Subject: OFFICIAL COMMENT:DynamicSHA
From: v.klima@volny.cz
Date: Sun, 14 Dec 2008 17:31:22 +0100 (CET)
To: hash-function@nist.gov
CC: hash-forum@nist.gov

Dynamic SHA is vulnerable to generic attacks.

According to security requirements (part 4.A iii) of the hash functions NIST expects the SHA-3 algorithm should be resistent to length-extension attacks.

Length-extension attack is not correctly understood and described in paragraph 6.1 of submitted Dynamic SHA documentations.

As a consequence, Dynamic SHA (with 256-bit and 512-bit outputs) function (h) is trivially vulnerable to length-extension attacks. Given h(m) and len(m) but not m, the attacker easily creates m' (with correct padding) and calculates h (m || m') simply from h(m) and m'.

Moreover, in the function's design there are no precautions against other generic attacks (multi-collisions etc.).

Best regards,
Vlastimil Klima

Subject: Re: OFFICIAL COMMENT:DynamicSHA
From: "?? ?" <xuzijiewz@gmail.com>
Date: Mon, 15 Dec 2008 05:18:53 -0500
To: Multiple recipients of list <hash-forum@nist.gov>

Hi!

I write the documentation too hurriedly. I make a mistake at
"Length-extension attack ". If I can change it , I will change it.

Because it is hard to find the collision of Dynamic SHA , I use no
precautions against other generic attacks (multi-collisions etc.). If
I know it is most important and it is not enough, I will some
precautions against other generic attacks (multi-collisions etc.).
such as message length.

Regards
Xu ZiJie

2008/12/15, v.klima@volny.cz <v.klima@volny.cz>:

> Dynamic SHA is vulnerable to generic attacks.
>
> According to security requirements (part 4.A iii) of the hash functions
> NIST expects the SHA-3 algorithm should be resistent to length-extension
> attacks.
>
> Length-extension attack is not correctly understood and described in
> paragraph 6.1 of submitted Dynamic SHA documentations.
>
> As a consequence, Dynamic SHA (with 256-bit and 512-bit outputs) function
> (h) is trivially vulnerable to length-extension attacks. Given h(m)
> and len(m) but not m, the attacker easily creates m' (with correct padding)
> and calculates h (m || m') simply from h(m) and m'.
>
> Moreover, in the function's design there are no precautions against other
> generic attacks (multi-collisions etc.).
>
> Best regards,
> Vlastimil Klima

Subject: OFFICIAL COMMENT:DynamicSHA
From: Sebastiaan Indesteege <sebastiaan.indesteege@esat.kuleuven.be>
Date: Thu, 23 Apr 2009 22:09:13 +0200
To: hash-function@nist.gov
CC: hash-forum@nist.gov

Dear,

We have found a practical collision attack on Dynamic SHA. It applies to all digest lengths. Collision pairs can be found in a matter of seconds on an average desktop PC. Attached to this e-mail is C source code demonstrating example collisions for DSHA-256 and DSHA-512.

Also, we have attacks on Dynamic SHA-2. A paper describing all of our attacks on Dynamic SHA and Dynamic SHA-2 is upcoming.

Best regards,

Jean-Philippe Aumasson, Orr Dunkelman, and Sebastiaan Indesteege.

--
Sebastiaan Indesteege sebastiaan.indesteege@esat.kuleuven.be
K.U.Leuven, ESAT/COSIC http://homes.esat.kuleuven.be/~sindeste
Kasteelpark Arenberg 10/2446 phone: +32 16 321049
B-3001 Leuven-Heverlee, Belgium fax: +32 16 321969

dshacoll.tar.gz	**Content-Type:**	application/x-gzip
	Content-Encoding:	base64

Subject: Re: OFFICIAL COMMENT:DynamicSHA
From: Guerre Bear <guerrebear@gmail.com>
Date: Mon, 27 Apr 2009 16:05:50 -0400
To: Multiple recipients of list <hash-forum@nist.gov>

Not sure what the point is of the c code is -- it just prints the two pre-computed messages and their hashes. Did you mean to post the code which calculated the two colliding blocks?

Guerre

On Thu, Apr 23, 2009 at 1:17 PM, Sebastiaan Indesteege <sebastiaan.indesteege@esat.kuleuven.be> wrote:

> Dear,
>
> We have found a practical collision attack on Dynamic SHA. It applies to all digest lengths Collision pairs can be found in a matter of seconds on an average desktop PC. Attached to this e-mail is C source code demonstrating example collisions for DSHA-256 and DSHA-512.
>
> Also, we have attacks on Dynamic SHA-2. A paper describing all of our attacks on Dynamic SHA and Dynamic SHA-2 is upcoming.
>
> Best regards,
>
> Jean-Philippe Aumasson, Orr Dunkelman, and Sebastiaan Indesteege.
>
> --
> Sebastiaan Indesteege sebastiaan.indesteege@esat.kuleuven.be
> K.U.Leuven, ESAT/COSIC http://homes.esat.kuleuven.be/~sindeste
> Kasteelpark Arenberg 10/2446 phone: +32 16 321049
> B-3001 Leuven-Heverlee, Belgium fax: +32 16 321969

Subject: Re: OFFICIAL COMMENT:DynamicSHA
From: Sebastiaan Indesteege <sebastiaan.indesteege@esat.kuleuven.be>
Date: Tue, 28 Apr 2009 05:03:55 -0400
To: Multiple recipients of list <hash-forum@nist.gov>

On Mon, Apr 27, 2009 at 04:02:29PM -0400, Guerre Bear wrote:

> Not sure what the point is of the c code is -- it just prints the two
> pre-computed messages and their hashes.

That is exactly the point. The collision example shows that we have a working, practical collision attack on Dynamic SHA. For a collision resistant hash function, it should not be feasible to come up with such an example.

We could have just given the colliding messages, but source code which uses the Dynamic SHA reference implementation makes it easier for anyone to verify the collision.

> Did you mean to post the code which calculated the two colliding blocks?

More information on how the attack works will be published soon.

Best regards,

Sebastiaan

--
Sebastiaan Indesteege sebastiaan.indesteege@esat.kuleuven.be
K.U.Leuven, ESAT/COSIC http://homes.esat.kuleuven.be/~sindeste
Kasteelpark Arenberg 10/2446 phone: +32 16 321049
B-3001 Leuven-Heverlee, Belgium fax: +32 16 321969

Subject: Re: OFFICIAL COMMENT:DynamicSHA
From: Jean-Philippe Aumasson <jeanphilippe.aumasson@gmail.com>
Date: Thu, 30 Apr 2009 09:56:10 -0400
To: Multiple recipients of list <hash-forum@nist.gov>

Our paper describing attacks on Dynamic SHA (and Dynamic SHA2) is now
available at the following URL:
http://131002.net/data/papers/ADIP09.pdf

It will appear soon as IACR ePrint report 2009/217.

On Thu, Apr 23, 2009 at 10:17 PM, Sebastiaan Indesteege
<sebastiaan.indesteege@esat.kuleuven.be> wrote:

> Dear,
>
> We have found a practical collision attack on Dynamic SHA. It applies to
> all digest lengths. Collision pairs can be found in a matter of seconds
> on an average desktop PC. Attached to this e-mail is C source code
> demonstrating example collisions for DSHA-256 and DSHA-512.
>
> Also, we have attacks on Dynamic SHA-2. A paper describing all of our
> attacks on Dynamic SHA and Dynamic SHA-2 is upcoming.
>
> Best regards,
>
> Jean-Philippe Aumasson, Orr Dunkelman, and Sebastiaan Indesteege.
>
> --
> Sebastiaan Indesteege sebastiaan.indesteege@esat.kuleuven.be
> K.U.Leuven, ESAT/COSIC http://homes.esat.kuleuven.be/~sindeste
> Kasteelpark Arenberg 10/2446 phone: +32 16 321049
> B-3001 Leuven-Heverlee, Belgium fax: +32 16 321969

Sara Caswell

From: hash-forum@nist.gov on behalf of ??? [xuzijiewz@gmail.com]
Sent: Monday, May 04, 2009 8:53 AM
To: Multiple recipients of list
Subject: Re: OFFICIAL COMMENT:DynamicSHA

I had not thought it is brocken so soon. Some zeros are in the calculation process, I had not thought of the method. I learn something about difference analysis from it. The times of mix message words is not enough :-).

Regards,
Xu ZiJie

2009/4/30, Jean-Philippe Aumasson <jeanphilippe.aumasson@gmail.com>:
>
> Our paper describing attacks on Dynamic SHA (and Dynamic SHA2) is now
> available at the following URL:
> http://131002.net/data/papers/ADIP09.pdf
>
> It will appear soon as IACR ePrint report 2009/217.
>
>
>
>
> On Thu, Apr 23, 2009 at 10:17 PM, Sebastiaan Indesteege
> <sebastiaan.indesteege@esat.kuleuven.be> wrote:
> > Dear,
> >
> > We have found a practical collision attack on Dynamic SHA. It
> > applies to all digest lengths. Collision pairs can be found in a
> > matter of seconds on an average desktop PC. Attached to this e-mail
> > is C source code demonstrating example collisions for DSHA-256 and DSHA-512.
> >
> > Also, we have attacks on Dynamic SHA-2. A paper describing all of
> > our attacks on Dynamic SHA and Dynamic SHA-2 is upcoming.
> >
> > Best regards,
> >
> > Jean-Philippe Aumasson, Orr Dunkelman, and Sebastiaan Indesteege.
> >
> > --
> > Sebastiaan Indesteege sebastiaan.indesteege@esat.kuleuven.be
> > K.U.Leuven, ESAT/COSIC http://homes.esat.kuleuven.be/~sindeste
> > Kasteelpark Arenberg 10/2446 phone: +32 16 321049
> > B-3001 Leuven-Heverlee, Belgium fax: +32 16 321969
> >
>
>