How secure boot outlocks Free Software

Rüdiger Weis

OpenTechSummit 2015

Rivest on TPM: You may not trust

Ron Rivest, 2002:

"The right way to look at this is you are putting a virtual set-top box inside your PC. You are essentially renting out part of your PC to people you may not trust."

Microsoft has allready deactivated UEFI-Secure-Boot-Modules

December 2013

Microsoft Security Advisory 2871690:

- 9 UEFI-Secure-Boot-Modules **stopped booting**

Windows 10: Lock In

MUST have TPM and Secure boot

"OPTIONAL": Switch off Secure Boot

MUST NOT switch off on smart phones and tablets

shim Hack

Fragile Trust Chain

booting? SingedByMicrosoft(.) **AND** SignedByUbuntu(.)

Cryptographic Problems

- Standard mistakes for standard documents
- Insufficient security parameters
- Cryptographic mistakes
- Security problems because of integration
- Key generation problem
- ...

Insufficient Security Parameters

- Standard mistaks for standard documents
  SHOULD versus MUST, use of MAY, ...

  Trusted Platform Module Library, Part 1: Architecture, March 15, 2013 , p. 37:

  > *"A TPM should implement an approved hash algorithm that has approximately the same security strength as its strongest asymmetric algorithm.*
  > *NOTE The TCG may create sets of algorithms that do not have the same security strength for the hash and asymmetric algorithms."*

- RSA 2048 bit not enough
- SHA1 still allowed
- ...

Still allowed: SHA1

- Look back:
  - CCC Datenschleuder, März 2005:
  - http://www.cryptolabs.org/hash/WeisCccDsHash05.html
- **Practical Attacks**

Integration of TPM

Integration of TPM functions in not secured hardware chips makes hacking easier.

Key Question Key Control

- "(The Microsoft approach) lends itself to market domination, lock out, and not really owning your own computer."

Whitfield Diffie, 2003:

"To risk sloganeering,
I say you need to hold the keys to your own computer"

Requirements

- Eckpunktepapier der Bundesregierung
  - Opt-In
  - Opt-Out
  - ...
- State-of-the-art Cryptography
- Privacy friendly Cryptography (DAA, PFS,...)
- International control and certification of the TPM manufacturing process
- Publication and certification of the secure boot code
- Anti trust evaluation of Microsoft
- ...

HowManyMillionBIOSWouldYouLikeToInfect$_{Full}$.pdf

Lighteater

- Corey Kallenberg and Xeno Kovah:
- "How many million BIOSes would you like to infect?"
- CanSecWest Vancouver 2015

"2 guys + 4 weeks + 2k$ =

Multiple vendors' BIOSes infected, with multiple infection capabilities"

- Acer
- Asus
- Dell
- Gigabyte
- HP
- Lenovo
- ...

Skynet (is) for WIMPs

- System Management Modus (SMM)
- Intels Active Management Technology (Intel AMT)
- Intels Serial-Over-LAN

Code has agency

Bruce Schneier, 5. September 2013

Remember this:

- The math is good, but math has no agency.
- Code has agency, and the code has been subverted.