NAS Prototype

Password Immunizer
Version 1.0

User Name:

Password:

Login | Cancel

Copyright © 2007 AntiPion
http://issrl.cs.memphis.edu/antipion
NAS Architecture

Front End

Login Request to be authenticated

Negative Authentication Process

Success

Authentication Failed

Failure Indicates a Potential Valid Request

Highly Secured Back End

Detector Set

Check with full set

Generate Detectors

Detector Generation Process

Train with all entries

Detector Generation Process

Access for Matching

Database of Valid Login entries

Update Database

Request to update

Add/Delete/Modify

Access for Matching

Positive Authentication Process

Success

Authentication passed

Authentication failed

Execute

Regular Interval
Results of Empirical Experiments

The table summarizes the results of experiments with varying: size of password files, AntiP coverage and Confusion parameters ($C_p$). The shaded results indicate that for a smaller password file, a reasonable size AntiPs and good detection rates are found in around 99% coverage and for small confusion parameters. But, very large password files lead to poor result. for this parameter setting, in which case, clustering of password data and/or changing in dimensionality can alleviate.

<table>
<thead>
<tr>
<th>AntiP Coverage</th>
<th>Confusion Parameter</th>
<th># Passwords = 500</th>
<th># Passwords = 1000</th>
<th># Passwords = 5000</th>
<th># Passwords = 10000</th>
<th># Passwords = 50000</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td># AntiP</td>
<td>DR</td>
<td># AntiP</td>
<td>DR</td>
<td># AntiP</td>
<td>DR</td>
</tr>
<tr>
<td>0.9</td>
<td>0.001</td>
<td>463.2</td>
<td>0.6053</td>
<td>804.8</td>
<td>0.558061</td>
<td>2980</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>420.7</td>
<td>0.573337</td>
<td>727.65</td>
<td>0.546811</td>
<td>713</td>
</tr>
<tr>
<td></td>
<td>0.1</td>
<td>210.35</td>
<td>0.417279</td>
<td>185.4</td>
<td>0.219994</td>
<td>130</td>
</tr>
<tr>
<td>0.95</td>
<td>0.001</td>
<td>757.3</td>
<td>0.792968</td>
<td>1344.55</td>
<td>0.758761</td>
<td>5640</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>692.95</td>
<td>0.7772</td>
<td>1121.6</td>
<td>0.730133</td>
<td>2827</td>
</tr>
<tr>
<td></td>
<td>0.1</td>
<td>317.35</td>
<td>0.573521</td>
<td>286.05</td>
<td>0.342639</td>
<td>164</td>
</tr>
<tr>
<td>0.99</td>
<td>0.001</td>
<td>1500.4</td>
<td>0.956289</td>
<td>2696.95</td>
<td>0.95195</td>
<td>12819</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>1389.05</td>
<td>0.951816</td>
<td>2281.8</td>
<td>0.940283</td>
<td>9283</td>
</tr>
<tr>
<td></td>
<td>0.1</td>
<td>811.2</td>
<td>0.853774</td>
<td>814.4</td>
<td>0.671861</td>
<td>312</td>
</tr>
</tbody>
</table>
Finding the optimal range \( (Cp) \)

Figure shows the changes of detection rate and the number of AntiPs with variations in confusion parameter \( (Cp) \). In particular, figure 4 (a) exhibits detection rate with varying sizes of password files while setting the AntiP coverage to 0.99. It is to be noted that in the interval 0.02-0.06 of confusion parameter \( (Cp) \) while the detection rate does not change significantly (figure 4(a)), the number of AntiP’s decrease rapidly (figure 4(b)). For example, with \( \#P = 3000 \) and confusion parameter =0.05, detection rate is 0.9 can be achieved with 4625 AntiPs, compared to 0.94 detection rate with 7446 AntiPs as in the case of \( Cp \) of 0.01.
Variation in number of AntiP’s with different settings of AntiP coverage and password file sizes with confusion parameter set to 0.05. AntiP set size varies almost exponentially with change in coverage whereas it does not increase beyond some limit for varying password set size.
Effects of eliminating smaller AntiPs

Variation of sizes of a pool of AntiP’s produced for password file size of 1000, 2000 and 3000. (b) Each pair of same colored lines represents variation of AntiPs and detection rates for a specific password file size. It is clear from the figure that if smaller sized AntiPs are eliminated, then the Detection rate decreases, but # AntiPs decreases faster than Detection rates. For example, if in case of 1000 valid passwords, if the AntiP sizes of 0.04 or smaller are eliminated, then #AntiP counts reduce to 83% of the original number, whereas, detection rate falls only to 95%.