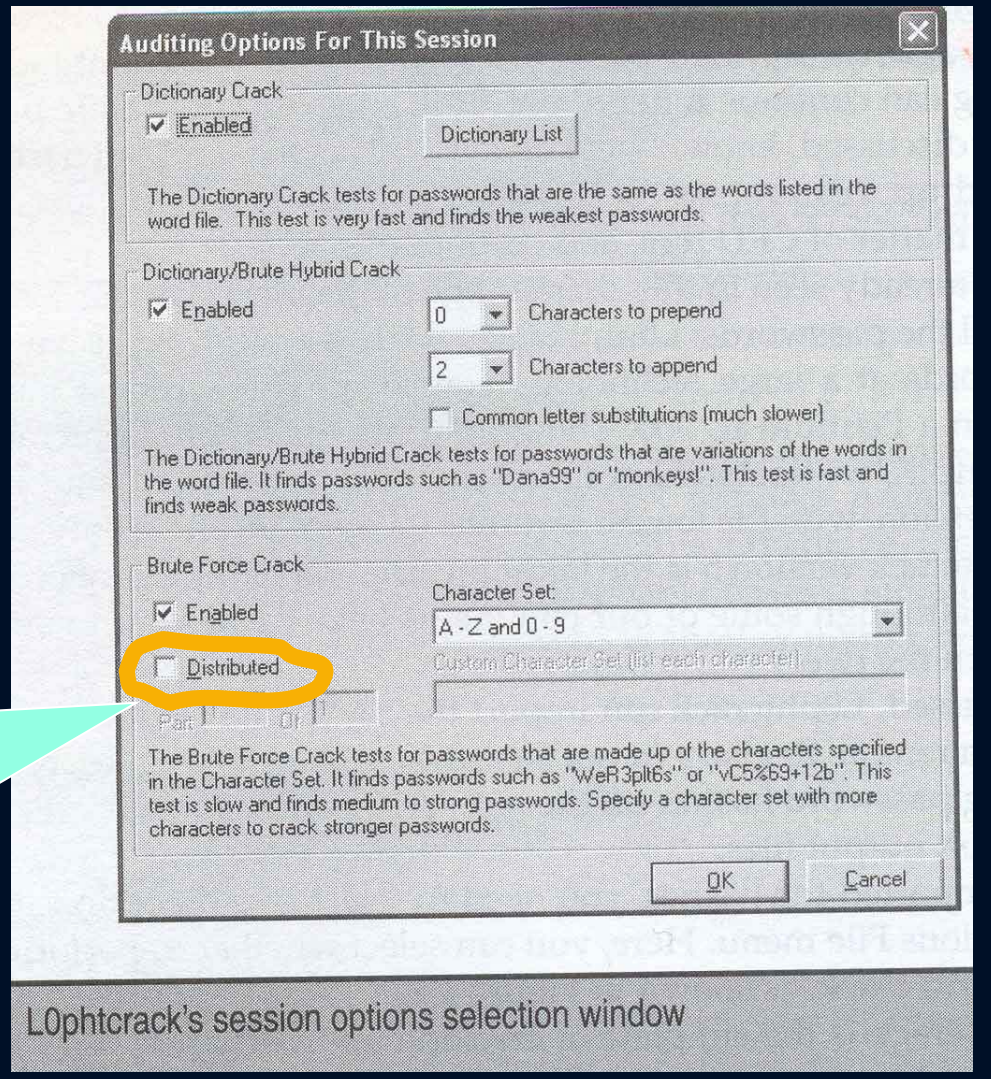
Figure 4-9 L0phtcrack at work cracking passwords. The weaker LanMan passwords are more easily guessed, eliminating the need to guess the more heavily enciphered NTLM passwords.

- Ένας πίνακας ουράνιου τόξου είναι ένας πίνακας που περιέχει καταγεγραμμένες την έξοδό πολλών hash συναρτήσεων για συγκεκριμένες λέξεις.
- Οι πίνακες που χρησιμοποιούνται συνήθως για την ανάκτηση ενός plaintext password μέχρι ένα ορισμένο μήκος που αποτελείται από μια περιορισμένη σειρά χαρακτήρων.
- χρησιμοποιεί λιγότερο χρόνο επεξεργασίας του υπολογιστή και περισσότερο αποθηκευτικό χώρο από ό, τι μια επίθεση brute force που υπολογίζει την hash για κάθε προσπάθεια. Η Χρήση ενός πλήκτρου λειτουργίας κάνει δύσκολη την επίθεση αυτή.



Επιθέσεις Offline
Περίπτωση: Lophtcrack

Η διαδικασία ανάκτησης μπορεί να κατανεμηθεί, δηλ. να υλοποιείται παράλληλα σε περισσότερους του ενός Η/Υ !!!



L0phtcrack's session options selection window

(Offline) Επίθεση Λεξικού (Dictionary Attack)

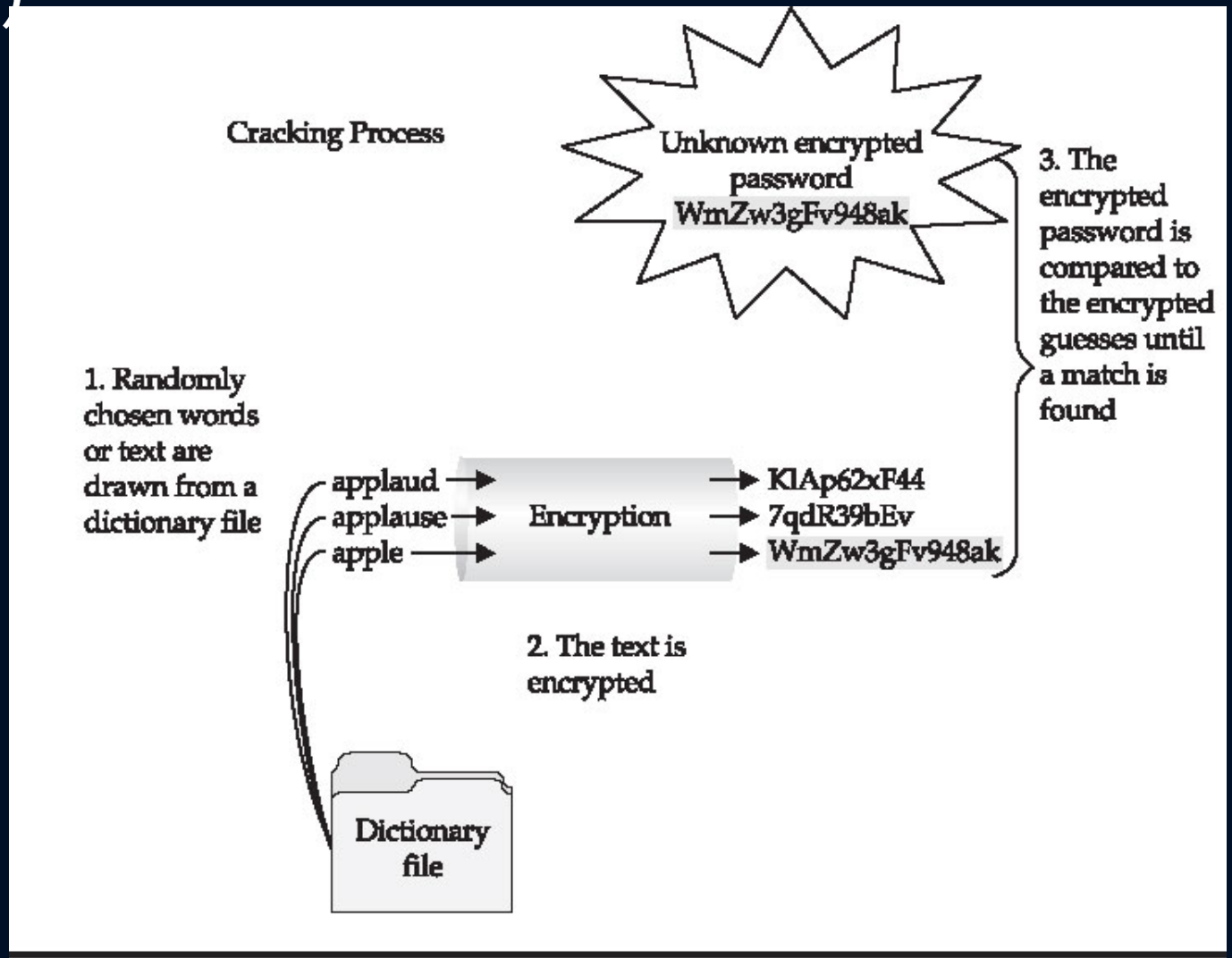


Figure 7-4. How password cracking is accomplished

Hacking Exposed Fifth Edition, McClure, Scambray and Kurtz, 2005

(Klein, 1990)

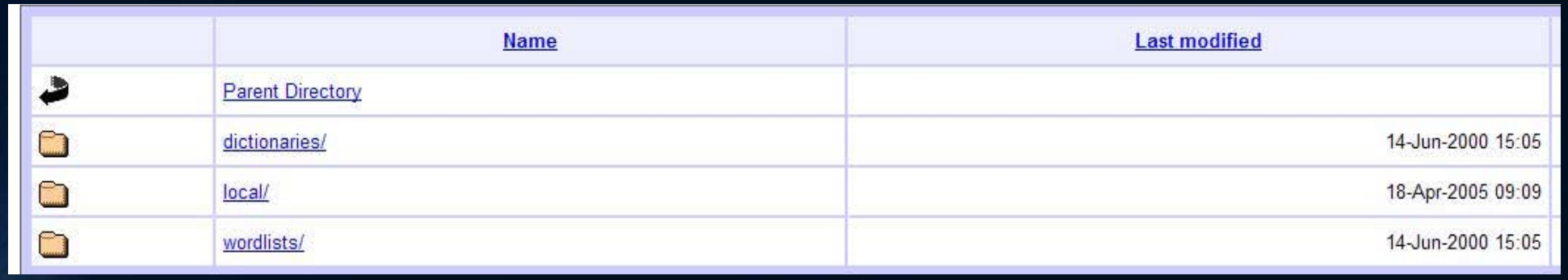
Table 20.5 Passwords Cracked from a Sample Set of 13,797 Accounts [KLE190]

Type of Password	Search Size	Number of Matches	Percentage of Passwords Matched	Cost/Benefit Ratio[a]
User/account name	130	368	2.7%	2.830
Character sequences	866	22	0.2%	0.025
Numbers	427	9	0.1%	0.021
Chinese	392	56	0.4%	0.143
Place names	628	82	0.6%	0.131
Common names	2239	548	4.0%	0.245
Female names	4280	161	1.2%	0.038
Male names	2866	140	1.0%	0.049
Uncommon names	4955	130	0.9%	0.026
Myths & legends	1246	66	0.5%	0.053
Shakespearean	473	11	0.1%	0.023
Sports terms	238	32	0.2%	0.134
Science fiction	691	59	0.4%	0.085
Movies and actors	99	12	0.1%	0.121
Cartoons	92	9	0.1%	0.098
Famous people	290	55	0.4%	0.190
Phrases and patterns	933	253	1.8%	0.271
Surnames	33	9	0.1%	0.273
Biology	58	1	0.0%	0.017
System dictionary	19683	1027	7.4%	0.052
Machine names	9018	132	1.0%	0.015
Mnemonics	14	2	0.0%	0.143
King James bible	7525	83	0.6%	0.011
Miscellaneous words	3212	54	0.4%	0.017
Yiddish words	56	0	0.0%	0.000
Asteroids	2407	19	0.1%	0.007
TOTAL	62727	3340	24.2%	0.053

[a]Computed as the number of matches divided by the search size. The more words that needed to be tested for a match, the lower the cost/benefit ratio.

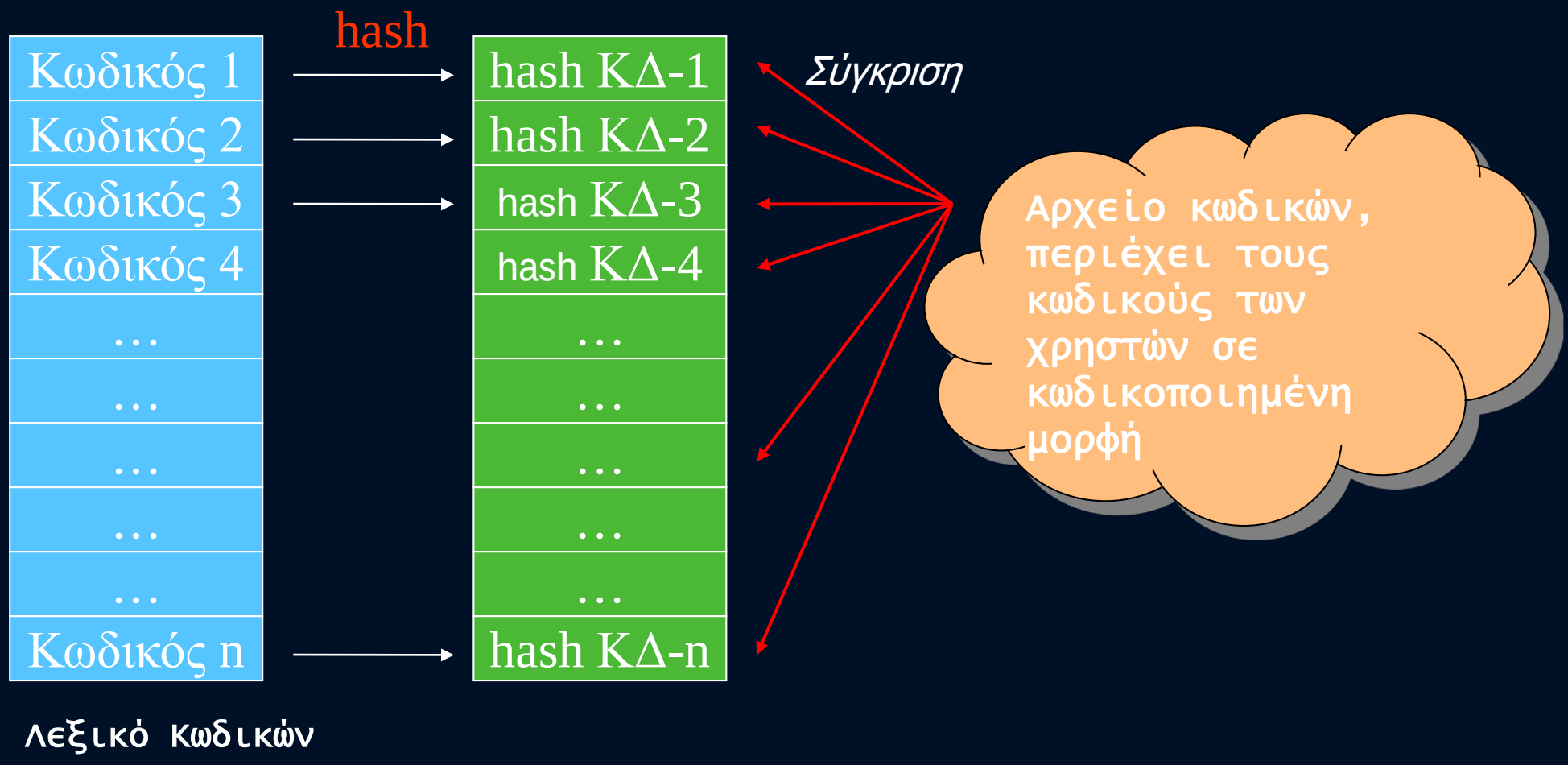
Επιθέσεις Λεξικού (Dictionary attacks)

- Λεξικά
  - Λίστες με πιθανούς (υποψήφιους) κωδικούς *



	Name	Last modified
	Parent Directory	
	dictionaries/	14-Jun-2000 15:05
	local/	18-Apr-2005 09:09
	wordlists/	14-Jun-2000 15:05

(Offline) Επίθεση Λεξικού (Dictionary Attack)



http://www.csse.monash.edu.au/courseware/cse2500/ppt/Authentication.ppt

Επιθέσεις Λεξικού (Dictionary attacks)

- Αν οι τιμές hash του λεξικού έχουν προϋπολογιστεί, τότε το «σπάσιμο» του (των) κωδικού (-ών) απαιτεί λιγότερο χρόνο !
  - Trade-off μεταξύ υπολογιστικού χρόνου & αποθηκευτικού χώρου

We generated several TB of rainbow tables for LM, NTLM, MD5, SHA1 and other hash algorithms.

The largest tables (ntlm_ascii-32-95#1-8 and md5_ascii-32-95#1-8, 576 GB each) crack any plaintext (all 95 chars on standard keyboard) up to 8 characters in 5 to 40 minutes on personal computer. It requires an exhaustive search of 6,704,780,954,517,120 (roughly $2^{52.5}$) plaintexts.

http://project-rainbowcrack.com/

RainbowCrack 1.4

File Edit Rainbow Table Help

Hash	Plaintext	Plaintext in Hex
0f5e96fb74127e9d1cfcbbc9ele60845	-K!f <7	2d4b2166203c37
d3f6a305f86602829750f8b7b6ef38d3	OQXaz,D	4f5158617a2c44
523a33c09dad64a00e6fd41491873b18	j]GF+t*	6a5d47462b742a
f8099235efcd5aa4726362c56324d168	j13J@Sj	6a31334a40536a
fd0a76f444a24bd18990c3f58f1f5aaf	,P7296)	2c503732393629
57c45cfc7e7f4de2c39f096660186aa4	}az_H}p	7d617a5f487d70
e7b53d09c35c4d56abf6c9c52bbdd3ad	52ER^9Q	353245525e3951
5f9013dd0b0e32ab4d89c2b4af074c69	|bAZ<aK	7c62415a3c614b
b8a4e37512a3ac76a567c1231244f3f4	41$N{R&	346c244e7b5226
7d5a2e2f03191156eb5f64aa2e7f933b	-B5 ~Fq	2d4235207e4671

Messages

```
statistics
----------------------------------------------------------
plaintext found:                                10 of 10
total time:                                     220.03 s
  time of chain traverse:                       109.19 s
  time of alarm check:                          48.11 s
  time of wait:                                 31.48 s
  time of other operation:                      31.25 s
time of disk read:                              140.25 s
hash & reduce calculation of chain traverse:    55448657022
hash & reduce calculation of alarm check:       11077939499
number of alarm:                                468123
speed of chain traverse:                        507.84 million/s
speed of alarm check:                           230.26 million/s
```