Practical Password Recovery on an MD5 Challenge/Response such as APOP

Yu Sasaki (The University of Electro-Communications)
Go Yamamoto (NTT)
Kazumaro Aoki (NTT)

(http://eprint.iacr.org/2007/101)

* We notified Information-technology Promotion Agency, Japan of the result followed by the Japanese ordinance, December 8, 2006. The notification number is IPA#10155887.
Tomorrow, Leurent will present the almost same result. (Research motivation is different.)

**Important point**

We have independently done the same research, but not submitted yet.

When did we do? → From October to November. Finished before FSE submission.

Why didn’t we submit? → Because we considered security problems.
• IPA requests to report some vulnerability of widely used software products.
• We respected the IPA’s policy so that we did not submit to conferences.
Recently, collision resistance of several hash functions were broken.

Some researches apply collision to applications.

How about challenge/response authentication?

We show collisions are used to recover user’s secret information in prefix C/R authentication such as APOP. (Only MD5 is used in APOP)

Challenge : $C$, Response : $\text{MD5}(C||\text{Secret})$
APOP and Chosen Challenge

We found, in Man-in-the-Middle environment, attacker can recover the first 3 characters of password.
### Attack Procedure

1. Fix the last 8 bits of M to be a character we guess.
2. Choose free part to yield a collision.
3. Send **C1**, **C2** to user, get responses **R1**, **R2**.
4. If **R1** == **R2**, guess is correct.

<table>
<thead>
<tr>
<th>M1</th>
<th>C1</th>
<th>P</th>
<th>Assword</th>
<th>PAD</th>
</tr>
</thead>
<tbody>
<tr>
<td>M2</td>
<td>C2</td>
<td>P</td>
<td>Assword</td>
<td>PAD</td>
</tr>
</tbody>
</table>

Common string:

Free part. Choose to make collision. Set a char we guess.

When recover more characters, fixed part will be long.

<table>
<thead>
<tr>
<th>M1</th>
<th>C1</th>
<th>P</th>
<th>a</th>
<th>Ssword</th>
<th>PAD</th>
</tr>
</thead>
<tbody>
<tr>
<td>M2</td>
<td>C2</td>
<td>P</td>
<td>a</td>
<td>Ssword</td>
<td>PAD</td>
</tr>
</tbody>
</table>
Conclusion and Future Work

- We showed how to recover 3 chars of APOP password.
- By combining exhaustive search, 8-9 chars are recovered.
- This is the first result applying collision to C/R authentication.

Why recoverable number is 3?

We use Wang’s collision attack that has a difference in the latter part of messages.

Can’t hold more identical values.
Statement In RFC:
Secrets should be long strings (considerably longer than 8-character)

Some may say recovering 3 characters is not enough, it’s not vulnerability.

We tried extension of APOP Attack.

Continue to next talk.
Thank you for your attention!!