ΤΕΙ ΗΠΕΙΡΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε
ΜΕΤΑΠΤΙΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

Ασφάλεια

ΛΙΑΓΚΟΥ ΒΑΣΙΛΙΚΗ
ΔΙΑΛΕΞΗ-ΙΙ

- Αρχικά χρησιμοποιούμε ένα user salt που είναι ένα t-bit τυχαίο αλφαριθμητικό

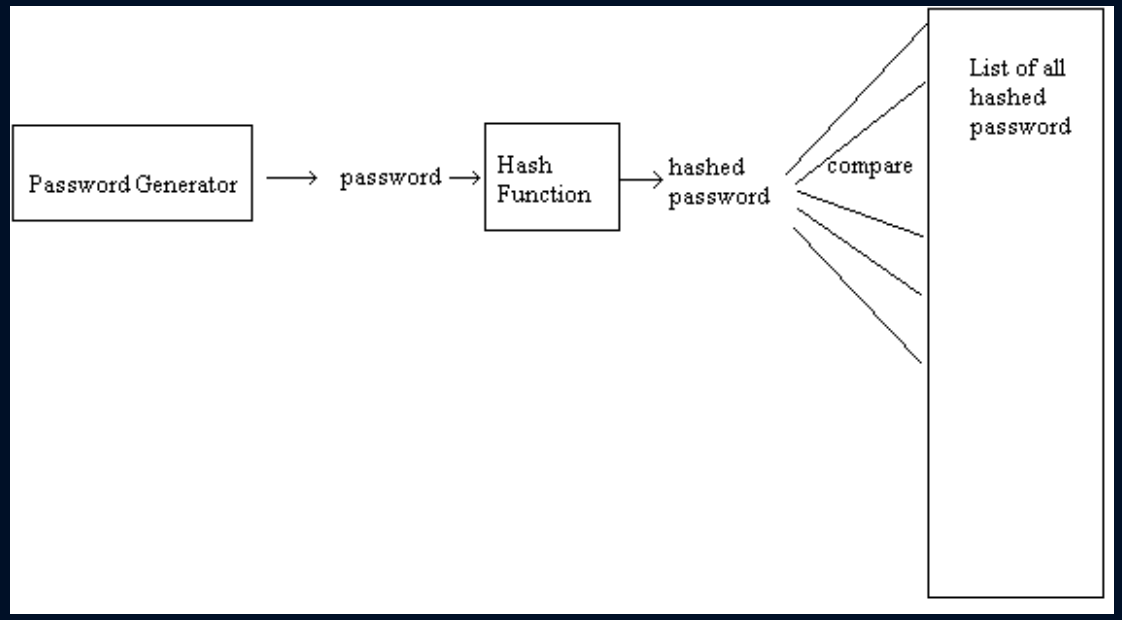
- Ο hashed κωδικός και το salt αποθηκεύονται στα αρχεία κωδικών
- Όταν ο χρήστης εισάγει το password το σύστημα κοιτά το salt και εφαρμόζει μια μονόδρομη συνάρτηση στο password όπως έχει τροποποιηθεί ή επαυξηθεί με βάση το salt

- Το salt βοηθάει να μην επιτρέπεται σε κάθε χρήστη να ανευρίσκουμε τον κωδικό, μιας και δύο χρήστες με τον ίδιο κωδικό έχουν διαφορετικά αρχεία κωδικών

Προστασία Αρχείου Κωδικών

Τεχνική "Salting"

- Μπορώ να δυσχεραίνω τις «μαζικές» offline επιθέσεις;
  - … τύπου «επίθεση σε οποιοδήποτε λογαριασμό»

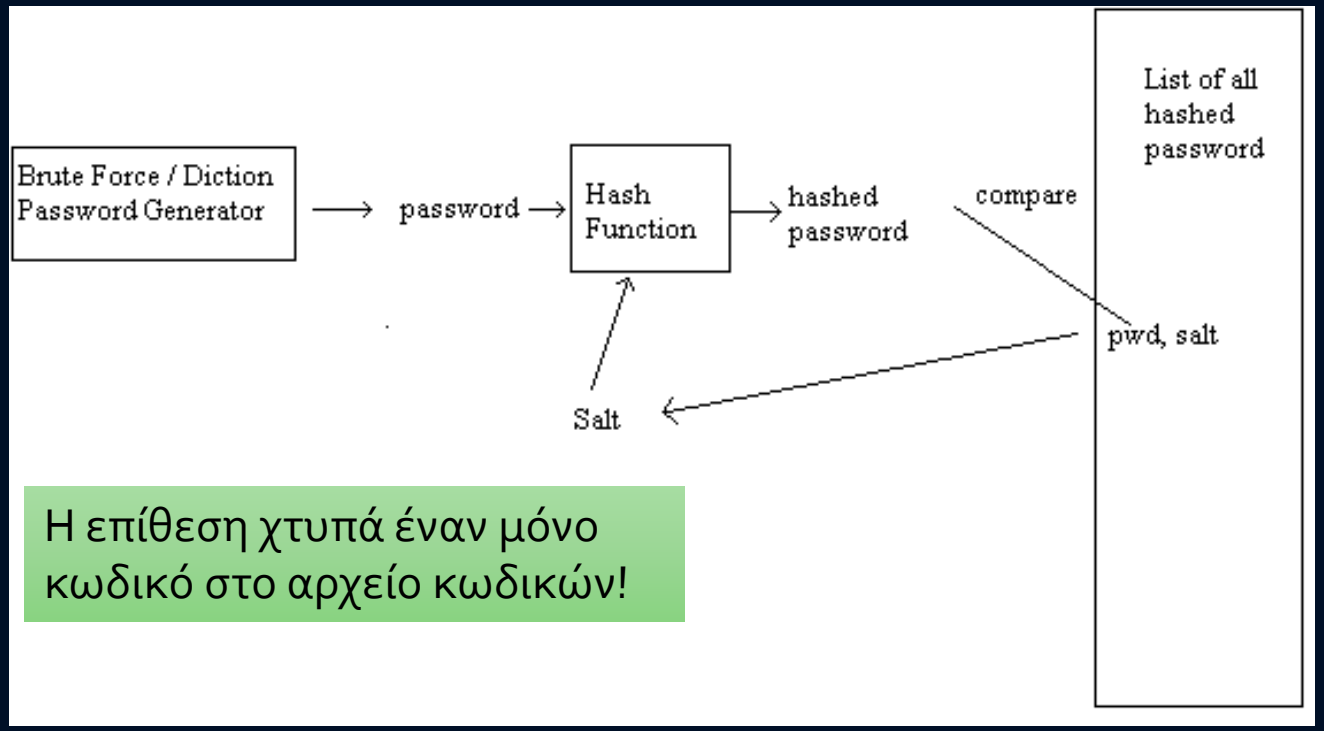


- Η παραπάνω επίθεση «χτυπά» ταυτόχρονα όλους τους κωδικούς στο αρχείο κωδικών του συστήματος

Προστασία Αρχείου Κωδικών

Τεχνική "Salting"

1. Αντιστοίχιση μιας τυχαίας τιμής (salt) σε κάθε password
   - Χρήση διαφορετικών salts για διαφορετικά passwords
2. Η τιμή hash δέχεται ως είσοδο το password ΚΑΙ το salt
3. Στο αρχείο κωδικών, αποθήκευση του: {hash(password, salt), salt}



Η επίθεση χτυπά έναν μόνο κωδικό στο αρχείο κωδικών!

Προστασία Αρχείου Κωδικών

Έλεγχος Πρόσβασης

(Gollmann, 2010)

Policies

1. Only privileged users may have write access to pass file
2. Only privileged users have read access to password file
   - Shadow password file

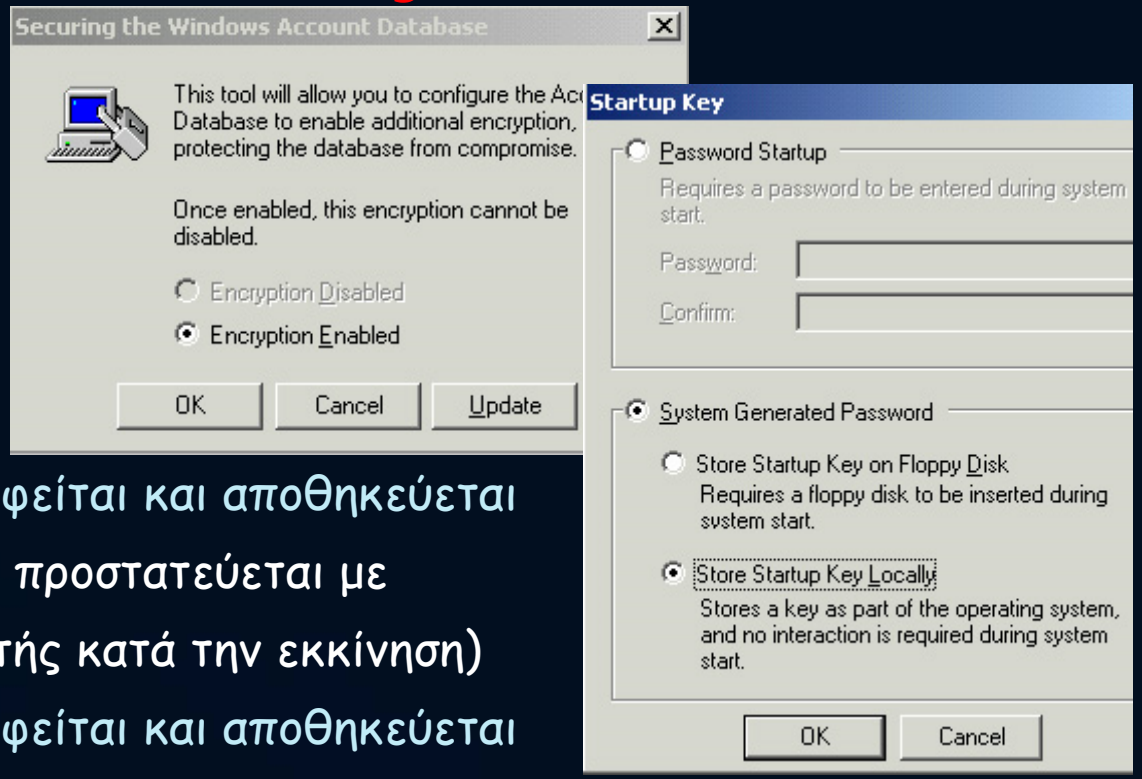
Προστασία Αρχείου Κωδικών

*

Περίπτωση: Syskey (Windows)- Protecting the SAM DB

a) Τα passwords αποθηκεύονται στη βάση SAM σε hashed μορφή

b) Η ΒΔ κρυπτογραφείται με ένα κλειδί *K*. Επιλογές:



1. Το K δημιουργείται, κρυπτογραφείται και αποθηκεύεται τοπικά. Η πρόσβαση στο κλειδί προστατεύεται με password (το δίνει ο διαχειριστής κατά την εκκίνηση)
2. Το K δημιουργείται, κρυπτογραφείται και αποθηκεύεται σε εξωτερικό μέσο (π.χ. USB, CD, smartcard). Το σύστημα εκκινεί όταν ο εισαχθεί το σωστό μέσο αποθήκευσης.

One Time Password(OTP)

- Δυο είσοδοι χρειάζονται για την δημιουργία ενός OTP
  - Χρονικός Παράγοντας ή Αριθμός Κλικς
  - Seed

- Τύποι OTP
  - Αυθεντικοποίηση με βάση τα χρόνο
  - Αυθεντικοποίηση με βάση το γεγονός
  - Αυθεντικοποίηση με βάση την πρόκληση(chalenge)

One Time Password(OTP)

	OTP Με βάση το χρόνο	OTP Με βάση το γεγονός	Challenge Response
Ασφάλεια	Πιο ασφαλές από το γεγονός	Λιγότερο Ασφαλές	Πιο ασφαλές από το χρονικό
Ευχρηστία	Εύχρηστο	Εύχρηστό	Πιο Περίπλοκο
Χρήση Πόρων Δικτύου	Έχει λίγο φόρτο δικτύου	Έχει λίγο φόρτο δικτύου	Χρειάζεται περισσότερο φόρτο δικτύου

OTP λίστας

- Παράδειγμα:
- Εφαρμόζουμε Hash στον κωδικό 1000 φορές, αποθηκεύουμε το αποτέλεσμα στο διακομιστή
- Ο client εφαρμόζει hash 999 φορές, και τα στέλνει στον server
- Ο Διακομιστής επαληθεύει τις τιμές που έλαβε με τις αποθηκευμένες τιμές
- Αποθηκεύει την hash που έλαβε
- Πρέπει να επανεκινέιται

4. One-Time Passwords

Το σχήμα του Lamport

Σκοπός (Lamport, 1981):

- Η Alice θα αυθεντικοποιηθεί έως n φορές, θα θυμάται μόνον ένα password και δε θα είναι δυνατές επιθέσεις επανάληψης

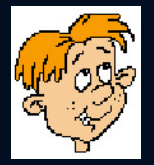
Πρωτόκολλο:

- Ένα master password P_A γίνεται hash n φορές με την κρυπτογραφική συνάρτηση H

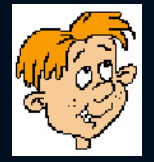
$$H^n(P_A) = H(\ldots(H(P_A))\ldots)$$

Χρήστες	Κωδικοί
Alice (ID_A)	$H^n(P_A)$
Carol (ID_C)	$H^n(P_C)$
Dave (ID_D)	$H^n(P_D)$

ID_A , $H^{n-1}(P_A)$



OKAY !!!



Χρήστες	Κωδικοί
Alice (ID_A)	$H^{n-1}(P_A)$
Carol (ID_C)	$H^n(P_A)$
Dave (ID_D)	$H^n(P_A)$

Το σύστημα S/KEY (Haller, 1994) στηρίζεται στο σχήμα του Lamport

Lamport's Hash

- One-time passwords
- Server αποθηκεύει n και $(hash^n$ (password)
- Ο χρήστης στέλνει x =($hash^{n-1}$ (password)
- Ο Διακομιστής υπολογίζει το hash (x), αν είναι ίσο με την αποθηκευμένη τιμή, αντικαθιστά την αποθηκευμένη τιμή με n-1, x
- Ασφαλής από υποκλοπές, παραβίαση του διακομιστή που δεν αποτελεί πρόβλημα για τον χρήστη
- Δεν χρησημοποιεί κρυπτογραφία δημόσιου κλειδιού
- Η Αυθεντικοποίηση δεν είναι αμοιβαία
- Προσθέστε salt στον κωδικό πρόσβασης πριν το hashing
  - Σε περίπτωση που η Alice χρησιμοποιεί τον ίδιο κωδικό σε πολλαπλά συστήματα
  - Το Salt πρέπει να αποθηκεύεται στο σύστημα της Αλίκης
  - Ο Server χρησιμοποιεί ($hash^n$ (password|salt)

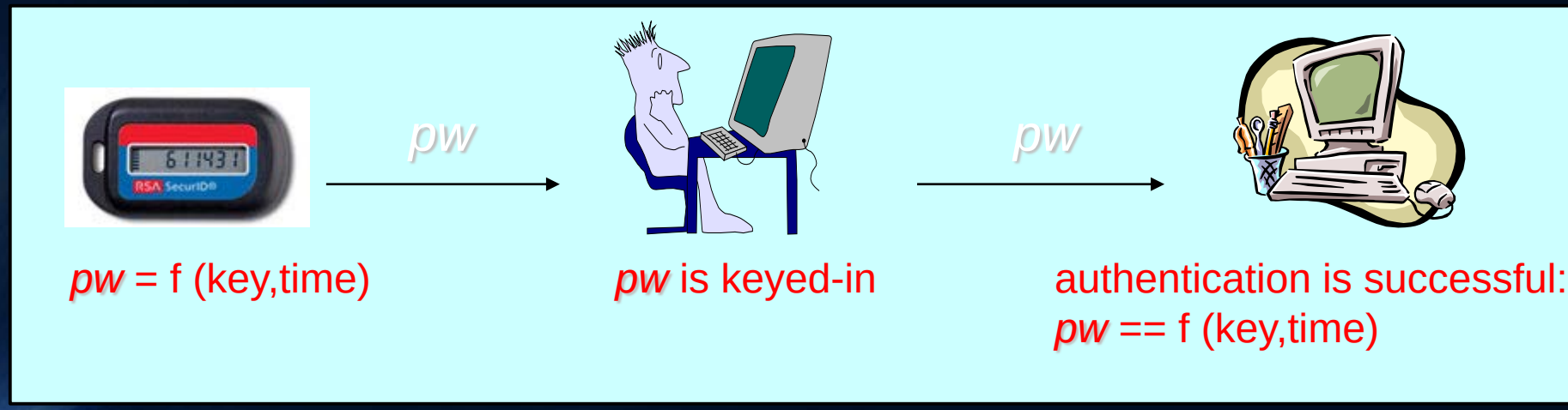
OTP Γεννήτριες(Tokens)

- παραδείγματα
  - RSA
  - VASCO Digipass
- Χρησιμοποιεί μπλοκ κρυπτογράφηση
  - επανειλημμένη κρυπτογραφήση
  - Συνεχώς ανανεώνονται κάθε x δευτερόλεπτα
  - Ενημέρωση κάθε φορά που πατάει το κουμπί ο χρήστης
- Ορισμένες δρουν σε δύο κατευθυνσεις
  - Ο χρήστης βάζει το OTP
  - Ο Διακομιστής επιστρέφει το OTP, στον χρήστη (με το χέρι) συγκρίνοντας το με την τιμή του token

One-Time Passwords

Ταυτοποίηση με tokens (Κάτι που έχω)

- Σύγχρονες τεχνικές
  - Η συσκευή και ο server «συντονίζονται»
    - π.χ. timestamps, counters
- Ασύγχρονες τεχνικές
  - Πρωτόκολλα πρόκλησης-απάντησης
    - Challenge-response protocols



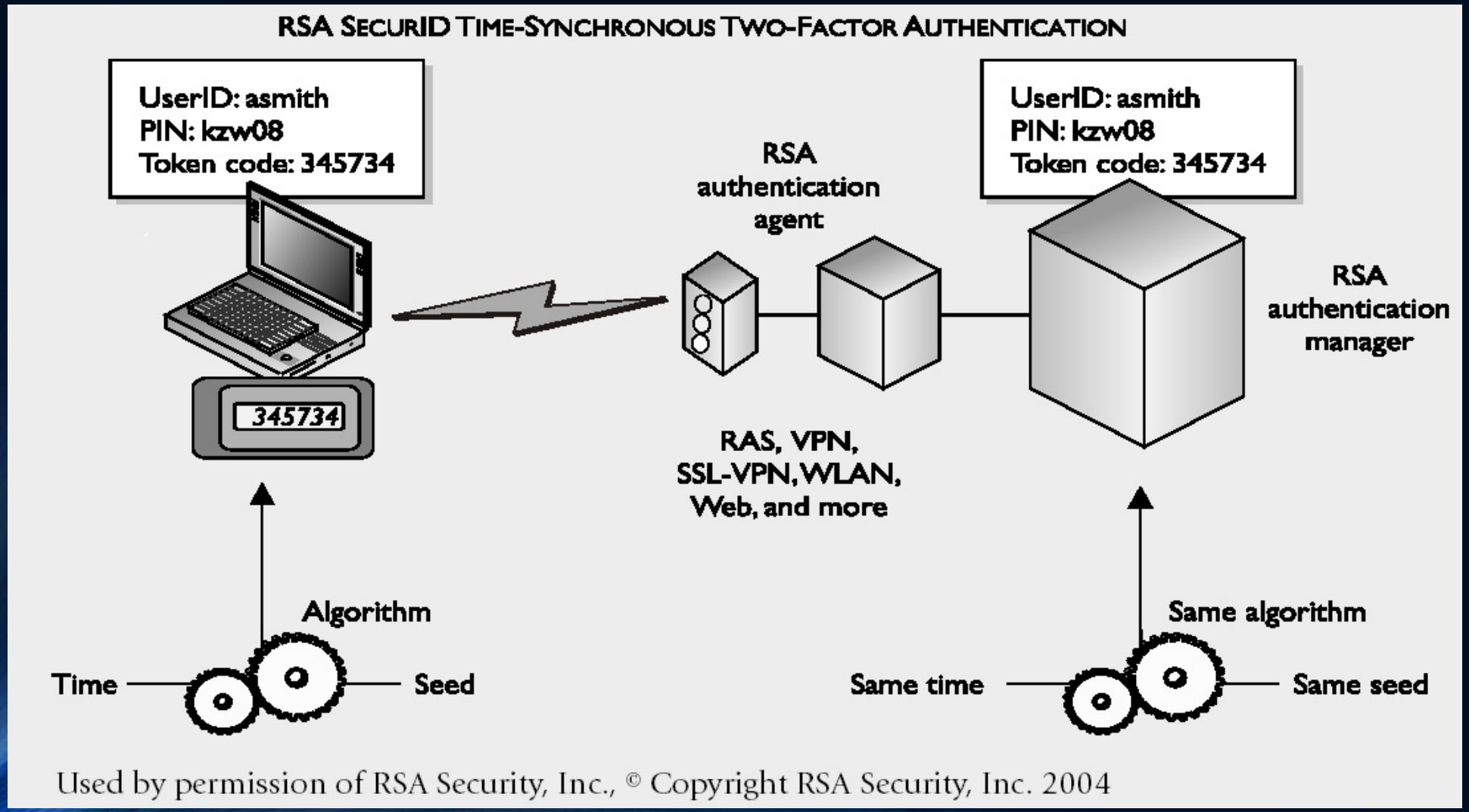
Σύγχρονες Τεχνικές

Προβληματισμοί στην χρήση Tokens

- Απαιτείται Βοήθεια
- Ο συγχρονισμός δεν είναι τέλειος
- Πρόβλημα λήξης της μπαταρίας
- Κόστος 15- 25 ευρω (τράπεζες με εκατομμύρια πελάτες)
- Ο χρήστης χρειάζεται ακόμα pin (κάτι που ξέρετε + κάτι που έχετε)
- Μόνο πρόσφατα εχει ενσωματωθεί με τα κινητά τηλέφωνα
- Ακόμα πιο σπάνιο να έχουν πολλαπλά tokens σε μια συσκευή
- Χρήση Μη-τυποποιημένων αλγόριθμων

One-Time Passwords* - Σύγχρονες Τεχνικές

Case: RSA SecurID



One-Time Passwords - Ασύγχρονες Τεχνικές

Case: 2-factor authentication

challenge

pw

challenge

pw

pw = f (key,challenge, [PIN])

challenge is keyed-in

pw is keyed-in

authentication is successful:
pw == f (key,challenge, [PIN])

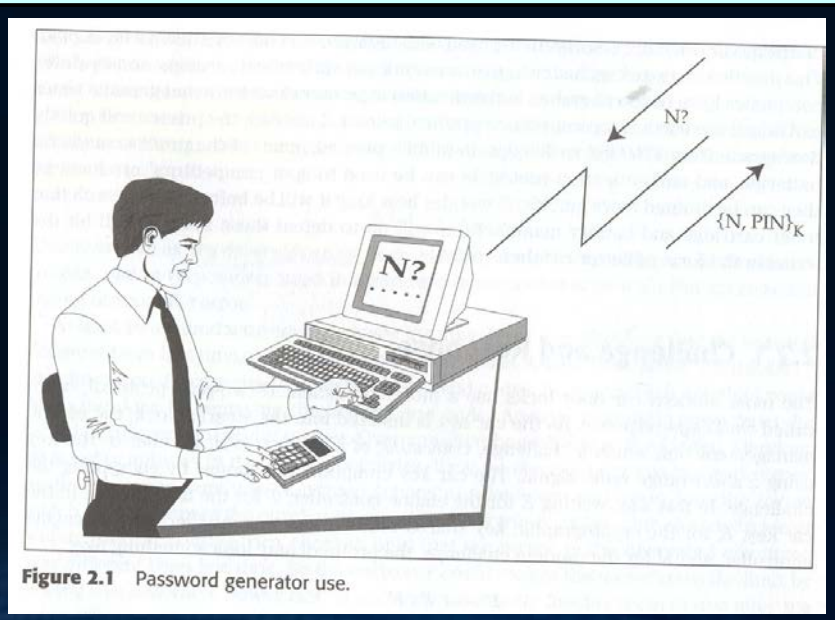


Figure 2.1 Password generator use.

Μειονεκτήματα ελέγχου ταυτότητας μονού παράγοντα

- Αν το μυστικό παραβιαστεί, μπορεί να επιτευχθειο πλήρης έλεγχος ταυτότητας
- Οι επιθέσεις phishing μπορεί να είναι επιτυχής και να κυνδινέψει ο έλεγχος ταυτότητας

- Authentication βασίζεται σε
- Παράγοντας της Γνώσης (κάτι που ξέρετε, σαν τον κωδικό πρόσβασης)
- Παράγοντας Κατοχής (κάτι που έχετε, όπως ένα τηλέφωνο ή άλλη ένδειξη)
- Παράγοντας ύπαρξης (κάτι που είναι, όπως ένα δακτυλικό αποτύπωμα ή άλλα βιομετρικά στοιχεία)

Security Engineering, Anderson, 2001 *

Case: *Γεννήτορες Κωδικών (2-factor authentication)*

- Το πρωτόκολλο:

1. Μια «έξυπνη» συσκευή έχει αποθηκευμένο το κλειδί K
2. *Ο Bob εισάγει τον αριθμό PIN στη συσκευή.*

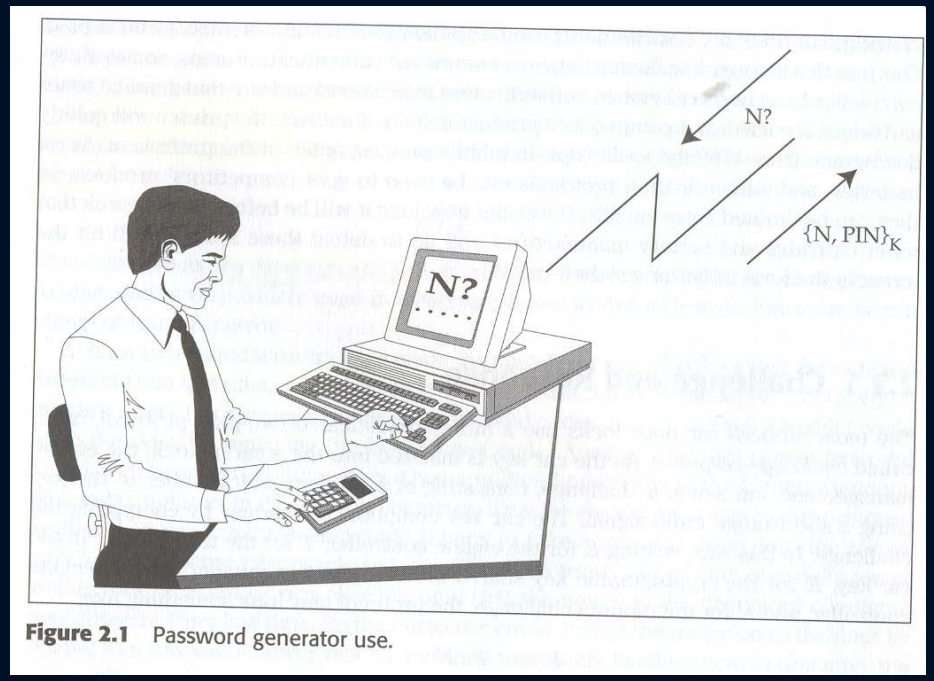
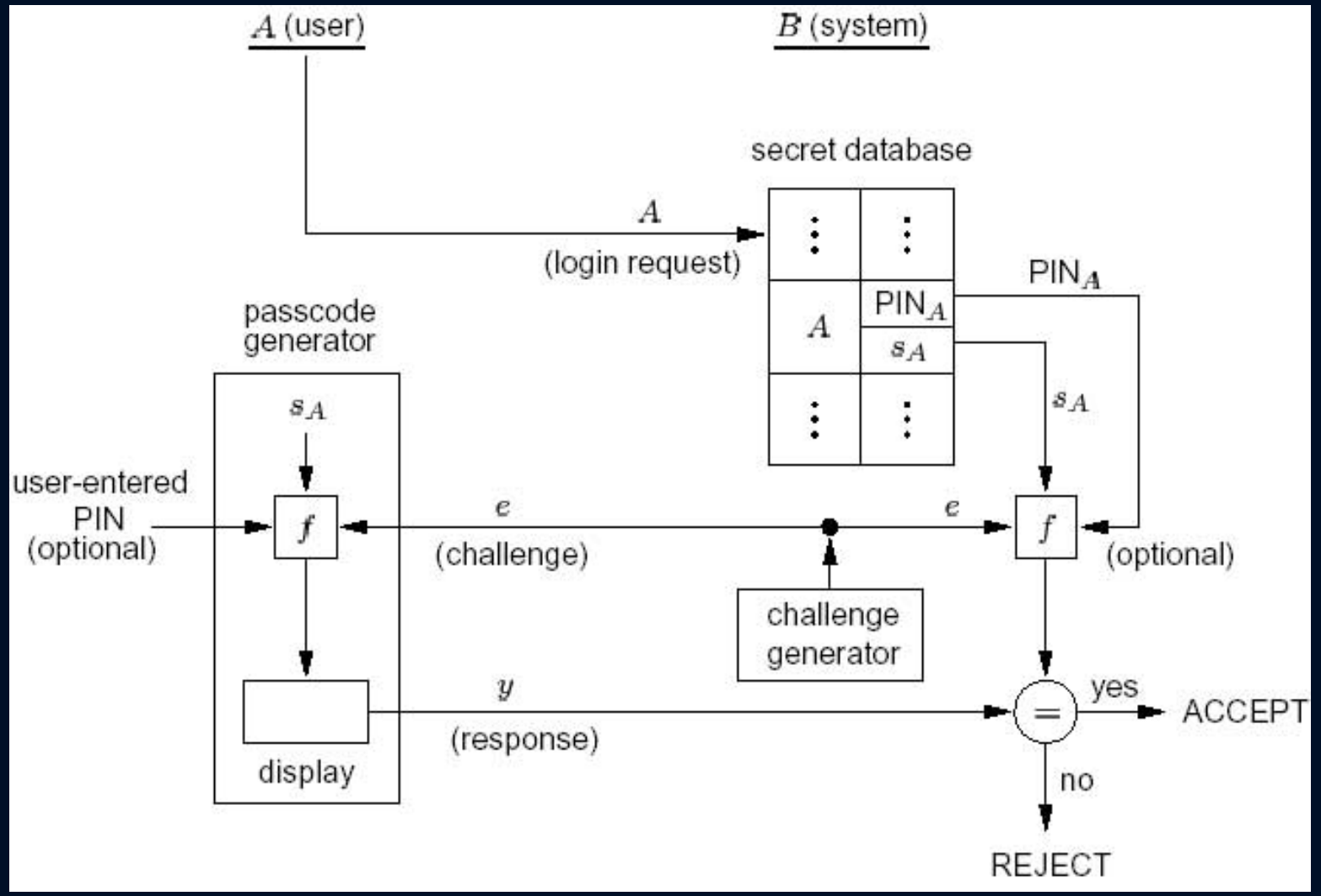


Figure 2.1 Password generator use.

3. Ο Bob πληκτρολογεί στη συσκευή την πρόκληση N
4. Η συσκευή χρησιμοποιεί το κλειδί K και την πρόκληση N, και υπολογίζει την απάντηση (response)

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

Case: *Γεννήτορες Κωδικών (2-factor authentication)*

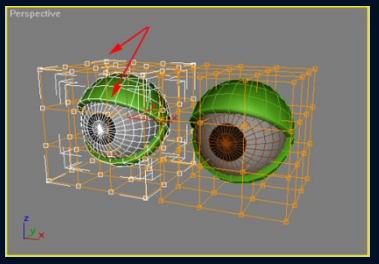


Υπηρεσίες και Μηχανισμοί Ασφάλειας

Πολιτικές Κωδικών Πρόσβασης

- Εκπαίδευση των χρηστών
  - Επιλογή «σωστών» κωδικών,
  - Ανοχή σε Κοινωνική Μηχανική,…
- Έλεγχος ασφάλειας κωδικών
  - Reactive and/or proactive password checker (Stallings – eClass)
- Διάρκεια ζωής κωδικών
  - Change default passwords
  - Password aging, password history
  - One-time passwords
- Έλεγχος αποπειρών εισόδου
  - π.χ. Κλείδωμα λογαριασμού για ένα χρονικό διάστημα
- Πολιτικές Ελέγχου (Audit)
  - Τι συμβάντα / προσβάσεις καταγράφει το Λ.Σ.
  - π.χ. Ημερομηνία & ώρα τελευταίας εισόδου, αναφορά αποτυχημένων αποπειρών,…
- Προστασία αρχείου κωδικών
  - Κρυπτογράφηση, Salting Δικαιώματα (π.χ. Shadow file),..

Εκπαίδευση των χρηστών – Μία μελέτη περίπτωσης



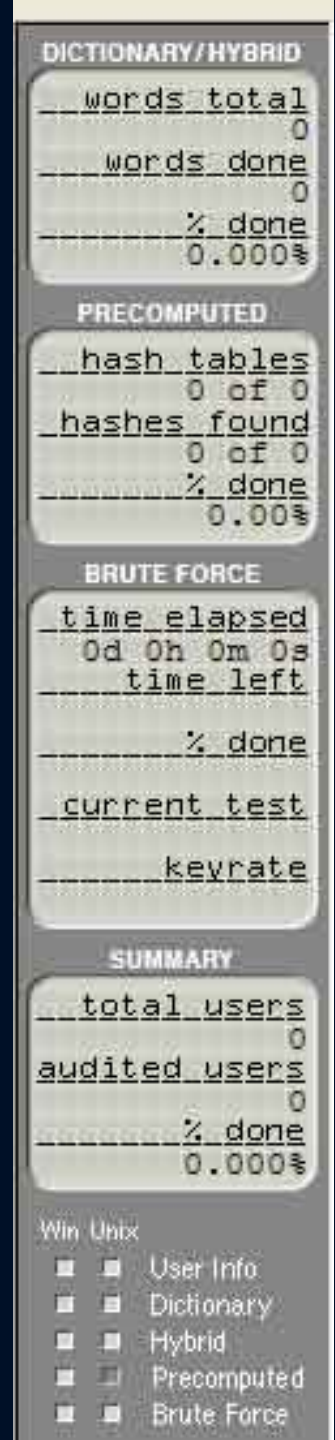
- 100 φοιτητές χωρίστηκαν σε 3 ομάδες (Anderson, 2008)
  - Στην «κόκκινη» ομάδα δόθηκαν οδηγίες για επιλογή σωστού κωδικού
    - (τουλάχιστον 6 χαρ., & ένας μη αλφαριθμητικός χαρ.)
  - Στην «πράσινη» ομάδα ζητήθηκε να σκεφθούν μια φράση (passphrase) και να επιλέξουν γράμματα από αυτή
    - π.χ "It's 12 noon and I am hungry" → I'S12&IAH
  - Στην «κίτρινη» ομάδα δόθηκε ένας πίνακας χαρακτήρων (γράμματα & αριθμοί): «Επιλέξτε 8 χαρακτήρες. Γράψτε τον κωδικό σε ένα χαρτί. Καταστρέψτε το χαρτί 1 εβδομάδα μετά…»

"*My son Aiden is three years older than my daughter Anna*"
→ Msaityotmda OR M$8ni3y0tmd@

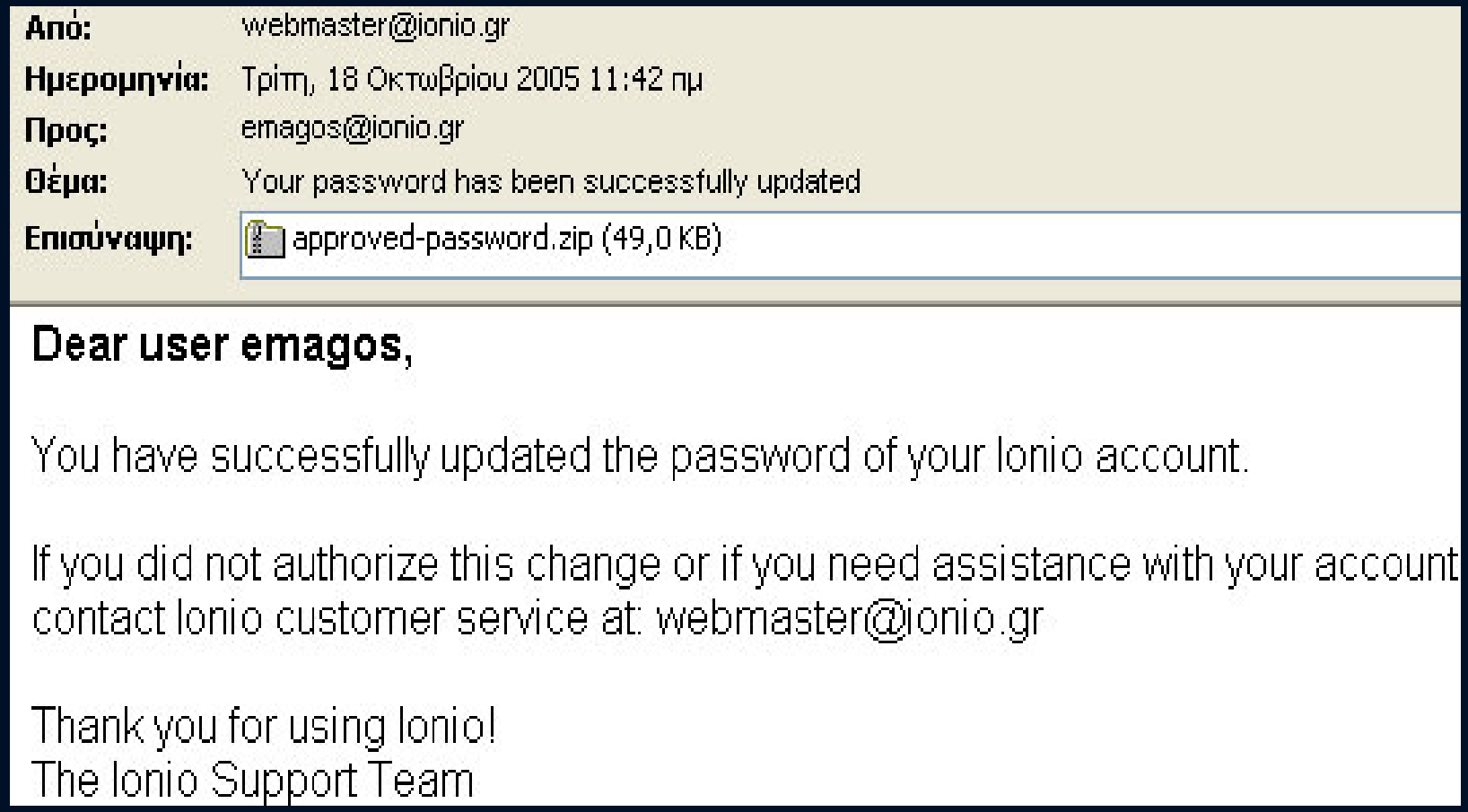
Εκπαίδευση των χρηστών – Μία μελέτη περίπτωσης

- 30% των κωδικών από την κόκκινη ομάδα «έσπασαν» εύκολα (χρησιμοποιώντας ειδικό λογισμικό – cracking software)
  - Οι άλλες 2 ομάδες είχαν 10% αντίστοιχο ποσοστό
- Οι χρήστες ρωτήθηκαν ως προς τη δυσκολία απομνημόνευσης
  - Η κίτρινη ομάδα είχε το μεγαλύτερο πρόβλημα…
- Συμπεράσματα ; …….

Πρόβλημα: Αν δημιουργούνται διαφορετικά passphrases για τη σύνδεση σε διαφορετικούς λογαριασμούς, το πρόβλημα απομνημόνευσης παραμένει…



Social engineering (1/3)



Από: webmaster@ionio.gr
Ημερομηνία: Τρίτη, 18 Οκτωβρίου 2005 11:42 πμ
Προς: emagos@ionio.gr
Θέμα: Your password has been successfully updated
Επισύναψη: approved-password.zip (49,0 KB)

Dear user emagos,

You have successfully updated the password of your Ionio account.

If you did not authorize this change or if you need assistance with your account contact Ionio customer service at: webmaster@ionio.gr

Thank you for using Ionio!
The Ionio Support Team

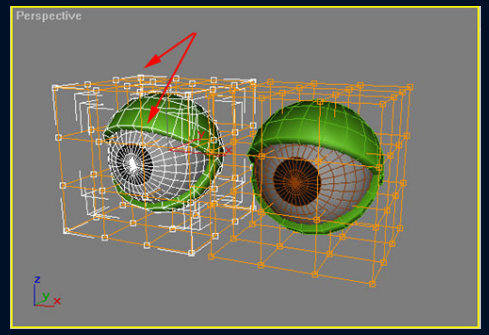
Social engineering (2/3)

"This is Ken Thompson. Someone called me about a problem with the *ls* command. He'd like me to fix it."

"Oh, OK. What should I do?"

"Just change the password on my login on your machine; it's been a while since I've used it."

"No problem."



Social engineering (3/3)

Πανεπιστήμιο του Sydney, 1996 (Anderson, 2008)

- «336 χρήστες έλαβαν e-mail με την υπόδειξη να αποστείλουν τον κωδικό τους ώστε να ενημερωθεί η βάση του δικτύου…»
  - 138 απέστειλαν το σωστό κωδικό
  - 30 απέστειλαν λάθος κωδικό
  - Ελάχιστοι ανέφεραν το γεγονός στον υπεύθυνο ασφαλείας

Problems: a) "what you know" is turned into "what you have"
b) The written copy is a single point of failure

Εκπαίδευση Χρηστών (κανό[illegible])

Make the password at least eight characters, if allowed by the ap[illegible]. A four- or five-character password can be cracked by a computer program in less than one minute. A 1[illegible]acter password, in contrast, has about 3,700 trillion possible character permutations and could take a regular c[illegible]er decades to crack.

Choose an unusual sequence of characters t[illegible]ate a password that will not be in a dictionary—for instance, mix in numbers and special characters with abbrevi[illegible]ns or unusual words you will remember. The password should be one that you can remember, yet one that doesn't [illegible]nform to a pattern a computer can readily figure out.

Don't use your name, your kids' or pets' names, your address, your birthdate, or other public information as your password.

Keep a written copy of the password in a place where no one but you can find it. Many people place passwords on self-sticking notes that are affixed to their monitors or taped to their desks—a practice that's almost as bad as having no password at all.

Use a different password for your highly sensitive activities (such as online banking or stock trading) than for Web sites that remember your settings or profile (such as online news, auction, shopping, or bookstore sites). Computers storing passwords used on nonsensitive Web sites are usually easier to break into than those storing passwords used on high-security sites, and if a hacker determines your password on a low-security site, he or she can use it on your accounts containing sensitive data if you use the same password on those accounts.

Change your passwords frequently.

Figure 4-6

Computers and Technology in a Changing Society, Second Edition, Deborah Morley, Charles Parker, 2004

Password Management

(Gollmann, 2010)

Bootstrapping Password Protection

a) Ideally: Out-of-Band, Physically

- e.g., In an enterprise, users could be asked to come to an office and collect their password personally

b) Convey the password by mail, email, or phone, or entered by the user on a web page

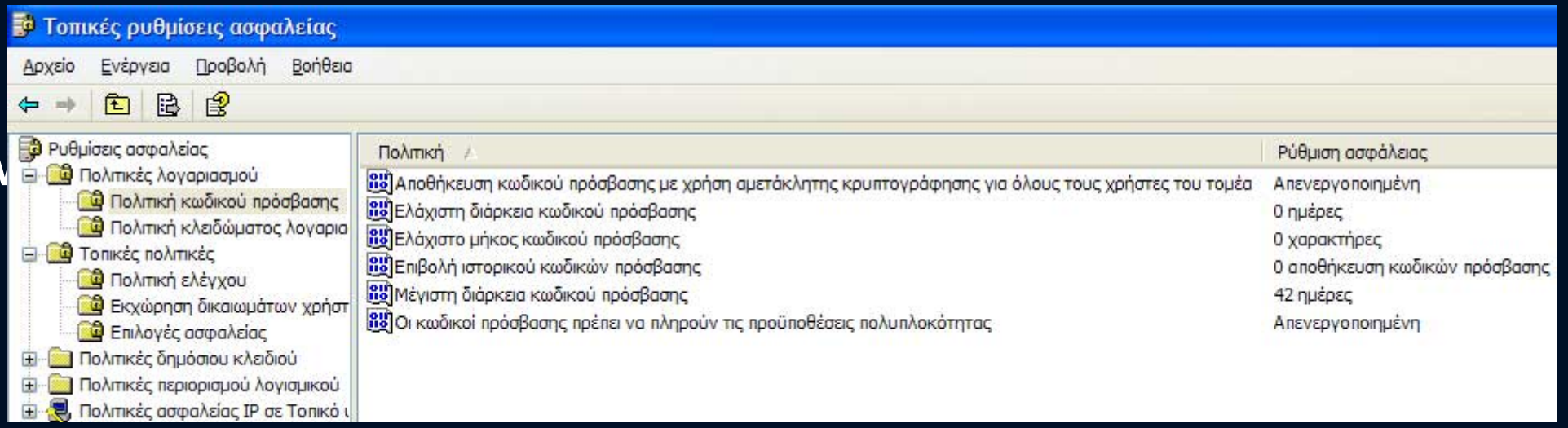
- Issues: Who might intercept/pick up the message?

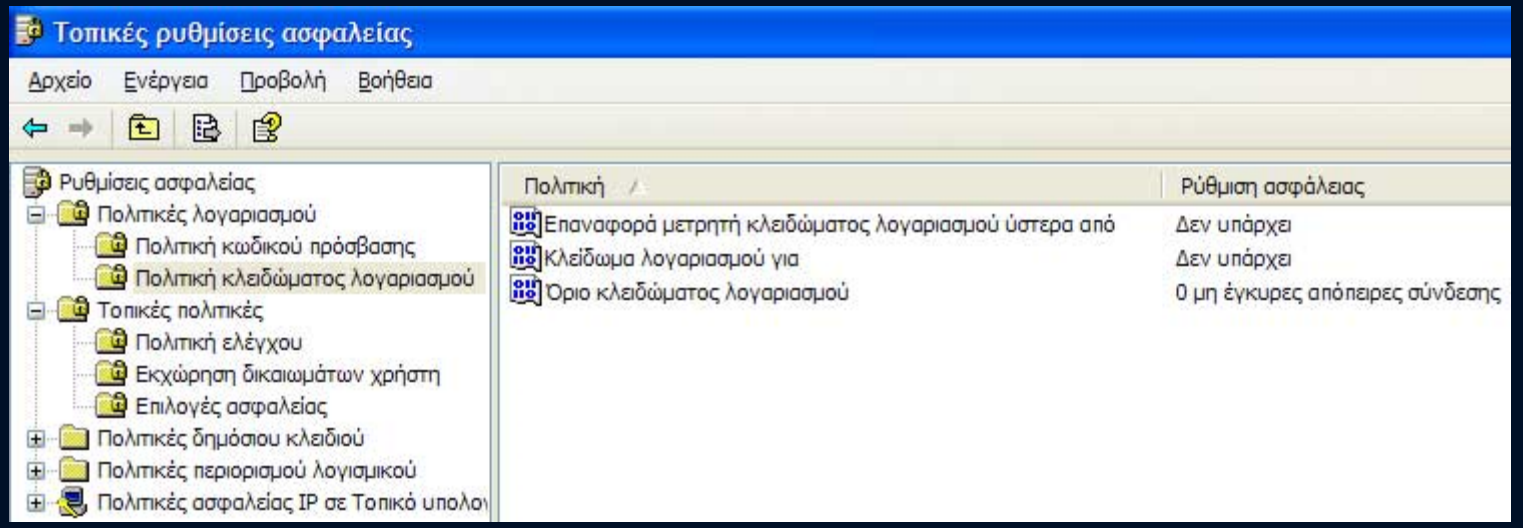
➢ Useful Techniques/Strategies

- Call back authorized phone numbers
- Send passwords that are valid for a single login
- Send mail by courier with personal delivery
- Request confirmation on a different channel to activate (e.g., SMS)

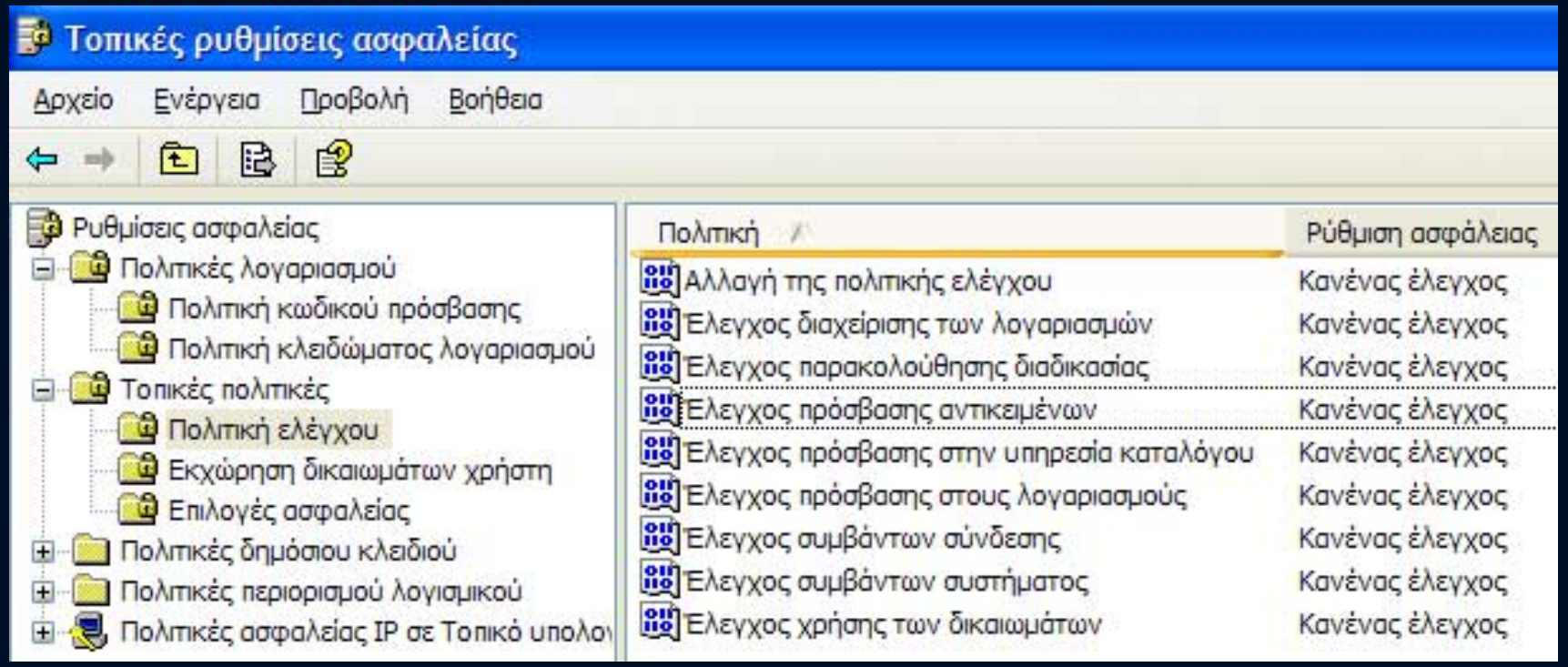
- Πατήστε 

+ R
- Εκτελέστε **secpol.msc** ή **gpedit.msc**


Τοπικές ρυθμίσεις ασφαλείας
Αρχείο Ενέργεια Προβολή Βοήθεια
Ρυθμίσεις ασφαλείας
Πολιτικές λογαριασμού
Πολιτική κωδικού πρόσβασης
Πολιτική κλειδώματος λογαρια
Τοπικές πολιτικές
Πολιτική ελέγχου
Εκχώρηση δικαιωμάτων χρήστ
Επιλογές ασφαλείας
Πολιτικές δημόσιου κλειδιού
Πολιτικές περιορισμού λογισμικού
Πολιτικές ασφαλείας IP σε Τοπικό υ
Πολιτική
Ρύθμιση ασφάλειας
Αποθήκευση κωδικού πρόσβασης με χρήση αμετάκλητης κρυπτογράφησης για όλους τους χρήστες του τομέα
Απενεργοποιημένη
Ελάχιστη διάρκεια κωδικού πρόσβασης
0 ημέρες
Ελάχιστο μήκος κωδικού πρόσβασης
0 χαρακτήρες
Επιβολή ιστορικού κωδικών πρόσβασης
0 αποθήκευση κωδικών πρόσβασης
Μέγιστη διάρκεια κωδικού πρόσβασης
42 ημέρες
Οι κωδικοί πρόσβασης πρέπει να πληρούν τις προϋποθέσεις πολυπλοκότητας
Απενεργοποιημένη


Τοπικές ρυθμίσεις ασφαλείας
Αρχείο Ενέργεια Προβολή Βοήθεια
Ρυθμίσεις ασφαλείας
Πολιτικές λογαριασμού
Πολιτική κωδικού πρόσβασης
Πολιτική κλειδώματος λογαριασμού
Τοπικές πολιτικές
Πολιτική ελέγχου
Εκχώρηση δικαιωμάτων χρήστη
Επιλογές ασφαλείας
Πολιτικές δημόσιου κλειδιού
Πολιτικές περιορισμού λογισμικού
Πολιτικές ασφαλείας IP σε Τοπικό υπολο
Πολιτική
Ρύθμιση ασφάλειας
Επαναφορά μετρητή κλειδώματος λογαριασμού ύστερα από
Δεν υπάρχει
Κλείδωμα λογαριασμού για
Δεν υπάρχει
Όριο κλειδώματος λογαριασμού
0 μη έγκυρες απόπειρες σύνδεσης

Windows: Πολιτική Ελέγχου



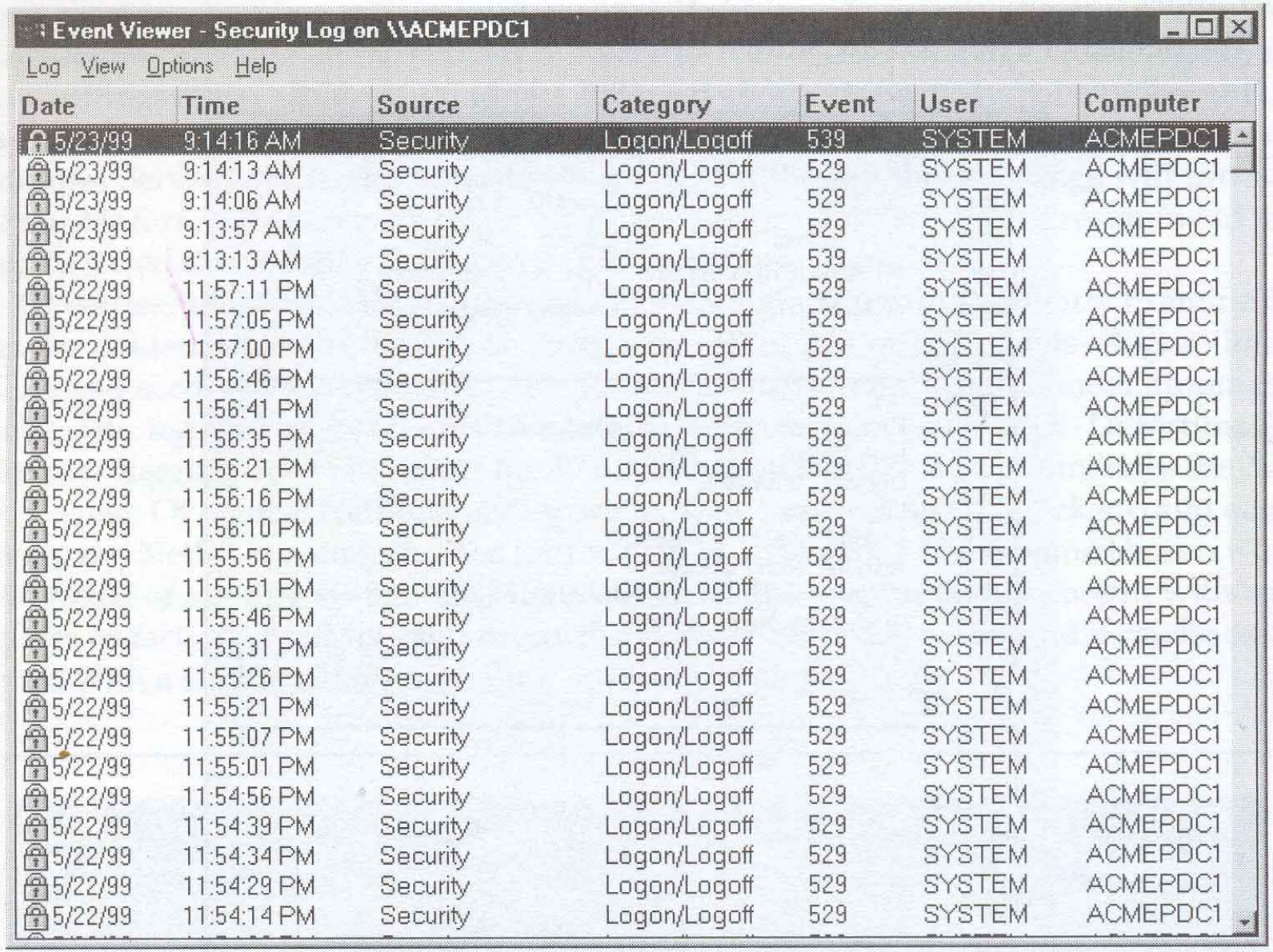


Figure 4-3 The Windows Security Log shows failed logon attempts caused by an automated password-guessing attack.