Bundesamt
für Sicherheit in der
Informationstechnik

The Impact of the IV on Multiblock Hash Collision Paths

M. Gebhardt, G. Illies, W. Schindler

Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn

Graz, March 16, 2006

Generic Description of a Collision Attack

hash function H

(e.g. MD5, SHA-1)

IV

N Steps

post additions

chaining value

related messages M / M‘

collision path

(1st block)

collision

(1-block attack)

near-collision

(multiblock attack; i.e

c.v. with part. properties)

Success Probability (I)

sufficient conditions $\longrightarrow$ (near-)collision path $\longrightarrow$ (near-)collision

Prob((near-)collision path) $\leq$ Prob((near-) collision)

To rate its risk potential it is crucial to at least estimate the complexity of an attack.

Success Probability (I)

The probability Prob((near-)collision path) may depend on bit conditions

- on the message block
- C_1, ..., C_N for the intermediate register word pairs (R_1,R'_1),..., (R_N,R'_N) before the post additions
- on carry bits
- Cp_{N-t+1}, ..., Cp_N on the register word pairs (R^{post}_1,R'^{post}_1),..., (R^{post}_t,R'^{post}_t) after the post additions (hash output = 32*t bit)

Transition probabilities (I)

Typical situation in Step n+1:

$$R_{n+1} = R_n + f(R_n,...,R_{n-t},M_{n+1},const_{n+1})$$

(may be interpreted as values

assumed by random variables)

Typical situation (e.g., for MDx attacks)

$$Prob(C_{n+1} | C_n, C_{n-1}, ..., C_{n-t+1}) \approx 2^{-|C_{n+1}|}$$

$|C_{n+1}|$: # bit conditions in C_{n+1}

(neglecting possible conditions on carry and message bits)

Transition Probabilities (II)

Post addition in Step n with $N\text{-}t+1 \leq n \leq N$

$$R^{post}_n = R_n + IV_{n-(N-t)}$$

fixed 32 bit word

Consequences:

- $Prob(C^p_n \mid C_n)$ depends on $IV_{n-(N-t)}$
- For a randomly chosen IV we have $Prob(C^p_n \mid C_n) = 2^{-|C^p_n|}$
- If $R'^{post}_n = R^{post}_n$ for $n = N\text{-}t+1,\ldots,N$ ($\leftarrow$ 1-block collisions) the transition probability = 1.

MD5, Block 1

Post additions in Steps 61- 63: 6 bit conditions

Published Wang Bit Conditions (Eurocrypt 2005):

- Transition probability for standard IV ≈ 0.005

Published Wang Collision (different bit conditions):

- Transition probability for standard IV ≈ 0.095
- Transition probability for IV = (0x 80000000, 0x EFCDAB89, 0x 82000000, 0x 00000000) = 0.5
- Transition probability for IV = (0x 00000000, 0x EFCDAB89, 0x 80000000, 0x 82000000) = 0

MD5, Block 1 and Conclusion

Example: Considering the bit conditions on the intermediate register values, on the carry bits and the postaddition conditions for a particular (not necessarily optimal) MD5-near-collision sample path (1st block, standard IV) we calculated

Prob(near-collision sample path after message modif.) = $2^{-36.61}$

Experimental results confirmed our stochastic model.

Conclusion: The IV may have significant impact on the probability of a particular near-collision-path in the first block. If several near-collision-paths result in the same near-collision this effect should diminish for Prob(near-collision), in particular, if the focus lies on near-collisions with related properties.

Bundesamt
für Sicherheit in der
Informationstechnik

Contact

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Werner Schindler
Godesberger Allee 185-189
53175 Bonn
Germany

Tel: +49 (0)1888-9582-652
Fax: +49 (0)1888-10-9582-652

Werner.Schindler@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de