

A Live Trojan Message for MD5 (Yet Another Reason Not To Use MD5)

Elena Andreeva¹ **Charles Bouillaguet**²
Orr Dunkelman² John Kelsey³

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

²École Normale Supérieure, Paris, France

³NIST, Gaithersburg, MD, USA



Crypto'09 Rump Session

Live Trojan Message



Attack Scenario

New Scenario: Trojan Message Attack

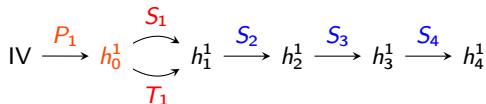
- 1 Bad guy chooses S (Trojan suffix).
- 2 Good guy chooses P and signs $H(P \parallel S)$.
- 3 Bad guy does something  really evil .
 - Here: **second preimage** of $P \parallel S$
 - (breaks the signature)

Restriction ☹️

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

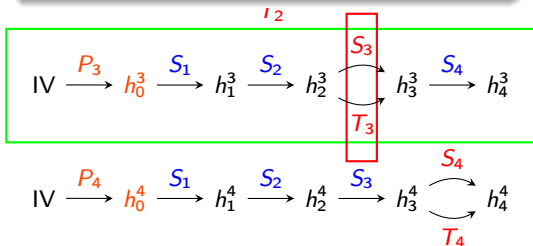
Trojan Message Attack: Online Part

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



No Time

Details Skipped !



Advertisement

The Google logo is centered on the page, rendered in its characteristic multi-colored font (blue, red, yellow, green, red) with a slight 3D effect and a trademark symbol.

trojan message attack

Google Search

I'm Feeling Lucky



[Advanced Search](#)
[Preferences](#)
[Language Tools](#)

Conclusion



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