Password Cracking 101

City of Phoenix
Information Security and Privacy Office
Agenda

• Computer accounts
• Password cracking methods
• Guess how long it takes to crack a password
• Creating a strong password
• Tools for home use
Computer Accounts

Credentials... I don't need no stinking Credentials!
Computer Accounts

- Identify you to the computer system or network
- Your permissions to access info and systems are based on your account
Passwords

• Verify that the person logging into the computer system or network is who he claims to be

• In other words, your password says you are the account owner

• aka authentication
Authentication Factors

• Something you know
  – Password
• Something you have
  – Badge, token, digital certificate
• Something you are (biometric)
  – Fingerprint, retina

• More factors = Stronger authentication
WANTED

Strong

Passwords

REWARD
Why Is a Strong Password Important?

- Like the key to your house, your password is the key to your computer account, your access privileges, and your information.
- Passwords provide the first line of defense against unauthorized access.
- Strong passwords help protect the confidentiality, integrity, and availability of your information and systems.
Strong passwords can’t be easily guessed.
Strong Passwords

Are Not Shared
Are These Strong Passwords?

yNiSEf0FtIz2LMpHyUCD
nXagQIcKHGrFVicxSYci
czYxanEDgSgwPKizEeMc
PmukcYUIcFFpnlGgejiL
0CTJiEVBقiaFl3HAwrmB
MsEFlwsXuOKvoYwfMnKO1
Strong Passwords

Are Easy to Remember

• So you don’t have to write them down
Strong Passwords
Can't Be Easily Cracked

• Password cracking: Using computing technology and power to discover a password

• A typical desktop computer can try between 100,000 and 1 million passwords per second
Making a Strong Password

• Contains a combination of words, numbers, and characters from an easy-to-remember sentence or phrase
• Does not contain words in a dictionary, regardless of the language
• Does not contain a proper name, such as your spouse’s name
• Does not contain numbers associated with you in any way, such as your dog’s birthday or your child’s social security number
Using a Password Strength Checker

- “Call me paranoid, but how do we know these sites aren’t harvesting the passwords they test?”

- Don’t use your actual password

- Use a “test” password with the same number of letters (caps and lower case), numbers, and special characters in the same locations as your actual password

- Your actual password would have the same strength
Cracking Methods

- **Dictionary**
  - Tries words in a dictionary (any language)

- **Pre-computed**
  - Compares encrypted password with lists of cracked passwords

- **Hybrid**
  - Checks common numbers or symbols substitutes for letters, such as 3 for E, or $ for S

- **Brute Force**
  - Attempts every combination of characters
WARNING

• Password cracking programs are available on the Internet

• Do NOT visit sites that host them
• Do NOT download them

• Why?
  – These sites often contain malware
## Time to Crack

<table>
<thead>
<tr>
<th>Password</th>
<th>Crack Method</th>
<th>Time to Crack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barbara1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chicago5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gandalf1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Time to Crack

<table>
<thead>
<tr>
<th>Password</th>
<th>Crack Method</th>
<th>Time to Crack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barbara1</td>
<td>Dictionary</td>
<td>0d0h0m0s</td>
</tr>
<tr>
<td>Chicago5</td>
<td>Dictionary</td>
<td>0d0h0m0s</td>
</tr>
<tr>
<td>Gandalf1</td>
<td>Dictionary</td>
<td>0d0h0m0s</td>
</tr>
</tbody>
</table>
## Time to Crack

<table>
<thead>
<tr>
<th>Password</th>
<th>Crack Method</th>
<th>Time to Crack</th>
</tr>
</thead>
<tbody>
<tr>
<td>October7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0ctobeR7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Crack Method</td>
<td>Time to Crack</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>October7</td>
<td>Dictionary</td>
<td>0d0h0m1s</td>
</tr>
<tr>
<td>0ctobeR7</td>
<td>Brute Force</td>
<td>0d2h23m7s</td>
</tr>
</tbody>
</table>
## Time to Crack

<table>
<thead>
<tr>
<th>Password</th>
<th>Crack Method</th>
<th>Time to Crack</th>
</tr>
</thead>
<tbody>
<tr>
<td>time2Fly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sp1drman</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qwert123</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Time to Crack

<table>
<thead>
<tr>
<th>Password</th>
<th>Crack Method</th>
<th>Time to Crack</th>
</tr>
</thead>
<tbody>
<tr>
<td>time2Fly</td>
<td>Brute Force</td>
<td>0d1h35m33s</td>
</tr>
<tr>
<td>Sp1drman</td>
<td>Brute Force</td>
<td>0d0h11m17s</td>
</tr>
<tr>
<td>Qwert123</td>
<td>Hybrid</td>
<td>0d0h0m25s</td>
</tr>
</tbody>
</table>
## Time to Crack

<table>
<thead>
<tr>
<th>Password</th>
<th>Crack Method</th>
<th>Time to Crack</th>
</tr>
</thead>
<tbody>
<tr>
<td>goBears4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>goBears!</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GoEag1es</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GoE@g1es</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Time to Crack

<table>
<thead>
<tr>
<th>Password</th>
<th>Crack Method</th>
<th>Time to Crack</th>
</tr>
</thead>
<tbody>
<tr>
<td>goBears4</td>
<td>Brute Force</td>
<td>0d2h33m58s</td>
</tr>
<tr>
<td>goBears!</td>
<td>Brute Force</td>
<td>0d2h32m58s</td>
</tr>
<tr>
<td>GoEag1es</td>
<td>Pre-computed</td>
<td>0d0h2m47s</td>
</tr>
<tr>
<td>GoE@g1es</td>
<td>Brute Force</td>
<td>0d5h13m38s</td>
</tr>
<tr>
<td></td>
<td>Duration</td>
<td>Method</td>
</tr>
<tr>
<td>-------</td>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td>GoEag1es</td>
<td>0d 0h 2m 47s</td>
<td>Precomputed H...</td>
</tr>
<tr>
<td>GoE@g1es</td>
<td>0d 5h 13m 38s</td>
<td>Brute Force</td>
</tr>
</tbody>
</table>
Time to Crack

<table>
<thead>
<tr>
<th>Password</th>
<th>Crack Method</th>
<th>Time to Crack</th>
</tr>
</thead>
<tbody>
<tr>
<td>4*20+7ya</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4sc&amp;7yrA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>87yr.aGo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Crack Method</td>
<td>Time to Crack</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>4*20+7ya</td>
<td>Brute Force</td>
<td>&gt; 1d6h24m3s</td>
</tr>
<tr>
<td>4sc&amp;7yrA</td>
<td>Brute Force</td>
<td>&gt; 1d6h24m3s</td>
</tr>
<tr>
<td>87yr.aGo</td>
<td>Brute Force</td>
<td>&gt; 1d6h24m3s</td>
</tr>
<tr>
<td>User Name</td>
<td>LM Password</td>
<td>&lt;8</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----</td>
</tr>
<tr>
<td>t-getty1</td>
<td>????????A</td>
<td></td>
</tr>
<tr>
<td>t-getty2</td>
<td>????????A</td>
<td></td>
</tr>
<tr>
<td>t-getty3</td>
<td>????????O</td>
<td></td>
</tr>
<tr>
<td>t-ghost</td>
<td>????????!</td>
<td></td>
</tr>
</tbody>
</table>
Key Take Away

• The longer and more complex a password, the harder it is to crack
Bad Passwords

- Personally related to you
  - Address, birthday, anniversary, license plate, social security number, favorite car, hobby, or sports team
- Job-related
  - Job title, work location
- Family-related
  - Spouse, children, or pets’ names or birthdays
- Similar to or match your User ID
- Dictionary words
  - No matter what the language
Picking a Strong Password

1. Create a password that's at least six characters long with a mix of letters and numbers.
3. It has to include letters and be at least six characters long.
4. How about ABC?
5. Letters and numbers and at least six characters long!!!
6. Foursome? Gaaa!!!
Unleash Your Creativity!

Base Passwords on a Phrase

• 4*20+7ya
• 4sc&7yrA
• 87yr.aGo

• Fourscore and seven years ago (Gettysburg Address)
Unleash Your Creativity!
Base Passwords on a Phrase

• Wygc?GB!
Use a Keyboard Pattern

- $3$5EdZxc
  - Forms the letter “I” (kinda)
How Many Passwords?

- Work
- Personal – high security
  - Online banking
- Personal – low security
  - News sites

- Recommended
  - Social media ONLY
Tools for Home Use

• Password Safe
  – Free Windows utility
  – Designed by Bruce Schneier
  – Keeps passwords securely encrypted on your computers
  – Just one “Safe Combination” to remember

• http://passwordsafe.sourceforge.net/

City of Phoenix does not endorse or support any tools for home use
Tools for Home Use

• **LastPass**
  – Free utility
  – Just one “master password” to remember
  – Can automatically log you on to web sites and complete forms needed to buy goods online


*City of Phoenix does not endorse or support any tools for home use*
Reminder

• Change default passwords
  – Passwords that “come with” a device or set by the vendor
You Can

• Protect yourself

• Pick strong, easy-to-remember passwords!
Resources

• Password Meter password strength checker
  – http://www.passwordmeter.com/

• Computer World’s review of password managers

• Password Managers
  – http://passwordsafe.sourceforge.net/
Thanks!

Questions? Contact ispo@phoenix.gov