REPLACES:

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: press release statement

TITLE: **ISO/IEC JTC 1/SC 27 statement of SHA-1**

SOURCE: SC 27 Plenary meeting

DATE: 2017-04-25

PROJECT:

STATUS: In accordance with Resolution 37 (contained in SC 27 N17530) of the 29th SC 27 Plenary meeting held in Hamilton, New Zealand, on 24th – 25th April 2017, this document is created for Press Release. It is being circulated within SC 27 for information.

ACTION: FYI

DUE DATE:

DISTRIBUTION: P-, O, and L-Members,
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-Chair
E. J. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors

MEDIUM: http://isotc.iso.org/livelink/livelink/open/jtc1sc27

NO. OF PAGES: 1 + 2

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Am DIN-Platz, Burggrafenstr. 6, D-10787 [D-10772 postal] Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-4-2652; E-mail: krystyna.passia@din.de;
HTTP://www.din.de/go/jtc1sc27

ISO/IEC JTC 1/SC 27 STATEMENT ON SHA-1

25th April 2017

Cryptographic hash functions that compute a fixed-length message digest from a variable length message are widely used for many purposes in cryptography, including digital signatures.

Recently, Google announced that a team of researchers from the CWI Institute in Amsterdam and Google have successfully demonstrated a practical collision attack on the SHA-1 hash function.

> https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html
> https://shattered.io/

In this context, a collision is an example of two distinct messages which, when input to SHA-1, produce the same digest.

SHA-1 is one of the hash algorithms specified in ISO/IEC 10118-3:2004 (Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions). In 2005, Wang et al. found a weakness in SHA-1, which suggested that finding a collision for SHA-1 is significantly easier than was previously expected. This caused ISO/IEC JTC 1/SC 27 to release a statement in 2006, which stated:

> *This attack [on SHA-1] is of particular importance in digital signature applications, such as time stamping, notarization and systems using public key certificates. Other applications of hash functions, such as Hash-based Message Authentication Codes (HMACs), standardized in ISO/IEC 9797-2, and key derivation, are believed to be unaffected by this attack.*
>
> *ISO/IEC 10118-3:2004 contains a number of other standardized hash-functions which produce longer hash codes <..>. ISO/IEC JTC 1/SC27 therefore recommends that all new developments should consider using one of these stronger hash functions.*

The statement above remains valid even though a collision for SHA-1 has now been found. The 4th edition of ISO/IEC 10118-3 will be published in 2017 and states that

SHA-1 does not provide a sufficient level of collision resistance for future digital signature applications, and should therefore only be used for legacy applications.

However, for applications where collision resistance is not required its use is not deprecated. The specified version of the standard, in addition to the SHA-2 family and WHIRLPOOL, includes a number of other hash functions (i.e. the SHA-3 family, the Streebog family and SM3).

ISO/IEC JTC 1/SC 27 therefore restates its recommendation that all new developments should consider using one of these hash functions.