

SOFTWARE ENGINEERING PROGRAMME
SOFTWARE AND SYSTEMS SECURITY

COMPUTING LABORATORY



Trusted Computing for Trusted Infrastructure

Andrew Martin

Oxford ICT Forum Conference
Wednesday 15th July 2009

Summary

MSc in Software and Systems Security

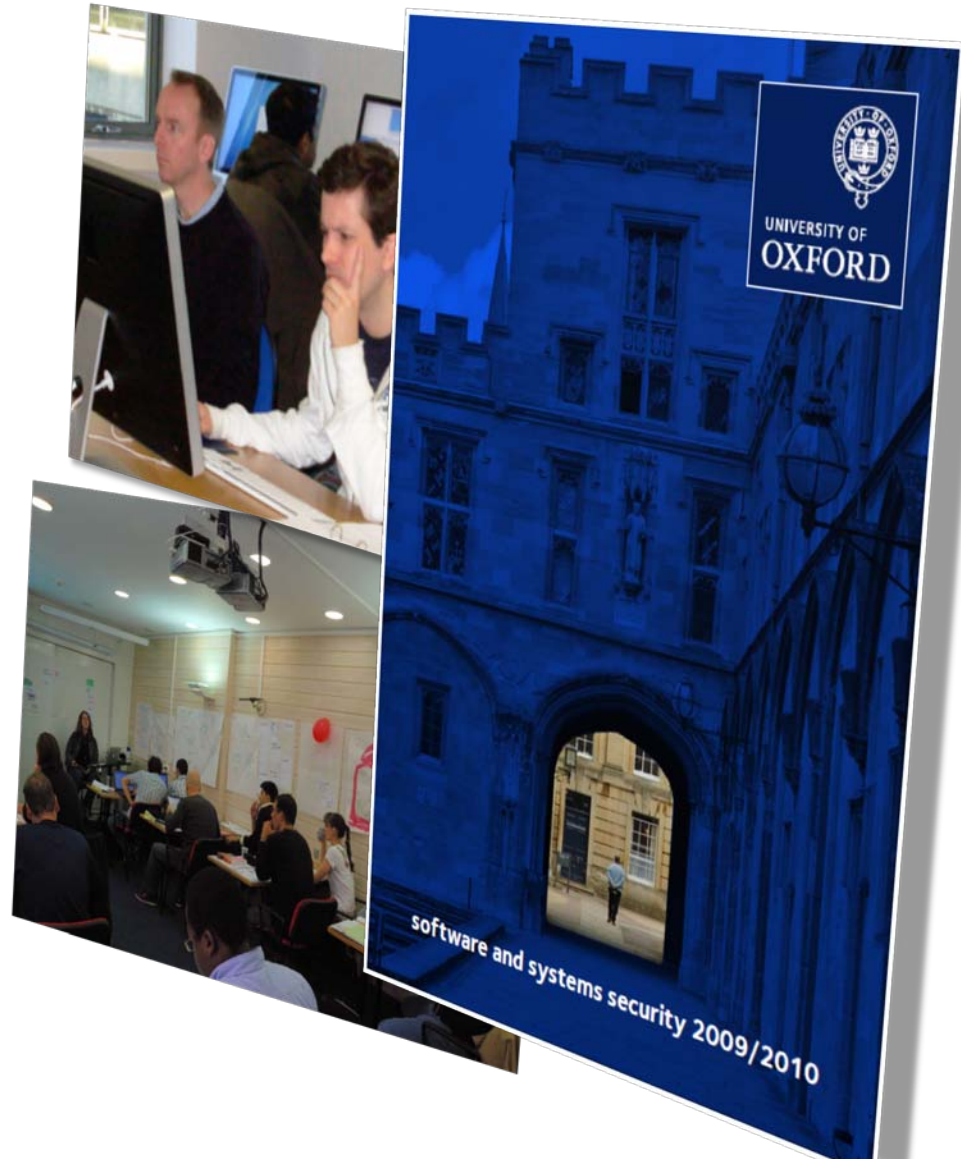
Trusted Computing

Trusted Infrastructure

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



Trusted Computing

Safer Computing

Intel TXT

AMD Presidio

MTM

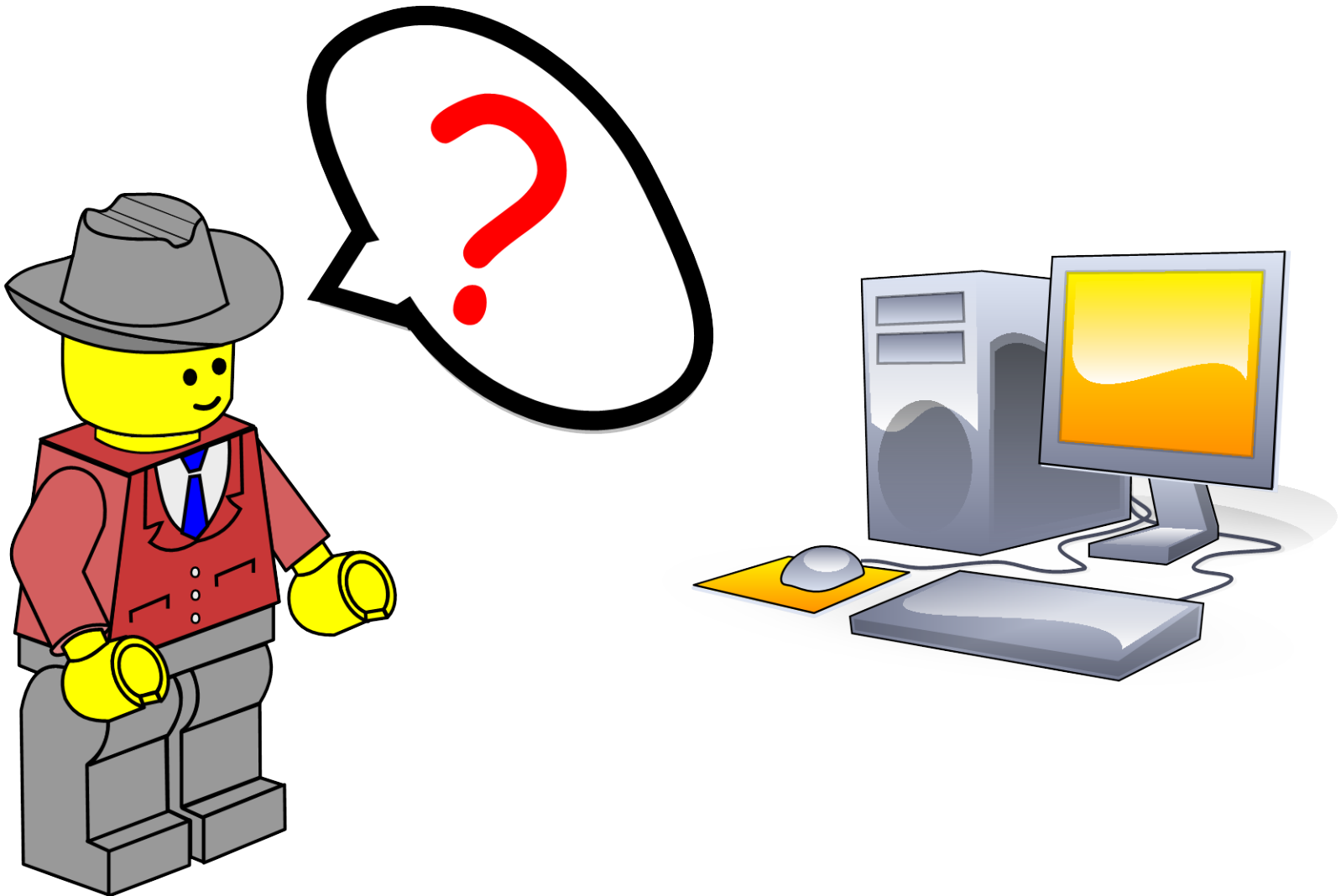
TrustZone

Opal disk

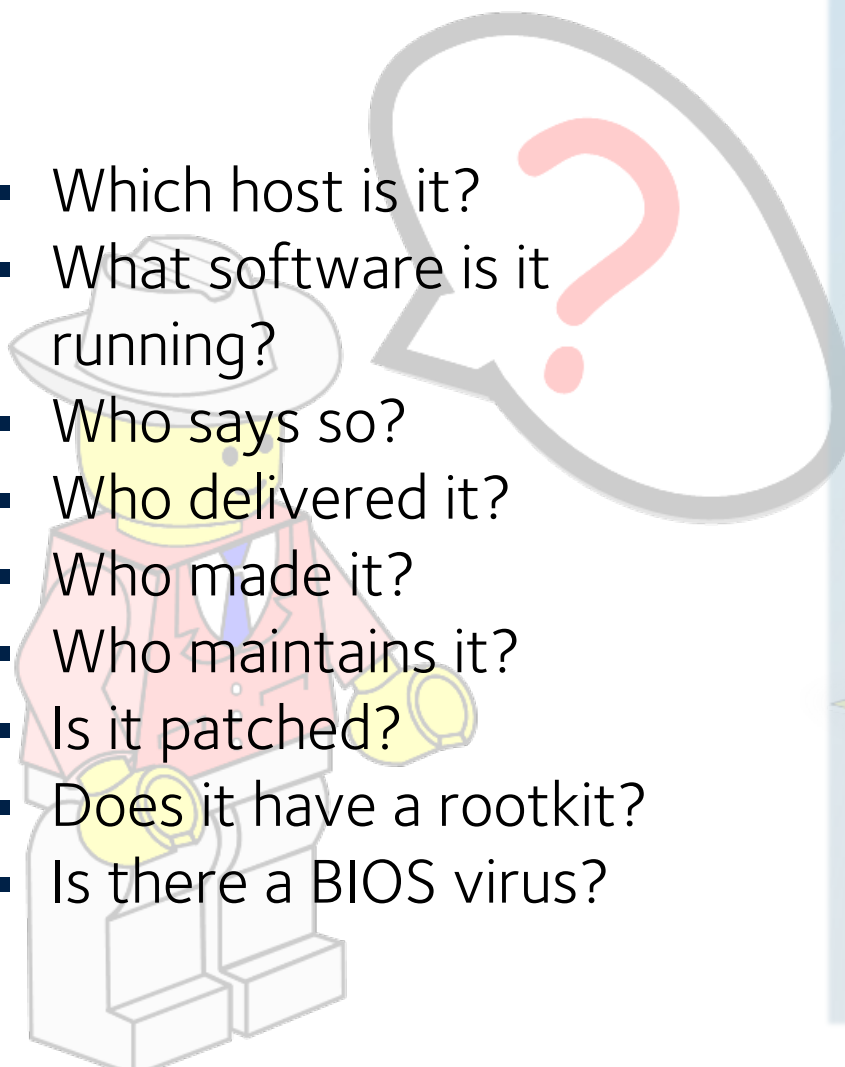
Bitlocker

Trusted
Network
Connect

Shall I Trust this host?

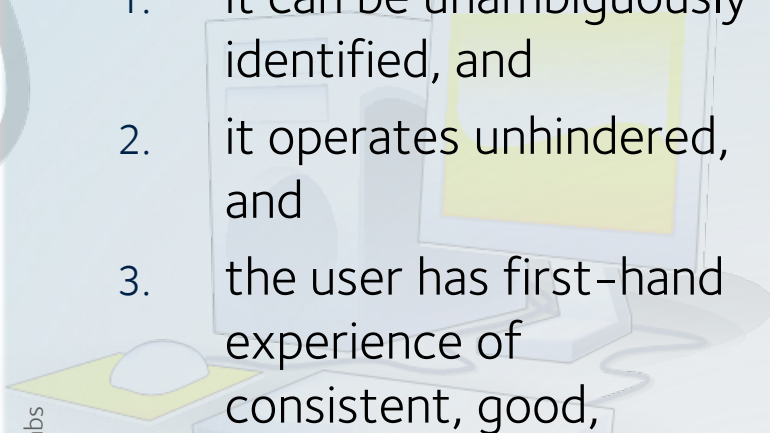


Shall I Trust this host?

- 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.
- 

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*).

application
software

middleware

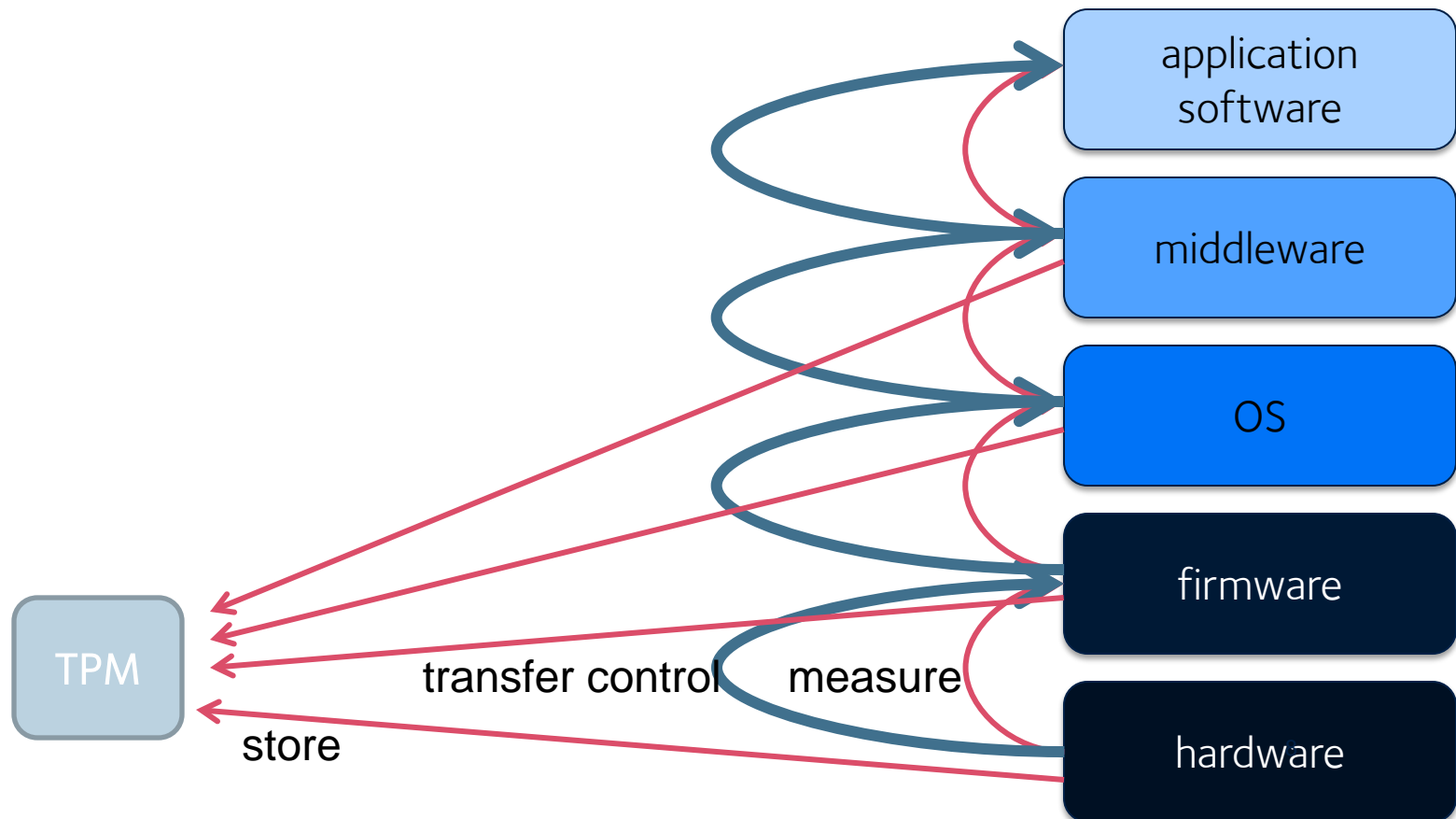
OS

firmware

hardware

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.

- and as a result, so do lots of open source enthusiasts

I don't think so.

- 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*.

Trusted Network Connect Concept

1. let me in!

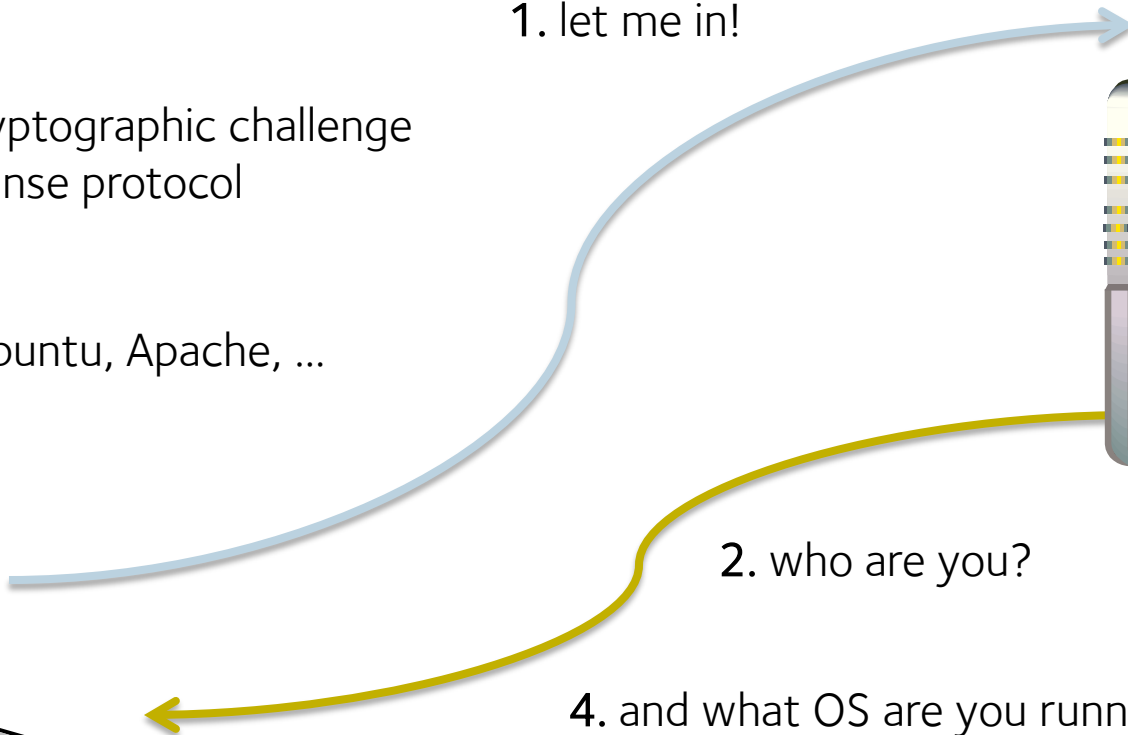
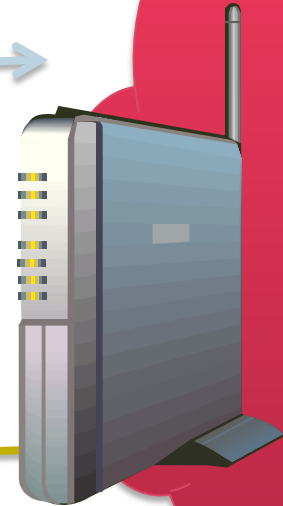
3. cryptographic challenge
response protocol

5. Ubuntu, Apache, ...

2. who are you?

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

6. prove it!



TNC and NAC, NAP, ...

TRUSTED
COMPUTING GROUP™

日本語

Certification

Resources

Join Now

Member Login

Trusted Computing

Solutions

Developers

Community

Media

Network Security Products Based on Trusted Network Connect Standards Test Interoperability And New Capabilities

Date Published: April 6, 2009

Network Security Products Based on Trusted Network Connect Standards Test Interoperability And New Capabilities

TNC Implementers Demonstrate Interoperability to Protect Network Health

PORTLAND, Ore., April 6, 2009 – Fifteen companies and organizations from around the world participated in testing a growing number of implementations of the Trusted Computing Group's Trusted Network Connect (TNC) specifications for network security and network access control.

Enterasys Networks, Fujitsu Limited, Great Bay Software, Infoblox, Juniper Networks, Lumeta Corporation, Trapeze Networks and several others participated in the group's fourth annual interoperability event, hosted by the University of New Hampshire Interoperability Laboratory (UNH-IOL). First-time attendees included Great Bay and Lumeta, while Enterasys, Juniper, and Trapeze Networks tested products for at least their third year.

Microsoft's implementation of NAP (Network Access Protection) in Windows XP SP 3 software was tested as working interoperably at the event as well.

The Trusted Computing Group (TCG) hosts the interoperability session to enable member companies to test implementations with TNC-based products from other vendors. The session provides interoperability in addition to providing discussion and sharing of best

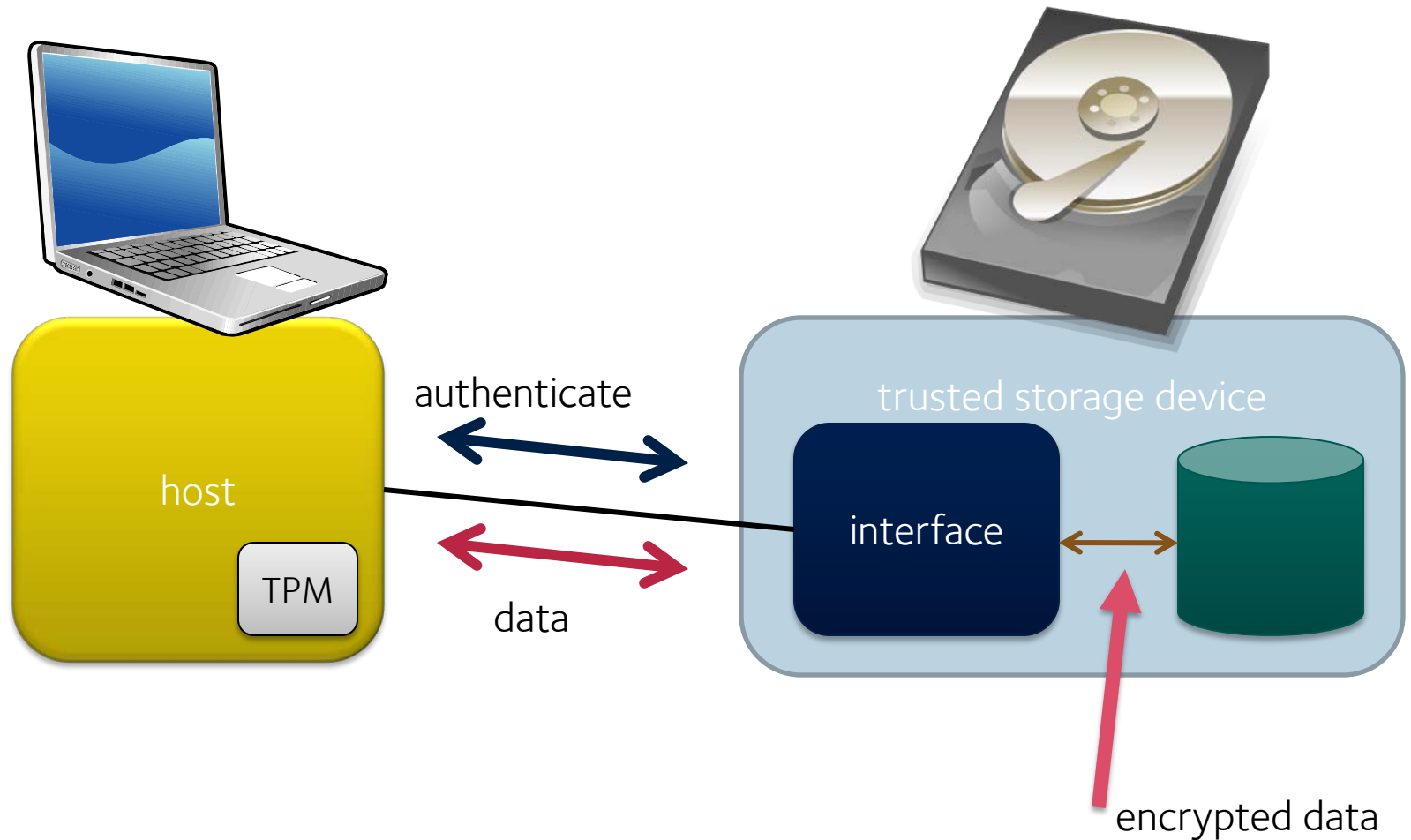
Open standard

OS-neutral

“Everyone”
involved: except
Cisco.

F-TNC for
eduroam

TCG Trusted Storage: concept



TCG Full Disk Encryption

Fast disk disposal/repurposing

Protect data against computer theft

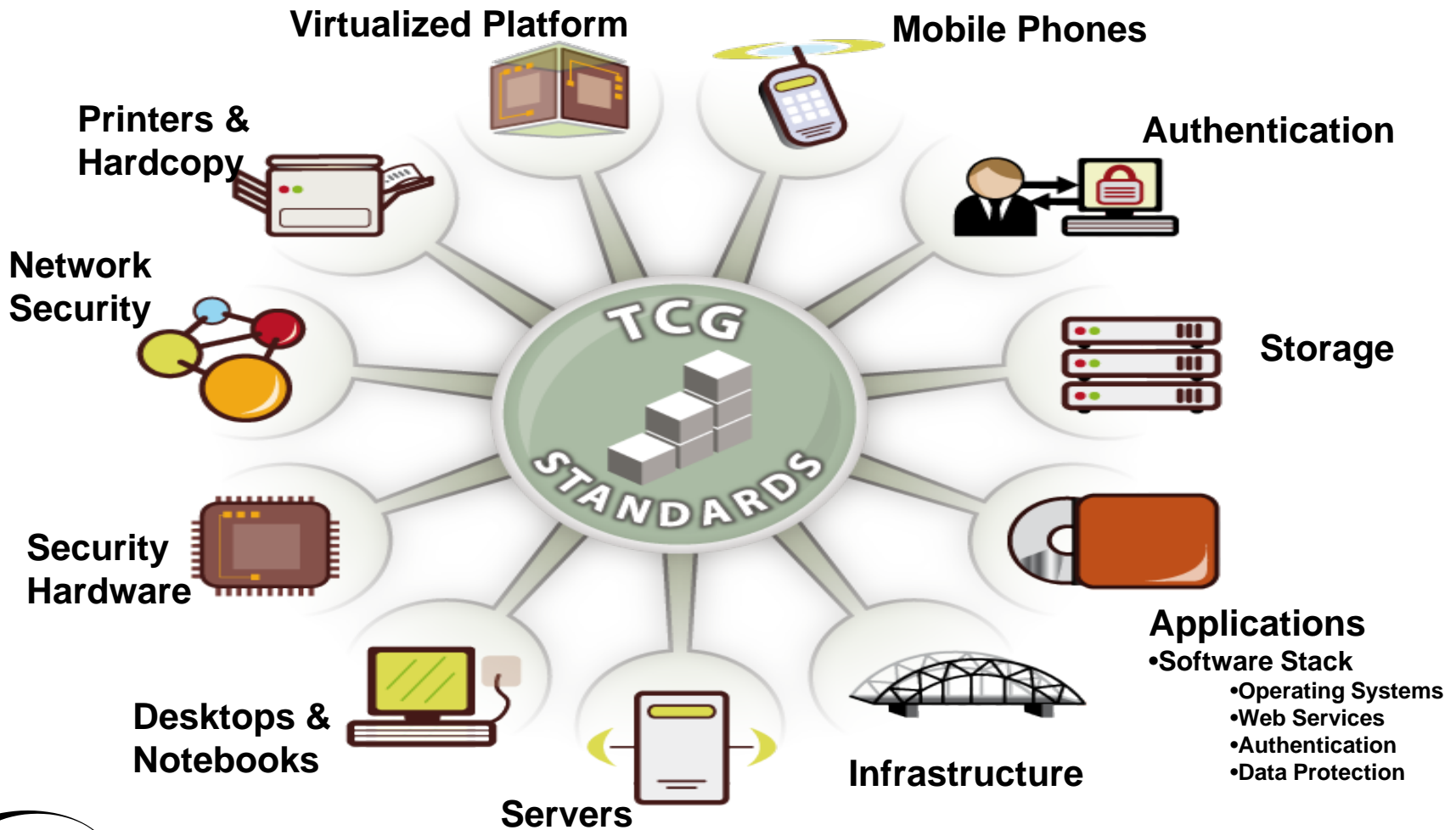
Independent of operating system

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



Research in Oxford

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

Scale this up to build trusted grids, trusted clouds

Trusted services,
trusted compilation

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

Interested to
explore

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

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