

Cyber Security

Knowledge Transfer Network

Knowledge Transfer Networks
A DTI business support solution
Delivered through the Technology Programme



TRUSTED COMPUTING SPECIAL INTEREST GROUP WHITE PAPER

You Mean You Trust a Computer?

Preface

Consider these two statements:

When you leave home, if you are the last person to leave, you probably follow a routine, like millions of others: checking the taps are off, the windows closed, and perhaps locked, the alarm is set, the doors are locked and that you have your money, credit cards, keys safely on your person.

When you get to work, you turn on your computer and start work, safe in the knowledge that the information on your computer, such as the online banking access, your personal details, and who was the last person to change the machine are secure.

Trusted Computing technology provides a firm foundation for engendering trust and security in computer systems

The first statement is common practice, and you can be even insured against loss, the second can be said to be true for very few people unless you carry your computer continually, and this means everywhere. In the past a computer where the configuration and usage can be implicitly trusted has been limited to bespoke military or critical infrastructure systems, now with new computers compliant with the Trusted Computer Group (TCG) [1] concept of Trusted Computing it is possible that more and more people can trust their computer, and perhaps in the near future be insured against the loss.

Introduction

We are now beginning to see the increasing availability of compliant Trusted Computer Group hardware and software technology in mainstream computing platforms. From a technical perspective, TCG technology provides a firm foundation for trust and security at the platform level; a trusted core which can be utilized to bootstrap trust and security in applications and services. In parallel we are witnessing significant industry momentum behind machine virtualization technology both in software and hardware, so that an application can run independent of the characteristics of its host. Together these technology paradigms promise significant potential for the delivery of Trusted Computing. However, in order for users to benefit from the promises of Trusted Computing they need to have appropriate access to services and applications. There remains a significant gap between the technology and standards development currently being witnessed and exploitable business models necessary for successful technology insertion. In order to benefit from Trusted Computing we need to understand what the potential uses and applications might be and the possible barriers to uptake (legal, social, procedural and technological), otherwise we may miss key requirements essential to successful delivery but not currently being addressed by the community.

The Trusted Computing Special Interest Group (SIG) was set up in an attempt to meet this challenge. The aim of the group has been to identify potential channels for the technology across a range of sectors; examine the possible business models and use cases; consider barriers and catalysts for building trust in the technologies; identify any significant gaps hindering the adoption of the emerging Trusted Computing technology and develop a strategy for accelerating adoption of Trusted Computing in appropriate environments.

The purpose of this white paper is to report on the findings, observations and recommendations of the Trusted Computing SIG. The paper is structured as follows: We start with an overview of the information security threat landscape as a means of establishing a context for the role of Trusted Computing technology. We then provide a brief introduction to Trusted Computing technology itself and explain at a high level its role in addressing some of the more serious issues existing or beginning to appear on the information security threat landscape. Trusted Computing technology is in a formative state; we provide a survey of this state including current and near term products and solutions, market penetration and market maturity. Following this introduction to Trusted Computing we look at some representative yet concrete examples of the business value that the use of Trusted Computing technology can bring, aiming to bring alive the clear benefits of the technology. Despite the clear benefits and the widespread availability of the core Trusted Computing technology components, the uptake of Trusted Computing has been slow. Trusted Computing technology cannot exist in isolation; it needs to be surrounded by an ecosystem encompassing infrastructural, social and educational aspects amongst others. We take time to describe the core aspects of a Trusted Computing ecosystem so as to develop a broader view on Trusted Computing that allows us to fully analyze why Trusted Computing uptake has so far been slow. With that in mind, the final and key section of this report presents what we feel are the major contributing factors to the slow uptake of Trusted Computing and our recommendations on how to improve this situation.

Despite the availability of Trusted Computing technology components uptake so far has been slow and general awareness of Trusted Computing is poor

The Information Security Threat Landscape

In this section we describe the current and evolving security threat landscape as motivating context for the introduction of TC technology. We introduce trust and confidence in the underlying IT systems as a key requirement in being able to capitalize on the next generation 'electronic business' opportunities.

More and more of our daily personal and working lives make use of personal computing platforms of one form or another and rely on the convenience afforded by interaction with online or electronic IT services and applications. Un-surprisingly the

More and more of our daily personal and working lives rely on computer systems of one form or another

number and variety of attacks against both personal home and business IT systems are increasing. Viruses and Trojan horses are well known threats; Identity theft and phishing and pharming attacks are becoming increasingly common. As the range, functionality and complexity of software systems grows to meet the appetite for online services, the potential for attacks rises accordingly. Simultaneously, with an increasing number of both personal and business financial transactions being carried out electronically and with the value of assets stored and accessed electronically rising we are beginning to see a more focused organized crime approach to attacking IT systems.

The number and variety of attacks against both personal home and business computer systems are increasing

Point security products exist but without a strong foundation of key security primitives the solutions are often lacking or not complete. For example, one of the significant and growing threats exploited by hackers nowadays is physical access to the computer. This has been illustrated numerous times by the stealing of laptops from governmental organizations and important companies, leading to considerable loss both in terms of money and privacy. Multi-factor authentication, such as the use of smartcards, improves the protection against such threats, but do not provide a solution in all situations. Full-disk encryption provides another level of protection, but key management then becomes a critical problem. Furthermore, the ability to bypass software (either because of vulnerabilities or of poor configuration) by modifying the hardware platform leads to attacks that cannot be countered by traditional security methods. This is also a category of attacks that is commonly found in mobile platforms, e.g. modification of the IMEI (International Mobile Equipment Identifier) number.

Trust is a big factor in driving businesses forward

Trust, more generally, is one big factor that will drive future businesses forward. The way we see future business processes requires technologies with adequate security infrastructure to provide for competitive advantage. People no more have trust on either the state or businesses to protect their data or preserve their rights to privacy. Therefore being trusted will become the key differentiator between the “haves” and the “have-nots” of business clientele base. If business IT security systems cannot fully authenticate and protect users, then they would take their business elsewhere. Consumer privacy needs to be respected and increasingly, businesses are using proven track record in security as their selling point in promoting services.

Trust is also a big issue in identity management, authentication and federation. Even with two or three factor authentication, where users are judged by what they know such as a password, what they have such as token or smartcard, and even what they are physically like by use of a biometric; federating ID relies so much on trust during initial registration, which if compromised will allow both the internal and external systems to be vulnerable. Although strong trusted authentication technology has been around for many years, it has not been very visible

and uptake has proven expensive, thus slowing uptake further. User monitoring is another big issue which consumers are finding very difficult to cope with, i.e. "the big brother syndrome". The technology for pervasive and/or invasive computing must be implemented in such a way as to not compromise trust. Companies need to reinforce individual's privacy such that trust in the technology should not be lost and only those who provide anonymity to users would be tomorrow's winners.

Trusted Computing Technology Overview

The ability to protect the integrity of a computer system through software alone is limited. This is because most operating systems cannot prevent unauthorized software from loading, before the operating system itself loads. Once unauthorized software has loaded it can cause problems for the user, the network and 3rd party clients. To counter this threat, the PC needs a basis of trust based in the hardware platform which cannot be changed by software. Trusted Computing is designed to make a trusted subsystem just as much a standard part of the PC platform as memory or graphics are today. Through a TCG compliant subsystem, core elements of trust are integrated into the platform.¹

These elements extend trust to the PC's BIOS, which extends its trust to the OS loader, which extends its trust to the OS, which in turn can extend its trust to applications. In this way, the TCG subsystem provides the foundation for a fully trusted PC platform and a foundation for IT managers to extend trusted computing across systems and networks for multiple users. The trusted system maintains authenticity, integrity, and privacy, while maintaining the freedom of choice that is central to the PC usage model.

Once a trusted secure environment has been defined the next issue is often how to operate with insecure applications or connections. A solution is to provide an isolated environment for such software, a virtual "sandbox". The provision of a virtual machine environment using virtualization software on a trusted computing host is an ideal solution. Transactions can be performed without affecting the underlying integrity of the client or host. Virtualization make software easier to migrate, thus aiding application and system mobility, thin client environments can be deployed on an as used basis rather than having to be configured for every different user. In addition it provides the

The TCG (Trusted Computing Group) have defined core platform elements to bootstrap trust and security in a platform

A combination of TCG technology and Virtualization is the key to providing usable and practical Trusted Computing platforms

¹ The Trusted Platform Module (TPM) is one of the TCG core elements of Trust. This small hardware chip is physically and permanently bound to the computing platform motherboard. It has 3 main functions: to act as a safe (immune from operating system and other software attacks) storage area for cryptographic secrets held on the platform, to provide un-forgable identities and to report on integrity measurements of software components on the platform

potential to run legacy software which cannot be rewritten to comply with TCG requirements.

In the future it is planned that mobile devices will also include trusted environment. Such concepts are have been developed by the TCG [2] and others such as IBM, Intel and NTT DoCoMo [3]. The underlying concept is the same for PCs. As mobile phones, PDAs and other devices become more open software platforms then attacks on the software content for profit or simple malice will increase. Only by the implementation of TC security can the balance of openness and integrity be maintained. A trusted mobile platform would allow the user to perform sensitive transactions over a wireless link and ensure only content or software which is trustworthy is loaded onto the mobile. In turn the rights of the network operator or in the case of a private business phone, the IT administrator, can be ensured and the integrity of data maintained should the device be lost, stolen and maltreated.

A key point to be made is that Trusted Computing technology in itself does not solve all computing trust and security problems. However, Trusted Computing technology does provide a firm foundation for identifying the components that are being trusted or relied on as part of any electronic interaction and also providing a robust measure of the integrity of those components. This is a critical first step that allows us to start providing more trustworthy and secure computing systems that users can have confidence in.

In the order of 100 million TPMs will expected to ship in 2007

Survey of the market for Trusted Computing

Trusted Computing technology has relevance across a number of market segments including Server and PC's, Mobile Phone, Consumer Electronics, Public Safety and Road Vehicles. Each of these market application areas has strong Trust and security requirements.

In the general PC and server space Trusted Computing technology has clear relevance, primarily around the protection against software attacks. Trusted Computing technology has an important part to play in the embedded market too. In 2005 the mobile phone market reached 2 billion units. A large number of these units are 'Smart Phone' type devices. With increasingly rich and complex functionality the software stacks on these mobile devices will require protection against software attacks just as in as general purpose PC's. The consumer electronics market also has strong trust and security requirements driven from both the connection of devices to the open Internet through to providing devices with sufficient protection mechanisms such that they can be considered such vehicles for the delivery of high value digital content. In the public sector initiatives such as the NHS electronic patient

health records and the proposed National Identity Register for ID cards include a duty of care over the management of the database systems where trust is absolute and key to public safety and life dependant services. Finally, as a market example the automotive industry is beginning to require strong trust and security mechanisms as more and more of the safety critical control systems within a car are implemented by software components running on embedded computers. Integrity of the software components is obviously a key requirement here as is the ability to perform trustworthy and secure updates and upgrade of software components.

Figure 1 below shows the expected sales figures for the TPM chip itself (source IDC) through to 2010. These figures largely reflect PC based shipments; the expectation is that embedded shipments of TPM technology will follow similar trends.

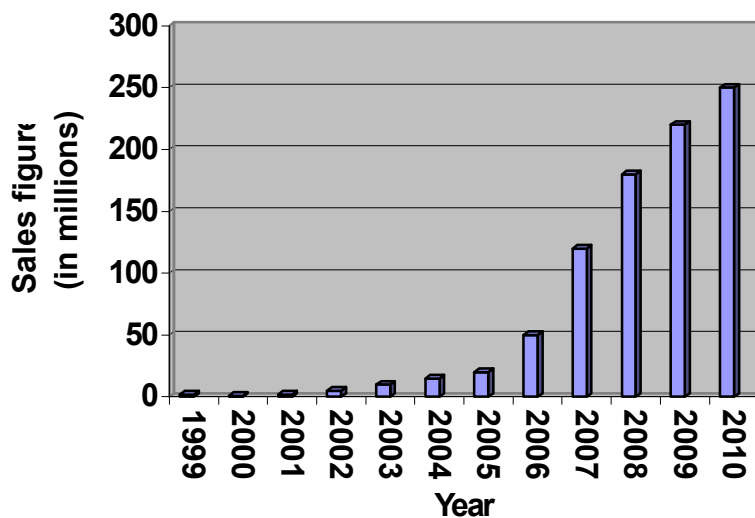


Figure 1: TPM sales evolution 1999-2010 (source IDC)

Current Trusted Computing based solutions

Whilst uptake of Trusted Computing technology has been slow, support for Trusted Computing group technology can now be found in mainstream operating systems such as Microsoft Vista [4] and Linux [5]. The Trusted Computing Group maintains a fairly comprehensive database of Trusted Computing technology related products [6].

Both Linux and Microsoft Vista now feature operating system support for Trusted Computing

Applications and Business drivers of Trusted Computing Technology

In this section we give examples of realistic and grounded examples of the use of TC technology to give the reader a view on some of the of the potential advantages of using Trusted Computing Group (TCG)'s Trusted Platform Modules (TPM) as an enabler for secure applications or services.

TPM's to enable secure end-to-end VPN solutions A complete VPN solution must have endpoint integrity mechanisms as one of its components, and there is nothing better than TPM enabled platforms to provide this mechanism. TCG's Trusted Network Connect (TNC) architecture enables the network operators to implement a secure end-to-end VPN solution by enforcing policies regarding endpoint integrity at or after network connections.

TPM's to provide multi-factor authentication and device protection Factors like 'something you know', 'something you have' and 'something you are' are used in combination to provide strong authentication. These can be used to authenticate access to your corporate network, your laptop or even your bank online. By using TPM enabled devices, users can achieve a simple two-factor authentication by combining something they know (a password) and something they have (TPM) to get access to services.

The need to secure corporate machines/laptops from theft and malicious attacks has increased dramatically over the past few years and TPM enhance the securing of platforms from these threats. By the utilization of TPM's one can achieve strong authentication support (access controls) and strong cryptographic support (Confidentiality and Integrity) for device protection against a whole range of threats.

TPM's to support Identity Management Solutions Platforms with a TPM can implement a secure and more reliable Identity Management Infrastructure. For BT, an identity enabled device using TPMs means a trusted container that can be used to deliver many secure and reliable services to the customers. BT, HP and Intel demonstrated "Provisioning of secure credentials to the consumer" using Liberty Alliance standards and Trusted Platform Modules at RSA Conference 2007, USA [7]. It is interesting to note also that Mobile operators are starting to embed SIM cards in laptops at about the same time as TPMs are becoming embedded in laptops. It could potentially be cost-effective to combine these elements rather than duplicating costs. A wide variety of wireless networks are now appearing (WLAN, WiMax, Wibro), and it seems unrealistic to require SIM cards to access all of them. However alternative secure solutions (e.g. based on TPM Trusted Network Connect or secure provisioning of temporary credentials) are becoming available.

Secure Online Banking The personal electronic transaction (PET) prototype demonstrator built as part of the Open Trusted Computing [8] uses Trusted Computing TPM technology in combination with virtualization technology to produce a system capable of securing a user's online banking transactions when carried out from their personal computer (PC). The user's PC runs a couple of virtual machines. One virtual machine runs a general purpose operating system such as Microsoft Windows or Linux. The user makes use of this for the majority of their work and it is known as the un-trusted compartment. A second virtual machine runs a cut-down operating system and simply a web browser as the only application. This is known as the trusted compartment. A mechanism is provided to allow a user to determine whether they are interacting with the trusted or un-trusted compartment. When wishing to interact with their bank's online service, the user switches to the trusted compartment and invokes the web browser (or client banking application). The remote banking service performs a remote TPM based system verification of the software integrity of the user's trusted compartment to make sure that the software in that compartment as is expected, i.e. no Trojan software has been injected for example. The verification also includes making sure that the virtualization layer being run by the user is considered sufficient to provide the isolation guarantees between the two compartments on the system so that the bank doesn't have to worry about what is running in the other (un-trusted) compartment on the system.

Mobile Phone Protection One example of the application of Trusted Computing technologies in the mobile platform will be the protection of the IMEI number. An unchangeable IMEI is important for constructing a robust blacklist of stolen phones; such a blacklist can ensure that a phone becomes unusable if it is stolen. This application is deemed critical for the protection of the mobile business model and of basic properties of the mobile platform. The ability of a TPM to provide safe storage of secrets on a platform, its ability to provide un-forgable platform identities and its platform integrity measurement and reporting capability make it a suitable base for the implementation of an unchangeable IMEI on a mobile platform.

The Trusted Computing Ecosystem

In this section we introduce the broader Trusted Computing Ecosystem that needs to fit in around the basic TC technology components including infrastructural (such as PKIs, etc), social and educational aspects.

The technology defined by the TCG and its implementation by TCG members and others is only one element of a broader range of new solutions that define Trusted Computing at large.



Trusted Computing
like any technology
needs an ecosystem

TPM chips and TSS² software are complemented by other elements like platform hardening (e.g. Intel Trusted Execution Technology or AMD-V) and virtualization technologies. Such platform hardening provides the means, for example to control low-level insecure accesses like DMA (Direct Memory Access) to a virtualization layer. The virtualization layer implements policy decision and enforcement to Operating Systems executing on top of it. The TPM is used to enable an authenticated boot routine where each software component that is started during the boot process is measured and measurements are stored securely inside the TPM, and to seal cryptographic keys (such as the one used for full-disk encryption) that are then protected in hardware inside the TPM. The new hardware platforms also implement a Dynamic Root of Trust for Measurement (DRTM) which can be used to start virtualization software in a trustworthy manner at an arbitrary point in time, thus removing the need for a complex authenticated boot.

In such an environment, all the various elements are equally contributing to the trustworthiness of the platform. Platform hardening limits the low-level functionalities and gives control to a virtualization layer. The virtualization layer is a small piece of software than can be thoroughly tested and verified in order to gain strong confidence of its robustness. The virtualization software can then be trusted to implement the security policy on the Operating Systems it executes. The TCG elements (TPM, TSS, TNC[1]) are functioning in parallel to these elements and provide the skeleton on which trust in the system is based.

At an even higher level, socio-psychological aspects of Trusted Computing play an important role in the public perception of the technology. The belief that Trusted Computing is an improvement is tied to both the trust in the TCG, the perception driven through the general press and direct experience with the current technology. While direct experience is still sparse due the youth of the technology and press coverage is still weak, the perception of the TCG by the general public is an important factor that the main TCG members are trying to address. The general fear about Trusted Computing is one aspect of a more global suspicion about control technologies helping solve security problems. These emotional aspects are difficult to correct, as usually people stick to their first impression. In this matter, education should contribute to correct perceptions of a threatening technology.

Legal problems are also bound to arise, for example between certification and open-source software, or DRM systems and fair usage policies. Some of these problems already have. Even in the open-source community, visions are split apart, for

² The TPM Software Stack (TSS) is the software layer that sits above the TPM hardware module and allows communication between the TPM and the platform operating system and applications.

example between Richard Stallman's (the originator of GNU and the GPL) GPL version 3 imposing limits on DRM and constraints on revealing cryptographic keys, and Linus Torvalds (the originator of Linux) viewpoint that technologies should not be limited in this way.

Main Observations on the slowness of Trusted Computing Uptake

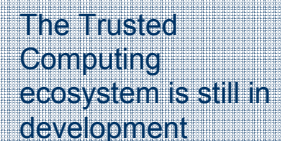
In this section we document our observations on why we feel TC uptake has been slow including identification of gaps in the broader space TC ecosystem.

TC technology is permeating by default (in the order of 100 million TPMs are expected to ship in 2007). As outlined earlier the potential market for Trusted Computing is very large ranging from the personal computing space through to a wide range of mobile and embedded computing applications. Use cases and applications of TC technology are plentiful but clear cost/benefit arguments are often missing from potential use cases.

Currently, application development around Trusted Computing technology is difficult. Open APIs for TC application development are not available. The only global API available is the one from the TSS, whose large documentation makes the work of developers difficult. More generally, public documentation needs to be released about the TSS and other TCG technologies, and not only via the TCG website.

Training on aspects of Trusted Computing technology is in a development phase. As Trusted Computing is a new technology, training and education has been limited to short articles, one lecture part in a general security training module and the First European Summer School on Trusted Infrastructure Technologies.³ Furthermore, the high number of large specifications written by the TCG makes the understanding of the technology as a whole complicated and Trusted Computing is an evolving technology whose elements are sometimes difficult to connect. These impediments increase the time taken to ingrate the topic of Trusted Computing into the curriculum. On the positive side, academic courses including modules on Trusted Computing from B.Sc. to PhD are now starting to be offered at several universities; Including Birmingham, Bristol, Cambridge, Edinburgh, Imperial College, Newcastle, Oxford, Kent, and Royal Holloway. The Second European Summer School on Trusted Infrastructure Technologies is planned later this year.

As the TPM shipment figures show, TC technology is available but often not visible to system users and implementers. In



The Trusted Computing ecosystem is still in development

³ Aimed at seeding academic research into Trusting Computing technology

particular to the non-business user, since all envisioned applications are business-oriented. Applications like e-Commerce and Transformational Government have yet to gain from Trusted Computing technologies as in a non-business environment; much more legacy equipment must be supported and cannot simply be replaced when it fails to meet the business's requirements.

Trusted Computing is not without its critics, and in many instances much has been published about the potential pitfalls, dangers and concerns over "Big Brother" issues, that have been written about the benefits [9]. This is due to some real concerns that the freedoms of users to access open networks and systems will be curtailed by TC. It is not foreseen that TC environments will become mandatory, at least for the home consumer, but much abuse of IT in the work place has been due to the lack of controls in the past. In the corporate world legislation and financial compliance rules such as The Sarbanes-Oxley Act of 2002 in the USA and the Companies Act 2006 in the UK require records and accounts to be securely held. TC will be a tool for the future to improve the management and auditing of such corporate information. This again might be seen as a negative step and a reduction in freedoms by many users, but might also be seen as an insurance tool for management and shareholders.

Recommendations

This section puts forward our thoughts and recommendations on addressing some of the problems we believe are hindering the uptake of Trusted Computing identified in the previous section. In general it seems that many of the aspects of the lifecycle and ecosystem around the introduction of Trusted Computing technology are in need of development even though the base technology components are readily available.

Our first recommendation is that general awareness of Trusted Computing across the spectrum of potential beneficiaries has to be raised. We feel this is best done by showing the value it can bring in simple non-technical terms as a compliment to the existing Trusted Computing Group technical material. There are various things that can be done: for example the dissemination of a White Paper such as this to as wide an audience as possible. Another option is for the organization of workshops on Trusted Computing. The First European Summer School on Trusted Infrastructure Technologies (intended to seed research interest around Trusted Computing) proved popular amongst the academic community – workshops targeted at other communities such as business or government could also be organized. It is also felt that the development of articles evangelizing the benefits of Trusted Computing again targeted and tailored for specific audiences such as the business community would be a great help in raising awareness.

Trusted Computing technology is increasingly widely available but so far has propagated by stealth

Awareness of Trusted Computing and the benefits it brings must be raised

As part of raising awareness and as a way to offer more specific and continuous support on various aspects of the Trusted Computing ecosystem and lifecycle, the group feels strongly that the establishment of a web based information resource for Trusted Computing would be appropriate.

An increase in awareness has to be backed by strong educational and development resources. This is required at various levels: from software engineering to board members. A list of institutions that offers degree and Masters in information security including Trusted Computing, and private companies who will offer training (e.g. as part of BS7799 training) is necessary we feel. From an academic point of view regular coverage of the Trusted Computing documents, projects and results; encouragement for security training establishments to integrate Trusted Computing into their curriculum; national workshops on Trusted Computing as a first step towards a national organization looking over the technology; organization of seminars on Trusted Computing are all important steps.

As noted earlier it is hoped that the availability of Trusted Computing support in mainstream operating systems will act as a catalyst for Trusting Computing application and solution development. Mainstream operating system support for Trusted Computing technology has been a definite gap in the Trusted Computing ecosystem. The support is now present but somewhat hidden. Again a knowledge base around how to take advantage of these operating system Trusted Computing features from both a developer and end user point of view would be beneficial. Further, whilst Trusted Computing technology components are appearing, documented experiences of the pragmatic and practical issues over how best to integrate Trusted Computing technology into existing and legacy IT infrastructures and how to take advantage of Trusted Computing at a wider level are rare. Development of Practitioners guidelines would be valuable.

Ongoing support of Trusted Computing needs is also very important. This could be via a consultancy database to answer questions of the form "If I wanted more, where can I get the information and support?"

In summary, we feel Trusted Computing is worthy of attention from a UK point of view both as a way of generally raising the UK security baseline and as a way of fostering innovation and collaboration between UK industry, academia and government. Both of these are aims of the KTN network and we believe we have identified definite areas in which support of the wider Trusted Computing space can help in meeting these aims. The KTN will be considering how best to take forward these recommendations. If you or your organisation would like to be part of future action in this space we want to hear from you.

References and Links

- [1] <https://www.trustedcomputinggroup.org/home>
- [2] <https://www.trustedcomputinggroup.org/groups/mobile/>
- [3] <http://www.trusted-mobile.org/>
- [4] http://www.microsoft.com/technet/windowsvista/security/protect_sensitive_data.mspx
- [5] <http://trousers.sourceforge.net/>
- [6] https://www.trustedcomputinggroup.org/kshowcase/view/catalogs_by_category?categories=All%20Categories
- [7] http://www.projectliberty.org/resource_center/presentations_webcasts/rsa_conference_workshop_liberty_alliance_identity_standards
- [8] <http://www.OpenTC.net/>
- [9] http://en.wikipedia.org/wiki/Trusted_computing#Disputes_and_criticism_of_trusted_computing

Authors and Contributors

Chris Dalton

HP, *Chairman of the Trusted Computing Special Interest Group*

Johnnes Arreymbi

University of East London

Nick Bone

Vodafone

Will Burton

CESG

Andy Cooper

University of Oxford

Sadie Creese

Warwick Digital Lab, WMG, University of Warwick

Jerry Fishenden

Microsoft

Dinesh Kallath

BT

Lyndon Lee

BT

Stephane Lo Presti

Royal Holloway, University of London

Andrew Martin

University of Oxford

Rob Rowlingson

QinetiQ

Chris Shire

Infineon

For further information on the work of the Trusted Computing Special Interest Group please contact the Chairman Chris Dalton – cid@hp.com or the group administrator Karen Barnett – kbarnett@QinetiQ.com

www.cybersecurity-ktn.com