# Your Password
# Your Identity
# Your Privacy

An instructional unit on password basics

prepared by
Raymond T. Albert, Ph.D. (ralbert@maine.edu)
University of Maine at Fort Kent

# Audience and Objectives

Intended Audience:

- All persons concerned about ways to protect their identity and privacy in the information age through a better understanding of passwords and their protection

Objectives: upon successful completion of this instructional module the learner should, without error, be able to …

- Agree that strong passwords and password practices contribute to protection of identity and privacy
- Discriminate passwords as *weak* or **strong**
- Recognize the role of passwords in authentication
- Recognize the relationship between authentication and both identity and privacy
- Identify a tool helpful to those who have many passwords to maintain

# Quick Quiz

Which of the following best describes the reason your password is easy to remember:

A. based on common dictionary words
B. based on common names
C. based on user/account name
D. is short (under 6 characters)
E. none of the above

(choose/click one)

# Your Identity and Privacy are at risk

Unfortunately,

- the characteristic you have selected also makes your password vulnerable to attack thus putting your Identity and Privacy at risk
- you are not alone

Lets take a look at a few more characteristics and practices that make a password vulnerable to attack …

# Your Identity and Privacy may still be at risk

There may be other characteristics of your password and its use that put your identity at risk

Lets take a quick look at a few more characteristics and practices that make a password vulnerable to attack …

# Characteristics of *weak* passwords

- *Weak* Passwords
  - based on common dictionary words
    - Including dictionary words that have been altered:
      - Reversed (e.g., “terces”)
      - Mixed case (e.g., SeCreT)
      - Character/Symbol replacement (e.g., “$ecret”)
      - Words with vowels removed (e.g., “scrt”)
  - based on common names
  - based on user/account identifier
  - short (under 6 characters)
  - based on keyboard patterns (e.g., “qwerty”)
  - composed of single symbol type (e.g., all characters)
  - resemble license plate values
  - are difficult for you to remember

# *Weak* password practices

- Weak Password practices
  - recycling passwords
  - recording (writing down) passwords
  - use of previously recorded passwords (combination of above practices)
  - use of password on two or more systems/contexts
    - Especially risky when passwords are reused in low-trust systems (e.g., online gaming) since increased exposure

**Factoid:** "The key element in password security is the crackability of a password combination… inadequate knowledge of password procedures, content, and cracking lies at the root of user's "insecure" behaviours."[6]

You now know the characteristics of weak passwords and password practices

Now lets explore

the characteristics of **strong** passwords and password practices …

# Characteristics of **strong** passwords

- Strong Passwords
  - contain at least *one of each* of the following:
    - digit (0..9)
    - letter (a..Z)
    - punctuation symbol (e.g., !)
    - control character (e.g., ^s, Ctrl-s)
  - are based on a verse (e.g., passphrase) from an obscure work where the password is formed from the characters in the verse
    - e.g., “ypyiyp” derived from the title of this module
    - sometimes referred to as a *virtual password*
  - are easily remembered by you but very difficult (preferably impossible) for others to guess

# **Strong** password practices

- Strong Password Practices
  - never recycle passwords
  - never record a password anywhere
    - exceptions include use of encrypted password “vaults”
  - use a different password for each system/context
  - be aware Trojan horse programs can masquerade as login prompts so always reset the system as appropriate to obtain a trusted login prompt
  - check for keyboard buffer devices/software that intercept keystrokes (including password capture)
  - change password occasionally
  - change your password immediately if you suspect it has been “stolen”
  - “passwords should be protected in a manner that is consistent with the damage that could be caused by their compromise.”[9]
  - monitor for possible eavesdroppers during entry of password
  - do not use the "Remember Password" feature of applications (e.g., Microsoft® Internet Explorer®).
  - inquire about proactive password checking measures with your system administration

You now know the characteristics of *weak* and **strong** passwords and password practices

Now lets explore

two common password attacks and ways to reduce the risk of being attacked …

# Password Attacks

- Most successful attacks are based on:
  - Dictionary attacks
    - "The guessing [often automated] of a password by repeated trial and error."[1]
  - Social engineering
    - "Social engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker."[2]

**Factoid:** "…passwords are inherently risky, because they are susceptible to attack."[5]

# Dictionary Attacks

- Most hackers utilize widely available password cracking dictionaries to uncover *weak* passwords

- **Ways to reduce Your risk:**
  - Create and use **strong** passwords

**Factoid:** "The use of passwords is a major point of vulnerability in computer security, as passwords are often easy to guess by automated programs running dictionary attacks."[3]

# Social Engineering

- Perhaps the most notorious social engineer Kevin Mitnick once stated,

  > "People are the weakest link. You can have the best technology … and somebody can call an unsuspecting employee. That's all she wrote. They got everything."[7]

- **Ways to reduce Your risk:**
  - Remain vigilant and inquisitive
  - Be aware that your password keystrokes may be observed by others
  - Confirm authorization and establish trust before releasing any important information

You now know two common password attacks and ways to reduce the risk of being attacked

Now lets explore

passwords in the context of Your Identity and Privacy …

# Passwords in the Context of Your Identity and Privacy

- What is a password?
  - "A password is information associated with an entity that confirms the entity's identity."[1]
- Why are passwords needed?
  - Passwords are used for *authentication*
    - Authentication can be thought of as the act of linking yourself to your electronic identity within the system you are connecting to
      - Your password is used to verify to the system that you are the legitimate owner of the user/account identifier
    - Commonly referred to as "logging in"

**Factoid:** "Passwords remain the most widely used authentication method despite their well-known security weaknesses."[4]

# Passwords in the Context of Your Identity and Privacy

- Passwords/Identity/Privacy
  - Attackers who obtain your password can authenticate themselves on various systems and in turn …

Access your personal information
(**invade Your Privacy**)

Impersonate you by acting on your behalf
(**steal Your Identity**)

**Factoid:** "Password mechanisms and their users form a socio-technical system, whose effectiveness relies strongly on the users' willingness to make the extra effort that security-conscious behavior requires."[4]

You now know passwords in the Context of Your Identity and Privacy

Now lets explore

a few password facts worth remembering…

# Password Facts worth Remembering

- Protection of Your Identity and Privacy in the information age hinges on sound password knowledge and practice
- Those who do not use strong passwords and password practices are often their own worst enemy
- If you feel you have too many passwords to remember then consider using a password vault (e.g., Password Safe)
- The risks are real, they affect you either directly or indirectly and they can be diminished by using **strong** passwords and password practices

**Factoid:** "[Studies] have shown that current password mechanisms have largely failed to consider usability, and that – given the increasing number of system and passwords – most users cannot cope with the demands imposed on them."[4]

# Password Safe

- “Many computer users today have to keep track of dozens of passwords: for network accounts, online services, premium web sites.”[8]
- “With Password Safe, a free Windows 9x/2000 utility from Counterpane Labs, users can keep their passwords securely encrypted on their computers. A single Safe Combination--just one thing to remember--unlocks them all.”[8]
- “Password Safe features a simple, intuitive interface that lets users set up their password database in minutes.”[8]
- “Best of all, Password Safe is completely free: no license requirements, shareware fees, or other strings attached.”[8]
- You can learn more about this product by visiting …

http://www.counterpane.com/passsafe.html

# Self-Test

Remember, better understanding leads to better protection of…

Your Password
your Identity
your Privacy

Do not cheat Yourself …

# Question 1

Strong passwords and password practices contribute to protection of identity and privacy.

A. TRUE

B. FALSE

(choose/click one)

# Correct!

Excellent,

strong passwords and password practices **do** contribute to protection of identity and privacy

Now let’s move onto the next question …

# Question 2

Which pair contains both a *weak* and a **strong** password?

A. cs101ra, ME11111
B. WYSIWYG, passwd
C. ig*hh4, f9%Wfh
D. kirk, on$7mur

(choose/click one)

# Correct!

Excellent,

**cs101ra, ME11111**
**(weak, common), (weak, license #)**

**WYSIWYG, passwd**
**(weak, common acronym), (weak, common)**

**ig*hh4, f9%Wfh**
**(strong), (strong)**

**kirk, on$7mur**
**(weak, common name), (strong)**

Now let’s move onto the next question …

# Question 3

What is the role of passwords in authentication?

A. to identify the user
B. to verify you are the legitimate owner of the user/account identifier
C. to provide security
D. none of the above

(choose/click one)

# Correct!

Excellent,

the role of passwords in authentication is **to verify you are the legitimate owner of the user/account identifier**

Now let’s move onto the next question …

# Question 4

Which of the following best describes the relationship between authentication and both identity and privacy?

A. Successful authentication validates identity and provides access to private information

B. Authentication is the validation of a user's identity

C. Anyone who authenticates themselves on a system using your credentials (user/account identifier, password) assumes your identity and has access to your personal information on that system

D. Identity theft and invasion of privacy are likely results of weak passwords and/or password practices

(choose/click one)

# Correct!

Excellent,

successful authentication validates identity and provides access to private information

Note, the other choices are either simple definitions or facts regarding the conditions or probable outcomes of fraudulent authentication (likely attributable to password theft)

Now let’s move onto the next question …

# Question 5

This is a tool helpful to those who have many passwords to remember.

A. ePassword Keeper
B. Password Safe
C. Sphinx
D. TK8 Safe

(choose/click one)

# Correct!

Excellent,

(actually, these are all tools helpful to those who have many passwords to remember)

ePassword Keeper, learn more by visiting …
http://www.edisys.com/Products/ePassword_Keeper/epassword_keeper.asp
Password Safe, learn more by visiting …
http://www.passwordsafe.com/
Sphinx (a hardware solution), learn more by visiting …
http://www.securetech-corp.com/sphinx.html
TK8 Safe, learn more by visiting …
http://www.tk8.com/safe.asp

Congratulations, you have answered all questions correctly …

# Remember, it is …

Your Password
your Identity
your Privacy

# References


1. Matt Bishop (2003) Computer Security. Pearson Education, Inc. ISBN: 0-201-44099-7.
2. Michael Whitman & Herbert Mattord (2003) Principles of Information Security. Course Technology, a division of Thomson Learning, Inc. ISBN: 0-619-06318-1.
3. Benny Pinkas & Tomas Sander (2002) Authentication and authorization: Securing passwords against dictionary attacks. *Proceedings of the 9th ACM conference on Computer and communications security*.
4. Dirk Weirich & Martina Angela Sasse (2001) Session 7: passwords revisited: Pretty good persuasion: a first step towards effective password security in the real world. *Proceedings of the 2001 workshop on New security paradigms*.
5. Peter G. Neumann (1994) Risks of passwords. *Communications of the ACM*, Volume 37 Issue 4.
6. Anne Adams & Martina Angela Sasse (1999) Users are not the enemy. Communications of the ACM, Volume 42 Issue 12.
7. Elinor Abreu (2000). Kevin Mitnick bares all. *NetworkWorldFusion News Online* (28 September 2000) [ Cited July 26, 2003 ]' available from the World Wide Web http://www.nwfusion.com/news/2000/0928mitnick.html
8. Counterpane Internet Security (2003). Password Safe software. [ Cited July 26, 2003 ] available from the World Wide Web http://www.counterpane.com/passsafe.html
9. United States Department of Defense Computer Security Center (1985). Department of Defense Password Management Guideline. CSC-STD-002-85 Library No. S-226,994 [ Cited July 26, 2003 ] available from the World Wide Web http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-002-85.html


Of particular value to instructors is the following work:


1. Dirk Weirich & Martina Angela Sasse (2001) Session 7: passwords revisited: Pretty good persuasion: a first step towards effective password security in the real world. *Proceedings of the 2001 workshop on New security paradigms*.

# WWW Resources

- http://web.mit.edu/net-security/www/pw.html
- http://www.umich.edu/~policies/pw-security.html
- http://www-cgi.cs.cmu.edu/~help/security/pass_sec.html
- http://www.alw.nih.gov/Security/Docs/passwd.html
- http://www.ucsc.edu/banner/01ePwdSecurity.html#Password%20Guidelines
- http://ithelp.indstate.edu/info/secure-passwords.html#general
- http://www.lbl.gov/ITSD/Security/guidelines/password.html#choose
- http://tigger.cc.uic.edu/~mbird/password.html
- http://psynch.com/docs/best_practices.html
- http://www.p-synch.com/docs/strength.html

# Incorrect

Perhaps a review may help, please select one of the following:

*Weak* passwords/practices

**Strong** passwords/practices

Password attacks

Passwords in the Context of Your Identity and Privacy

Password Facts worth Remembering