Trusted Computing

Juliet Uhlott and Hau-Wen Chang

Clarifying Misinformation on TCPA
Dave Safford
Trusted Computing
Wikipedia
Outline

• Some Notes
• Ross Anderson’s TCPA FAQ
• Lucky Green Defcon Presentation
• Bill Arbaugh’s Comment
• Summary
Some Notes

- David Stafford’s rebuttal to Trusted Computing FAQ by Ross Anderson is based on version 1.0, which has been updated as version 1.1 now.
- TCPA is now the Trusted Computing Group (TCG)
- Palladium is now called Next Generation Secure Computing Base (NGSCB)
- The Fritz which is the core of trusted computing is called Trusted Platform Module (TPM) now.
Q: What does TCPA / Palladium do, in ordinary English?

A: "The obvious application is digital rights management (DRM)". "Palladium ... will build on the TCPA hardware".

– The DRM problem is done by Palladium not TCPA.
– The Goal of TCPA is to secure user’s private keys, and their encrypted data against viruses or other attacks.
– The original motivation
Q: How does it work?

A: "When you boot up your PC, Fritz [the TCPA chip] takes charge. He checks that the boot ROM is as expected, executes it, measures the state of the machine; then checks the first part of the operating system, loads and executes it,..."

  – The TCPA chip doesn’t execute anything.
  – It accepts request data, and replies with response data.
The initial version of TC had Fritz supervising the boot process.
- PC ended up in a predictable state, with known hardware and software.

The current version has Fritz as a passive monitoring component that stores the hash of the machine state on start-up.
- End up in the approved state, cryptographic keys can be released to decrypt TC applications and data.
- Ends up in the wrong state, the hash will be wrong and Fritz won't release the right key.
… "Fritz checks that the hardware components are on the TCPA approved list, that the software components have been signed, and that none of them has a serial number that has been revoked."

– None of this exists anywhere in the TCPA specifications, or shipping product.

– These things could theoretically be done on any operating system.
Ross Anderson’s TCPA FAQ (Cont.)

• The operating system security kernel bridges the gap between the Fritz chip and the application security components. It checks
  – Hardware components are on the TCG approved list.
  – Software components have been signed.
  – None of them has a serial number that has been revoked.
Ross Anderson’s TCPA FAQ (Cont.)

- Q: **Can't TCPA be broken?**
- A: "The early versions will be vulnerable to anyone with the tools and patience to crack the hardware...from phase 2, the Fritz chip will disappear inside the main processor."
  - Reading the bus to the TCPA chip cannot reveal a private key.
  - TCPA was designed to protect the user’s data from external attack, not from attack by the owner.
• Q: *But isn't PC security a good thing?*
• A: "... about virus... but neither TCPA nor Palladium will fix that: viruses exploit the way software applications use scripting."
  – TCPA cannot prevent stupidity in software applications.
  – Viruses that try to gain access to your sensitive data can be detected and blocked by TCPA, by its refusing to unseal sensitive keys in the compromised environment.
  – Spam? Privacy?
Q: Scary stuff. But can't you just turn it off?

A: "… you can’t turn Fritz off … booting in untrusted mode, he still checks that the operating system isn’t on the serial number revocation list."

– There is no "serial number revocation list“. It could be done, with or without TCPA.

If you turn TC off, Fritz won't hand out the keys you need to decrypt your files and run your bank account. Your TC-enabled apps won't work as well.
Ross Anderson’s TCPA FAQ (Cont.)

- Q: Ugh. What else?
- A: "TCPA will undermine the General Public License (GPL)... It will not make full use of the TCPA features unless you have a certificate for it that is specific to the Fritz chip on your own machine."
  
  – They are working on releasing TCPA code for Linux under the GPL.
  
  – There is no such thing as TCPA certification of code.
Lucky Green’s Defcon Presentation

• "TCPA’s Business Objectives:" are to "Prevent use of unlicensed software:“, and "Digital Rights Management".
  – The main goals are to secure the user’s private keys and encrypted data against external software attack.
Lucky Green’s Defcon Presentation (Cont.)

- "[TCPA] chip: tamper resistant, surface mounted".
- "TCP OS Boot Process" diagram contains the constructs "Approved Hardware List", "Serial Number Revocation List", and "OS binary decrypt"
- "Palladium is a TCPA Operating System".
- "GPL... source alone is worthless without a TPM-specific certificate."
Bill Arbaugh’s Comment

• "Both [integrity protection and trusted storage] use trusted root certificates as this basis [of their security guarantees.]
  – The only time a certificate is needed is if you want to be able to prove to a third party that you have an approved TCPA chip.
  – The best defense for privacy conscious users is simply to turn off the endorsement key."
Bill’s 5 specific suggestions

- "Allow owners to load their own trusted root certificates."
- "Allow the TPM to be completely disabled."
- "Allow for complete privacy."
- "Work with the open source community"
- "Hold a technical workshop"
Summary

• The Author tries to defense that TCPA is mere a platform which provides security functions and protects private key.

• It shouldn’t be responsible for the applications build on it, especially for the controversial Palladium and DRM.