Passwords in the wild

Slides from
• Dave Levin 414-spring2016
Storing passwords in Linux

Stored in /etc/shadow

- Algorithm:
  - 1: MD5-based
  - 2: Blowfish
  - 5: SHA-256
  - 6: SHA-512

- Last changed (days since 1/1/1970)
  - Min #days until must change
  - Max #days until must change
  - #days before expire to warn
  - (#days to wait from expire to disable)
  - (#days this has been expired)
Passwords and Computer Security

- In 2012, **76% of network intrusions exploited weak or stolen credentials** (username/password)
  - Source: Verizon data breach investigations report

- First step after any successful intrusion: install **sniffer** or **keylogger** to steal more passwords

- Second step: run cracking tools on password files
  - Cracking needed because passwords are not (or at least *should not be*) stored in the clear
Gary McKinnon

• 2001 and 2002: hacked into 97 US military and NASA computers searching for evidence of free energy suppression and UFO coverups
  • “… shut down the entire US Army’s Military District of Washington network of over 2000 computers for 24 hrs”
  • “… rendered [US Naval Weapons Station Earle]’s entire network of over 300 computers inoperable at a critical time immediately following 11 September 2001”

• Method: Perl script randomly looking for blank and default passwords to administrator accounts
Old password surveys

• Klein (1990) and Spafford (1992)
  • 2.7% guessed in 15 minutes, 21% in a week
  • Much more computing power is available now

• Univ. of Michigan: 5% of passwords were “goblue”

• Zviran and Haga (1999)
  • Password usage at DoD facility in California
  • 80% of passwords were 4-7 characters in length; 80% used alphabetic characters only; 80% of the users had never changed their password
RockYou Hack (2009)

- Social gaming company
- Database with 32 million user passwords from partner social networks
- Passwords stored in the clear
- December 2009: entire database hacked using a SQL injection attack and posted on the Internet
Passwords in RockYou database

### Password Popularity - Top 20

<table>
<thead>
<tr>
<th>Rank</th>
<th>Password</th>
<th>Number of Users with Password (absolute)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>290731</td>
</tr>
<tr>
<td>2</td>
<td>12345</td>
<td>79078</td>
</tr>
<tr>
<td>3</td>
<td>123456789</td>
<td>76790</td>
</tr>
<tr>
<td>4</td>
<td>Password</td>
<td>61958</td>
</tr>
<tr>
<td>5</td>
<td>iloveyou</td>
<td>51622</td>
</tr>
<tr>
<td>6</td>
<td>princess</td>
<td>35231</td>
</tr>
<tr>
<td>7</td>
<td>rockyou</td>
<td>22588</td>
</tr>
<tr>
<td>8</td>
<td>1234567</td>
<td>21726</td>
</tr>
<tr>
<td>9</td>
<td>12345678</td>
<td>20553</td>
</tr>
<tr>
<td>10</td>
<td>abc123</td>
<td>17542</td>
</tr>
<tr>
<td>11</td>
<td>Nicole</td>
<td>17168</td>
</tr>
<tr>
<td>12</td>
<td>Daniel</td>
<td>16409</td>
</tr>
<tr>
<td>13</td>
<td>babygirl</td>
<td>16094</td>
</tr>
<tr>
<td>14</td>
<td>monkey</td>
<td>15294</td>
</tr>
<tr>
<td>15</td>
<td>Jessica</td>
<td>15162</td>
</tr>
<tr>
<td>16</td>
<td>Lovely</td>
<td>14950</td>
</tr>
<tr>
<td>17</td>
<td>michael</td>
<td>14898</td>
</tr>
<tr>
<td>18</td>
<td>Ashley</td>
<td>14329</td>
</tr>
<tr>
<td>19</td>
<td>654321</td>
<td>13984</td>
</tr>
<tr>
<td>20</td>
<td>Qwerty</td>
<td>13856</td>
</tr>
</tbody>
</table>
GAWKER MEDIA WEBSITES HACKED, STAFF AND USER PASSWORDS LEAKED

Gawker Media, the blog powerhouse built by Nick Denton, has been hacked.

After bringing the company’s websites to a standstill Sunday, one or more hackers operating under the name Gnosis released a 500-MB file apparently containing Gawker’s source code, commenter and staff passwords, and internal conversations between the company’s employees.

The e-mail addresses and passwords of hundreds of thousands of Gawker users have been compromised, the hackers said.

It’s the worst security breach in New York-based Gawker’s eight-year history, and a wake-up call to all web publishers. (Click here to access your Wired.com profile if you feel the need to change your password for this website.)
GAWKER MEDIA WEBSITES HACKED, STAFF AND USER PASSWORDS LEAKED

Gawker Media, the blog powerhouse built by Nick Denton, has been hacked.

After bringing the company's websites to a standstill Sunday, one or more hackers operating under the name Gnosis released a 500-MB file apparently containing Gawker's source code, commenter and staff passwords, and internal conversations between the company's employees.

The e-mail addresses and passwords of hundreds of thousands of Gawker users have been compromised, the hackers said.

It's the worst security breach in New York-based Gawker's eight-year history, and a wake-up call to all web publishers.

(Click here to access your Wired.com profile if you feel the need to change your password for this website.)

2010 - Gawker
Stored passwords encrypted
188,279 decrypted & released
Gawker Passwords (2010)

Gawker Media Password Lengths
Percentage of passwords plotted against password length in characters. Divided by email provider.

What passwords did users have?
Percentage of users from each email service with each password

Source: Anonymized set of 188,279 leaked Gawker Media passwords