Trusted Computing and the Digital Crime Scene

ARTICLE:

TRUSTED COMPUTING AND THE DIGITAL CRIME SCENE

By **Yianna Danidou** and **Burkhard Schafer**

This paper analyses the future of digital forensics in an environment where control is increasingly taken away from PC users and remotely managed by trusted third parties, typically to improve internet security. Trusted Computing (TC) is used as the most developed example to illustrate some of the possible legal issues that arise.

Introduction

Consider the following physical world crime scene scenarios:

1. The house of a suspect in a murder inquiry is searched. In a locked room, and a locked chest within that room, a bloodied knife is found that has the DNA of a murder victim on its blade. The room and the chest were securely locked, the owner of the house being the only one with a key that he never left out of his sight. There is no sign that either lock was tampered with, or that anyone other than the owner has ever been in the room.

2. As above, but this time there are clear signs that someone had at least tried to force both locks, and there are some signs that someone other than the owner had been in the room and interfered with some of the furniture.

3. As in 1 above, but this time, the owner had given a key to the room, but not the chest, to a cleaning agency. They had entered the room several times, but there is no reason to believe they had interest in the chest, or the ability to open it.

4. As in 3, but this time, the owner has given copies to both the room and the chest to a security company that patrolled the house regularly and checked all rooms and storage facilities for intruders or explosive devices. The company had outsourced several of its activities to other partner companies, making copies of the key available to them as needed. Their records confirm without doubt that nobody but the owner and employees or agents of the company entered the room between the time of the murder and the police search that seized the knife.

What can we say in these four scenarios about the evidential value of the knife? Intuitively, it seems clear that the owner of the house in scenario 1 has some explaining to do. Objects found in his possession can be clearly attributed to him, and there is no obvious explanation for the knife other than that he hid it there. Equally, it seems intuitively clear that the situation is considerably different in scenario 2. Someone other than the owner probably had access to the room and the chest, and not only that, the methods used to gain entry indicate the third party had criminal intentions. In scenarios 3 and 4, the situation is much less clear. In 3, much will depend on the details of the case: the trustworthiness of the employees of the cleaning company, their effectiveness in vetting employees, the degree of supervision of employees while they were in the room, and the number of people that could have entered the room. Where someone had the ability to enter the room, the difficulty of opening the chest becomes a factor. Even if the senior managers or directors of the organization did not have any reason to frame the owner, the position of the employees must also be considered. In scenario 4, the situation is even more complex. On the one hand, the type of manipulation encountered in scenario 2 can be ruled out with much more confidence. This also affects scenario 1, or rather our justification to believe that

the specific situation at the heart of an investigation falls into that category. It rules out the possibility that a burglar may have opened the chest (scenario 2), but was so good at his job that he did not leave any traces behind, making it look like scenario 1. On the other hand, a very high degree of trust is now placed with the security company and its employees. While in 2, the owner and unknown third parties may have placed the knife in the chest, in 4 there are is a finite number of suspects, the owner and the people he employed for his security.

Why this matters for a journal on digital evidence. To understand this, we have to transfer our scenarios into the virtual realm, where the house becomes a PC, the room an individual program running on the PC, and the chest contains the equivalence of individual files created by that program. Scenario 1 now exemplifies how lawyers, and arguably also the police, have often naively thought about the "crime scene computer". In this view of the world, the owner (or password holder) is the only one with access to its content, and if illegal material is found on such a device, there is at the very least a strong assumption that it is there with the owner's knowledge and consent. In England, aspects of this view have found their way into the law in the form of an evidential presumption: computers, as a mechanical instrument, are presumed to be in order. This assumes, amongst other things, that programs are not corrupted by third parties.[1] For many reasons, this picture was always at best an overly simplistic version of reality that relied on numerous highly problematic assumptions, such as how many people are physically located within range of the computer that might have been able to use it if they wanted to; whether it really was protected by passwords; whether the computer was set up to ensure a password had to be put in each time the computer 'went to sleep'; whether the wi fi was on or not, and if it was on, whether the security provisions were sufficient enough to prevent a third party from entering the computer from outside.

It is this last aspect, the inability of a third party entering from the outside, that concerns us in this paper. The problems with this specific assumption came to the forefront of the attention of the law when facts similar to scenario 2 were the subject of prosecutions or civil actions. Scenario 2 is broadly the equivalent to the Trojan defence as used in the cases of Matt Bandy,[2] Aaron Caffrey and several others.[3] Caffrey was acquitted by a jury of the charge of unauthorised computer modifications, which were part of a DoS attack against the Port of Houston's computer system in September 2001. Caffrey successfully argued that the evidence against him was planted on his machine by the real attackers, and that his computer had been 'zombified' by an unspecified Trojan that gave the attackers control of his PC. Even though a forensic examination of Caffrey's PC found attack tools (our 'bloody knife'), it did not find any traces of a Trojan infection (our 'scratch marks on the lock'). Nonetheless, the jury accepted the defence argument that a Trojan could wipe itself – blurring the line between our scenario 1 and 2 above. To the extend that Caffrey's argument was convincing, we could never be certain if we are really dealing with an unproblematic scenario 1, or a problematic scenario 2.

Matt Bandy, a minor himself, was prosecuted for the possession of child pornography. Facing a possible sentence of imprisonment of up to 90 years, the ability of his defence team to show that his computer's protection had been disabled and that his computer had at the time been infected by more than 200 viruses and other malware, including Trojans that could have allowed third party access to his computer, allowed him to enter a plea bargain that resulted in an 18 month suspended sentence. His case illustrates two points that will be relevant later: first, the tendency by users to disable protective software (for instance to 'free up' CPU) or to fail to update it is an enabling factor for cybercrime. Second, at least according to the defence team, the police was overly naïve in assuming a 'scenario 1' type setting, without testing the necessary assumptions with sufficient rigour.

Malicious outsiders are, however, not the only problem that demonstrates the problematic assumptions underlying scenario 1. Almost every computer user will have granted – knowingly or unknowingly – at one time or another an automated update agent in the computer the right to obtain access to the internet and to download updates. In this respect, we are almost always in a 'scenario 3' type setting, where the digital equivalent of

1 *For a critical discussion of this presumption and the often unrealistic assumptions it is based on, see Stephen Mason, general editor, Electronic Evidence (2nd edn, LexisNexis Butterworths, 2010) chapter 5*

2 *For an analysis of the Bandy investigation see Stephen Mason, editor, International Electronic Evidence (British Institute of International and Comparative Law, 2008), pp. lxxv-lxxxiii.*

3 *Susan W. Brenner, Brian Carrier and Jef Henninger, ' The Trojan Horse Defense in Cyber crime Cases' , 21 Santa Clara Computer & High Technology Law Journal, 1 (2004-2005) pp. 3-50. Links to several unreported uses of the Trojan defense can be found here: http://www.forensicswiki.org/wiki/Legal_issues*

'domestics' carry out largely unseen work on our computers all the time. While it is unlikely that anyone working for an anti-virus vendor would hold a grudge against a particular person, and could circumvent the internal auditing and security measures to use that permission to install an illegal program or file on their computer, it is equally true that at any given point in time, a large number of organizations can legitimately make changes on the owner's computer system.

It is however scenario 4 that is at the centre of this paper. As with its off-line counterpart, it allows us to rule out with a high degree of confidence evidence planted by malicious third parties as described in scenario 2. On the other hand, every crime scene now becomes potentially tainted should the trust in the third party and its employees be misplaced. Trusted computing can be seen as such a security service, and to understand why it is nonetheless seen as an appealing model by many, we have to discuss in more detail the regulatory and risk assessment environment that gave rise to the TC initiative. Unsophisticated users have long been identified as the weakest link in any strategy to make the internet more secure against cyber attacks. It is their computers that provide the raw material for botnets, the main tool for denial of service attacks, when they forget or fail to update their system with patches, let their anti-virus software expire or forget to update the virus signatures.[4] Once sufficiently large, these botnets in turn can also threaten the systems of more resourceful and sophisticated users, including servers that are crucial for the very functioning of the internet.[5] An apparently obvious solution from the point of view of the technicians is to remove the responsibility of providing security for the computer from the general user, and assign it to a third party. This in turn creates several legal issues for the employees of these third parties, and several of them are discussed in more detail below. For instance, it is necessary to consider if exclusionary rules against illegal searches by the police are applicable by analogy, or if a third party employee finds incriminating material by accident, what the liability is if he chooses not to report it. For obvious reasons, any third party entering into a contract to perform such a service will need certain rights to obtain access to a computer or system to perform the contract effectively. As noted above, whether or not this is acceptable becomes a question of trust – there is nobody a king or president has to trust more than his bodyguards, because they tend to be the only people allowed to carry weapons in her presence – but as history illustrates, such trust can be misplaced.

However, if the future of internet security includes a shift of responsibility (and control) away from ordinary users to professional organizations, a number of issues need to be considered, such as:

1. The conditions by which it can be considered to be rational to trust the security providers.

2. When and if potential interference with the digital crime scene might become an issue.

3. How the criminal law and the law of evidence should respond to such a shift in responsibility, especially if it is the private sector, as opposed to the state, that takes on the role of securing (parts of) the internet infrastructure.

4. Whether it is necessary to adjust laws that were written mainly at a time when policing was the epitome of sovereign authority.

To explore some of the possible legal issues that arise by this strategy, the concept of the Trusted Computing initiative is considered in this paper as a case study. The first part will discuss the regulatory and political environment that gave rise to the initiative, then the

4 Stephen E. Henderson and Matthew E. Yarbrough, 'Frontiers of Law: The Internet and Cyberspace: Suing the Insecure?: A Duty of Care in Cyberspace', 32 (Winter 2002) New Mexico Law Review, 11; Ulrich Bayer, Imam Habibi, Davide Balzarotti, Engin Kirda, Christopher Kruegel, 'A view on current malware behavior', LEET'09: 2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats, 21 April 2009, Boston, MA, USA, available at http://www.eurecom.fr/people/vs_bayer.en.htm; it should be noted at this point that these solutions are themselves far from sufficient to provide perfect security – for a discussion, see e.g. Daniel Bilar, 'Known knowns, known unknowns and unknown unknowns: anti-virus issues, malicious software and internet attacks for non-technical audiences', Digital Evidence and Electronic Signature Law Review 6 (2009), pp 123-131. However, the experience with available security measures shows that no technological solution, however sophisticated, can be expected to work if it relies ultimately on active user involvement and allow the override of automated protection mechanisms by the owner of the computer.

5 While state agencies that should know better have found themselves victims of hacking attacks, the damage in these cases was typically restricted to the computer system in question. With botnets, on the other hand, the victim is not just the user who lets his computer become infected, but also third parties and ultimately, the very functioning of the internet can become threatened. It is this third party effect that changes the legal and practical landscape, and goes some way in explaining why the solution to sustainable internet security is seen mainly in addressing the large number of relatively unsophisticated users. From a legal perspective, it is this involvement of parties other than the immediate victim that we think creates unique legal challenges.

article will briefly explain the technical aspects of this specific project, before canvassing the possible legal issues. Trusted Computing serves to illustrate that the analysis discussed in this paper is not mere speculation, but it should be kept in mind that the main interest is in the *type* of response to cyber crime.

Whom to trust with internet security

In recent years, politicians have begun to take cyber crime more seriously. For instance, the UK government recognizes the detrimental effect that a cyber attack could have on the economy and the social well being of the country.[6] In 2011, cyber crime remained the one field of policing that not only survived the recent spending cuts, but benefited from substantial additional investment as a result of reports that estimate the loss due to cyber crime for the UK at £27 billions.[7] The threat of cyber attack is now classified as a "tier one risk", next to international terrorism using chemical, biological, radiological or nuclear attack by terrorists, a military crisis or an influenza pandemic.[8]

An influential House of Lords report[9] in 2007 described the shortcomings of present approaches to internet security, and critically discussed in great clarity and detail the regulatory alternatives that governments are facing and their respective shortcomings: shift the risks and responsibilities even further to users (for instance, by leaving the user with any losses incurred because their computer is not sufficiently secured, or creating a strong evidential presumption that they were negligent if their data is stolen); make it a state priority to provide considerable new investment in the IT infrastructure, or to provide incentives to the private sector to provide software programs that are more secure, by imposing more, and more easily enforceable, liability on the software vendor for writing programs that are vulnerable to attacks.

The internet was not originally intended as a platform where people spend a substantive percentage of their lives, engage in commercial activity on a large scale, or work, play and socialize, and to interact in various forms with their governments. As the internet becomes more central to the lives of some people, it is inevitable that criminals will exploit its weaknesses to a much greater extent than previously. At one brief point in time, the main threat seemed to come from overenthusiastic teenagers designing viruses, but the risks are now from highly organized criminal groups with significant resources, both in terms of expertise and computing power.[10] In addition, entire nation states can be subject to successful cyber attacks, possibly with the tacit approval or open participation of foreign states, or at the very least "rough agencies" close to state security agencies or the military.[11] With hindsight, the development of the internet might usefully have included security as a design feature. Starting again from the beginning is not a feasible option, which means that any response is likely to be a patch added to the existing system rather than a complete rebuild. Attempts to deal with the increasing number of reported cyber crime incidents include more legislation, user training, public awareness, and other technical security measures.[12]

However, the internet will remain imperfect, and things will go wrong. Indeed, the futile search for perfect security may ultimately do more harm than good, by creating a misplaced sense of security in technology that might increase the use to take greater risks. This in turn raises two related questions from a legal perspective:

1. Who should be given the role of minimizing the harm, together with the rights and authority that comes with such a role.

2. Who can be held legally liable if harm occurs.

These two questions are connected. In the most radical answer to question 2, software producers could also be held liable for the harm done to one of their customers when flaws in the software enable a hacker to steal sensitive data.[13] Rather, they would also be held liable if the computer subsequently

6 *The Government reply to the fifth report from the House of Lords Science and Technology committee, (Cm7234, 2007, The Stationery Office Limited); Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, (Cm7948, 2010, The Stationery Office Limited).*

7 *The Cost of Cyber Crime, (Cabinet Office and Detica, 2011), available at http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime.*

8 *A Strong Britain in an Age of Uncertainty: The National Security Strategy, (Cm7953, 2010, The Stationery Office Limited) p. 27*

9 *Personal Internet Security, Volume 1 Report (HL Paper 165–I, 2007, The Stationery Office Limited).*

10 *Paul Hunton, ' The growing phenomenon of crime and the internet: A cybercrime execution and analysis model' , (2009) Computer Law & Security Review, 25(6), 528-535.*

11 *US-CCU Special Report, Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008, (US Cyber Consequences Unit, August 2009), available at http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.*

12 *Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space, (Cm7642, 2009, The Stationery Office Limited).*

13 *Existing liability regimes for faulty software have largely failed to provide an incentive to software producers to make safety an overriding concern. While in theory, contractual liability for negligent design flaws does exist, it rarely results in successful actions.*

becomes part of a botnet and harms third parties, outside the contractual nexus. This, obviously, would be a strong incentive for software developers to invest in program safety. However, if there were such a radical change of the liability regime, it would be necessary to give them the rights and privileges necessary to enforce, if necessary, the new safety features that they have developed, if necessary against their own customers. Similarly, owners of computers could also be held liable for third party harm if their computer was used in a botnet attack. In both cases, the treatment of computers would be analogous to the way in which some jurisdictions treat ownership of guns – legal to own, but where a third party comes to harm, the owner faces liability if they are negligent.[14]

As mentioned above, the House of Lords' report[15] identified three possible answers: to rely on laws and policing by the state, with a general responsibility similar to that as exists for other critical infrastructure; to provide incentives by requiring users to protect themselves, or to treat it as a technological problem that is left best to software professionals in the 'enabling' industries, from PC manufacturers to ISPs. Edwards[16] offers a helpful analysis of these different regulatory strategies.

The first option is funded by the taxpayer for the benefit of a very specific segment of the economy, in effect a hidden subsidy for bad software design – analogous to asking the government to use tax to constructing even safer roads so that vehicle manufacturers can spend less on designing safer braking systems. In addition, governments only act within national borders, which seriously limits their efficiency in addressing what is a global problem. Making users responsible for their own safety was traditionally, as the report notes, the preferred option by government and business alike – but as security experts have noted, this is an entirely unrealistic notion: the average user does not have the technological sophistication to protect himself, and, as one response to the report stated, "consumers were not required to purify or boil water, when the source of contamination was within the water supply infrastructure itself. Instead suppliers were required to maintain a secure network, and treated water up to exacting standards. The end-user simply had to switch on the tap to get pure, drinkable water".[17] Finally, there is the option of holding the private sector and the software industry responsible for the safety of the internet.[18]

For several reasons, the strategy of holding the private sector and the software industry responsible for the safety of the internet has much to recommend itself to policy makers. Internet service providers, hardware developers and software vendors enjoy the commercial benefits from the internet, and their know how and expertise means they are best placed to protect the user against the most common dangers. Furthermore, many of these companies already operate globally, avoiding some of the limitations that governments would inevitably face, and also avoiding the need for an international treaty that take along time to negotiate. Putting the industry at the centre of the effort to create a secure internet is indeed one of the recommendations of the report, if necessarily backed by legal sanctions. Releasing inherently vulnerable software and hardware to consumers, in this view, should carry the same liability that a water vendor would incur for the safety of the manufacture of the glass bottles used in storing the water.

This course of action would, naturally, create a significant risk to technology companies, exposing them to potentially costly litigation. Arguably, a much better strategy for the industry is to pre-empt any additional legislation by improving security voluntarily. The TC initiative can be seen as a first response to this, with software companies and hardware developers taking on the responsibility for (aspects of) the internet infrastructure.[19]

Trusted Computing Group – aims and objectives

TCG was formed as a result of concerns for the exposure of data on systems, system compromise because of software attack and lack of methods to prevent misappropriation of theft.[20] The term 'trust'

14 *Andrew J. McClurg, 'Armed and Dangerous: Tort Liability for the Negligent Storage of Firearms', 32 (2000), Connecticut Law Review, pp 1189-1125.*

15 *Personal Internet Security, Volume 1 Report (HL Paper 165–I, 2007, The Stationery Office Limited).*

16 *Lillian Edwards, ' Dawn of the Death of Distributed Denial of Service: How to Kill Zombies', (2006) Cardozo Arts & Entertainment Law Journal, 24:23, pp. 23-62.*

17 *Personal Internet Security, Volume 1 Report (HL Paper 165–I, 2007, The Stationery Office Limited) at 3.30.*

18 *Personal Internet Security, Volume 1 Report (HL Paper 165–I, 2007, The Stationery Office Limited) at 3.20.*

19 *It is at this point important to note that in our analysis, TC is more than just a sophisticated tool to protect individual computers, an "anti-virus system +". It does not just protect a computer, it also communicated with other machines that this computer is safe and protected – and will permit communication only between systems that signal their "trustworthiness" in this way. It therefore has the capacity not only to create more secure machines; it is capable of creating a more secure network of trust. As mentioned above, it is this horizontal, third party effect that creates unique legal questions.*

20 *Brian Berger, ' Trusted computing group history', Information Security Technical Report, (2005), 10:2, pp 59-62.*

has many different interpretations. The relevant concept here arises from the field of trusted systems, in accordance with RFC 2828.[21] Thus, Trusted Systems are asserted to be systems that can be relied upon to perform certain security policies in an expected way, with behavioural consistency: TC "refers to a computer system for which an entity has some level of assurance that (part or all of) the computer system is behaving as expected".[22] The outcome ultimately would be to allow the user to 'blindly trust' his computer again, without a constant need for the user to monitor the computer itself. The purpose of TCG project is to provide assurance to the computer user to trust his own computer and for 'others' to trust that specific computer.[23]

Thus the aim of the TC is to protect the software and data in computer platforms (servers, desktops, laptops, PDAs, mobile telephones and many more)[24] from external attacks and physical theft, with the added intention of improving security for remote access. It aims to "enable entities with which the computer interacts to have some level of trust in what the system is doing".[25] This protection is provided by implementing isolated execution environments. In such environments, total isolation of software and data is preserved to ensure protection from possible interference either from other software processes (in the sense that no memory or resource sharing will be taking place) or from connected devices (in the sense that no device will obtain access to the CPU), while processing. When a user fills in data through their web browser, none of the other programs on the computer need to 'see' what the user is doing. By isolating the programs this way, the user might lose some functionality, for instance not to be able to use the Word spellchecker in programs other than Word, but malicious programs cannot intercept and record what the user is doing. Trusted platforms purport to provide such environments by providing a collection of isolated environments for operating systems, applications and applets in which to operate on data; and defines which applications will be permitted to operate on selected data.[26] For instance, a user can decide to protect his private data (financial information, personal data) by choosing which applications that his platform will be permitted to obtain access and operate on his private data – and no other program will be given access to this information. Additionally, trusted platforms can offer assurances about their behaviour and identity both in hardware and software.[27]

Technical analysis of Trusted Computing technology

How the Trusted Platform works

Trusted platforms (TP) provide a technological implementation and interpretation of the factors that must be simultaneously true in order to achieve "trust" and are defined by the TCG:[28]

1. *Unambiguous identity:* In order for something to be able to be trusted, it must be unambiguously identifiable, thus every component of a TP must be known and identifiable.

2. *Unhindered operations:* Something can be trusted if it behaves in an expected manner for a particular purpose. A component of a TP has been designed to perform a particular task and follow a designed behaviour.

3. *Attestation:* The process of reliably verifying and guarantying that something is to be trusted, by observing its constant good behaviour. In analogy, for a TP to be trustworthy there needs to be some

21 *Boris Balacheff, Liqun Chen, Siani Pearson, Graeme Proudler and David Chan, 'Computing Platform Security in Cyberspace', Information Security Technical Report, (2000), 5(1), 54-63; Chris J. Mitchell, 'What is Trusted Computing?', in Trusted Computing, edited by Chris J. Mitchell (The Institution of Engineering and Technology, 2008), Vol. 6, pp 1-10; Trusted Computing Group Glossary Retrieved 15/7/2011, 2011, from http://www.trustedcomputinggroup.org/developers/glossary/; R. Shirey, (2000) RFC2828: Internet Security Glossary.*

22 *E. Gallery and C. J. Mitchell, 'Trusted mobile platforms', in Aldini Alessandro and Gorrieri Roberto, eds, Foundations of security analysis and design IV (Springer-Verlag, 2007), pp 282-323; Chris J. Mitchell, 'What is Trusted Computing?', in Trusted Computing edited by Chris J. Mitchell (The Institution of Engineering and Technology (IET), London, UK, 2008), Vol. 6, pp 1-10.*

23 *Howard F. Lipson, 'Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues' Special Report, (November 2002, CMU/SEI-2002-SR-009).*

24 *G. Proudler, 'Concepts of trusted computing', in C. J. Mitchell, ed, Trusted Computing (The Institution of Engineering and Technology, 2005), Vol. 6, pp 11-27.*

25 *Chris J. Mitchell, 'What is Trusted Computing?', in Chris J. Mitchell, ed, Trusted Computing (The Institution of Engineering and Technology, 2008), Vol. 6, pp 1-10.*

26 *G. Proudler, 'Concepts of trusted computing', in C. J. Mitchell, ed, Trusted Computing (The Institution of Engineering and Technology, 2005), Vol. 6, pp 11-27.*

27 *Eimear Gallery and Chris J. Mitchell, 'Trusted Computing: Security and Applications', Cryptologia 33:3 (July 2009), pp 217-245; Michiel Broekman, End-To-End Application Security Using Trusted Computing (Masters Thesis) (Oxford University, University of Nijmegen, 15 August 2005).*

28 *TCG Infrastructure Working Group Architecture Part II – Integrity Management (v 1.0 17 November 2006 Final) p 9; Eimear Gallery, 'Who are the TCG and what are the Trusted Computing concepts?', in TRUST2008 (Villach, Austria, 2008).*

way that the platform can report its integrity state (the platform's current state) as a whole to the external world. For that, each component comprising a TP uses a function to report its state of integrity.

TPs are designed for the protection and processing of private or secret data. This means that the occasional benefits of different applications sharing data are reduced in favour of greater security. As explained earlier, this is achieved through isolated execution environments, where software and data is protected from external interference, and they can offer assurances about their behaviour (of both the hardware and software environment).[29]

Direct anonymous attestation protocol

The central part of the hardware is the protocol which implements Trusted Computing, known as Direct Anonymous Attestation (DAA). Consider that we have a user's device with a TPM that communicates with another device called the verifier, who wants to know (via authentication) if the user uses a TPM.[30] However the user needs to preserve his anonymity and privacy through this procedure, otherwise the verifier will be able to know all about the user's past and future transactions. To achieve this, the verifier should only verify that the user uses a genuine TPM, but he should not be able to know which particular TPM he is using. From its name, the basic logic of the protocol can be derived thus: provides proof without a Trusted Third Party involvement (Direct); non-disclosure of the identity of the signer (Anonymous); and requirement of statement or claim from a TPM (Attestation).

The aims of the TCG are achieved by integrating a trusted hardware module into a platform (a mobile telephone, a laptop). Although it is not compulsory to implement a TPM in hardware, it is actually a requirement, because solutions implemented only by the use of software have been proved inherently weak (due to programming faults).[31]

TCG solves the privacy problem by making use of a trusted third party, which in this case is called the 'Privacy Certification Authority' (PCA). Every TPM creates a key pair using the RSA algorithm and this key pair is called an 'Endorsement Key' (EK). The EK is created only once and PCA keeps a record of the Endorsement Key of every valid TPM. Whenever a TPM wants to verify itself to a verifier, it creates another pair of RSA keys which is called an 'Attestation Identity Key' (AIK) and sends that key pair to the PCA. The PCA then authenticates this public key that refers to the EK. The PCA will check if the EK is contained in its list of valid EKs. If it is contained in the list, the PCA issues a certificate for the AIK to the TPM. The TPM can now send the AIK's certificate to the verifier and authenticate itself. Although this is a solution for the trusted computing problem, it has a major disadvantage: the PCA is involved in every transaction and thus it must be available at all times and under all conditions. However, at the same time it must provide as much security as an ordinary certification authority which would normally operate off-line. Moreover, if the PCA and the verifier join together, or the PCA's transaction records are revealed to the verifier by some other means (this can be solved by using blind signatures), the verifier will still be capable of uniquely identifying a TPM. Consequently, the problem with the privacy and anonymity issue endures.

A better solution was proposed by Ernie Brickell, Jan Camenisch and Liqun Chen. This solution was adopted by the TCG in the new specification of the TPM (1.2) in 2003. It associates techniques "developed for group signatures, identity escrow, and credential systems", and the scheme proposed can be described as a group signature scheme, but one which does not have the opportunity to open signatures but with a mechanism to detect false TPMs.[33]

Both hardware (the Trusted Platform Module (TPM)) and software (the Trusted Support Services (TSS)), are combined in a Trusted Computing System. The software must contain TC-enabled applications. The role of the hardware by contrast is emphasized in the 'Fritz' chip. This smartcard chip – named after Senator

29 *Eimear Gallery and Chris J. Mitchell, 'Trusted Computing: Security and Applications', Cryptologia 33:3 (July 2009), pp 217-245.*

30 *Ruediger Weis, Stefan Lucks, Andreas Bogk, TCG 1.2 - Fair play with the 'Fritz' chip?, 4th International System Administration and Network Engineering Conference, Amsterdam, 2004; Ernie Brickell, Jan Camenisch, and Liqun Chen, 'The DAA scheme in context', in Chris J. Mitchell, ed, Trusted Computing (The Institution of Engineering and Technology, 2008), Vol. 6, pp 143-174.*

31 *Siani Pearson, 'Trusted Computing Platforms, the Next Security Solution', Trusted E-Services Laboratory HP Laboratories Bristol, HPL-2002-221, available at http://www.hpl.hp.com/techreports/2002/HPL-2002-221.pdf.*

33 *Ernie Brickell, Jan Camenisch and Liqun Chen, 'Direct Anonymous Attestation', a paper presented at the Proceedings of the 11th ACM conference on Computer and communications security (2004), Washington DC, USA, available at http://eprint.iacr.org/2004/205.pdf; Ernie Brickell, Jan Camenisch and Liqun Chen, chapter 5 'The DDA in context' in C. Mitchell, ed, Trusted Computing, (IEE, 2005) pp 143-174.*

Fritz Hollings, a US politician with a long history of legislative attempts to ensure that PCs do not support production of 'unauthorized content' – is placed on the motherboard which constantly checks the software and hardware that are running on the machine. If both are found to be authorized, the operating system (OS) boots up and assures any third parties that the machine is indeed the machine that it is claimed to be, and the software that is running on it is indeed the software that is claimed to be.

TCG proposed a technology that makes use of four main features, discussed below. For the technology to work, it is necessary to install new hardware on existing computers. The features can work individually, and they can also work in conjunction with each other.

Memory curtaining

Memory curtaining refers to a "strong, hardware-enforced memory isolation feature" in order to avoid reading and writing memory between several programs.[34] In TC, the operating system should have access to this type of memory, so if an adversary enters the operating system it would not be possible for him to enter and interfere with any program and its memory. The advantages of using a hardware feature instead of software – which could operate in a similar fashion – are: backwards compatibility; the ability to use code again, and that fewer changes need to be made to hardware drivers and application software.[35]

Secure I/O

Under secure I/O threats posed by keyloggers and screen-grabbers are minimized, because it provides a secure hardware path from the keyboard or mouse (i.e. the user) to an application and vice versa. No program can intercept the data from the point where the user types it in and it appears on the application. By doing this, none of the software programs will know what the user typed as a command or input to another program and how the application responded. Protection from physical attacks is provided and any programs that intentionally "corrupt, modify, or mislead the user, will be prevented from running or operating".[36]

Sealed storage

Until recently, any keys and passwords used by applications were stored locally on the hard drive. This was not secure, because keys could be obtained by any intruder or virus. It is important to ensure that only legitimate users can obtain access to these valuable and secret data. This is what sealed storage purports to achieve. It is characterised as "an ingenious invention that generates keys based in part on the identity of the software requesting to use them and in part on the identity of the computer on which that software is running".[37]

Remote attestation

The aim of remote attestation is to allow 'unauthorized' changes to software to be detected. It remotely traces any changes made to any application and allows a third party to decide whether the platform is considered trustworthy. This feature is significant, because it helps to prevent the sending of data to or from a compromised or untrustworthy computer and certifies that no unauthorised program has been installed, updated or modified in the hardware or software on the user's machine. Moreover, "this allows an entity to authenticate the software configuration of a platform that is not under its control".[38]

The TCG chip provides three main groups of functions. These are:

1. Public key functions: used for key pair generation, public key signature, verification, encryption and decryption purposes.

2. Trusted boot functions: this ensures that data are 'trusted', because the data stored while booting are the same with the data at the time of sealing. Trusted booting combines both authentic booting, which creates a log containing the programs that are loaded on the computing device, and secure booting, which ensures that the computing device is

34 Seth Schoen, Trusted Computing: Promise and Risk, (Electronic Frontier Foundation, 2003), available at http://www.eff.org/files/20031001_tc.pdf.

35 Mike Burmester and Judie Mulholland, ' The advent of trusted computing: implications for digital forensics' in Proceedings of the 2006 ACM symposium on Applied computing (ACM, 2006), pp 283-287.

36 Mike Burmester and Judie Mulholland, ' The advent of trusted computing: implications for digital forensics' in Proceedings of the 2006 ACM symposium on Applied computing (ACM, 2006), pp 283-287, p 285.

37 Seth Schoen, Trusted Computing: Promise and Risk, p 4.

38 Jason Reid, Juan M. Gonzalez Nieto, Ed Dawson and Eiji Okamoto, Privacy and Trusted Computing, in Proceedings of the 14th International Workshop on Database and Expert Systems Applications, (IEEE Computer Society Washington, 2003), pp 383-388, p 384

in a secure state.

3. Initialization and management functions: these allow the user to switch on or off the functionality, to reset the chip and take ownership.[39]

TCG provides protection to sensitive authentication information from attacks by hackers. This is achieved by protection provided to the user's private key. In addition, by sealing the master encryption key under a TCG register, it is possible to protect a user's sensitive files and data.[40]

Consequences for the regulatory environment

From the beginning, TC has been controversial within the academic and scientific world, the computer industry, and the end-user community.[41] The proponents of TC suggest that TC promises to provide four crucial advantages: reliability, security, privacy and business integrity. These, it is claimed, when taken together, guarantee a system that will be available when needed; will resist any attack by protecting the system and the data; will provide privacy to the user, and finally it will provide businesses with the ability to interact efficiently and safely with their customers. Additionally, TC should provide protection from viruses, because a check will be applied to all files trying to 'enter' the system, as well as the implementation of new applications aiming at providing greater protection.

From the point of view of the software vendors and content industry, TC aims to provide more trustworthiness, but paradoxically, from the point of view of the user, the outcome could be perceived as less trustworthy, with more power held by organizations that enjoy little public trust.[42]

Critics of TC consider that restrictions will be imposed on users, because the owner of a PC does not have root access to cryptographic keys, and therefore users will no longer be in control their own computer.[43] The validity of this argument is also confirmed by proponents of TC,[44] but they claim that this is a feature, not an error, as it will restrict issues such as *user override*. As noted above, the user has the ability to disable soome of the safety features. Where such features are rendered inoperative, the computer becomes open to cyber attack. It is for this reason that it is suggested it is necessary to rebalance the degree by which users can override such features that are put in place by the manufacturer and still remain trustworthy.[45] Consequently, the user will no longer be in full control of their own computer because they are not permitted to obtain access to the private keys that purport to make the user trustworthy, thus it is asserted that the trust is based on what is promoted as being a 'well designed machine', not badly educated humans.

Richard Stallman, the founder of the Free Software Foundation and creator of the GNU Project and Free Software Foundation, is one of the harshest opponents of TC. Stallman considers that 'treacherous computing' is a more accurate name for TC, and states that this technology will allow content providers and computer companies to make computers obey them. It is possible for users' data to be edited and deleted remotely, without any notification to the user or owner of the computer.[46] In the context of this article, this possibility is central to scenario 4 above:

a) The extent that a TC system provides for the Trojan defence, when remote access to files by a third party is a necessary prerequisite for the system to fulfil its function, and

b) The legal duties, if any, that should be imposed on TC providers to maintain the integrity of 'digital crime scenes'.

39 *David Safford, Clarifying Misinformation on TCPA, (IBM Research, October 2002) available at http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf.*

40 *David Safford, The Need for TCPA, (IBM Research, October 2002), available at http://www.research.ibm.com/gsal/tcpa/why_tcpa.pdf.*

41 *For an extensive discussion on the controversy and the reasons behind the controversial nature of TC see: Catherine Flick, The Controversy over Trusted Computing (University of Sydney B.Sc. thesis, June 2004) at http://liedra.net/misc/Controversy_Over_Trusted_Computing.pdf*

42 *Yianna Danidou and Burkhard Schafer, ' In Law We Trust? Trusted Computing and Legal Responsibility for Internet Security' , in Dimitris Gritzalis and Javier Lopez, eds, Emerging Challenges for Security, Privacy and Trust (Springer Boston, 2009), Vol. 297, pp 399-409.*

43 *Lucky Green, Trusted Computing Platform Alliance: The Mother(board) of all Big Brothers (2002), a presentation at DEFKON 10, available at http://www.cypherpunks.to/TCPA_DEFCON_10.pdf; Richard Stallman, Can you trust your computer? 2002, available at http://www.gnu.org/philosophy/can-you-trust.html.*

44 *Moti Yung, ' Trusted Computing Platforms: The Good, the Bad, and the Ugly' , in Rebecca N. Writght, ed, Financial Cryptography Lecture Notes in Computer Science Volume 1/1973 (7th International Conference, FC 2003, Guadeloupe, French West Indies, 27-30 January 2003, revised papers), pp 250-254.*

45 *Moti Yung, ' Trusted Computing Platforms: The Good, the Bad, and the Ugly' , in Rebecca N. Writght, ed, Financial Cryptography Lecture Notes in Computer Science Volume 1/1973 (7th International Conference, FC 2003, Guadeloupe, French West Indies, 27-30 January 2003, revised papers), pp 250-254.*

46 *Richard Stallman, Can you trust your computer?.*

Programs that use TC when installed will be able to continually download new authorization rules through the internet and impose those rules automatically on the computer. In such circumstances, it is claimed that computers may apply the new instructions that have been downloaded without the user being made aware of the new instructions, to such a degree that a user will no longer be able to fully interact with his own computer.[47] This shows that in the context of computer forensics and crime investigation, the Digital Rights Management (DRM) heritage of TC becomes a potential issue. Digital Rights Management, which was one of the original aim for developing TC technology, will be used for e-mail, documents and multimedia which can disappear or remain unreadable on certain computers, thus altering programs and files – with obvious consequences when the evidential value of such files and programs have to be evaluated.

Legal responsibility in an age of TC

A significant aim of this paper is to argue that if the internet is to be made more trustworthy through technological rather than legal solutions, the provider of that security will need to obtain access to user's hard drives, and have the ability to extract information and to reconfigure the software on the machine. TC can be seen as a first step in this direction. In this analysis, in conceptual terms the TC approach amounts to a part privatization of what is, in the off-line world, an essential state function. Safety becomes a commodity, and its exchange is primarily governed by contract. Contract, and possibly the law of tort, has consequently been seen often as the obvious solution to the regulatory issues that TC raises.[48] However, this perspective leaves the re-balancing act between the customer or computer user and the software company to a mix of market forces, competition law and good faith interpretation of contractual terms that cannot adequately address the interest of third parties in the security of the internet, and in particular fails to address the interest of the state and law enforcement agencies.

To the extent that scenario 4 is a realistic depiction of the new realities of investigative work in a trusted computing environment, several choices become available. One is to do nothing. In this case, the issue of access is similar to scenario 3. Since no legal challenge against the validity of digital evidence on the basis of an update agent or similar software on a computer that grants other organization access to it has been made to date, this could be considered as a mere theoretical concern. The risk is that should such a case ever arise, a large number of convictions could suddenly become unreliable in retrospect. Alternatively, if our analysis of TC as privatization of a core state function is considered seriously, it is necessary to create a legal duty on TC providers to ensure that any interaction with individual computers does not affect the integrity of the data for evidential purposes. Just as the police are required to observe the requirements of the chain of custody, and to document the chain appropriately, TC providers could be required to develop protocols with the explicit requirement of legal admissibility. This option would also highlight the potential privacy issues raised by trusted computing, making the quasi-policing role of TC more visible. This, arguably, could act as a deterrence for the uptake of the technology, but this assumes that consumers will be left with a choice in the matter.

A related issue is the use of forensic diagnostic tools. One of the problems with TC that is frequently raised in the literature is the possibility that it will not allow certain programs, especially open source programs, to run on a computer. This could at least theoretically prevent commonly used forensic tools such as Encase running on a suspect's computer.[49] Any attempt to deal with this problem generically may be more difficult than it seems, given the dual nature of many hacking tools – the very software that a system administrator uses to ensure safe working of a computer, or that is needed for a forensic analysis, are also capable, in the wrong hands, to be used for malicious purposes – the difference between hacking and auditing or administration tools lies not in the code, but the use it is put to. This became visible in Germany's much criticized attempt to prohibit the

47 *Ross Anderson, Trusted Computing Frequently Asked Questions/TCG/LaGrande/NGSCB/ Longhorn/Palladium/TCPA – Version 1.1. (2003), available at http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html; Richard Stallman, Can you trust your computer?.*

48 *Yianna Danidou and Burkhard Schafer, ' In Law We Trust? Trusted Computing and Legal Responsibility for Internet Security' , in Dimitris Gritzalis and Javier Lopez, eds, Emerging Challenges for Security, Privacy and Trust (Springer Boston, 2009), Vol. 297, pp 399-409.*

49 *Stephen Mason, ' Trusted computing and forensic investigations' Digital Investigation Volume 2 Number 2, pp 189 – 192.*

possession of software that can be used for hacking purposes, and led one journalist to add as a by-line: 'Will the last security expert to leave Germany turn off the lights?'[50] By the same token, many of the functions necessary to perform a forensic investigation on a computer – which by definition often means to 'force' the suspect computer to reveal its secrets by, for example, breaking passwords or searching for stenography – will look for all intents and purposes for the TC system, which is similar to the very type of process it is designed to prevent from running.

This in turn leads to another problem: whether it is desirable in principle that TC provides the purported 'total' security from attacks. At first glance this question might seem absurd, but it is necessary to understand that the entire field of internet security is based on a fundamental paradox: *what works for the victim also works for the criminal, and what works for the criminal can also work for the police.* This was epitomized in the debate around secure encryption in the late 1990s: while strong encryption protects honest citizen against data thieves and other criminals by protecting sensitive communication such as bank details, it also protects criminals, their clandestine communications and on-line money laundering activities.[51] Complex compromise solutions had to be designed, which typically combine restrictions on some technologies with legal requirements to hand over keys as part of an investigation.[52] One of the potentially strongest selling points for TC and proof of its potential to enhance privacy is that a number of oppressive regimes prohibit their citizens from downloading the related TPM technology. However, the technology is neutral. That TC is considered to be suspicious by regimes that prefer its citizens to not discuss politics without the ability of the police to eavesdrop should also raise concerns for governments worried about organized on-line crime.

It is also not an option to provide the public with a 'weak' form of TC that remains vulnerable to being penetrated by the police or other state agencies. As indicated above, organized criminals, often with a background in the disintegrating security agencies of the Eastern European block, can match those of official agencies. More plausible is the idea that the state will impose a requirement to leave sufficient weak spots so that when authorized by a court, the TC provider is in a position to obtain access to the data. This is very similar to the provision of the Regulation of Investigatory Powers Act 2000 in the UK that creates obligations to reveal the password to encryption keys. In such an environment, TC providers face a stark choice: promise a lot, and risk liability when things fail, or make it clear in the contract that TC cannot guarantee safety – which would risk to undermine acceptance and take-up by users. It is noteworthy to mention at this point that Windows Vista and Windows 7 are already using the Trusted Platform Module to facilitate the BitLocker Drive Encryption. It is undoubtedly the case that users are not aware of this, but even if they were aware, they would not be able to understand its features.

Even more directly relevant in considering police investigations in a TC environment, is that some investigative methods used by the police use the same technologies that criminal hackers use to exploit computer vulnerabilities. In Germany, the 'Federal Trojan' was a piece of software that opened back doors in the computers of crime suspects, to permit clandestine monitoring of their activities.[53] Even more controversially, the recent attack on Iran's computer infrastructure for the nuclear industry was very likely the result of actions by a 'friendly' state power (friendly, that is, to the US and UK as main sponsors of TC) using a similar, Trojan based approach.[54] A technological solution such as TC that cannot distinguish in principle between good governmental Trojans and bad criminal Trojans and prevents both from functioning, creates potential for conflicts, both technological and legal, that need to be further explored. One answer, for instance, could be to create a further responsibility for the TC developers, that is, the duty to compromise their own product under certain circumstances. This in turn

50 *John Leyden, 'Germany enacts anti-hacking law' The Register, 13 August 2007.*

51 *David Friedman, 'A World of Strong Privacy: Promises and Perils of Encryption', Social Philosophy and Policy, 13:2 (1996), 212-228; for examples of cases that have been prosecuted in relation to encrypted materials, see Stephen Mason, general editor, Electronic Evidence, (2nd edn, LexisNexis Butterworths, 2010), 1.34 and 10.228 – 10.250.*

52 *R. C. Barth and C. N. Smith, 'International Regulation of Encryption: technology will drive policy', in Brian Kahin and Charles Nesson, eds, Borders in Cyberspace: Information Policy and the Global Information Infrastructure (Cambridge: MIT, 1997), pp. 283-300.*

53 *Wiebke Abel and Burkhard Schafer, 'The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822', (2009) 6:1 SCRIPTed 106, available at http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp.*

54 *Nicolas Falliere, Liam O Murchu and Eric Chien, 'W32.Stuxnet Dossier Security Response' (version 1.4, Symantec Corporation), p 69, available at http://www.symantec.com/en/ca/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf*

would require a set of legal instruments, on the one hand to compel them to cooperate, and on the other a qualified privilege for any harm that might arise from such cooperation. Decisions also would have to be taken regarding the procedural requirements to be used to compel TC providers to cooperate with criminal investigations, in particular the degree (if any) of judicial oversight and warrant requirements. Hence, balancing the legal obligations, privileges, immunities and burdens in a way that is at the same time equitable to consumers and software vendors requires considerably more complex responses by the law than change to the liability regime that the House of Lords envisaged.[55]

A final issue arises from the DRM heritage of TC, and also how issues traditionally discussed in terms of privacy protection can take a new dimension in the context of criminal law and criminal investigations. As noted above, it seems that the TC providers can obtain sufficient information from the computers of TC users not only to prevent unauthorized programs or files from running (for instance to prevent the playing of an illegal copy of a music track), but also the possibility of removing programs. Given such power, it is possible to infer that the TC provider would at least have constructive knowledge about the content of the user's computer. Increasingly, legal systems create an obligation to inform the police if they have knowledge of illegal activity. For instance, the 2001 Anti-Terrorism, Crime and Security Act 2001 in the United Kingdom makes it an offence to fail to disclose information to the police that would be "of material assistance in preventing or leading to the arrest of persons engaged in the commission of an act of terrorism" (section 117 Information about acts of terrorism). In Germany, an even broader duties exist to bring certain crimes to the attention of the authorities. Article 138 of the Criminal Code (StGB) mandates that failing to disclose information about a large number of offences, from terrorism and treason to murder, kidnap and dangerous interference with the railway, carries a sentence of up to five years. It is therefore of some relevance to decide what type of knowledge is required by these criminal offences, if fully automated processes that permit the identification and retrieval of information count as 'knowledge' for the purpose of these laws (and if not, if they should be included), and indeed how much actual knowledge TC providers could or should have about the content of their customers' hard drive. It could be possible for instance, to look for the hash value of movie clips known to have content of abusive images of children, in addition to clips that are merely illegally downloaded.[56]

This is not the first time that technological processes create an unintended side effect in relation to criminal liability – a case in point was whether Google was technically in possession of illegal images when their web crawlers created cached versions of the web sites they visited, stored on Google servers. In the case of TC, the problem is not 'possession' but 'knowledge'. Nonetheless, special privileges may have to be created by law to exempt them from an overly onerous reporting requirement, especially as this would make them even more visible as part of a surveillance operation on behalf of the state and in potential conflict with their customers.

Conclusions

Internet security has finally gained the interest that it deserves from the governmental point of view.[57] Consumers also need to be confident in internet security. TC proposes a technical solution, where security is neither entrusted to the user, nor enforced by the state, but is found in every unit of the internet. This paper has outlined that this amounts to a dramatic shift of power away from consumers and state regulatory bodies to the software providers, and such a move will only be acceptable if it is accompanied by an equivalent shift in legal responsibility. While the House of Lords[58] is right in its emphasis on the responsibility of software and hardware producers, it may have underestimated the amount of adjustments in the legal regime that this requires. The authors contend that TC is best understood as the outsourcing of state functions to the private sector, and with that arises the requirement to provide, on the one hand, adequate

55 *Personal Internet Security, Volume 1 Report (HL Paper 165–I, 2007, The Stationery Office Limited), p 121.*

56 *U.S. v. Cartier, 543 F.3d 442 (8th Cir. 2008).*

57 *Emma Downing, Cyber Security – A new national programme (SN/SC/5832, 19 January 2011) House of Commons Library; Intellect reacts to the National Security Strategy and Strategic Defence and Security Review (21 October 2010), available at http://www.intellectuk.org/media-releases/6378; Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, (Cm7948, 2010, The Stationery Office Limited).*

58 *Personal Internet Security, Volume 1 Report (HL Paper 165–I, 2007, The Stationery Office Limited), p. 121.*

protection for citizens, and on the other, a rational framework that grants the necessary legal privileges while imposing certain responsibilities on TC providers, making them more like the 'special constables' they in fact will become.

Yianna Danidou is a computer scientist (B.Sc., M.Sc.). She is acting as the Head of Computer Science department at the American College in Nicosia, Cyprus and at the same time is a PhD candidate at the School of Law of the University of Edinburgh with research interests in law and IT.

http://www.yiannadanidou.eu/

I.Danidou@sms.ed.ac.uk

Burkhard Schafer is Professor of Computational Legal Theory at the University of Edinburgh, and Director of its SCRIPT Centre for IT and IP law.

http://www.law.ed.ac.uk/staff/burkhardschafer_69.aspx/

B.schafer@ed.ac.uk