Extended APOP Password Recovery Attack

Yu Sasaki, Lei Wang, Kazuo Ohta and Noboru Kunihiro
(The University of Electro-Communications)

31 characters can be recovered.

Remark: This research was done only by UEC.
We respect the IPA’s policy so that we reported the discovery of the new attack to IPA.

We are sorry for not explaining all the details. We will explain the concept.
Properties for Extending the Attack

Need to construct a new MD5 collision attack.

Necessary Properties

1. $\Delta M$ exists only in early part.
2. Many collisions are computed fast.

<table>
<thead>
<tr>
<th>C1</th>
<th>password</th>
</tr>
</thead>
<tbody>
<tr>
<td>C2</td>
<td>password</td>
</tr>
</tbody>
</table>

Can hold long $\Delta M$!!

Our Approach: Use Boer’s attack (‘93)

If initial value (IV) can have specific differences, $\text{MD5(IV1, } M \text{)} = \text{MD5(IV2, } M \text{)}$ can be generated fast.

The same $M$, no difference. Satisfy both properties!!
Our New Attack

Problems of Boer’s attack

Boer’s attack needs $\Delta IV$, doesn’t work for MD5 IV.

We constructed IV Bridge that connects MD5 IV and Boer’s $\Delta IV$.

![Diagram showing IV Bridge and MD5 IV]  

Results

• Experimentally confirmed 31 chars were recovered.
• This attack efficiently recovers up to 61 characters.
Differential Path of Our Attack

Sorry, we can’t show it now.
Conclusion and Countermeasures

- We found Boer’s attack would efficiently work for APOP attack.
- We experimentally confirmed that 31 characters of APOP passwords were recovered. (By Leurent’s assumption, it takes 31 hours.)

Countermeasures

- Set strict restrictions on acceptable challenge string. (printable chars only, less than 512 bits, etc.)
- Stop using MD5. Stop using prefix approach.
Enough to say “vulnerability”? 

Thank you for your attention!!