University of Nijmegen

Can you trust your trusted computing platform?

Jaap-Henk Hoepman
Security of Systems (SoS) group
Department of Computer Science
University of Nijmegen, the Netherlands
jhh@cs.kun.nl
www.cs.kun.nl/~jhh

Outline

- TCPA functions
- The risks of TCPA
  - *Freedom*
  - *Privacy*
- What causes those risks?
- A better TCPA

Main TCPA functions

- **Public key functions**
  - *Generation, sign/verify, encrypt/decrypt*
- **Trusted boot functions**
  - *Store system state in PCR*
  - *Seal data under PCR*
- **Remote attestation**
  - *Prove system state to third party*

University of Nijmegen

TCPA vs Smart Card

- Similar functions
  - *Cryptography*
  - *Sealed storage*
- Similar functionality
  - *Protect data*
  - ***Enforce third party policies***

University of Nijmegen

TCPA PC vs standard PC (1)

- **TCPA**
  - *Applications can check system state*
    - may refuse to run
    - may restrict functionality
  - *Other systems can check system state*
    - may refuse connection
    - may conceal data
- **Standard**
  - *Applications unaware of state*
    - can run on modified OS
    - reverse engineering
  - *Other systems unaware of state*
    - all systems equally (un)trusted

University of Nijmegen

TCPA PC vs standard PC (2)

- Distinction is fuzzy….
  - *M$ could do most TCPA stuff in software too*
- … but TCPA much harder to circumvent
  - *if it really requires hardware hacks ;-)*
- TCPA does not specify any policies itself…
  - *It's up to M$ and others to define them!*

University of Nijmegen

TCPA & DRM policies

- **Multimedia**
  - *play only (no save/ no copy) music*
  - *refuse to play illegal music*
- **Documents**
  - *restrict distribution*
  - *delete old documents*
  - *cancel email*
  - *censor documents*

TCPA & Freedom

- Owner no longer controls PC
- Restrict use of certain software
  - *Apps may refuse to run*
  - *Third parties may refuse connection*
- Threat to open source (GPL)
  - *source may get hijacked*

University of Nijmegen

TCPA & Privacy

- No control over PC
  - *implies less trust in PC*
- Remote attestation
  - *Pseudonymous*
  - *Traceable*

University of Nijmegen

TCPA & Economics

- **Normal situation**

- **With TCPA**
  - *There may be no procedure to convert*
  - *Third party policies may prevent conversion*

University of Nijmegen

User advantages?

Not that many…
So, can't we ignore it?

- ➔ **Yes, some…**
  - ◆ *Stop malicious code*
    - ■ **Virusses, trojan horses, worms**
  - ◆ *Authentication*

University of Nijmegen

Problem: Lock-in

Trusted TCPA users

$0.50 each song

itunes

$1 each song

Non TCPA users / untrusted users

Source of the problem

- TCPA
  - *Complete disable not possible*
- Privacy
  - *Not completely guaranteed*
- Remote attestation
  - *Enforced through “lock-in”*
- Economics of IT

University of Nijmegen

Possible solutions

- Trusted root certificates
  - *Allow users to change them*
- Privacy
  - *Allow truly anonymous, unlinkable certificates*
- Remote attestation
  - *Remove it!*
    - **but this requires “external” forces…**

Conclusions

- TCPA poses serious freedom/privacy threats
- It also provides user benefits
- Freedom of choice diminishing…