Extended APOP Password Recovery Attack

Yu Sasaki, Lei Wang, Kazuo Ohta and Noboru Kunihiro

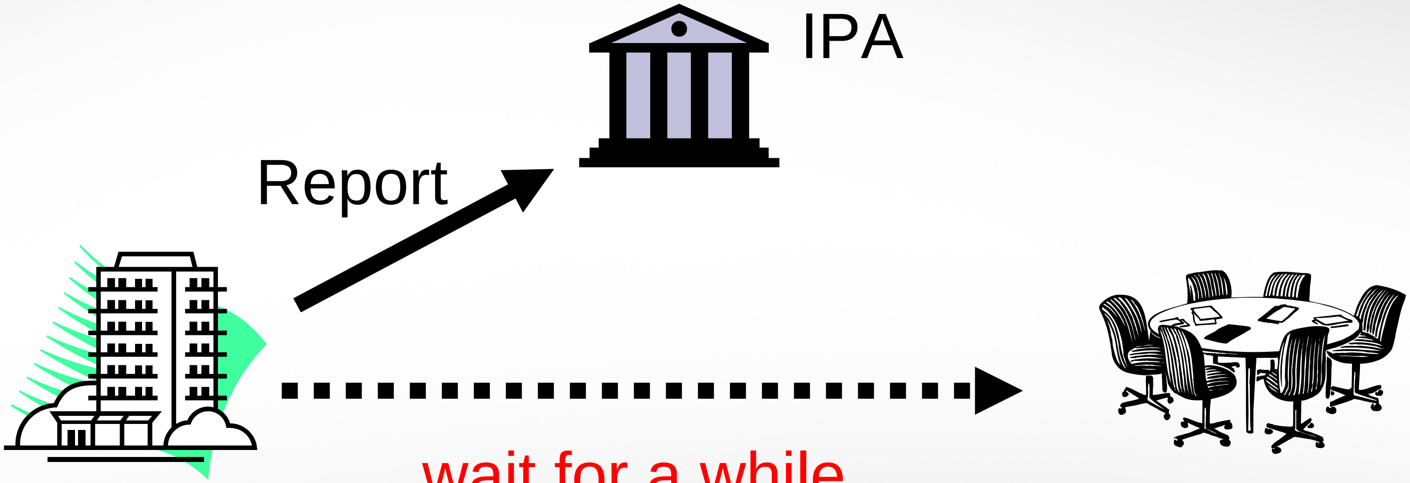
(The University of Electro-Communications)

31 characters can be recovered.

Remark: This research was done only by UEC.

Again Guideline of IPA

We respect the IPA’s policy so that we reported the discovery of the new attack to IPA.



IPA

Report

Research lab

wait for a while

Conference

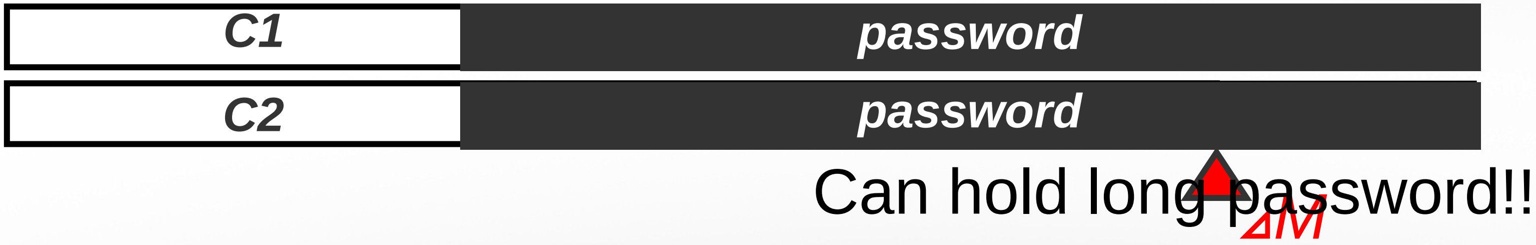
We are sorry for not explaining all the details.
We will explain the concept.

Properties for Extending the Attack

Need to construct a new MD5 collision attack.

Necessary Properties

1. ***⊿M*** exists only in early part.
2. Many collisions are computed fast.



Can hold long password!!

Our Approach: Use Boer’s attack (‘93)

If initial value (IV) can have specific differences,

MD5(***IV1,M***)=MD5(***IV2***, ***M***) can be generated fast.

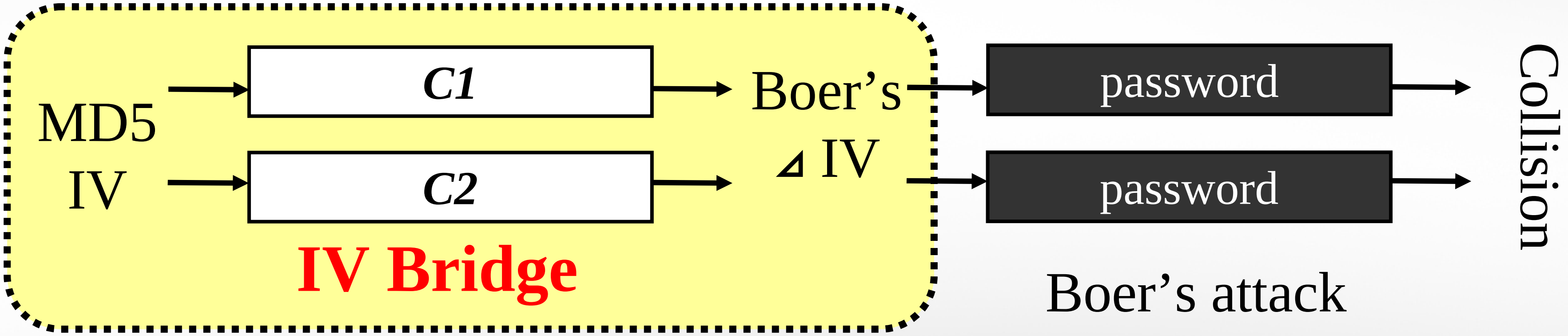
The same ***M***, no difference. Satisfy both properties!!

Our New Attack

Problems of Boer’s attack

Boer’s attack needs ***⊿IV***, doesn’t work for ***MD5 IV***.

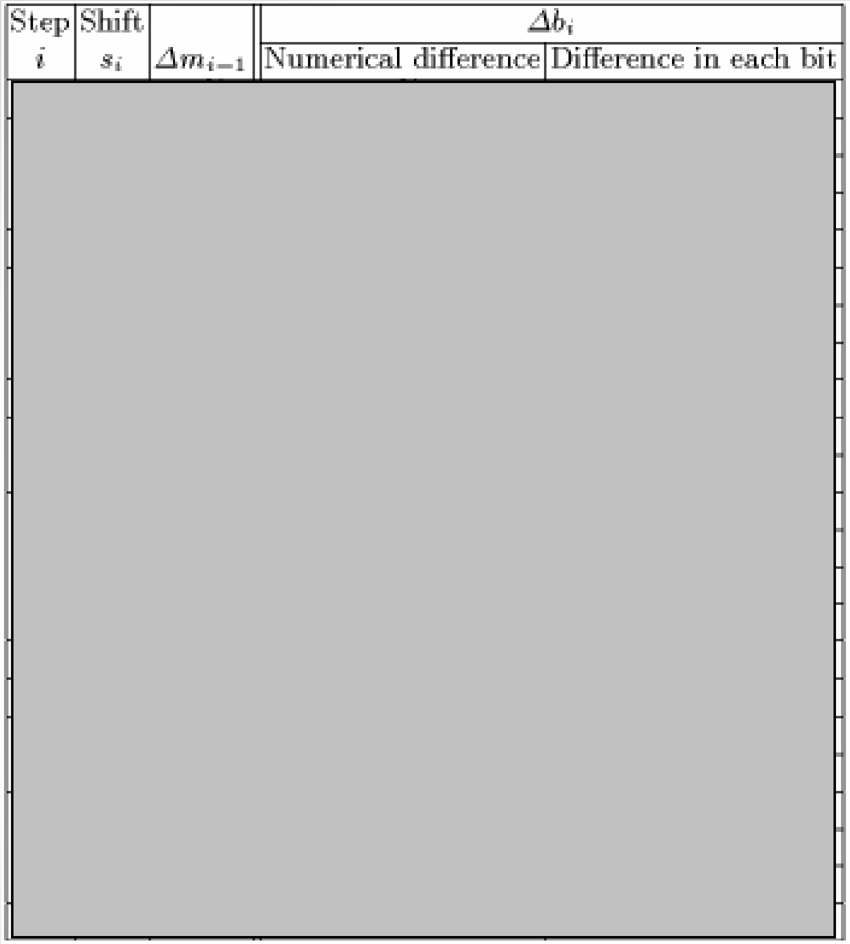
We constructed ***IV Bridge*** that connects ***MD5 IV*** and Boer’s ***⊿IV***.



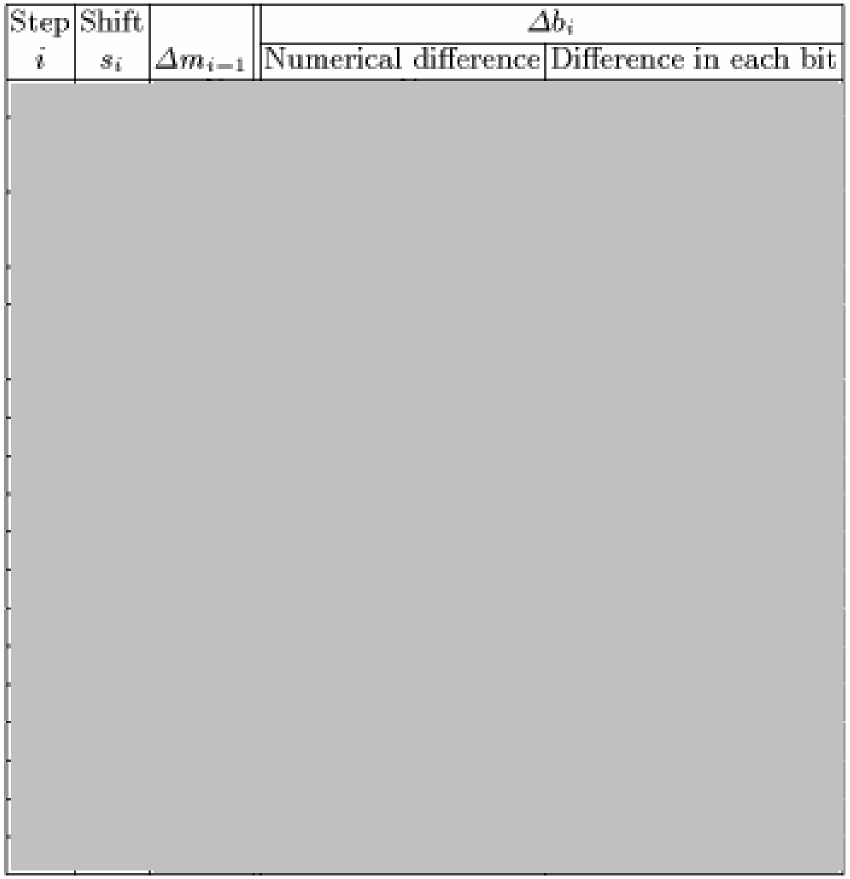
Results

- Experimentally confirmed **31** chars were recovered.
- This attack efficiently recovers up to 61 characters.

Differential Path of Our Attack



Step	Shift		Δb_i	
i	s_i	Δm_{i-1}	Numerical difference	Difference in each bit



Step	Shift		Δb_i	
i	s_i	Δm_{i-1}	Numerical difference	Difference in each bit

Sorry, we can’t show it now.

Conclusion and Countermeasures

- We found Boer’s attack would efficiently work for APOP attack.
- We constructed ***IV Bridge*** that connects ***MD5 IV*** and Boer’s ***⊿IV***.
- 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 !!