

[REVS] Data Tastes Better Seasoned: Introducing the ASH Family of Hashing Algorithms

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0115.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/25/05

To: list@securiteam.com

Date: 25 Jan 2005 18:45:56 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Data Tastes Better Seasoned: Introducing the ASH Family of Hashing Algorithms

SUMMARY

Over the recent months it has become clear that the current generation of cryptographic hashing algorithms are insufficient to meet future needs. The ASH family of algorithms provides modifications to the existing SHA-2 family.

These modifications are designed with two main goals:

- 1) Providing increased collision resistance
- 2) Increasing mitigation of security risks post-collision. The unique public/private sections and salt/pepper design elements provide increased flexibility for a broad range of applications. The ASH family is a new generation of cryptographic hashing algorithms

DETAILS

Background:

The late discoveries leave the United States' National Security Agency's (NSA) SHA-1/224/256/368/512 as the only mainstream algorithms for which cryptographers have yet to find collisions. These are also the only

Securiteam: [REVS] Data Tastes Better Seasoned: Introducing the ASH Family of Hashing Algorithms

algorithms specified as the SHS (Secure Hash Standard) under FIPS (Federal Information Processing Standard) 180–2.[4]

However, even these algorithms are showing weaknesses. In late August 2004 the National Institute for Standards and Technology (NIST, the same body which releases the SHS and the FIPS) applauded the recent research and announced the phase out of SHA–1 by 2010[5]. Though these algorithms have remained strong and cryptanalysis on the newer algorithms have turned up no significant problems, it has become apparent that the current class of algorithm is rapidly becoming insufficient for future security needs.

The ASH algorithms attempt to fill this need. Offering increased flexibility and security, the ASH algorithms are intended to provide modifications that will enhance overall security. Due to the security record of the SHA family and the availability of the new algorithms released in 2002, SHA–256 and SHA–512 have been chosen as the base algorithms for ASH–1 and ASH–2.

Objectives:

The ASH algorithms avoid the necessity to design new algorithms from the ground up. Instead, the ASH algorithms are based on an existing algorithm. For ASH–1 and ASH–2, algorithms in the SHA family have been selected. ASH is designed to treat the actual hash function as a black–box that can easily be changed as newer and improved hash functions are created. ASH reorders and modifies data as it is fed into the hash function, this results in increased security and offers improved mitigation of collisions when they do take place.

The goal is to increase resistance, not provide an absolute solution to any particular problems as to do so would be impossible or infeasible.

ASH's series of modifications are not SHA specific and can be applied to any iterative hashing function. For the first several algorithms, ASH is merely SHA with alterations to the datastream as it enters the hashing function. (Hence the similarity in the names of the algorithms.)

However, the modifications increase the flexibility of the algorithms immeasurably. A pepper (explained later) is also used. The pepper allows for multiple dynamic sections to be generated. Each section can be verified to increase the security of the system. (This is discussed the the Secret Seasoning section.)

Download Information:

The paper can be found at:

<<http://xxx.lanl.gov.nyud.net:8090/pdf/cs.CR/0501038>>

<http://xxx.lanl.gov.nyud.net:8090/pdf/cs.CR/0501038>

ADDITIONAL INFORMATION

The original article can be found at:

<<http://xxx.lanl.gov.nyud.net:8090/abs/cs.CR/0501038>>

Securiteam: [REVS] Data Tastes Better Seasoned: Introducing the ASH Family of Hashing Algorithms

<http://xxx.lanl.gov.nyud.net:8090/abs/cs.CR/0501038>

=====

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.