Melissa from Bakersfield (BHS)

Alfonso

Operational Security
Securing systems & networks - "free time" on Thurs afternoons
Users, authentication, access control
Social Engineering

Format
Morning
  2 sessions
  9:00 ~ 10:15
  10:30 ~ noon
Lunch
  noon ~ 1:30
Afternoon
  Hands-on sessions and/or detailed lectures

Surveys & Contact Info

Ethics & Legality
  Must have strong ethical background
  Legal framework
    Federal - criminal & civil
    State - criminal & civil
  Basic safeguards
    Permission is key
    Maintain boundaries
    Avoid liabilities
  Ethics
    Many codes of ethics from professional societies
What is security?
- Traditional
  - Confidentiality
  - Integrity
  - Availability
- Generalized
  - Threats / Risks / Vulnerabilities
  - Prevention / Mitigation
  - Response

Awareness
- Risk / Benefit analysis
  - Threats → Risks → Costs → Benefits
  - Acceptable level of risk
  - Mitigation / prevention plan
  - "Best practices"

Operational Security
- Physical security matters
- Identity in a computer system
  - "Entity" or "role-based" identity
    - User database
      - Username, authentication method

Auth methods
- Something you know
- Something you have
- Something you are

Password Storage
- Plain text
- Hashed - One way encryption
  - Easy: password → hash
  - Hard: hash → password

Letters & Numbers | Example: password has 6 letters (lowercase)
Example: password has 6 letters (lowercase) $26 \cdot 26 \cdot 26 \cdot 26 \cdot 26 \cdot 26 \rightarrow 26^6 = 308,915,776$

1 million guesses/sec

$\frac{308,915,776}{1,000,000} \approx 309$ seconds

$\frac{308,915,776}{20,000,000} = 15$ seconds

Letters & Numbers

$36^6 = 2,176,782,336$

$\frac{2,176,782,336}{1,000,000} = 2,177$ seconds

$\approx 36$ min

$\frac{2,176,782,336}{20,000,000} = 108$ seconds

Upper Case, Lower Case & Numbers

6 characters $62^6 = 56,800,235,844$

1 million / second $\rightarrow 568,000$ seconds $\rightarrow 946$ minutes $\rightarrow 15.7$ hours

20 million / second $\rightarrow 28,410$ seconds $\rightarrow 47$ mins

10 characters $62^{10} = 839,299,365,868,340,224$

1 million / second $= 839,299,365,868$ seconds

$139,883,227,641$ mins

$9,714,113$ days

20 million / second $= 419,649,682,933$ seconds

$485,706$ days
500 million/second = 1,678,598,731 seconds
19,428 days

Factors That Affect Password Difficulty

- Length of password (exponent)
- Characters chosen for password (base)
- Random choosing

Factors That Affect Guess Rate

- Types of passwords (e.g., dictionary is easy)
- Hash Algorithm
  - How the computer turns the password into a hash
- Processors available
  - More cores → More guesses
- CPU crackers use the general-purpose processor
  - Cores can do multiple computations
- Have multiple cores to divide workload
- GPU crackers use the graphical processor
  - Allows many more simultaneous calculations

<table>
<thead>
<tr>
<th>Alg</th>
<th>1 card (6990)</th>
<th>25 cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTLM</td>
<td>7-9 billion/sec</td>
<td>350 billion/sec</td>
</tr>
<tr>
<td>MD5</td>
<td>5-7 billion/sec</td>
<td>180 billion/sec</td>
</tr>
<tr>
<td>SHA1</td>
<td>2-3 billion/sec</td>
<td>63 billion/sec</td>
</tr>
</tbody>
</table>

```````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````