Trusted Computing for Trusted Infrastructure

Andrew Martin

Oxford ICT Forum Conference
Wednesday 15th July 2009
Trusted Computing entails a small change in PC platform design giving rise to significant and useful capabilities for application-level security and stronger network access control. Computers incorporating the Trusted Platform Module are now widely available and deployed - but few TPMs are turned on. In this talk, we give an overview of the ideas of Trusted Computing, we survey the products coming to the market, and we describe the research being done in Oxford in designing Trusted Grid and Cloud services.
MSc in Software and Systems Security

- Oxford University MSc by part-time study
- Week-long modules throughout the year: enrol in any term
- Computing Lab and ContEd
- No exams! Take-home assignments and project
- Wide selection of modules

- Does your employer believe in education?
- Substantial cost: half-price for University and College employees.
  - Numbers may be limited in each year.
What is Trusted Computing?

- TPM
- TCPA
- TCG
- NGSCB
- Palladium
- Intel TXT
- AMD Presidio
- MTM
- TrustZone
- Opal disk
- Bitlocker
- Trusted Network Connect
Shall I Trust this host?
Shall I Trust this host?

- Which host is it?
- What software is it running?
- Who says so?
- Who delivered it?
- Who made it?
- Who maintains it?
- Is it patched?
- Does it have a rootkit?
- Is there a BIOS virus?

Steps to trust

It is safe to trust something when:

1. it can be unambiguously identified, and
2. it operates unhindered, and
3. the user has first-hand experience of consistent, good, behaviour or the user trusts someone who vouches for consistent, good, behaviour.

Graeme Proudler, HP Labs
Building a record of platform state

- hardware is relatively hard to subvert:
  - make the most of this
- use cryptography for platform identity
- use cryptographic hash as a measurement of components
- two main elements:
  - new Trusted Platform Module to manage secure storage
  - changed boot chain to capture measurements during boot (alternative is late launch).
Building a record of platform state

- concept is to have each component in the chain be *measured* by the preceding one.
Using measurements

Report your configuration to a third party (with a cryptographic signature)

- report configuration to the desktop user?

‘Seal’ data: encrypt it, and have the TPM release the decryption key only when the platform is in the right state

- e.g. Microsoft BitLocker

(in mobile phone) abort the boot if the measurement gives the wrong answer
Is Trusted Computing Evil?

Ross Anderson seems to think so.

Richard Stallman seems to think so.

I don’t think so.

- and as a result, so do lots of open source enthusiasts
- many of the myths around it are false
- but clearly, it has good and bad uses.

Not wanting to put words in people’s mouths: *evil* is rather strong. They might, rather have said something like *unwelcome.*
1. let me in!

2. who are you?

3. cryptographic challenge response protocol

4. and what OS are you running? antivirus? patch level?

5. Ubuntu, Apache, ...

6. prove it!
TNC and NAC, NAP, ...

Open standard
OS-neutral
“Everyone” involved: except Cisco.
F-TNC for eduroam
TCG Trusted Storage: concept

- Host
- TPM
- Trusted storage device
- Interface
- Encrypted data
- Data
- Authenticate
TCG Full Disk Encryption

Fast disk disposal/repurposing

Protect data against computer theft

Independent of operating system

Lock individual drives to particular machines

makes a hard drive useless to a drive thief

Effectively extends TPM’s protection from a handful of registers to a large data store
TCG: Standards for Trusted Computing

Mobile Phones

Authentication

Applications
- Software Stack
  - Operating Systems
  - Web Services
  - Authentication
  - Data Protection

Network Security

Privacy & Access

Virtualized Platform

Desktops & Notebooks

Security Hardware

Servers

Storage

Printers & Hardcopy

Infrastructure
Employ *Trusted virtualization* to deliver assured execution of Grid jobs (Condor etc.)

Scale this up to build trusted grids, trusted clouds

- strong guarantee that this web service does what it says on the tin

- trial deployments of TNC
- coupled with virtualization
- trusted virtual domains
- mobile trusted applications

Interested to explore
Conclusion

TC is here, and is going to keep getting more significant

• it’s a genuine “game changer”

It begins to affect many aspects of systems design and management

• should make life better :-)

It’s not evil :-) but it’s not a magic bullet either.

• majority of TC software right now is open source, for example.

MSc module on the subject, 19th-23rd October 2009

• can be taken on a stand-alone basis, as well.
SOFTWARE ENGINEERING PROGRAMME
SOFTWARE AND SYSTEMS SECURITY

Andrew Martin, MA, DPhil, MBCS, CEng, CITP
Deputy Director, Software Engineering Programme

Wolfson Building, Parks Road, Oxford OX1 3QD, UK.
+44 (0) 1865 283605
Andrew.Martin@comlab.ox.ac.uk
www.softeng.ox.ac.uk/andrew.martin