Passwords - The Magic Words
Let authorized users work - keep others out
WELCOME

TUTORIAL
Passwords by Stan Reichardt
St. Louis Unix Users Group

Copyright by Stan Reichardt, 2001
Passwords - The Magic Words

*Let authorized users work - keep others out*

**WHAT ARE PASSWORDS?**

`passwd` - update a user’s authentication tokens(s)
`passwd` - password file

Password - A combination of characters that verifies your identity to the computer.

Password - A secret combination of letters and numbers used to verify the account owner.

-- source: SAIR Linux & GNU Certification Guide
Passwords - The Magic Words

Let authorized users work - keep others out

DEFINITIONS

password - A secret combination of letters and numbers used to verify the account owner.

login - the account name that identifies the user to the system.

security - protection from unauthorized access, tampering and denial of service.

-- Intrusion Detection, Rebecca Gurley Bace
Passwords - The Magic Words

*Let authorized users work - keep others out*

MORE DEFINITIONS

backdoor - A hole placed in your security by a cracker. It allows the cracker to bypass normal security and gain easy access to your system.

cracker - An individual with malicious intent who breaks into computer systems or breaks copy protection on software products.

exploit - Method by which a cracker gains access to your system.

hacker - Someone who works with or programs computers in a creative way for the pure enjoyment of it.
Passwords - The Magic Words

*Let authorized users work - keep others out*

STILL MORE DEFINITIONS

telnet - A virtual terminal protocol (or a program based on that protocol) for establishing a login session on a remote computer.

Trojan Horse - A malicious program that mimics the behavior of a legitimate system program, usually by attaching itself to other programs.

threat - any situation or event that has a potential to harm a system.

trust - the confidence that what is expected of a system entity corresponds to actual behavior. -- R.Bace
Passwords - The Magic Words

*Let authorized users work - keep others out*

YET MORE DEFINITIONS

user name - The name a user types on a terminal to log on to the system.

virus - A self-replicating program that can spread itself from computer to computer, usually by attaching itself to other programs.

vulnerability - weaknesses in systems that can be exploited in ways that violate security policy.

worm - A program that copies itself from computer to compute over the network, consuming system resources as it goes.
password - A secret word or code used to serve as a security measure against unauthorized access to data. It is normally managed by the operating system or DBMS. However, the computer can only verify the legitimacy of the password, not the legitimacy of the user.

-- Source: TechEncyclopedia - www.techweb.com
Authentication is the process of determining whether someone or something is who or what it is declared to be. The most common form of authentication is the use of logon passwords, the weakness of which is that passwords can often be forgotten, stolen or accidentally revealed. The tokens in this category offer more stringent forms of authentication so that users need to both have something (the token) and know something (the PIN or password) to gain access.

-- source: SANS Institute poster 2001
Passwords - The Magic Words
*Let authorized users work - keep others out*

BACKGROUND BASICS

. Userid & password
. File ownership
. File permissions
Passwords - The Magic Words
Let authorized users work - keep others out
WHY DO PASSWORDS MATTER?

Most systems are cracked, root access gained, by means of using a normal user account.
Passwords - The Magic Words
*Let authorized users work - keep others out*
THE TECHNIQUE

sentry - Halt! Who goes there?
soldier - Sergeant Snorkel.
sentry - Advance and be recognized.
soldier - (whisper) (gives the password).
Passwords - The Magic Words

Let authorized users work - keep others out

WITH COMPUTER

computer - Login:
user - snorkel

computer - Passwd:
user - ******
Passwords - The Magic Words
*Let authorized users work - keep others out*
WITHOUT PROTECTION

Imperial Stormtrooper - Let me see your identification.
Ben (Obi-wan) Kenobi - You don’t need to see his identification.

Imperial Stormtrooper - We don’t need to see his identification.
Ben (Obi-wan) Kenobi - These are not the droids your looking for.

Imperial Stormtrooper - These are not the droids we’re looking for.
Ben (Obi-wan) Kenobi - He can go about his business.

Imperial Stormtrooper - You can go about your business.
Ben (Obi-wan) Kenobi - Move along.

Imperial Stormtrooper - Move along. Move along.
Passwords - The Magic Words
*Let authorized users work - keep others out*

**USER RESPONSIBILITIES**

. Do not share user accounts
. Select a good password and keep it private
. Log off when not using system
. Use file permissions on files and directories
. Notify Sys Admin if password compromised
Passwords - The Magic Words
Let authorized users work - keep others out
SYS ADMIN RESPONSIBILITIES

. Teach the users
. Teach management
. Secure the system
Passwords - The Magic Words
*Let authorized users work - keep others out*
SYS ADMIN RESPONSIBILITIES

**Teach the users**
- Written policy
- Training classes
- Specific information:
  HOW TO CHOOSE A GOOD PASSWORD
Passwords - The Magic Words

*Let authorized users work - keep others out*

SYS ADMIN RESPONSIBILITIES

**Teach management**
- They are users too!
- They are the worst offenders
- They must understand to support any policy
- They must approve policy
Secure the system
- Use shadowed passwords
- Make sure shadow file is not readable
- Run crack programs to find weak passwords
- Check log files
Passwords - The Magic Words

*Let authorized users work - keep others out*

TIPS FOR SYS ADMIN

. Avoid beginning login ID with capital letters.

. Avoid using root login as much as possible.

. Avoid using root password same as user password.
Passwords - The Magic Words  
*Let authorized users work - keep others out*  
**TWO PRINCIPLES**

. Protect your password.

. Choose a hard-to-guess password.
Passwords - The Magic Words
Let authorized users work - keep others out
FIRST PRINCIPLE

**Protect your password.**

. Don’t write down password, memorize it.

. Avoid using same password on every system.

. Never give your password to anyone.

. Watch out for shoulder surfers.

. Untrusted systems might gather passwords.

. Don’t trust any password forever.
Choose a hard-to-guess password.

. Avoid words that can be found in dictionary.

. Avoid names of any kind.

. Avoid anything personal: names, pets, hobbies, dates, numbers

. Avoid simple variations like reversing letters, appending numbers.
Choose a hard-to-guess password (continued).

. Use mixed case characters, numbers and punctuation.

. Use long passwords.

. Use non-words with words.

. Use various letters keyed from a memorable phrase.
Passwords - The Magic Words

*Let authorized users work - keep others out*

HOW TO CHOOSE A GOOD PASSWORD

- understand problems
- avoid common mistakes
- make them easy to remember
Passwords - The Magic Words
*Let authorized users work - keep others out*

PROBLEMS

**Problem Login IDs and passwords:**

. Too many of them

. Too hard to remember
Passwords - The Magic Words

Let authorized users work - keep others out

NEVER (ALWAYS) WRITE DOWN PASSWORDS

. Issued by somebody in Pittsburgh
 . Too hard to remember
  . Changed every 30-60-90 days
 . - too many to remember

 . Needed when you get new job
 . Needed when you get stressed
 . Needed when you get back from Florida
 . Needed when you get run over by truck

 . Never write them on the wall
 . Never write them on the calendar
 . Never write them on back of new $100 bill
Passwords - The Magic Words

*Let authorized users work - keep others out*

BAD EXAMPLES

mx - too short (should be at least six characters)

secrets - word in dictionary

sterces - word in dictionary reversed

secret3 - word in dictionary with number tacked on

53cr3t5 - word with number 5 substituted for S, 3 for E
Passwords - The Magic Words

*Let authorized users work - keep others out*

MORE BAD EXAMPLES

**xyzzy** - secret words from games, books

**tweety** - name of pet, person, project

**winston** - names, unusual or otherwise

**qwerty** - keyboard sequence

**240HIK** - my vehicle license plate

**Sony15sf** - the monitor on my desk
Passwords - The Magic Words
*Let authorized users work - keep others out*

**BETTER EXAMPLES**

2oLd4U - auto license plate - vanity style

3bmChtr - 3 blind mice, SEE how they run

Ott4fs - One, two, three, 4, five, six

nwh4iie - oNe, tWo, tHree, 4, fIve, sIx, sEven

Mrci7yo! - My rusty car is 7 years old!

2emBp1ib - 2 elephants make BAD pets, 1 is better

itMc?Gib - is that MY coat? Give it back
Passwords - The Magic Words

Let authorized users work - keep others out

HOW ARE PASSWORDS CREATED

**seed** - The starting value used by a random number generation routine to create random numbers.

-- Source Techencyclopedia [www.techweb.com](http://www.techweb.com)

**encryption** - crypt

**encryption** - md5 (better)
Brute force -- try all possible combinations

One-way hash function -- In cryptography, an algorithm that generates a fixed string of numbers from a text message. The "one-way" means that is extremely difficult to turn the fixed string back into the text message. One-way hash functions are used for creating digital signatures for message authentication.  
  -- Source Techencyclopedia  www.techweb.com
Passwords - The Magic Words
Let authorized users work - keep others out
HOW ARE PASSWORDS STORED

$> cat /etc/passwd
root:Fu4h2p&xhig2s:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
amd:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
.....
named:x:25:25:Named:/var/named:/bin/false
squid:x:23:23::/var/spool/squid:/dev/null
stan:Ey5j2y7lph3wp:500:500:stan reichardt:/home/stan:/bin/bash
zac:Gg9vrj6zbxk44:501:501:Zac Reichardt:/home/zac:/bin/bash
abby:UyyB4h58Nckaq:502:502:Abby Reichardt:/home/abby:/bin/bash
Passwords - The Magic Words

Let authorized users work - keep others out

HOW SHOULD PASSWORDS BE STORED

```
$> ls -l /etc/shadow
-r-------- 1 root root 882 Jul 6 11:19 /etc/shadow

$> cat /etc/shadow
root:$1$gHHKnO34$8cGMwzW7QSI9MAocpDQoI0:11509:0:99999:7:-1:-1:134539268
bin:*:11200:0:99999:7::
daemon:*:11200:0:99999:7::
adm:*:11200:0:99999:7::
lp:*:11200:0:99999:7::
.....
named:!!:11200:0:99999:7::
squid:!!:11200:0:99999:7::
stan:$1$0Qjyo6uG$tSehM2kKGfGOy7u/SpOGV/:11200:0:99999:7:-1:-1:134540380
zac:$1$vZLPURpp$Ndyx.LB0ZU.dBOO0yqIvT/:11364:0:99999:7:-1:-1:134540380
abby:$1$2rIxYE1k$Z9WP10qFrwgiS.gjtpSWt/:11335:0:99999:7:-1:-1:134540380
```
How much time does it take to break a short password?

Virtually, no time at all.
**Passwords - The Magic Words**

*Let authorized users work - keep others out*

**TIME TO BREAK A RANDOM PASSWORD**

<table>
<thead>
<tr>
<th>Number of Characters</th>
<th>Possible Combinations</th>
<th>Average Time to Discover</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>36</td>
<td>6 minutes</td>
</tr>
<tr>
<td>2</td>
<td>1,300</td>
<td>4 hours</td>
</tr>
<tr>
<td>3</td>
<td>47,000</td>
<td>5 days</td>
</tr>
<tr>
<td>4</td>
<td>1,700,000</td>
<td>6 months</td>
</tr>
<tr>
<td>5</td>
<td>60,000,000</td>
<td>19 years</td>
</tr>
<tr>
<td>6</td>
<td>2,000,000,000,000</td>
<td>630 years</td>
</tr>
<tr>
<td>7</td>
<td>78,000,000,000,000</td>
<td>25,000 years</td>
</tr>
<tr>
<td>8</td>
<td>2,800,000,000,000,000</td>
<td>890,000 years</td>
</tr>
<tr>
<td>9</td>
<td>100,000,000,000,000,000</td>
<td>32,000,000 years</td>
</tr>
<tr>
<td>10</td>
<td>3,700,000,000,000,000,000</td>
<td>1,200,000,000 years</td>
</tr>
</tbody>
</table>

---

**Notes:**
- A password of length 1 has 36 possible combinations.
- A password of length 2 has 1,300 possible combinations.
- A password of length 3 has 47,000 possible combinations.
- A password of length 4 has 1,700,000 possible combinations.
- A password of length 5 has 60,000,000 possible combinations.
- A password of length 6 has 2,000,000,000 possible combinations.
- A password of length 7 has 78,000,000,000 possible combinations.
- A password of length 8 has 2,800,000,000,000 possible combinations.
- A password of length 9 has 100,000,000,000,000 possible combinations.
- A password of length 10 has 3,700,000,000,000,000 possible combinations.

---

**Time to Break:**
- A password of length 1 takes 6 minutes to break.
- A password of length 2 takes 4 hours to break.
- A password of length 3 takes 5 days to break.
- A password of length 4 takes 6 months to break.
- A password of length 5 takes 19 years to break.
- A password of length 6 takes 630 years to break.
- A password of length 7 takes 25,000 years to break.
- A password of length 8 takes 890,000 years to break.
- A password of length 9 takes 32,000,000 years to break.
- A password of length 10 takes 1,200,000,000 years to break.
**Passwords - The Magic Words**

*Let authorized users work - keep others out*

**TIME TO BREAK A MNEMONIC PASSWORD**

<table>
<thead>
<tr>
<th>How Chosen</th>
<th>Example</th>
<th>Number of Possibilities</th>
<th>Average Time To Discover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Al</td>
<td>2,000 (name dictionary)</td>
<td>5 hours</td>
</tr>
<tr>
<td>Name</td>
<td>Charlotte</td>
<td>2,000 (name dictionary)</td>
<td>5 hours</td>
</tr>
<tr>
<td>Word</td>
<td>a</td>
<td>60,000,000(spellchecker)</td>
<td>7 days</td>
</tr>
<tr>
<td>Word</td>
<td>instrument</td>
<td>60,000,000(spellchecker)</td>
<td>7 days</td>
</tr>
<tr>
<td>Two words</td>
<td>dogcat</td>
<td>3,600,000,000</td>
<td>1,140 years</td>
</tr>
</tbody>
</table>

**NOTE: Information from 1990**
## Passwords - The Magic Words

*Let authorized users work - keep others out*

### TIME TO BREAK A MNEMONIC PASSWORD

<table>
<thead>
<tr>
<th>How Chosen</th>
<th>Example</th>
<th>Number of Possibilities</th>
<th>Average Time To Discover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mix dates</td>
<td><em>ATA02CTW08</em></td>
<td>3,700,000,000,000,000,000</td>
<td>1,200,000,000,000 years</td>
</tr>
<tr>
<td>&amp; initials</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poem line</td>
<td><em>Maryhada</em></td>
<td>10,000,000,000,000,000,000,000,000</td>
<td>3,000,000,000,000,000,000 years</td>
</tr>
<tr>
<td></td>
<td><em>littlelamb</em></td>
<td>000,000,000,000,000,000</td>
<td>000,000,000,000,000,000 years</td>
</tr>
<tr>
<td>Poem,First</td>
<td><em>Mahaalila</em></td>
<td>100,000,000,000,000,000</td>
<td>32,000,000,000 years</td>
</tr>
<tr>
<td>2 letters</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Information from 1990
### Passwords - The Magic Words

*Let authorized users work - keep others out*

**TIME TO BREAK A RANDOM PASSWORD**

<table>
<thead>
<tr>
<th>Number of Characters</th>
<th>Possible Combinations</th>
<th>Average Time To Discover</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>36</td>
<td>6 minutes</td>
</tr>
<tr>
<td>2</td>
<td>1,300</td>
<td>4 hours</td>
</tr>
<tr>
<td>3</td>
<td>47,000</td>
<td>5 days</td>
</tr>
<tr>
<td>4</td>
<td>1,700,000</td>
<td>6 months</td>
</tr>
<tr>
<td>5</td>
<td>60,000,000</td>
<td>19 years</td>
</tr>
<tr>
<td>6</td>
<td>2,000,000,000</td>
<td>630 years</td>
</tr>
<tr>
<td>7</td>
<td>78,000,000,000</td>
<td>25,000 years</td>
</tr>
<tr>
<td>8</td>
<td>2,800,000,000,000</td>
<td>890,000 years</td>
</tr>
<tr>
<td>9</td>
<td>100,000,000,000,000</td>
<td>32,000,000 years</td>
</tr>
<tr>
<td>10</td>
<td>3,700,000,000,000,000</td>
<td>1,200,000,000 years</td>
</tr>
</tbody>
</table>
Passwords - The Magic Words

*Let authorized users work - keep others out*

TIME TO BREAK A RANDOM PASSWORD

Source: HOWTO: Password Cracking Techniques
http://geodsoft.com/howto/password/cracking_passwords.htm

<table>
<thead>
<tr>
<th>--</th>
<th>36</th>
<th>52</th>
<th>68</th>
<th>94</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0.47 sec</td>
<td>1.41 sec</td>
<td>3.14 sec</td>
<td>8.3 sec</td>
</tr>
<tr>
<td>4</td>
<td>16.8 sec</td>
<td>1.22 min</td>
<td>3.56 min</td>
<td>13.0 min</td>
</tr>
<tr>
<td>5</td>
<td>10.1 min</td>
<td>1.06 hr</td>
<td>4.04 hrs</td>
<td>20.4 hrs</td>
</tr>
<tr>
<td>6</td>
<td>3.7 hrs</td>
<td>13.7 day</td>
<td>2.26 mon</td>
<td>2.63 mon</td>
</tr>
<tr>
<td>7</td>
<td>9.07 day</td>
<td>3.91 mon</td>
<td>2.13 yrs</td>
<td>20.6 yrs</td>
</tr>
<tr>
<td>8</td>
<td>10.7 mos</td>
<td>17.0 yrs</td>
<td>145 yrs</td>
<td>1,930 yrs</td>
</tr>
<tr>
<td>9</td>
<td>32.2 yrs</td>
<td>882 yrs</td>
<td>9,860 yrs</td>
<td>182,000 yrs</td>
</tr>
<tr>
<td>10</td>
<td>1,160 yrs</td>
<td>45,800 yrs</td>
<td>670,000 yrs</td>
<td>17,079,000 yrs</td>
</tr>
</tbody>
</table>
Passwords - The Magic Words
Let authorized users work - keep others out
FILES

/etc/passwd    - password file
/etc/group    - user group file
/etc/shadow    - encrypted password file

/etc/securetty - file lists ttys from which root can log in
/etc/nologin   - prevent non-root users from logging into system
/etc/issue     - pre-login message and identification file
/etc/issue.net - identification file for telnet sessions

/var/log/wtmp  - contains all the good logins.
/var/log/btmp  - contains all the bad login attempts.
Passwords - The Magic Words

Let authorized users work - keep others out

EDITING PASSWORDS

- usually by using an ASCII editor on /etc/passwd file
- commands are available to edit the password or group files

vipw - password file
vigr - groups file
Passwords - The Magic Words

*Let authorized users work - keep others out*

**CHANGES BY USER**

- users cannot directly edit files
- commands used to edit the password

*passwd* (1) update a user’s authentication tokens(s)

*userpasswd* (1) GUI tool to allow users to change their passwords
Passwords - The Magic Words
Let authorized users work - keep others out
SAMPLE OF TOOLS

sniffer FAQ - network equivalent of over the shoulder password capture. www.boran.com/security/sniff.html

crack - best known Unix password cracking program
www.users.dircon.co.uk/~crypto/index.html

John the Ripper - faster than Crack, with many features
www.openwall.com/john/

Viper - GUI based Windows program
www.wilter.com/~wf/

Slurpie - can run in distributed environments
www.jps.net/coati/archives/slurpie.html
Passwords - The Magic Words

Let authorized users work - keep others out

SECURITY

use good passwords

watch log files

/var/log/wtmp
/var/log/bwtmp

replace weak services
Replace telnet with ssh
Replace pop3 with:
- fetchmail and ssh
- qmail-pop3d (only works with qmail)
- popa3d
Passwords - The Magic Words

Let authorized users work - keep others out

TELNET REPLACEMENTS

. stelnet - an SSL-wrapped telnet solution
. ssh
. OpenSSH
Passwords - The Magic Words

*Let authorized users work - keep others out*

SOME ALTERNATIVES

smart cards
biometric stuff:
  - fingerprints
  - retina scans
  - voice patterns
  - keystroke recognition
Passwords - The Magic Words
Let authorized users work - keep others out
COMMERCIAL ALTERNATIVES

commercial packages (tools):
  . ActivCard - ActivCard
  . Digipass - VASCO Data Security
  . PrivateCard - Cylink
  . SecureID - Security Dynamics
  . COPS - COPS
  . SAFEWORD - Secure Computing
  . Defender - AXENT Technologies
  . TrustBroker - CyberSafe
  . CryptCard - Global Technologies Group, Inc. (GTGI)
  . ELKey - Global Technologies Group, Inc. (GTGI)
  . Praesidium - SpeedCard - Hewlett Packard
  . Conclave Policy Server - ODS Networks
Passwords - The Magic Words
Let authorized users work - keep others out
FUTURE

single sign on - allowing users to get access to multiple computers and applications without learning many different passwords. Hopefully, without the administrative burden of duplicating each user id and group id across multiple systems.

AVOID: r* commands like rlogin, rsh and rcopy

AVOID: Network Information Service (NIS)
- a/k/a yellow pages
Passwords - The Magic Words

*Let authorized users work - keep others out*

SINGLE SIGN ON TOOLS

commercial packages (tools):
  . AutoSecure - Platinum
  . Focal Point - Okiok Data
  . Global Sign On - IBM
  . Access Master - BullSoft, div. of Bull Worldwide Info Systems
  . Secure Single Sign-On - by Schumann Security Software
  . PassGo SSO - AXENT Technologies
  . TrustBroker - CyberSafe
Passwords - The Magic Words
Let authorized users work - keep others out

REFERENCES

*man* (info) - login, passwd, last
*aupropos* - login, passwd, password, group

"Rescued by Unix" by Augie Hansen, Jamsa Press, 1976
"Computer Security, Understanding Computers"
    A Time-Life Books series, 1990

"Learning the Unix Operating System, 3rd Edition"
    by Grace Todino, et al, O’Reilly, 1993

"Network Security in a Mixed Environment"
    by Dan Blacharski, IDG, 1998

"Intrusion Detection" by Rebecca Gurley Bace, MacmillanTechPub, 2000

"SAIR Linux & GNU Certification"
    by Tobin Maginnis, JWiley&Sons, 2000

"Linux Security Toolkit" by David A. Bandel, M&T Books, 2000

"Red Hat Linux 7 Bible" by Christopher Negus, IDG Books, 2001
Passwords - The Magic Words

*Let authorized users work - keep others out*

RESOURCES

SLUUG  *Password File Tutorial* - Mike Kriz, May 1999

SLUUG  *Security Tutorial* - Dave Mills,

- How To Choose A Good Password
  http://wwwinfo.cern.ch/pdp/as/security/cern/ documentation/password.html

System Administration, Networking and Security Institut
  http://www.sans.org/newlook/publications/roadmap.htm

University of Western Australia - UnvCommSvc
Passwords - The Magic Words
Let authorized users work - keep others out

SUMMARY

- Recap of the keypoints
- Suggestions and observations
- Questions, comments and other feedback on these materials to stan@sluug.org

PDF files available at http://www.sluug.org/~stan