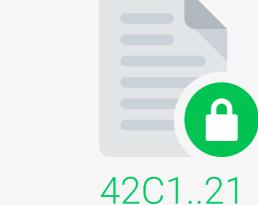
SHAttered

The first concrete collision attack against SHA-1 https://shattered.io

A collision is when two different documents have the same hash fingerprint



SHA-1







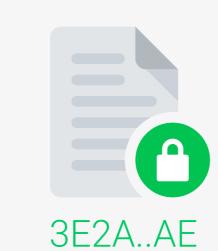


Doc 1

Doc 2







Bad doc





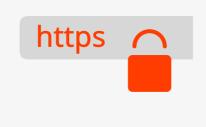
Normal behavior - different hashes

Collision - same hashes

Potentially Impacted Systems



Document signature



HTTPS certificate



Version control (git)

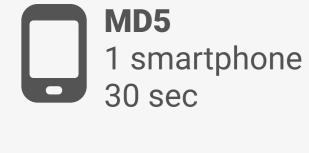


Backup System

Attack complexity

9,223,372,036,854,775,808 SHA-1 compressions performed

Shattered compared to other collision attacks







Defense



Use SHA-256 or SHA-3 as replacement



Use shattered.io to test your PDF



Google products are already protected

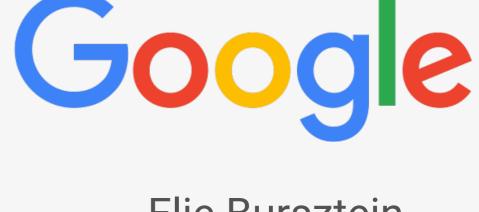


Use collision detection code

Team



Pierre Karpman



Elie Bursztein Ange Albertini Yarik Markov