Distributed Systems Security

Authentication Practice - 3

Prof. Steve Wilbur
s.wilbur@cs.ucl.ac.uk

Z08

Lecture Objectives

- Examine reliance placed on user and system authentication
- Review password-based approaches

Z08

Problems

- How does user protect their secret keys?
- What threats are there?

Z08

Key Rings

- User will probably have several secret keys
  - signing keys
  - encryption keys
  - role-based keys
  - different key lengths (512-bit, 1024-bit, DES etc.)
  - etc.
- Need to store encrypted keys on key ring
  - or on encrypted file store
- May also include public keys of correspondents but here need for security not so great
- Need key to secure key ring or encrypted file store from loss, hacking etc.

Z08

Key Ring Keys

- Key ring key needs to be stored securely
  - On magnetic card? With PIN number?
  - On smart card?
  - Use of password?
  - Use of pass-phrase?
- Security is only as good as the weakest link
- So, how secure are passwords/pass-phrases?

Z08

Password Security

- How secure are passwords?
- System Storage
  - Should never be stored in clear text, although many applications and operating systems may still use ineffective password encryption
  - Login process may indicate to hackers legitimate user names by form of response or time taken checking password
  - Storage and visibility of encrypted passwords may allow users with same password to recognise this
    - Concatenate *salt* with password - usually date and time to disguise this

Z08

Password Security - 2
Attacks

- Brute force - try "all" possible passwords
- Try probable passwords
- Try probable passwords for user
- Attack system password file
- Ask the user

[Pfleeger, p. 256]

Z08

Password Security - 3
Brute Force Attack

- Assumes all possible passwords are equally likely
- Since humans are involved this is pessimistic assumption
- However, for passwords from 26 character set up to 8 characters in length there are $26^9-1 \approx 5*10^{12}$ possibilities

Each Attempt	Time Taken
1millisecond	150 years
1microsecond	2 months

- Probably only takes half this time on average

Z08

Password Security - 4
Probable Passwords

- Many people choose short, easy to pronounce, common words
- At 1 attempt per millisecond [from Pfleeger]:

Word Length	Time Taken
3 characters	18 secs
4 characters	8 minutes
5 characters	3.5 hours

- But, "apgwx" is much more unlikely than "relax"
- Use of dictionary of 80,000 words reduces search time for all English words to 80 seconds

Z08

Password Security - 5
User Related Weaknesses

- Many people choose strings related to themselves:
  - Phone number
  - Car registration
  - Spouse name, cat name, etc.
- May be only a few hundred possibilities
- "Ask the User"
  - Large number of passwords means need to write them down
  - In drawer, etc.

Z08

Password Security - 6 Published Analyses

- Morris & Thompson 1979:

1 ASCII char	0.5%
2 ASCII chars	2%
3 ASCII chars	14%
4 alpha chars	14%
5 alpha, same case	21%
6 lowercase alpha	18%
Dictionary words	15%
Total of above	86%

- Klein 1990: 2.7% guessed in 15 minutes, 21% in less than a week of machine time
- Spafford 1992: average password length 6.8 chars and 28.9% were only lowercase alpha

Z08

Password Security - 7 Guidelines

- Use wider range than a-z, including punctuation and control characters
- Use long passwords - some systems now insist on at least 8 characters
- Avoid names and words - 300 million 6 character alpha combinations, but only 150,000 in dictionary
- Choose unlikely password that you can remember - 2Brn2B
- Change password regularly even if not suspicious
- Don't write it down
- Don't tell anyone else, ever!

Z08

Password Security - 8
Challenge-Response Authentication

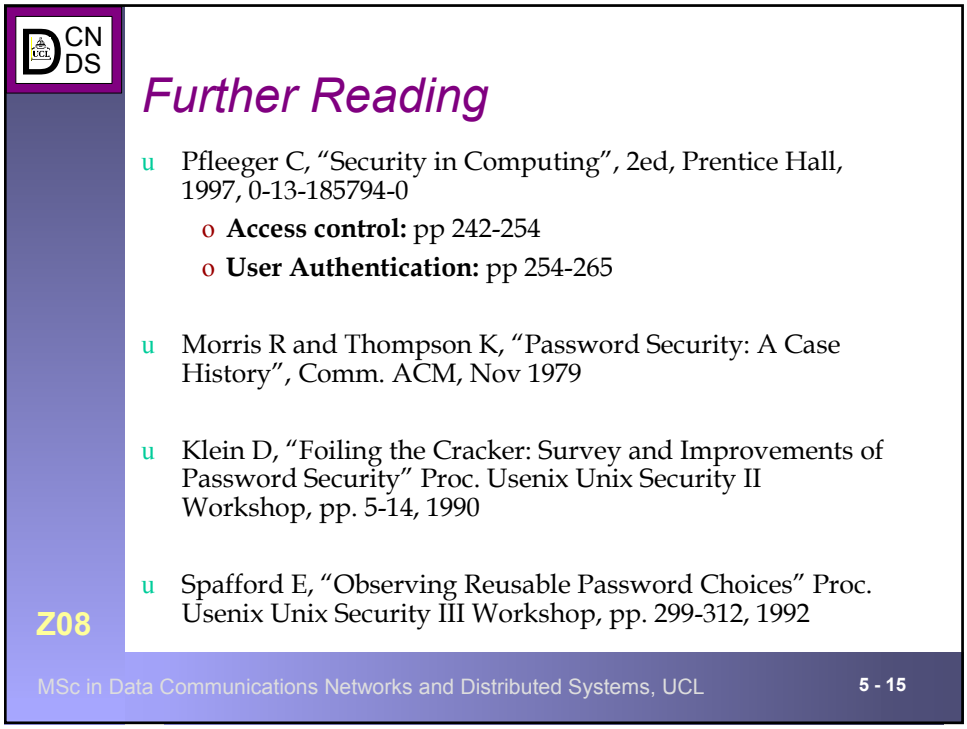
- Password system for login uses a static protocol which might be replayed if captured
- Might use challenge-response dialogue as only or additional measure
- Users are each assigned unique mathematical functions
- Machine issues challenge (number) to which function is applied and response keyed in
- Special calculator may be provided for purpose
- (Compare with telephone banking and set of personal info provided by you which can be used as a challenge)

Z08

Authentication Summary

- Users can be authenticated by:
  - Something they know (Password)
  - Something they possess (Card)
  - Something they are (Biometrics)
- All have weaknesses
  - Passwords - see earlier
  - Cards - loss - use of PIN to reduce vulnerability
  - Calculator - loss, failure
  - Biometrics - false positives and false negatives, damage to fingerprint in accidents, stress affecting signatures and keyboard timing and accuracy, etc

Z08


CN
DS
Further Reading
u Pfleeger C, "Security in Computing", 2ed, Prentice Hall, 1997, 0-13-185794-0
o **Access control:** pp 242-254
o **User Authentication:** pp 254-265
u Morris R and Thompson K, "Password Security: A Case History", Comm. ACM, Nov 1979
u Klein D, "Foiling the Cracker: Survey and Improvements of Password Security" Proc. Usenix Unix Security II Workshop, pp. 5-14, 1990
u Spafford E, "Observing Reusable Password Choices" Proc. Usenix Unix Security III Workshop, pp. 299-312, 1992
Z08
MSc in Data Communications Networks and Distributed Systems, UCL
5 - 15