ΤΕΙ ΗΠΕΙΡΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε
ΜΕΤΑΠΤΙΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

Ασφάλεια

ΛΙΑΓΚΟΥ ΒΑΣΙΛΙΚΗ
ΔΙΑΛΕΞΗ-ΙΙ

Password Generators

- Computer-Generated passwords (Stallings 2010, p. 20-25)
  - Specific software
  - OS-aided application
  - Web sites *,*

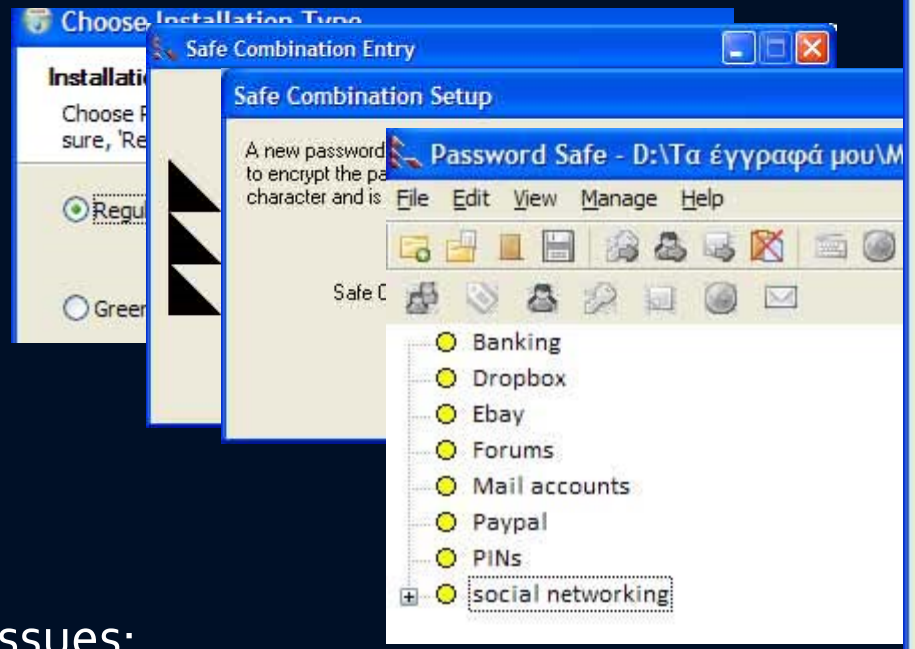
Problem: If the passwords are quite random in nature, users will not be able to remember them (for different passwords in different place, the problem gets worse)

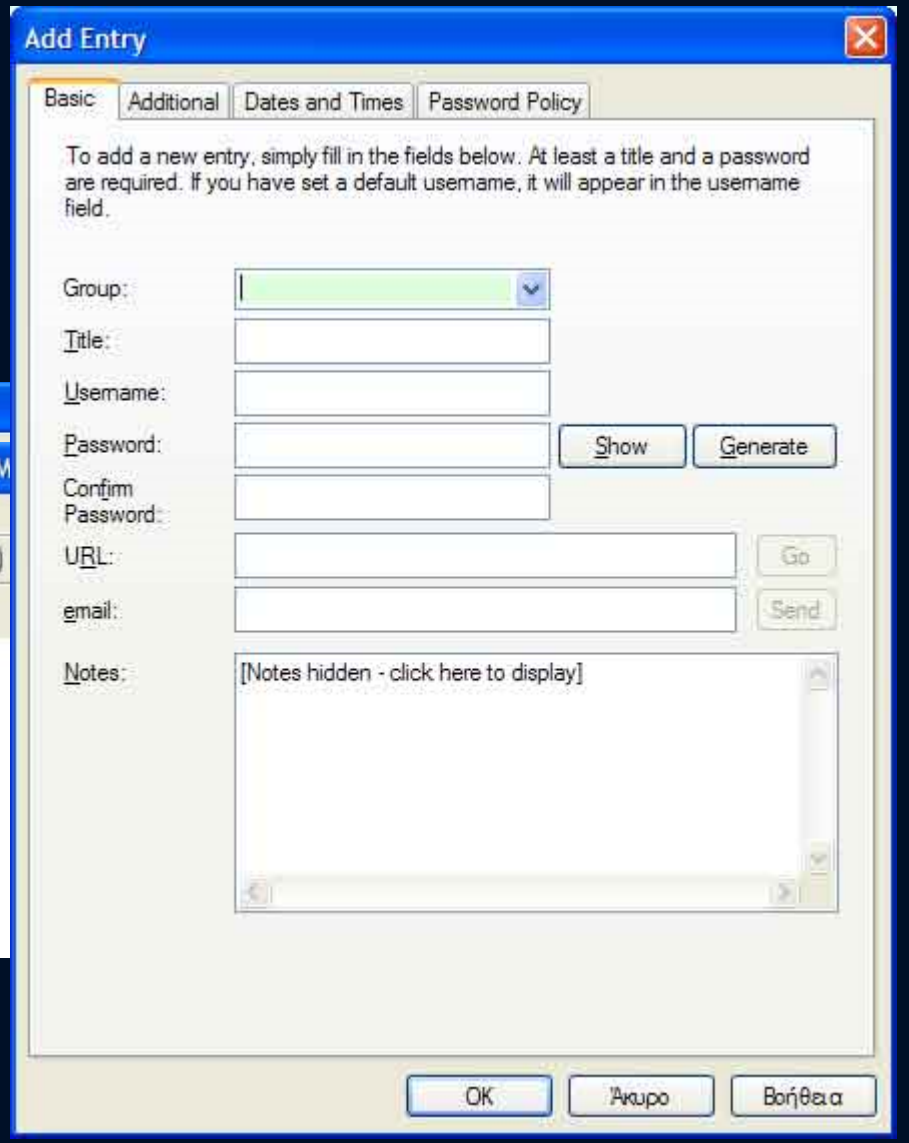
Συνήθως, λύσεις αυτού του τύπου, συνδυάζονται με έναν password manager: Το προσωπικό αρχείο κωδικών κρυπτογραφείται με κλειδί που προκύπτει από ισχυρό passphrase.

*, *, *, *

Password Managers

Περίπτωση: Password Safe





- Issues:
  - Keyloggers
    - Λύση: 2-factor authentication
  - Usability,…

♪

Password Safe

- είναι ένα password manager πρόγραμμα για χρήση με τα Microsoft Windows.
- Το λογισμικό διαθέτει μια ενσωματωμένη γεννήτρια κωδικών πρόσβασης που παράγει τυχαίους κωδικούς πρόσβασης.
- Ο χρήστης μπορεί επίσης να ορίσει τις παραμέτρους για τη δημιουργία κωδικού πρόσβασης (μήκος, σύνολο χαρακτήρων, κλπ),
- δημιουργώντας μια«Ονομαστική Πολιτική κωδικού πρόσβασης" με την οποία μπορεί να δημιουργηθεί διαφορετικούς κωδικούς πρόσβασης.

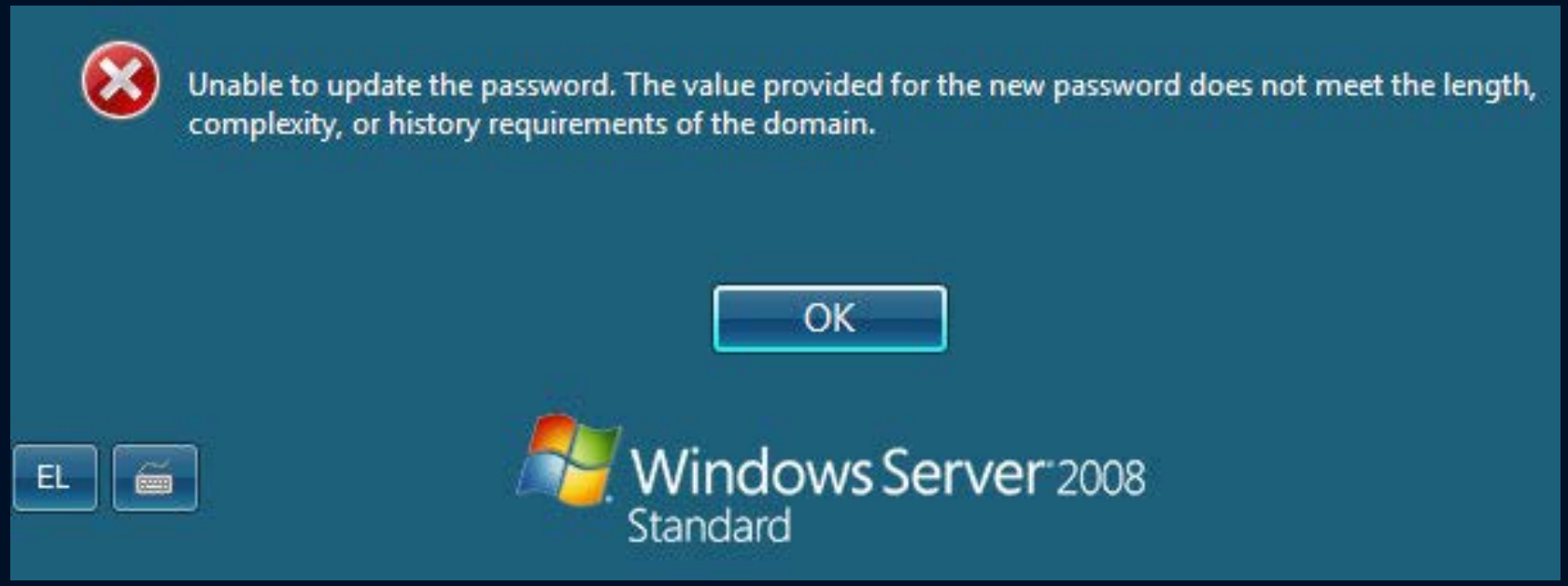
Storing your passwords in the Cloud

Case: LastPass

LastPass is a freemium password management service which stores encrypted passwords in the cloud.
LastPass is standard with a web interface but also includes plugins and apps for many modern web browsersand includes support for bookmarklets.

- Issues:
  - Who do you trust?
  - Single point of failure, …
  - Perhaps a nice solution if combined with 2-factor

Password checkers



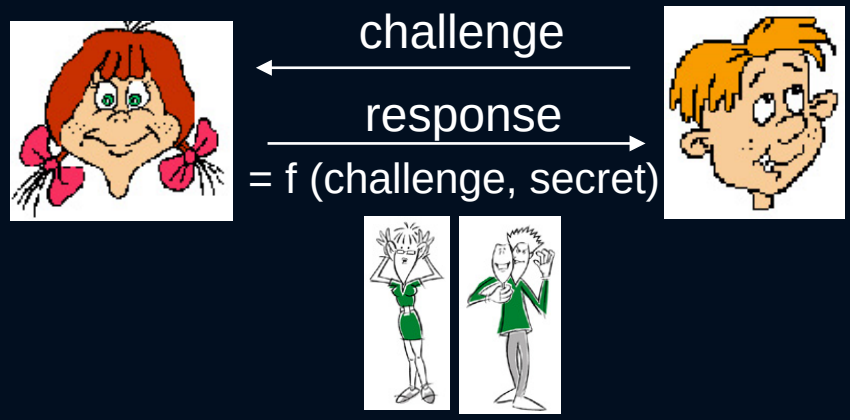
Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001 *

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

5. Πρωτόκολλα Πρόκλησης-Απάντησης

(Challenge Response)

- Η «ιδέα» πίσω από τα πρωτόκολλα πρόκλησης-απάντησης είναι η εξής:
  - Η Alice «αποδεικνύει» γνώση ενός μυστικού (που αυτή και ο Bob μοιράζονται), χωρίς να αποστείλει το μυστικό στο Bob!
- Η τεχνική περιγραφεται ως εξής:
  1. Ο Bob στέλνει στην Alice μια αριθμητική τιμή (πρόκληση)
     - Μοναδικός, Τυχαίος αριθμός (nonce – number used once)



2. Συνδυάζοντας την πρόκληση με το μυστικό που γνωρίζει, η Alice επιστρέφει μια τιμή (απάντηση)
   - Χρήση μίας (μονόδρομης) κρυπτογραφικής συνάρτησης f

Challenge-response

- Ο Client και ο server διαμοιράζονται ένα κοινό κλειδί k
- Γενικά: Ο server στέλνει το R? χρήστης στέλνει f (k, R)
- Τι πληροφορία πρέπει να χρησιμοποιηθεί εδω?

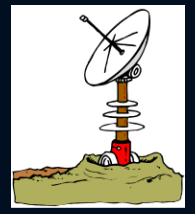
- Μειονεκτήματα
  - Dictionary attack αν τι κ έχει χαμηλή εντροπία (αντιμετοπίζεται)
  - Όχι-ασφαλής κατά παραβίαση του διακομιστή

“Friend-or-foe”

SAAF
Impala
K

2. $F_K(R)$

1. R



Namibia
K

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

Αυθεντικοποίηση Οντότητας (Συμμετρικές Τεχνικές)

Κρυπτογραφικό *Πρωτόκολλο 1*

1. ISO Two Pass Unilateral Authentication Protocol

- Ο Bob ταυτοποιεί την Alice

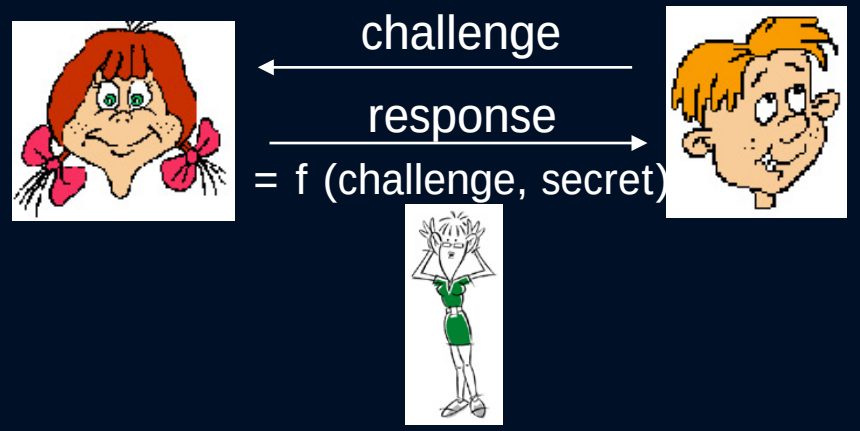
$$A \leftarrow B : r_B \quad (1)$$
$$A \rightarrow B : E_K(r_B, B^*) \quad (2)$$

Εδώ το rB είναι ένας τυχαίος αριθμός. Με τη λήψη του μηνύματος (2) , ο Β αποκρυπτογραφεί το κρυπτογραφημένο και ελέγχει αν περιέχει την πληροφορία του μήνυματος (1).
Στο τέλος του πρωτοκόλλου ο Β μπορεί να συμπεράνει ότι ο Α είναι ενεργός.

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

Πρωτόκολλα Πρόκλησης-Απάντησης

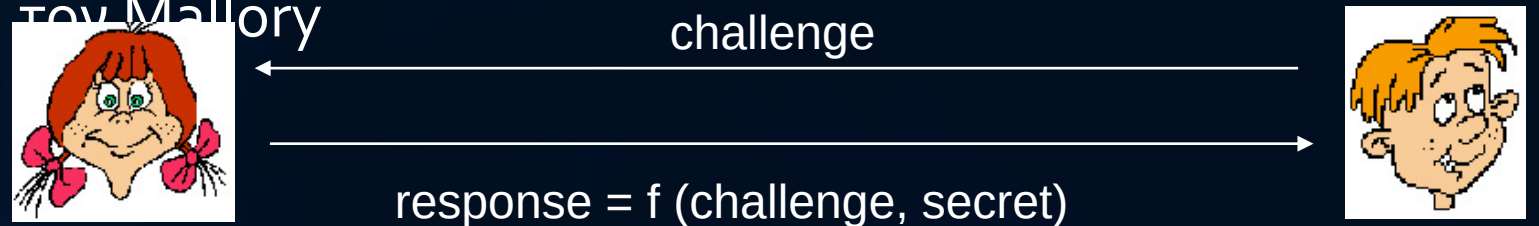
- **Ερώτηση 1**: Γιατί το challenge πρέπει να είναι μοναδικό;
- **Απάντηση**: ώστε ο Bob να γνωρίζει ότι η Alice ήταν ενεργή τη στιγμή που εκτελέστηκε το πρωτόκολλο
  - Αλλιώς, η απάντηση της Alice μπορεί να είναι αποτέλεσμα «επίθεσης επανάληψης» (replay attack) από τον Mallory

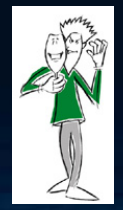


Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

Πρωτόκολλα Πρόκλησης-Απάντησης

- **Ερώτηση 2**: Γιατί το challenge πρέπει να είναι τυχαίο;
- **Απάντηση**: Αλλιώς, η απάντηση της Alice ίσως είναι αποτέλεσμα «επίθεσης επανάληψης» (replay attack) από τον Mallory





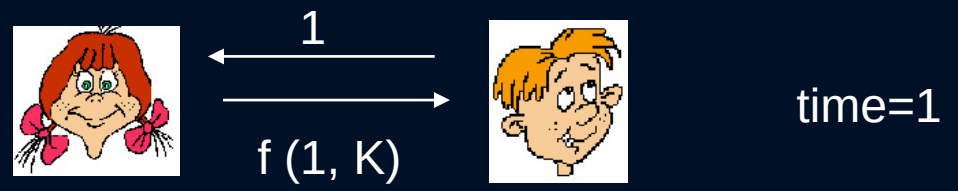
Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

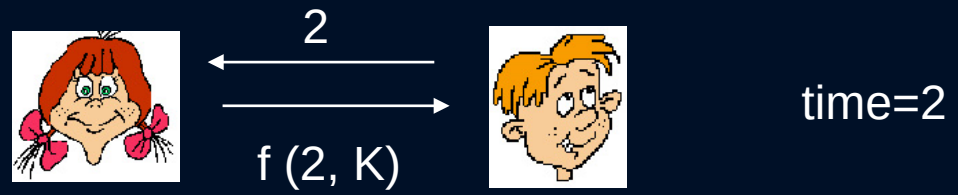
Μία επίθεση πλαστοπροσωπίας

(όταν το challenge δεν είναι τυχαίο)

- **Σενάριο**: Ο Bob στέλνει κάθε φορά ως challenge έναν ακέραιο i, ώστε:

  for (i=1;i<=1000;i++) send i;

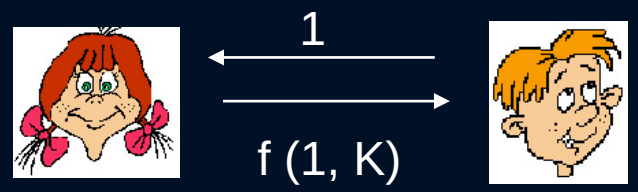




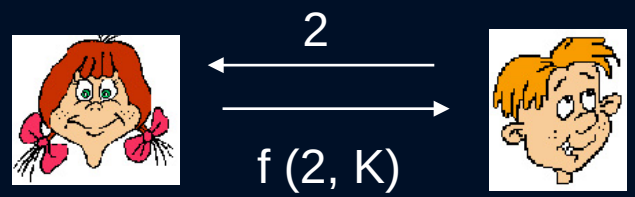
Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

Μία επίθεση πλαστοπροσωπίας

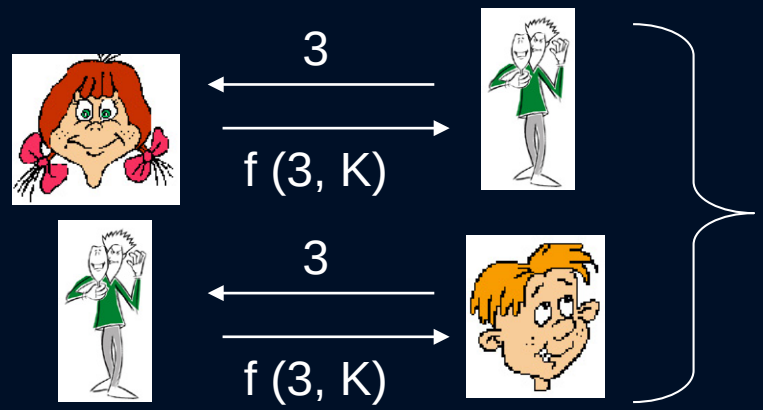
(όταν το challenge δεν είναι τυχαίο)



time=1



time=2



time=3

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

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

Αυθεντικοποίηση Οντότητας (Συμμετρικές Τεχνικές)

Κρυπτογραφικό *Πρωτόκολλο 1 - Παραλλαγές*

1. ISO Two Pass Unilateral Authentication Protocol

- Ο Bob ταυτοποιεί την Alice

$$A \leftarrow B : r_B \quad (1)$$
$$A \rightarrow B : E_K(r_B, B^*) \quad (2)$$

- Ο Bob ταυτοποιεί την Alice

$$A \leftarrow B : r_B \quad (1)$$
$$A \rightarrow B : E_K(r_A, r_B, B^*) \quad (2)$$
$$A \leftarrow B : E_K(r_B, r_A) \quad (3)$$

- Ο Bob ταυτοποιεί την Alice με τη χρήση timestamps

$$A \rightarrow B : E_K(t_A, B^*) \quad (1)$$

Χρονοσημάνσεις: Ένα βήμα αντί Δύο !!!

Η χρήση χρονοσημάνσεων είναι ασφαλής, εφόσον: α) Η Alice και ο Bob είναι συγχρονισμένοι, β) Το ρολόι του Bob δε μπορεί να «πειραχτεί» από τον Mallory…

Χρήση κρυπτογραφικής συνάρτησης MAC

- Ο χρήστης στέλνει <time, MAC(time)>
- Τι θα συμβεί αν είχε χρησιμοποιηθεί κρυπτογράφηση, ή hash?
- Τι γίνεται με απλή αποστολή MAC(time)?
- Καμία κατάσταση του server? ενιαίο μήνυμα
- Σκέψεις;
  - Απαιτεί συγχρονισμένα ρολόγια
  - Πρέπει να προφυλαχθεί από την αναπαραγωγή …
  - Τι και αν ο χρήστης έχει το ίδιο κλειδί σε πολλούς διακομιστές;
  - Clock reset επιθέσεις? Clock DoS επιθέσεις!
  - Δεν ‘έχει αμοιβαίο έλεγχο

Καλύτερα αμοιβαία αυθεντικοποίηση

- Διπλή πρόκληση-απάντηση σε 4 γύρους
- Ο client στέλνει το όνομά του
- Server στέλνει ένα nonce R
- Ο client στέλνει MAC (R) και το R '
- Server στέλνει MAC (R ')

αμοιβαία αυθεντικοποίηση σε 3 γύρους?

- Μπορούμε να συμπιέσει το προηγούμενο πρωτόκολλο, σε 3 γύρους;
- O client στέλνει το όνομά τους, το R '
- Server στέλνει MAC (R ') και R
- O client στέλνει MAC (R)
- Φαίνεται εντάξει ...

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

Αυθεντικοποίηση Οντότητας (Συμμετρικές Τεχνικές)

Κρυπτογραφικό *Πρωτόκολλο 2 – Χρήση Συνάρτησης MAC*

- Το πρωτόκολλο αποτελεί παραλλαγή του Πρωτοκόλλου 1
  - Η Συνάρτηση Κρυπτογράφησης αντικαθίσταται από ένα MAC

$$
\begin{aligned}
A \leftarrow B: &\quad r_B && (1)\\
A \rightarrow B: &\quad r_A,\ h_K(r_A, r_B, B) && (2)\\
A \leftarrow B: &\quad h_K(r_B, r_A, A) && (3)
\end{aligned}
$$

Το πρωτόκολλο είναι γνωστό και ως SKID3s

Σημείωση: Στην πράξη, οι συναρτήσεις MAC (ή ψηφιακής υπογραφής) χρησιμοποιούνται για αυθεντικοποίηση (Οντότητας ή/και Μηνύματος), ενώ οι συναρτήσεις κρυπτογράφησης από-κλειστικά και μόνον για την προστασία της εμπιστευτικότητας ενός μηνύματος !

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

Αυθεντικοποίηση Οντότητας και Μηνύματος

- Μπορεί π.χ. το Πρωτόκολλο 2 να προσφέρει, εκτός από αυθεντικοποίηση χρήστη και **αυθεντικοποίηση μηνύματος**;

$$
\begin{aligned}
A \leftarrow B: &\quad r_B && (1)\\
A \rightarrow B: &\quad r_A,\ h_K(r_A, r_B, B) && (2)\\
A \leftarrow B: &\quad h_K(r_B, r_A, A) && (3)
\end{aligned}
$$

- Απάντηση: ΦΥΣΙΚΑ!
  - Απλώς, θα πρέπει να εισαχθεί κατάλληλα το μήνυμα στην κρυπτογραφική συνάρτηση

$$
\begin{aligned}
A \leftarrow B: &\ r_B && (1)\\
A \rightarrow B: &\ r_A, m_1, h_K(r_B, r_A, m_1) && (2)\\
A \leftarrow B: &\ m_2, h_K(r_A, m_2) && (3)
\end{aligned}
$$

αμοιβαία αυθεντικοποίηση σε 3 γύρους?

- Όχι σφαλής! (επίθεση αντανάκλασης με δύο συνδέσεις κεντρικών υπολογιστών ...)
  - Επίσης ευάλωτα σε off-line επιθέσεις κωδικού χωρίς υποκλοπές
- Για να βελτιωθεί η ασφάλεια,
  - χρήση ασύμμετρης κρυπτογράφισης
- Δεν υπάρχει τέτοια επίθεση στο αρχικό πρωτόκολλο
  - Αρχή της ασφάλειας: ας αποδείξει την ταυτότητά του πρώτα αυτός που ξεκινά το πρωτόκολλο
- Ένα καλό παράδειγμα ότι ο σχεδιασμός ασφαλών πρωτοκόλλων είναι πολύ λεπτή!
  - Μια άλλη προειδοποίηση κατά την τροποποίηση υφιστάμενων πρωτοκόλλων,

παραβίαση του διακομιστή

- Τα πρωτόκολλα με συμμετρικά κλειδιά είναι ευάλωτα σε περιπτώσεις παραβίασης του συστήματος
- Μπορούμε να λύσουμε αυτή την περίπτωση?

Πρωτόκολλο δημοσίου κλειδιού/ υπογραφές

- Ο Server αποθηκεύει pk; Ο user αποθηκεύει sk
- Server στέλνει R; Ο user υπογράφει το R
  - Χρησιμοποιώντας ένα ασφαλές σχήμα κρυπτογράφησης…
- Είναι ασφαλές σε υποκλοπές ή σε παραβίαση τουserver?
  - Αν χρησιμοποιήσουμε και κρυπτογράφηση?

- Σημείωση: εισβολέας μπορεί να κάνει το χρήστη να υπογράψει οτιδίποτε …
- Βασικά θα πρέπει να χρησιμοποιείται μόνο για τον έλεγχο ταυτότητας

Schneier, Bruce. Applied Cryptography.
John Wiley & Sons, Inc., 2nd edition, 1996.

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

Αυθεντικοποίηση Οντότητας (Τεχνικές ΔΚ)

Κρυπτογραφικό Πρωτόκολλο 3

- Πώς ο Bob μπορεί να ταυτοποιήσει μια οντότητα Α ως την Alice, χρησιμοποιώντας τεχνικές Δημόσιου Κλειδιού;
  1. Κρυπτογράφηση: Ο Bob κρυπτογραφεί μια πρόκληση C με το ΔK_A της Alice, και στέλνει το μήνυμα στην οντότητα Α.
     - Αν η Α είναι όντως η Alice, μπορεί να αποκρυπτογραφήσει το μήνυμα και να στείλει ως απάντηση το C

- Μονόδρομη Ταυτοποίηση

$$A \leftarrow B : B, P_A(r, B) \quad (1)$$
$$A \rightarrow B : r \quad (2)$$

Μπορείτε να το μετατρέψετε σε αμφίδρομη ταυτοποίηση;

- Αμφίδρομη Ταυτοποίηση

$$A \rightarrow B : \quad P_B(r_1, A) \quad (1)$$
$$A \leftarrow B : \quad P_A(r_1, r_2) \quad (2)$$
$$A \rightarrow B : \quad r_2 \quad (3)$$

Schneier, Bruce. Applied Cryptography.
John Wiley & Sons, Inc., 2nd edition, 1996.

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

Αυθεντικοποίηση Οντότητας (Τεχνικές ΔΚ)

Κρυπτογραφικό Πρωτόκολλο 4

2. Ψηφιακή Υπογραφή: Ο Bob στέλνει στην Alice ένα challenge. Η Alice υπογράφει το challenge με το ΙΚ της & στέλνει την απάντηση στον Bob. Ο Bob επαληθεύει με το ΔΚ της Alice

a) Μονόδρομη Ταυτοποίηση

$$A \leftarrow B : r_B \quad (1)$$
$$A \rightarrow B : cert_A, r_A, B, S_A(r_A, r_B, B) \quad (2)$$

b) Αμφίδρομη Ταυτοποίηση

$$A \leftarrow B : r_B \quad (1)$$
$$A \rightarrow B : cert_A, r_A, B, S_A(r_A, r_B, B) \quad (2)$$
$$A \leftarrow B : cert_B, A, S_B(r_B, r_A, A) \quad (3)$$

c) Μονόδρομη Ταυτοποίηση με χρονοσημάνσεις (timestamps)

$$A \rightarrow B : cert_A, t_A, B, S_A(t_A, B) \quad (1)$$

Αυθεντικοποίηση Οντότητας

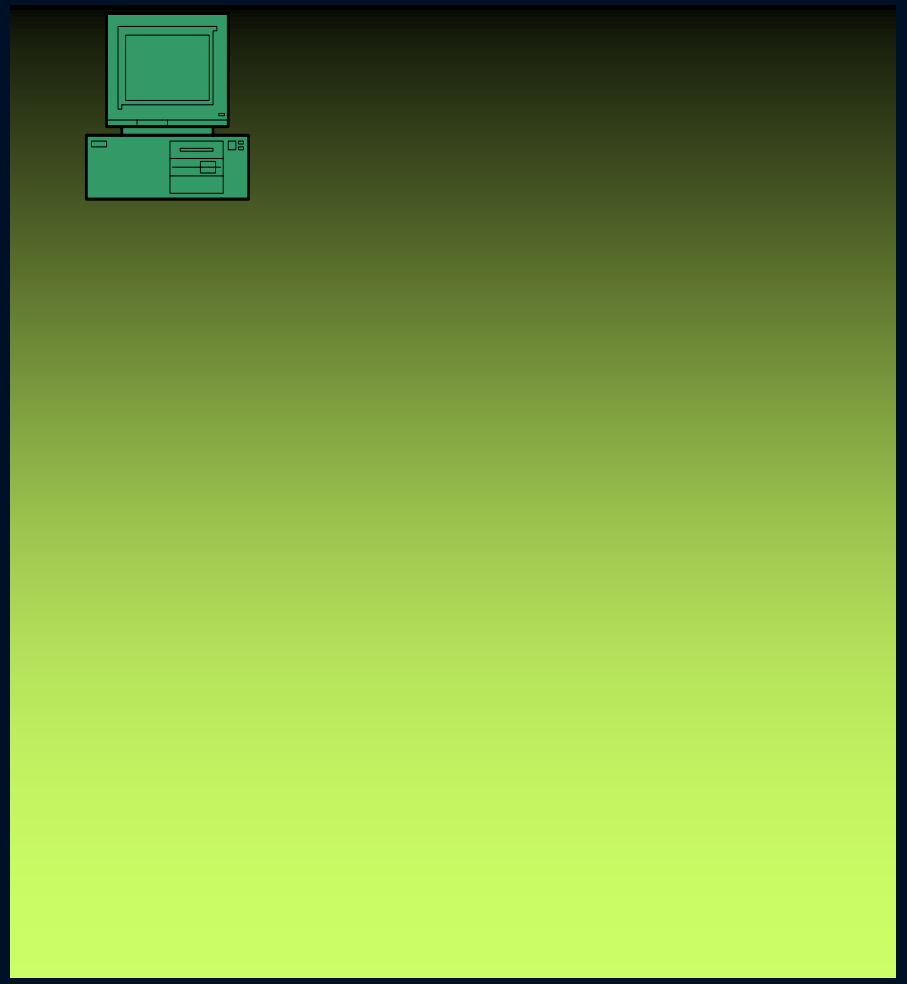
Αυθεντικοποίηση Process/Host <---> Process/Host

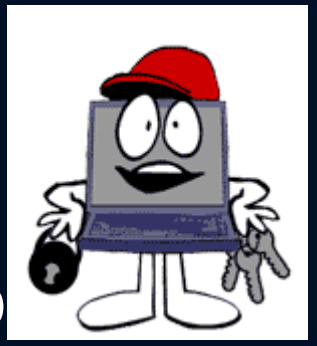
Εκτός των άλλων, οι παραπάνω τεχνικές (πρόκληση-απάντηση, χρονοσημάνσεις) χρησιμοποιούνται από τα περισσότερα πρωτόκολλα αυθεντικοποίησης αυτής της κατηγορίας

Αυθεντικοποίηση *Process/Host <---> Process/Host*

CHAP (Challenge-Response Authentication Protocol)

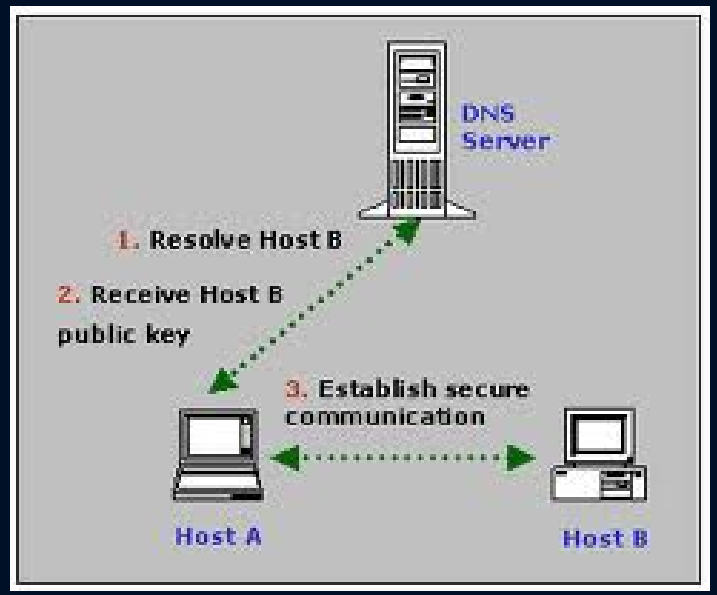
- Περίπτωση
  - Αυθεντικοποίηση PPP (Point-to-Point Protocol) με το υπο-πρωτόκολλο CHAP
  - Αφορά: συνδέσεις χρηστών dial-up ή DSL με Παρόχους ISP
    - Μυστικό = Password





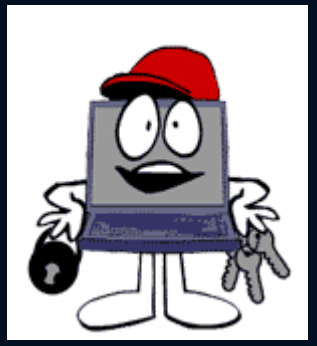
Περίπτωση: Ταυτοποίηση Host-to-Ho

- Network-Based Authentication
  - Ταυτοποίηση βάσει IP διεύθυνσης (IP-based authentication)
  - Ταυτοποίηση βάσει ονόματος DNS (name-based authentication).



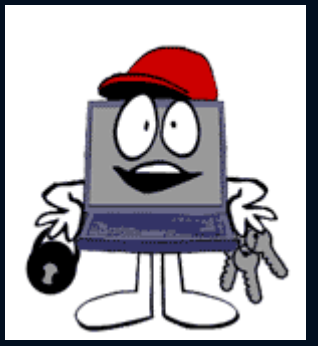
http://www.scrapeboxhelp.com/scrapebox-proxies-setting-up-private-proxies-in-scrapebox

Περίπτωση: Ταυτοποίηση Process/Host <--> Process/Host



- Network-Based Authentication
  - Ταυτοποίηση βάσει της IP διεύθυνσης (IP-based authentication)
  - Ταυτοποίηση βάσει ονόματος DNS (name-based authentication).
- Προηγμένες (κρυπτογραφικές) τεχνικές.
  - Χρήση τεχνικών challenge-response
    - Windows security (client-server): LM, NTLM, Kerberos
  - Άλλες κρυπτογραφικές τεχνικές
    - Κέντρα Διανομής Κλειδιού (π.χ. Kerberos – με χρονοσημάνσεις),
    - Αυθεντικοποίηση με Πιστοποιητικά Δημόσιου κλειδιού (π.χ. SSL, Ssh, DNSSec),…
    - … Θα εξεταστούν σε άλλες ενότητες

Περίπτωση:
Windows client-server authentication



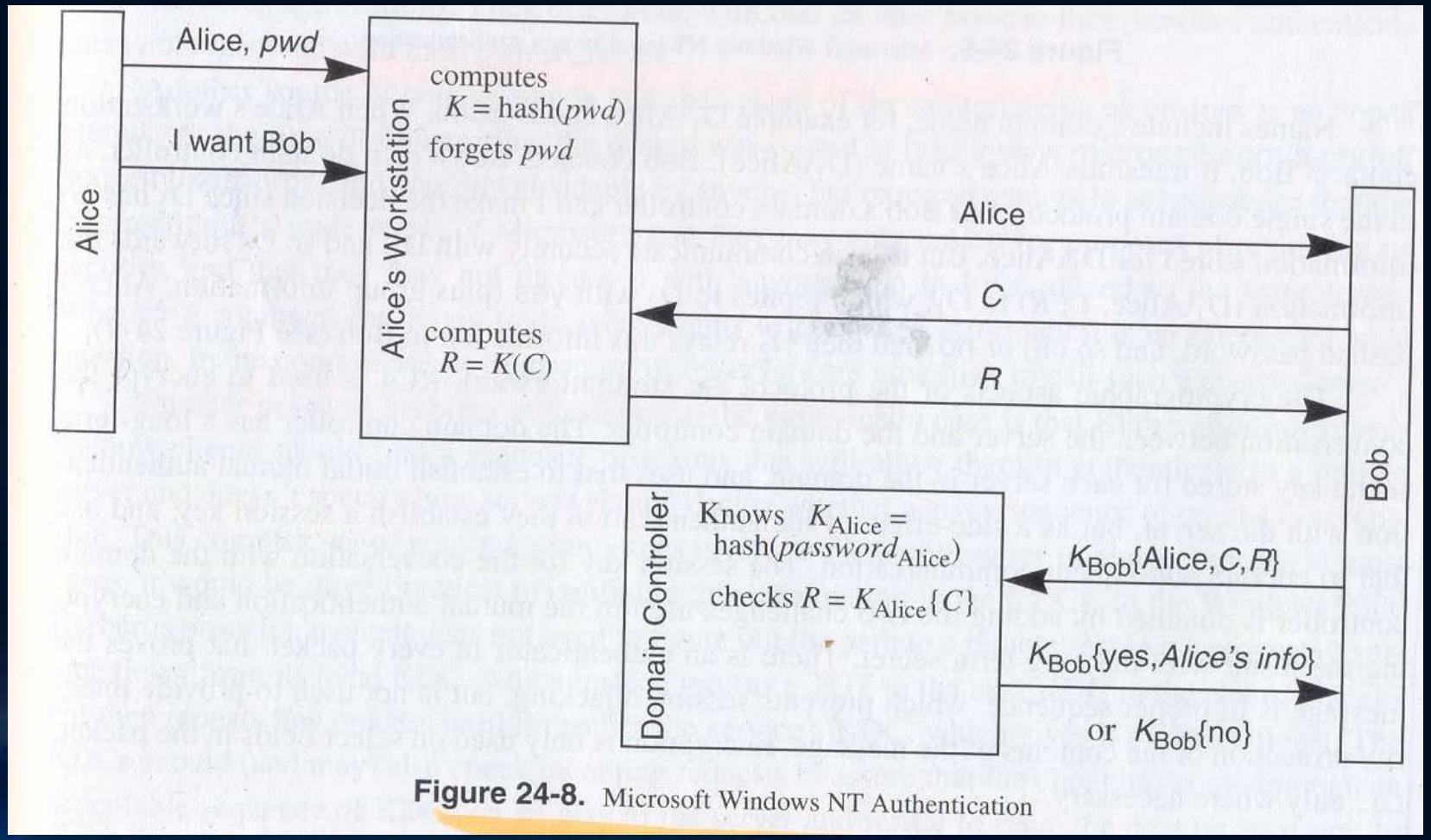


Figure 24-8. Microsoft Windows NT Authentication

Kaufman et al, 2002

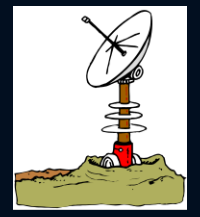
6. Επιθέσεις Πλαστοπροσωπίας

Η Επίθεση "MIG-in the MIDDLE" (Anderson, 2001)

SAAF
Impala
K

3. R

4. $F_K(R)$



Angola

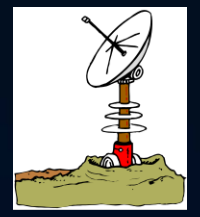
2. R

5. $F_K(R)$

Russian
MiG

6. $F_K(R)$

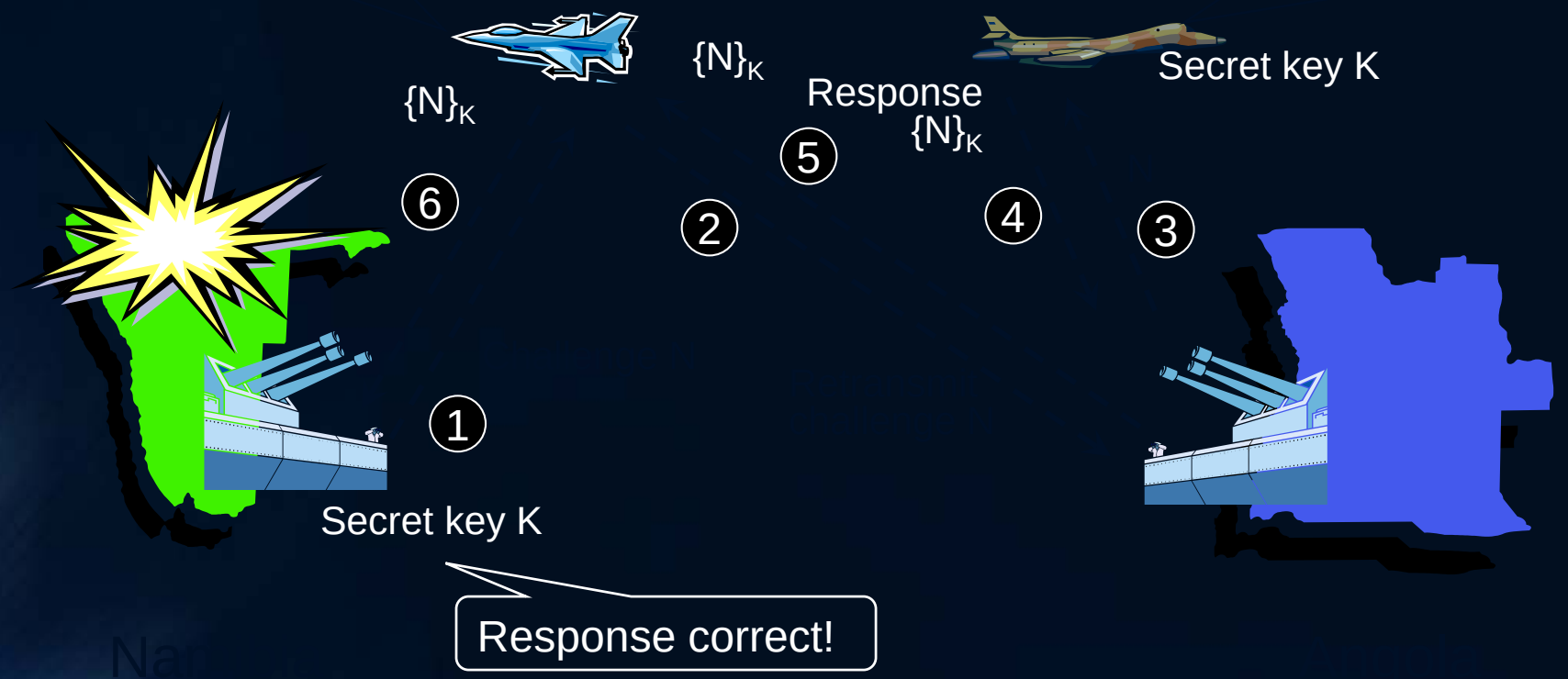
1. R



Namibia
K

6. Επιθέσεις Πλαστοπροσωπίας *

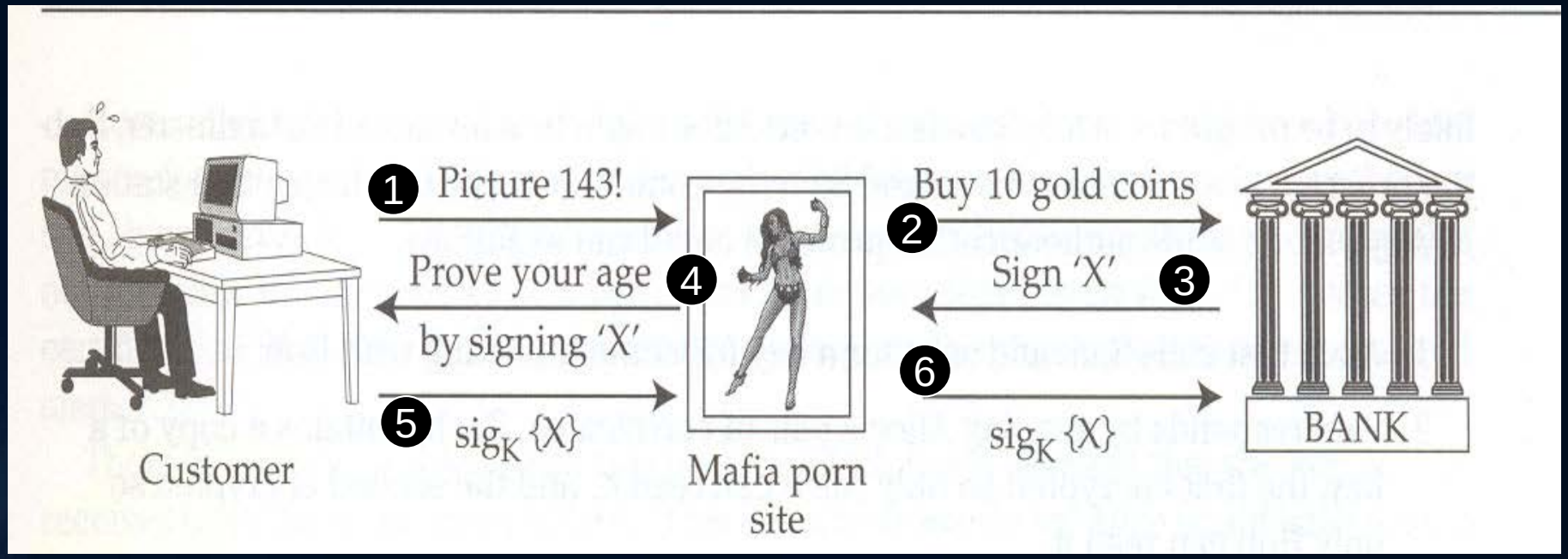
Η Επίθεση "MIG-in the MIDDLE" (Anderson, 2001)



http://www.cs.utexas.edu/~shmat/courses/cs378_spring05/03auth.ppt

6. Επιθέσεις Πλαστοπροσωπίας

Η Επίθεση "Mafia in the Middle" (Anderson, 2001)



6. Επιθέσεις Πλαστοπροσωπίας ♪
Phishing Scams

Phishing is a criminal mechanism employing both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as usernames and passwords. Technical-subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords - and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes).

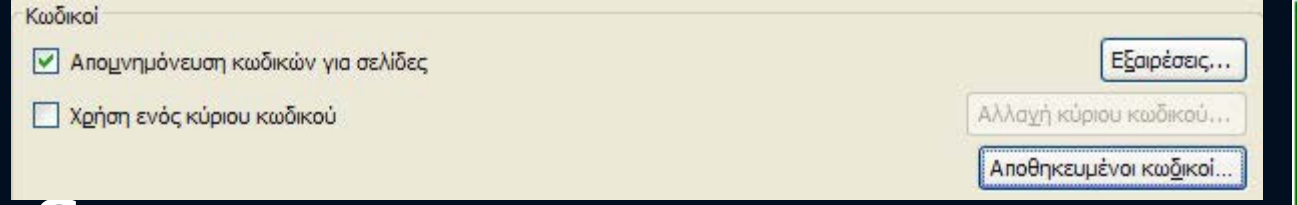
Uptimes by TLD, 1H2011

TLD	Average (HH:MM)	Median (HH:MM)
All	54:37	10:45
.com	47:33	9:55
.net	81:43	11:42
.org	60:32	9:55
.info	47:13	15:35
.biz	37:14	9:31
.tk	37:31	15:35
.cc	75:55	17:44
.br	52:10	13:40
.uk	50:40	11:37
.ru	61:41	12:40
.fr	62:10	17:31
.pl	57:43	14:11
.au	74:37	17:32

l Highlights for 1st Half, 2011

	Jan.	Feb.	March	April	May	June
Number of unique phishing email reports received by APWG from consumers	23,535	25,018	26,402	20,908	22,195	22,273
Number of unique phishing web sites detected	29,815	31,544	38,173	33,008	35,213	28,148
Number of brands hijacked by phishing campaigns	339	335	313	333	331	310
Country hosting the most phishing websites	USA	USA	USA	USA	USA	USA
Contain some form of target name in URL	69.82%	74.97%	72.38%	72.16%	78.82%	76.55%

(APWG 2011a, 2012b)



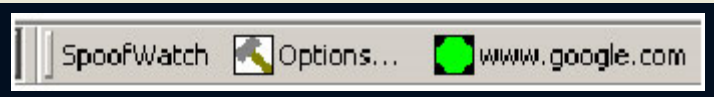


Figure 6: Remote hashing

Phishing Scams

- Μορφές (Ross et al, 2005)
  - E-mail campaigns *
  - SSL sessions to spoofed sites
  - MITM attacks
  - Common password attacks
  - …

- Anti-Phishing research:
  - Password hashing (Ross et al, 2005)

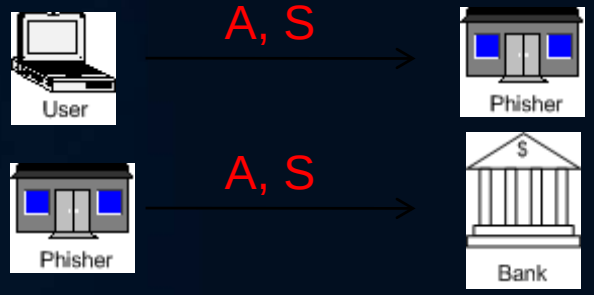
$$hash(pwd, dom)$$

  - Encrypting (browser-) cached passwords with master pass *
    - π.χ. Firefox security *
  - Phishing alert toolbars e.g., SpoofGuard, netcraft (Zhu et al, 2004) * *
  - Extended validation Certs *, *, *, *
  - 2-factor Authentication *
    - Issues: real MITM, usability,..
  - 2-channel authentication *

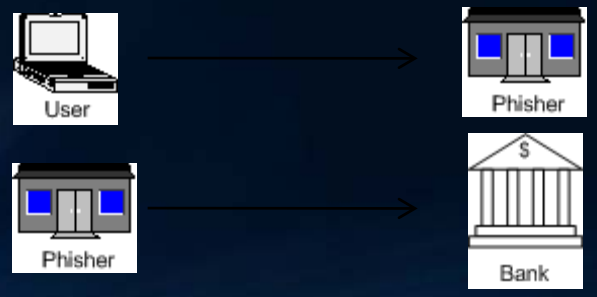
Phishing Scams In Online Banking

The problems and Solutions

- Problem 1: "Classical" phishing



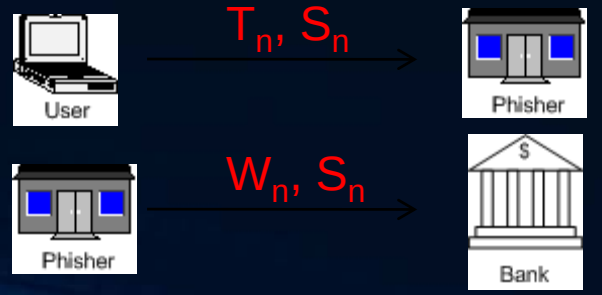
- Solution 1: one-time passwords A, S_n
- Problem 2: Phisher P adapts: A, S_n



..but P can only use the password on one occasion

- Solution 2: A may contact the bank soon and discover fraud
- Problem 3: MITM for whole session, phisher doesn't logoff.
- Solution 3: Bank B asks a fresh pswd for every transaction
- Problem 4: P replaces a transaction by a wicked one:

*

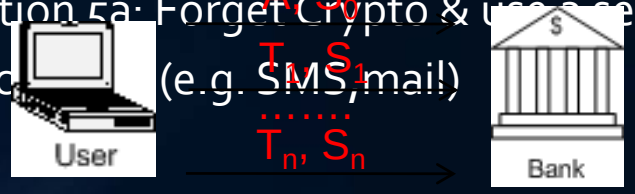


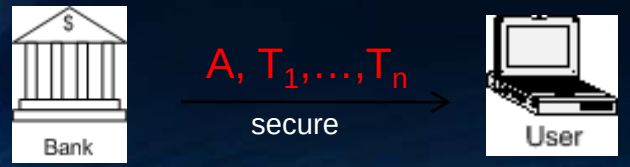
Phishing Scams In Online Banking

The problems and Solutions

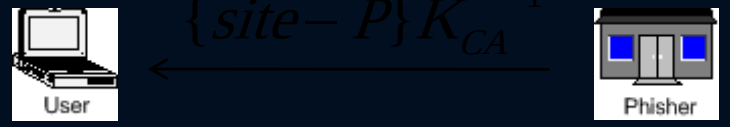
- Solution 4: "sign" transactions:

- Problem 5a: A needs SW to do this (Browser? Smartcard?)
- Solution 5a: Forget Crypto & use a secure B-A c… (e.g. SMS, mail)

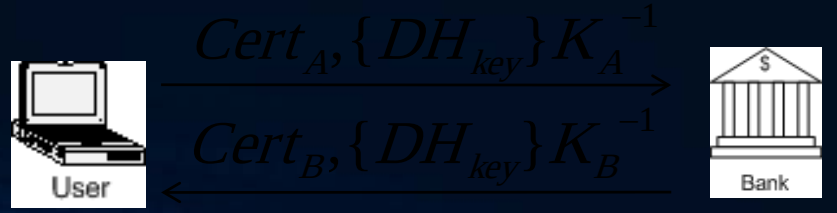




- Problem 6a: P uses a pswd to vali-date change of A's mail address.
- Solution 6a: Change of contact details requires out-of-band
- Solution 5a': Back to Crypto: TLS
- Problem 6b: P may have a Cert !



- Solution 6b: Client certificates



Phishing Scams In Online Banking

The problems and Solutions

- Problem 7:
  - PKI Cert mgmt issues
  - Banking at home only
  - Browsers can be fooled
  - Malware steals Cert and PR_{key}
  - P may tell A: "Your CERTs expired, send them to us"
- Solution 9:
  - Chip and Pin cards. 3-D Secure
  - Chip Authentication Program
- Problem 9:
  - A lot of security issues ☹
- Solution 10
  - Customer Education

7. Single Sign-On (SSO) in the Web
Federated Identity Management

- The goal: A single logon should work everywhere *
- The problem: if same {user, pswd} is used everywhere, identity theft is made easy.
- The idea: Federated Identity Management ♪
  - Each user U chooses an "identity service provider" P
  - Relying parties redirect U to P for authentication

- The technologies
  - openID 1.0 (Fitzpatrick, 2006)
  - openID 2.0 (Recordon & Reed, 2006)
  - Cardspace,… *
- The problems *, *
  - Concerns about phishing *
  - Lack of demand from users and relying parties *

Sir
Fe

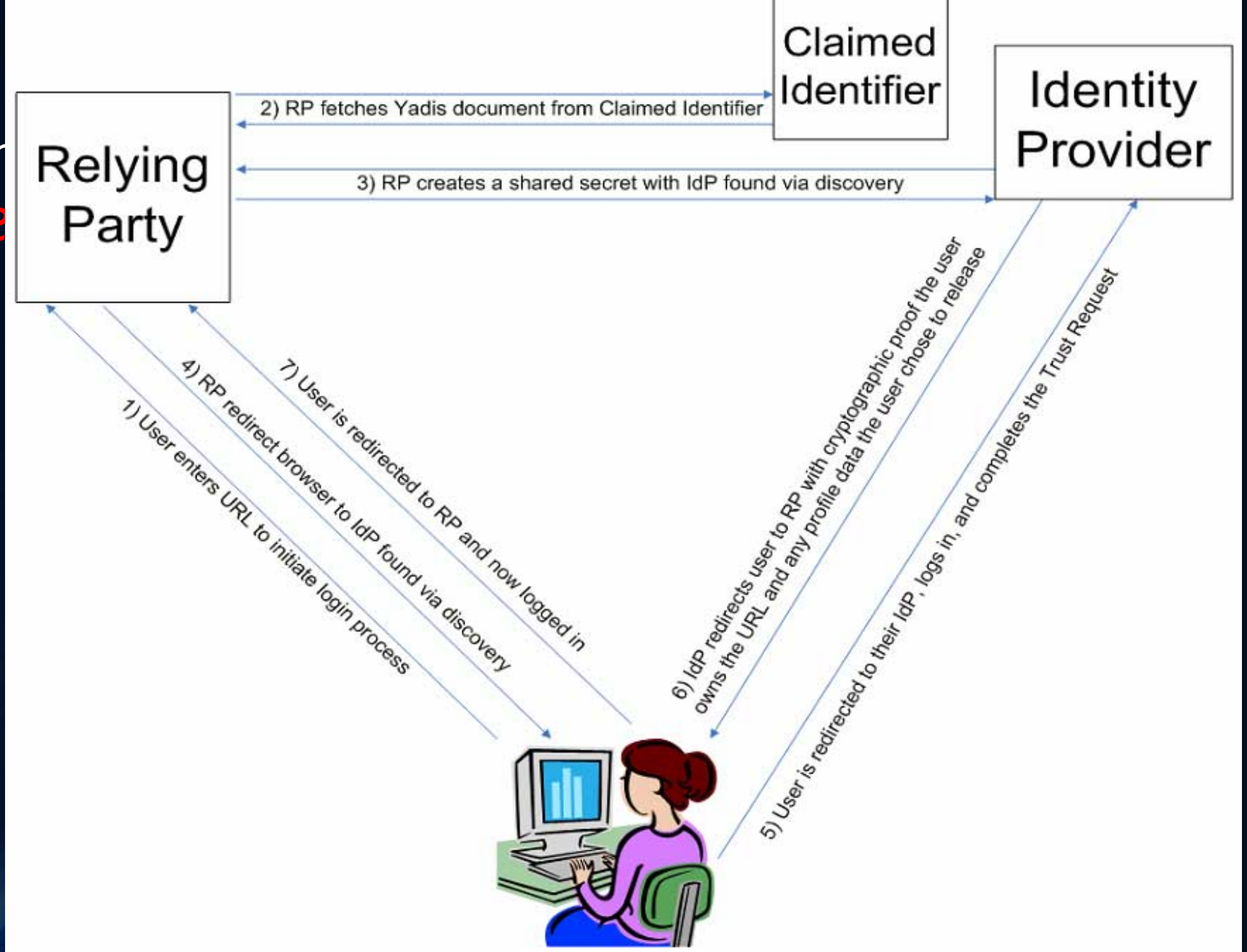


Figure 4: The basic OpenID 1.1 protocol flow

(Recordon & Reed, 2006)