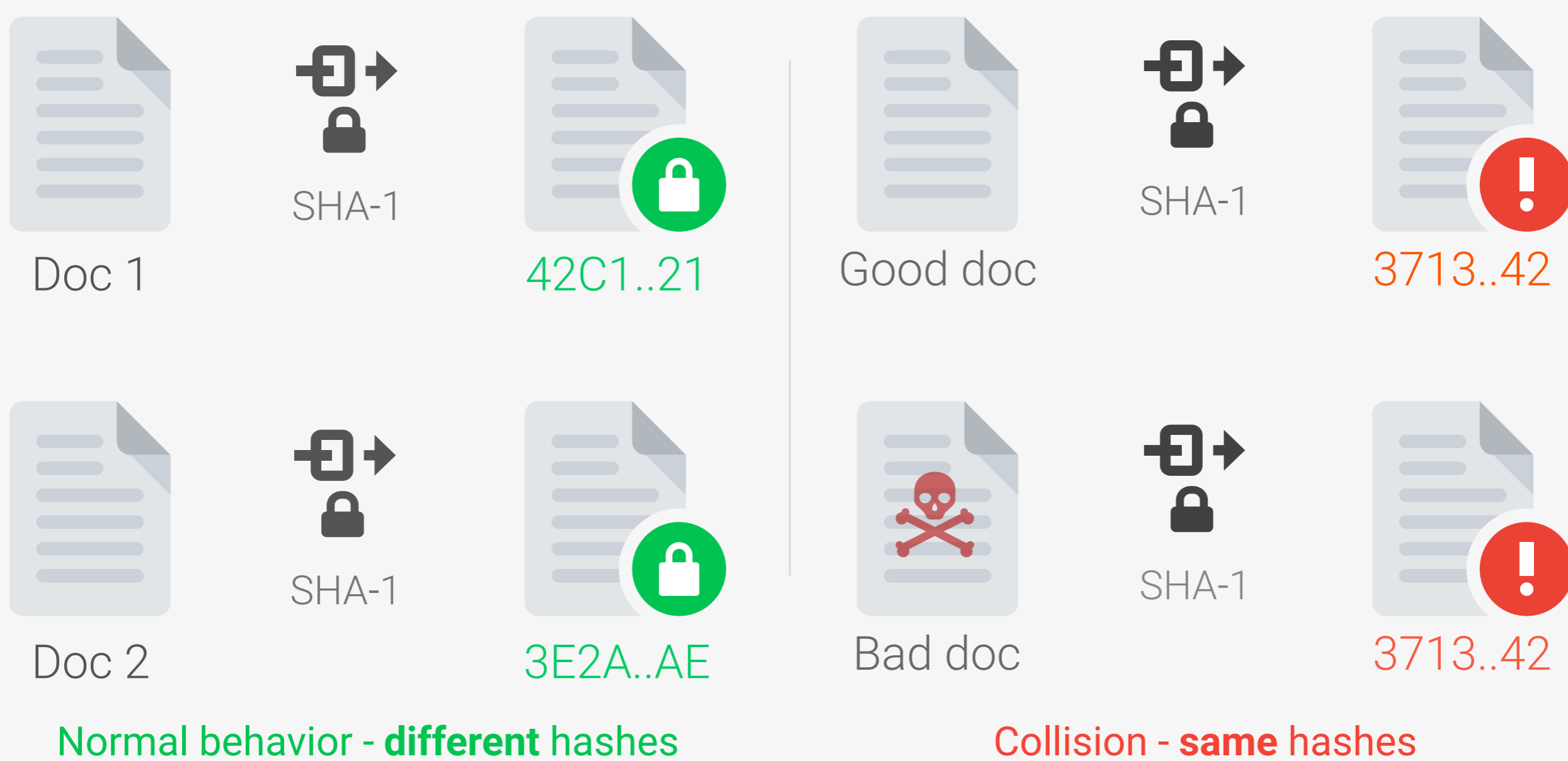


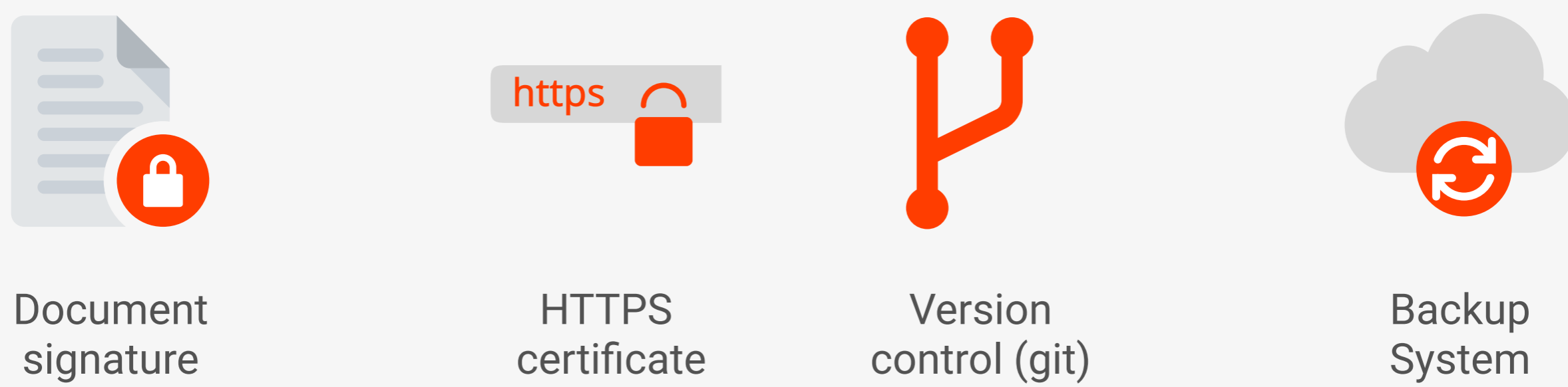
# SHattered

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

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



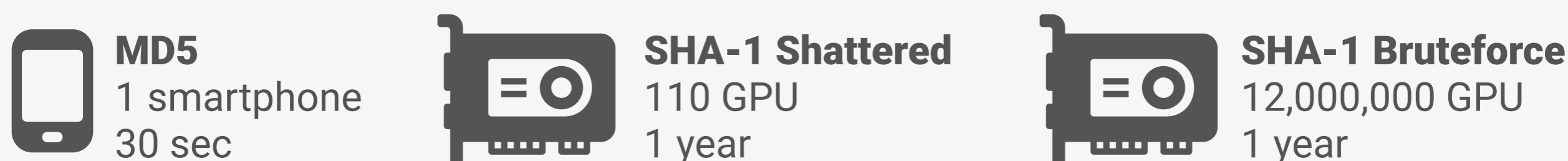
## Potentially Impacted Systems



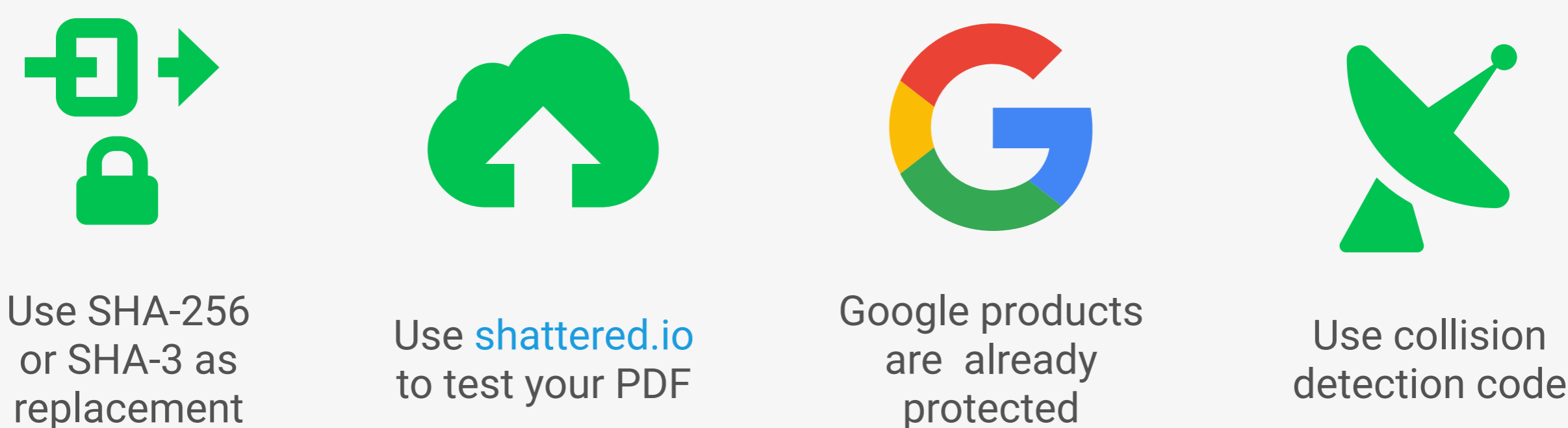
## Attack complexity

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

## Shattered compared to other collision attacks



## Defense



## Team

CWI

Marc Stevens  
Pierre Karpman

Google

Elie Bursztein  
Ange Albertini  
Yarik Markov

learn more at <https://shattered.io>