Stellingen

bij het proefschrift

Attacks on Hash Functions and Applications

door Marc Stevens

1. Constructing a rogue Certification Authority certificate as described in Chapter 4.2 would cost only around 2700 USD, of which 2000 USD is spent on renting publicly available computing power for one day at Amazon EC2 and 700 USD on buying certificates. This is significantly less than the financial damage malicious parties can cause with such a rogue Certification Authority certificate within the short amount of time before their attack is detected.
Chapter 4 of this thesis

2. To construct a collision attack that is faster than a brute-force attack, it is not enough to have a differential path with high success probability over steps $K, \ldots, S-1$, i.e., all steps after the first K steps that use the message block bits exactly once. It is also necessary that the differences $\delta W_K, \ldots, \delta W_{S-1}$ assumed by the differential path can efficiently be obtained.
Chapter 5 of this thesis

3. There exists an efficient tunnel for MD5 that affects $Q_{26}, \ldots, Q_{64}$ using simultaneous changes in $Q_3[b]$ and $Q_{14}[b]$ and corrections in m_2, m_3, m_6, m_{13} and m_{14}, which is an improvement over tunnels $\mathcal{T}_1, \ldots, \mathcal{T}_8$ (see p. 99).
Chapter 6 of this thesis

4. The total complexity of the identical-prefix collision attack for SHA-1 given in Section 7.6 is equivalent to approximately 2^{61} SHA-1 compressions.
Chapter 7 of this thesis

5. To be secure against collision attacks on MD5 or SHA-1, using collision detection results in a significantly higher runtime complexity compared to using a fast secure alternative such as SHA-2-256.
Chapter 8 of this thesis

6. There exists a collision attack on the compression function of MD5 that for given IHV_{in} computes message blocks M and M' such that

$$\text{MD5Compress}(IHV_{\text{in}}, M) = \text{MD5Compress}(IHV_{\text{in}}, M')$$

with an average complexity equivalent to about $2^{49.8}$ calls to MD5Compress. This compression function attack directly constitutes an identical-prefix collision attack on MD5 resulting in 512-bit colliding messages.
[Ste12]

7. Hash functions are among the main cryptographic workhorses and used in many ways in security applications. However, current hash function standards often lack standardized secure extensions for common use cases such as randomized/keyed hashing. It is desirable that future hash function standards include such secure extensions.

8. In practice a "provably secure" designed cryptographic primitive is not always preferable over an ad-hoc designed cryptographic primitive.

9. Let C be a smooth hyperelliptic curve defined over a finite field of characteristic 2. In the Jacobian $G = J(C)$, computing the double $P + P$ of a point $P \in G$ can be done significantly faster than computing an arbitrary sum $P + Q$ of points $P, Q \in G$ and $P \neq Q$.
[LS04]

10. Replacing an insecure cryptographic primitive with a secure alternative in practice often requires a lot of effort, coordination and in particular time. Hence, when a significant weakness is found in a cryptographic primitive and security is a top priority, it is ill advised to wait with replacing the weak primitive with a secure alternative until realistic attacks appear.

11. An old wisdom dictates that "attacks always get better; they never get worse" (presumably originated with the US National Security Agency). However, this does not always hold for the generally perceived best attack complexity.

12. A good heuristic towards solving a problem is that exact methods lead to better (if not optimal) solutions compared to heuristic methods.

References

[LS04] Tanja Lange and Marc Stevens, *Efficient Doubling on Genus Two Curves over Binary Fields*, Selected Areas in Cryptography (Helena Handschuh and M. Anwar Hasan, eds.), Lecture Notes in Computer Science, vol. 3357, Springer, 2004, pp. 170–181.

[Ste12] Marc Stevens, *Single-block collision attack on MD5*, Cryptology ePrint Archive, Report 2012/040, 2012.