Crypto wars: Revenge Of The Sith or A New Hope?

2016-05-22 – **Hétpecsét Szakmai fórum**

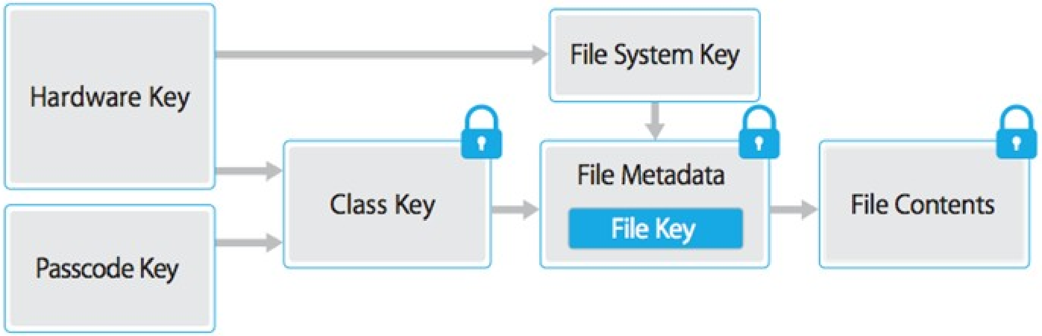
tresorit

Szilveszter Szebeni
CIO

Content

- Why the FBI ~~cannot~~ could not access an iPhone 5c?
- History, some similar stories.
- Two sides to the story.

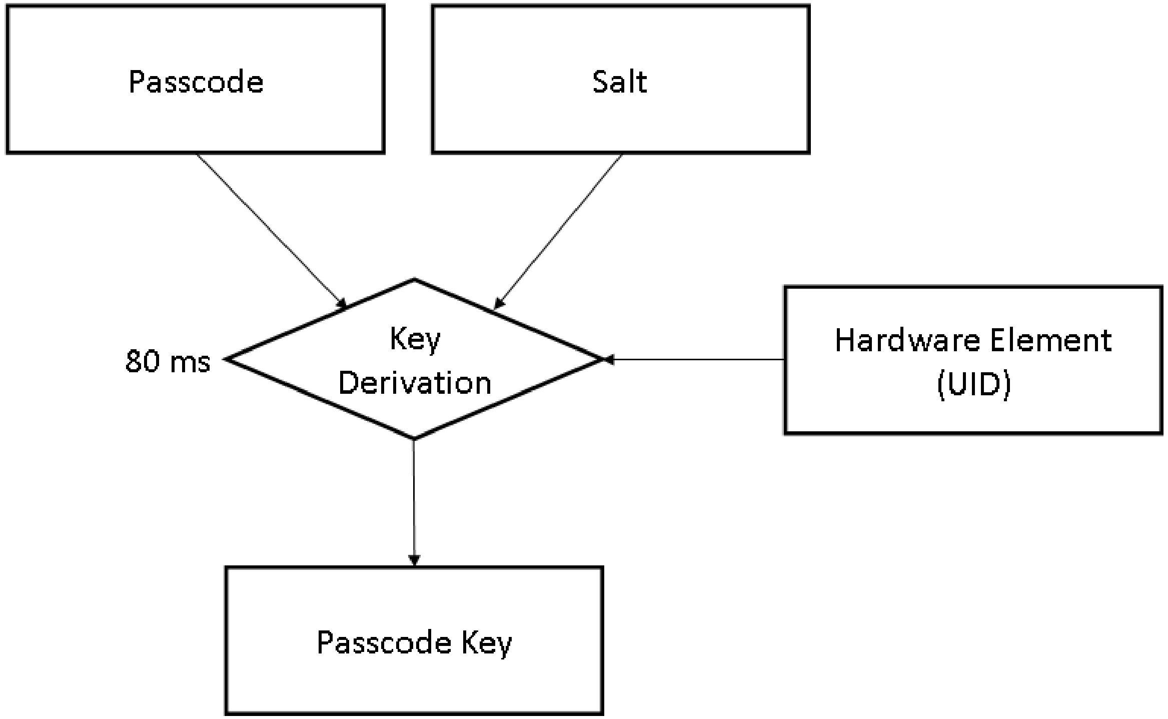
iOS - File Data Protection



Source: https://www.apple.com/business/docs/iOS_Security_Guide.pdf

tresorit

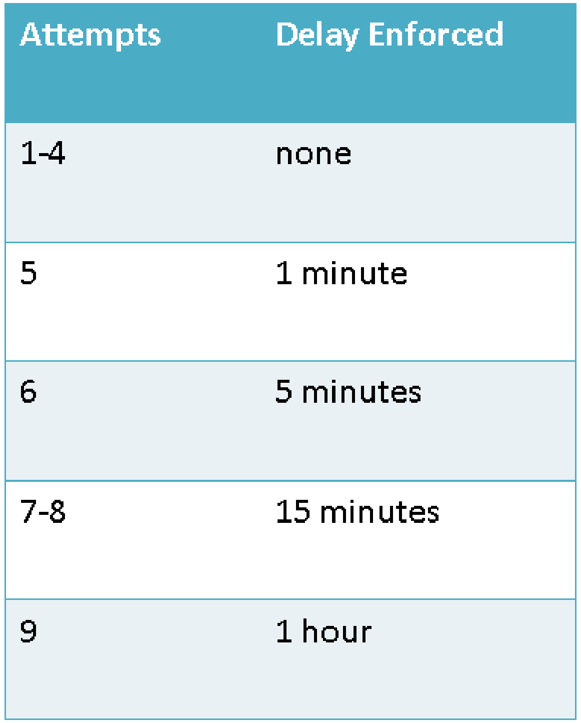
iOS Passcode key



Passcode	Brute Force Time
4 numbers	13 sec
6 numbers	22 hours
10 numbers	9259 days
6 alphanum	2015 days

tresorit

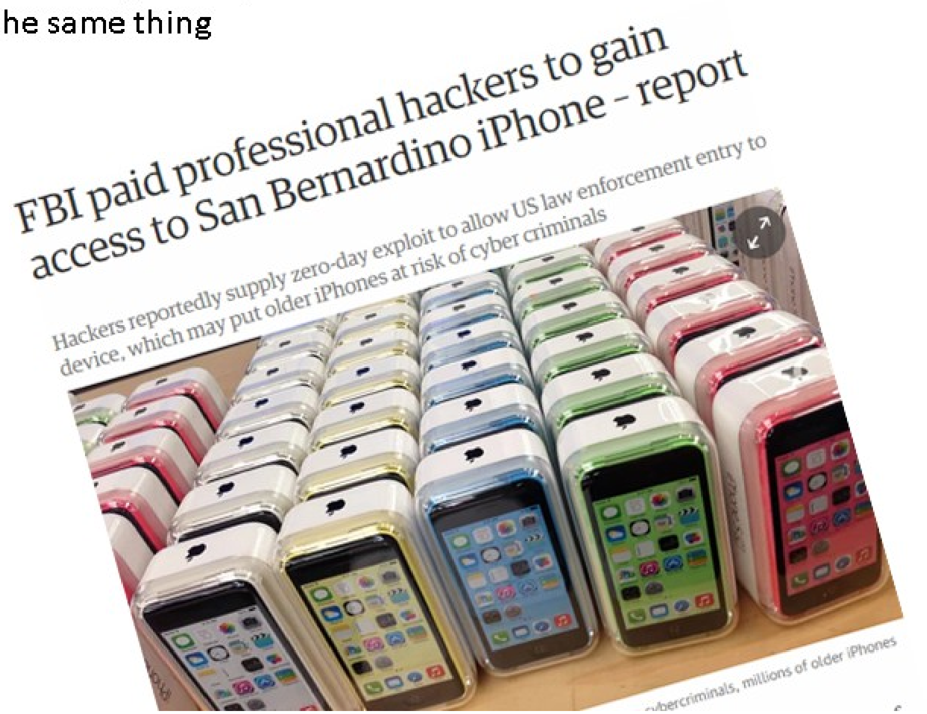
Software delays



Attempts	Delay Enforced
1-4	none
5	1 minute
6	5 minutes
7-8	15 minutes
9	1 hour

How to hack the iPhone

- Convince Apple to send a SW update to the phone
  - No software delays for passcode tries
  - Automatic brute forcing of the passcode
- Find a 0-day to do the same thing



FBI paid professional hackers to gain access to San Bernardino iPhone - report

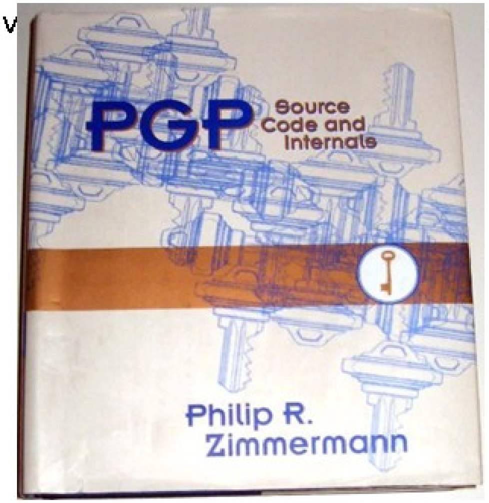
Hackers reportedly supply zero-day exploit to allow US law enforcement entry to device, which may put older iPhones at risk of cyber criminals

ybercriminals, millions of older iPhones

History

History - PGP

- 1991 Pretty Good Privacy (PGP) published by Zimmermann
  - United States Customs Service started a criminal investigation for violating the Arms Export Control Act
  - 1996 Case is dropped
- 1996 Encryption removed from Munition List.
- 2000 U.S. Gov on export of cryptogr



WARNING
This shirt is classified as a munition and may not be exported from the United States, or shown to a foreign national
RSA
encryption in perl

History – Clipper Chip 1993-1996

- Clipper Chip Encryption device with a built-in backdoor
- Compulsory for US phone manufacturers
- Backlash
  - Algorithm Secret
  - Non-US manufacturers cannot be forced to comply
  - Fear of illegal surveillance

tresorit

History – Bullrun

- Weak random number generator Dual_EC_DRBG (2007)
- RSA Security $10 million in a secret deal to use it.
- 2013 Snowden leak
- Exact technical details are not known.

Two sides to the story

Two sides of the story

- Should we make impenetrable black boxes?
- “Everyone would be walking around with a Swiss bank account in their pocket.
- We make privacy/security tradeoffs all the time.
- Why should your data be considered different?

- If there exists some master key to break encryption you are considerably weakening it.
- Which government should own the front door?
- Encryption systems are easy to create, even if illegal criminals will have access to them.

Questions?

tresorit