

[REVS] Making a Faster Cryptanalytic Time–Memory Trade–Off (Cracking Windows Passwords in 5 Seconds)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0094.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/23/03

To: list@securiteam.com

Date: 23 Jul 2003 12:06:03 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Making a Faster Cryptanalytic Time–Memory Trade–Off (Cracking Windows Passwords in 5 Seconds)

SUMMARY

In 1980, Martin Hellman described a cryptanalytic time–memory trade–off that reduces the time of cryptanalysis by using precalculated data stored in memory. This technique was improved by Rivest before 1982 with the introduction of distinguished points that drastically reduces the number of memory lookups during cryptanalysis. This improved technique has been studied extensively but no new optimizations have been published ever since. We propose a new way of precalculating the data that reduces by two the number of calculations needed during cryptanalysis. Moreover, since the method does not make use of distinguished points, it reduces the overhead due to the variable chain length, which again significantly reduces the number of calculations. As an example, we have implemented an attack on MS–Windows password hashes. Using 1.4GB of data (two CD–ROMs) we can crack 99.9% of all alphanumerical passwords hashes (237) in 13.6 seconds whereas it takes 101 seconds with the current approach using

distinguished points. We show that the gain could be even much higher depending on the parameters used.

DETAILS

Introduction:

Cryptanalytic attacks based on exhaustive search need a lot of computing power or a lot of time to complete. When the same attack has to be carried out multiple times, it may be possible to execute the exhaustive search in advance and store all results in memory. Once this precomputation is done, the attack can be carried out almost instantly. Alas, this method is not practicable because of the large amount of memory needed. In [4] Hellman introduced a method to trade memory against attack time. For a cryptosystem having N keys, this method can recover a key in $N^{2/3}$ operations using $N^{2/3}$ words of memory. The typical application of this method is the recovery of a key when the plaintext and the ciphertext are known. One domain where this applies is in poorly designed data encryption system where an attacker can guess the first few bytes of data (e.g. "#include <stdio.h>"). Another domain are password hashes. Many popular operating systems generate password hashes by encrypting a fixed plaintext with the user's password as key and store the result as the password hash. Again, if the password–hashing scheme is poorly designed, the plaintext and the encryption method will be the same for all passwords. In that case, the password hashes can be calculated in advance and can be subjected to a time–memory trade–off. The time–memory trade–off (with or without our improvement) is a probabilistic method. Success is not guaranteed and the success rate depends on the time and memory allocated for cryptanalysis.

ADDITIONAL INFORMATION

A demonstration web page has been implemented at:
<<http://lasecpc13.epfl.ch/ntcrack/>> <http://lasecpc13.epfl.ch/ntcrack/>.

The original article can be downloaded from:
<<http://lasecwww.epfl.ch/pub/lasec/doc/Oech03.pdf>>
<http://lasecwww.epfl.ch/pub/lasec/doc/Oech03.pdf>.

The information has been provided by <<mailto:philippe.oechslin@epfl.ch>>
Philippe Oechslin.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list–unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list–subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.