Can Crypto Hardware be Trustworthy?

Benedikt Stockebrand
Stepladder IT Training+Consulting GmbH

November 2014

Part I

The Current Situation

So-called “IT Security”

So-called “IT Security”

- Do we have to prove IT systems to be insecure?

So-called “IT Security”

- Do we have to prove IT systems to be insecure?
- . . . or should the vendor demonstrate their security instead?

So-called “IT Security”

- Do we have to prove IT systems to be insecure?
- . . . or should the vendor demonstrate their security instead?
- For more on this:
  `http://www.youtube.com/watch?v=7bTaKSZQKhc`

"Secure Hardware" I

- What do names like
  - Trusted Computing Platform Alliance (TCPA)
  - Trusted Computing Group (TCG)
  - Trusted Platform Module (TPM)
  - Secure Boot
  - . . .

  try to insinuate?

“Secure Hardware” II

- Do we blindly want to trust all the
    - manufacturers
    - component suppliers
    - logistics operators
    - distributors
    - customs authorities
    - investigative authorities
    - so-called “intelligence” agencies
    - standard issuing authorities
    - . . . and whoever else

  involved?

“Tamper Protection”?

“Tamper Protection”?

In some cases, this is

“Tamper Protection”?

In some cases, this is

- unnecessary

“Tamper Protection”?

In some cases, this is

- unnecessary
- exceedingly difficult

“Tamper Protection”?

In some cases, this is

- unnecessary
- exceedingly difficult
- or a convenient excuse to peddle snake oil.

Auditability I

- Can I audit a TPM module or the crypto features of a CPU. . .
- . . . without destroying it?
- . . . with affordable and available tools?
- . . . with available know-how?
- . . . and with a reasonable amount of effort?

Auditability II

- Is auditability possible?

Auditability II

- Is auditability possible?
- Not with attackers, who
  - have unlimited resources
  - have unlimited technical skills
  - have unlimited insider knowledge
  - have unlimited political and judicial backing
  - nonchalantly ignore applicable laws
  - have support from the manufacturers
  - don’t make mistakes

Auditability II

- Is auditability possible?
- Not with attackers, who
  - have unlimited resources
  - have unlimited technical skills
  - have unlimited insider knowledge
  - have unlimited political and judicial backing
  - nonchalantly ignore applicable laws
  - have support from the manufacturers
  - don't make mistakes
- But we can and should raise the bar for real world attackers

Risk Assessment of Attacks

- Rational vs. irrational motivation
- Extent of access
- Risk of discovery
- Personal risk for attacker
- Scope, or targeted vs. blanket attack

Attack Types

- Passive snooping
- Active manipulation/injection of fake data

Attack Types

- Passive snooping
- Active manipulation/injection of fake data
- Installation of backdoors in operational devices

Attack Types

- Passive snooping
- Active manipulation/injection of fake data
- Installation of backdoors in operational devices
- Replacement of operational devices

Attack Types

- Passive snooping
- Active manipulation/injection of fake data
- Installation of backdoors in operational devices
- Replacement of operational devices
- Targeted distribution of manipulated devices

Attack Types

- Passive snooping
- Active manipulation/injection of fake data
- Installation of backdoors in operational devices
- Replacement of operational devices
- Targeted distribution of manipulated devices
- Manipulation of entire product series or product families

Attack Types

- Passive snooping
- Active manipulation/injection of fake data
- Installation of backdoors in operational devices
- Replacement of operational devices
- Targeted distribution of manipulated devices
- Manipulation of entire product series or product families
- Manipulation of standards and specifications

Attack Types

- Passive snooping
- Active manipulation/injection of fake data
- Installation of backdoors in operational devices
- Replacement of operational devices
- Targeted distribution of manipulated devices
- Manipulation of entire product series or product families
- Manipulation of standards and specifications
- Attacks at the political level

Defense Strategies I

- Technical
- Economic
- Political

Defense Strategies II

- Restore the burden of proof
- Restore vendor liability
- Diversity
- Auditability

Part II

Current Projects

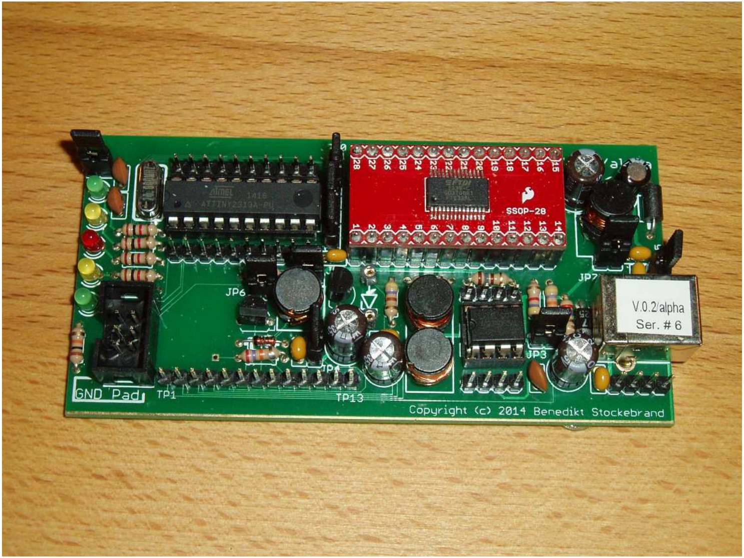
The Cryptech Project

- Complete crypto chip (HSM, hardware security module)
- FPGA based (with an option to go ASIC later on)
- Includes
  - Hardware random number generator (HWRNG)
  - Cryptographically secure pseudo random number generator (CSPRNG)
  - Cryptographic checksums/hashes
  - Encryption/decryption
  - Key store
- Fully open design
- Designed for auditability

My ARRGH Project I

- Auditable Real Random Number Generator Hardware
- Hardware random number generator (HWRNG) only
- No need for tamper protection
- DIY oriented
- No need for FPGA
- Intended to support various microcontrollers

My ARRGH Project II



Part III

Surprises

FIPS 140 I

- Full title: “Security Requirements for Cryptographic Modules”
- Published by NIST
- Compliance mandatory for various uses
- Contains requirements for random number generator tests

FIPS 140 I

- Full title: “Security Requirements for Cryptographic Modules”
- Published by NIST
- Compliance mandatory for various uses
- Contains requirements for random number generator tests

- No explanation on the tests defined were given

FIPS 140 II

- Test blocks of 20 000 bits for “randomness”
- Blocks “insufficiently random” are silently discarded. . .

FIPS 140 II

- Test blocks of 20 000 bits for "randomness"
- Blocks "insufficiently random" are silently discarded...
- ... which happens with ca. 0.8% of truly random blocks...

FIPS 140 II

- Test blocks of 20 000 bits for “randomness”
- Blocks “insufficiently random” are silently discarded. . .
- . . . which happens with ca. 0.8% of truly random blocks. . .
- . . . which itself introduces significant bias. . .

FIPS 140 II

- Test blocks of 20 000 bits for “randomness”
- Blocks “insufficiently random” are silently discarded. . .
- . . . which happens with ca. 0.8% of truly random blocks. . .
- . . . which itself introduces significant bias. . .
- . . . in what is used as seed for CSPRNGs.

FIPS 140 III

- In FIPS 140-2 these tests were removed again. . .

FIPS 140 III

- In FIPS 140-2 these tests were removed again. . .
- . . . and again without explanation.

FIPS 140 IV

- Why did the test names (monobit, poker, runs, long run) sound familiar?

FIPS 140 IV

- Why did the test names (monobit, poker, runs, long run) sound familiar?

  Donald E. Knuth,
  The Art of Computer Programming
  Volume 2: Seminumerical Algorithms
  Second Edition 1981 (First Edition 1969)

FIPS 140 IV

- Why did the test names (monobit, poker, runs, long run) sound familiar?

  Donald E. Knuth,
  The Art of Computer Programming
  Volume 2: Seminumerical Algorithms
  Second Edition 1981 (First Edition 1969)

- . . . which covers

FIPS 140 IV

- Why did the test names (monobit, poker, runs, long run) sound familiar?

  Donald E. Knuth,
  The Art of Computer Programming
  Volume 2: Seminumerical Algorithms
  Second Edition 1981 (First Edition 1969)

- . . . which covers
  - generic (non-crypto)

FIPS 140 IV

- Why did the test names (monobit, poker, runs, long run) sound familiar?

  Donald E. Knuth,
  The Art of Computer Programming
  Volume 2: Seminumerical Algorithms
  Second Edition 1981 (First Edition 1969)

- . . . which covers
  - generic (non-crypto)
  - pseudo random number generators
- . . . rather than crypto grade true random number generators

FIPS 140 V

- Would open source help?

FIPS 140 V

- Would open source help?
- The Linux `rngtools` (`rngd`, `rngtest`) implement FIPS 140

FIPS 140 V

- Would open source help?
- The Linux `rngtools` (`rngd`, `rngtest`) implement FIPS 140
- So open source alone is obviously not enough

The FTDIgate Stunt

- September 29 FTDI released an updated driver for their FT232 UART↔USB chip family...

The FTDIgate Stunt

- September 29 FTDI released an updated driver for their FT232 UART↔USB chip family...
- ... which effectively bricked fake chips

The FTDIgate Stunt

- September 29 FTDI released an updated driver for their FT232 UART↔USB chip family...
- ... which effectively bricked fake chips
- ... and which was then distributed through Windows Update from October 14

The FTDIgate Stunt

- September 29 FTDI released an updated driver for their FT232 UART↔USB chip family. . .
- . . . which effectively bricked fake chips
- . . . and which was then distributed through Windows Update from October 14
- . . . which effectively bricked even more fake chips

The FTDIgate Stunt

- September 29 FTDI released an updated driver for their FT232 UART↔USB chip family. . .
- . . . which effectively bricked fake chips
- . . . and which was then distributed through Windows Update from October 14
- . . . which effectively bricked even more fake chips
- . . . and all without any physical access.

Part IV

References

Ressourcen

The Limits of Cryptography
EasterHegg 2014, Stuttgart
`http://www.youtube.com/watch?v=7bTaKSZQKhc`

BIVBlog: Benedikt's IT Video Blog
`http://www.stepladder-it.com/bivblog/`
Video-Blogs rund um IT im allgemeinen und Crypto-Hardware (und IPv6) im speziellen

The Cryptech Project
`https://cryptech.is/`

Contact Information

Stepladder IT
Training+Consulting GmbH
Benedikt Stockebrand

Fichardstr. 38
D-60322 Frankfurt/Main

`contact@stepladder-it.com`

Web pages:
`http://www.stepladder-it.com/`
`http://www.benedikt-stockebrand.de/`

Video Blog:
`http://www.stepladder-it.com/bivblog/`