A Live Trojan Message for MD5

(Yet Another Reason Not To Use MD5)

Elena Andreeva[1] **Charles Bouillaguet**[2]
Orr Dunkelman[2] John Kelsey[3]

[1]K.U. Leuven, ESAT/COSIC, Leuven-Heverlee, Belgium

[2]École Normale Supérieure, Paris, France

[3]NIST, Gaithersburg, MD, USA

Crypto'09 Rump Session

Live Trojan Message

Attack Scenario

New Scenario: Trojan Message Attack

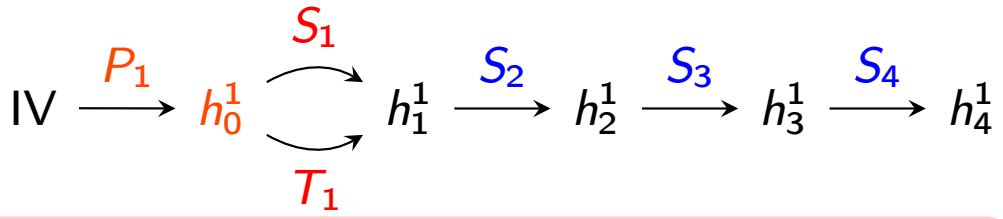
1. Bad guy chooses S (Trojan suffix).
2. Good guy chooses P and signs $H(P \,||\, S)$.
3. Bad guy does something ☠ really evil ☠.
   - $\rightarrow$ Here: second preimage of $P \,||\, S$
   - $\rightarrow$ (breaks the signature)

Restriction ☹

Prefix P has to be drawn from a public, "small" set.

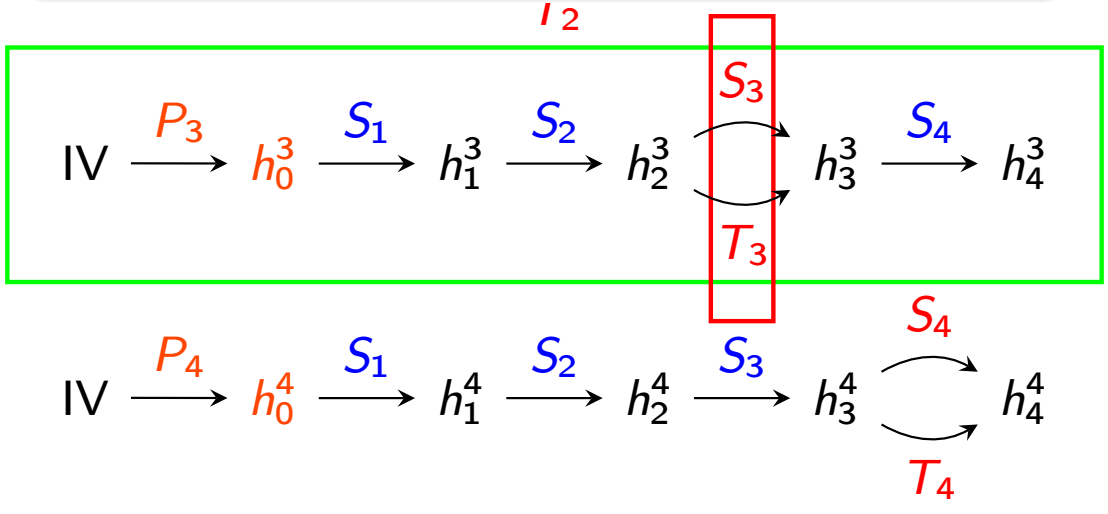
Trojan Message Attack: Online Part

1. We commited to $S = S_1 \,||\, S_2 \,||\, S_3 \,||\, S_4$.
2. Good guy chooses $P = P_3$, setting $M = P \,||\, S_1 \,||\, S_2 \,||\, S_3 \,||\, S_4$.
3. $M' = P \,||\, S_1 \,||\, S_2 \,||\, T_3 \,||\, S_4$ is a second preimage.



No Time

Details Skipped !



Advertisement

Conclusion

Don't Let Your Kids Hash Something Given By Strangers !