TRUSTED COMPUTING: ADDRESSING INSIDER THREATS TO THE BANKING AND FINANCIAL SECTOR

Gene L. Tang

Department of Computer Science
University of Auckland, Auckland, New Zealand

ABSTRACT

Insiders have the potential to cause major financial loss and damage to the reputation of an organisation, particularly in the Banking and Finance Sector where transaction between consumers and other organisations occur almost every second. As Trusted Computing (TC) comes into age, this paper considers the potential that this technology can offer to protect the assets of the Banking and Financial Sector from insiders.

Trusted Computing is a family of new specifications established by the Trusted Computing Group (TCG) with the goal of making computers more "secure" through dedicated hardware.

This paper considers the role TC can play to insider threats from the perspective of prevention and detection, as well as from the eleven proactive strategies to mitigate insider threats, established in the NTAC/CERT study of insider threats to the Banking Sector.

The paper finds that TC can be used to limit insider attacks; however, further study of insider attacks need to be completed before the application of the technology can be successfully implemented.

1. INTRODUCTION

Insider threats to the computer and information systems of the Banking and Finance Sector are as common, if not more common, than external threats [1, 2]. Trusted Computing provides a technology that may have the potential to limit, or stop these insider threats.

Insiders are members of any group, which may be limited in number of people and who have restricted access; this includes any members of an organization such as employees or contractors [1]. A threat is an unwanted event that may result in harm to an asset, often employing and exploiting known vulnerabilities [3]. An "Insider Threat" is therefore an act designed to perpetrate harm on an organisation by individuals within the organisation who have been authorised to use the information systems [2]. For simplicity, this paper refers to insiders as only those who attempt to perpetrate harm on the organisation.

As this world becomes increasingly commercialised through globalisation, the reliance on the Banking and Finance Sector has become ever more significant, affecting daily the world's entire population. Following growth of this industry, the threat of insider attacks to organisations within it has become more and more evident and dangerous. This has been exemplified through the increasing dependence on information systems and computer systems, which expose further vulnerabilities with complexity [1, 2].

Trusted Computing (TC) represents the 'next-generation' of personal computer security [4], with the goal of providing greater internet security to end-users through the use of a specialized piece of hardware integrated into existing computing hardware. TC provides mechanisms that offer security from threats; such as those on the internet (e.g. hackers); through to protection from physical theft [5]. By protecting client machines protection can be extended to servers that are used by the clients [6]. TC security is achieved through improved secret protection of data as well as through attestation of identities [5]. Open specifications of TC and the TPM are provided by the Trusted Computing Group (TCG) [5].

This paper considers the potential of TC to protect against insider threats to the Banking and Finance Sector, as opposed to the external threats which TC are also designed to counteract. Application of TC is based on the eleven proactive strategies to combat insider threats outlined by a CERT/NTAC study regarding inside threats to the computer systems of the Banking and Finance Sector [5, 7]. These eleven strategies act as the evaluation criteria to determine the success of TC as a tool against insider threats.

Results of this evaluation finds that the application of TC to protect against insider threats is limited and generally provides better security from external threats rather than insider threats. TC can, however, supplement existing practices and procedures to also successfully protect against internal threats due to the features it provides, particularly in data protection. Further research is required to determine more suitable applications of TC.

2. BACKGROUND

2.1. Overview of Trusted Computing Technology

An overview of Trusted Computing goals and technology are provided in this section, full details of the TCP specification can be found in [5, 8]. This paper is based on the TCP Specification 1.1b [5]. Please note that the TCP Specification provides only a standard, and implementations of TC hardware are proprietary. Furthermore, few manufacturers of TC hardware release details, therefore technical detail within this paper is limited to the specification only [9, 10].

2.1.1. Definition of Trust

According to the TC Specification, the definition of trust and a trusted entity is defined as one that: "… always operates as expected for the intended purpose" [5]. Therefore this paper takes the approach that a trusted computer is one whose software (and hardware) has not been tampered with, since only then would it function for its intended purpose [5].

2.1.2. Motivation for Trusted Computing

The goal of the Trusted Computing Group (TCG) is to create a ‘safer client-side computer’, in which the computer and the data that resides on it are secured from external threats through hardware and software mechanisms [5, 11]. The security, or trustworthiness of the platform can also be reported to the user or a third party if required.

The Trusted Computing (TC) Initiative was prompted due to the increasing number of attacks by hackers and malicious programs on client-side computers, as well as due to the seriousness of these attacks [6]. As attacks become increasingly common, there is an increasing threat to users and businesses, particularly since sensitive data, like passwords, is becoming more commonly stored in electronic format [6]. TC aims to reduce these threats using specialized hardware and TC-enabled software on the client-side machines [5, 11].

2.1.3. Features of Trust Computing

Security features are commonly considered obstacles to convenience to many customers and are often disabled or circumvented. Furthermore they do not provide any tangible benefits with regard to the software that the customer buys [5].

TC aims to be the first successful ubiquitous deployment of platform security [5], by being useful, low cost and effective. The ubiquitous aim would firstly be achieved by making the extra hardware required for a Trusted Platform low in cost [5]. Next the features are categorised into three areas [4, 5]:

- *Immediate Benefits:* Provide immediate protection of data and secrets such as by bulk encryption of data and digital signing, without requiring any significant modification to the Operating System. These mechanisms should only allow authorized people to view the data when the data is stored or being transmitted (Data Security).

- *Intermediate Benefits:* Provide features that prevent the release of data and secrets to a platform unless the software environment is trusted (that is not tampered with), thereby preventing misuse of data by wrong software. This requires alterations to the OS and the computer’s boot sequence (Data Safety and Integrity).

- *Long-term Benefits:* The final set of features is attestation identities, which identify a platform’s trustworthiness. Provided a Public Key Infrastructure is established, then remote applications and computers can use these identities to determine if they want to allow another computer to access them.

This paper assumes that all of these features are available and successfully deployed, in order to assess their performance.

2.1.4. The Trusted Platform

Technology derived for TC is designed to be implemented on any computing device, such as a PC or mobile phone [5]. These devices, known as Trusted Platforms (TP), require four hardware components currently being developed, to meet the security objectives and features outlined by TCG [4]:

- *Secure I/O:* Secure I/O replaces the existing computer I/O (keyboard/screen) with secure hardware instead of software, thereby guaranteeing that I/O software cannot be tampered with. This hardware uses encryption and decryption to transmit data from the keyboard to the application and from the application to the screen, to ensure that data cannot be tampered with whilst in transit. This prevents attacks from keyloggers and screen watchers.

- *Curtained Memory:* Curtained memory allocates memory to a program, and prevents other programs (including the Operating System) from reading or writing its allocated memory. This is important, particularly if a malicious program is trying to access and modify the running program or its data.

- *Sealed Storage:* Sealed storage protects private and sensitive information by encrypting the data with a key derived from the software and hardware that exists on the computer. This requires the hardware to provide some form of cryptographic engine, hence limiting the data mobility and allowing it to be read on that computer only.

- *Remote Attestation:* Remote Attestation allows changes to a user's computer to be detected by the user and others, ensuring that private information is not sent to (or from) an unsecured computer. This is achieved by using a certificate verifying that the computer has not been tampered with and is therefore trusted.

These four features provide a secure path of work: a file is protected by Secure I/O as data is being entered in; Curtained Memory protects it when it is being worked on; Sealed Storage protects it while it is being stored; and Remote Attestation protects it from untrusted software when it is being worked on from other computers.

The Trusted Platform Module (TPM) is a hardware component, whose specifications are provided by TCG. The TPM acts as the *'root of trust'* for the TP and provides the functionality for two of the above features: Sealed Storage and Remote Attestation [5]. Along with providing these features, the TPM provides a mechanism that supervises the boot process of a computer to determine if the computer is in a 'trusted' state (that is, the OS and applications have not been tampered with by malicious programs). Determining the state is important, as TC Applications (typical applications written to take advantage of the security hardware) and the OS will only function correctly in a trusted state.

A fully functional TP also contains software configured to support and take advantage of these hardware components. This means the Operating System and applications (TC Applications) must be altered to support these extensions and use them.

2.2. Insider Threats to Banking and Finance Sector

Insiders represent a major threat to businesses. With the Banking and Finance Sector increasing at a rate of 1.2% every year [12] and given that it accounts for 20.4% of the US GDP [12], this industry is highly likely to be susceptible to major financial losses due to insiders.

According to the 2005 Tenth Annual CSI/FBI Computer Crime Survey [13] which surveys organisations from various different industries, 56% of respondents reported some form of insider attack or misuse, and the remaining 44% simply did not know if they had experienced inside attacks or not. The survey also found that insider activity occurred as often as outsider activity, accounting for approximately US$70 million in losses (or 54% of total losses) [13]. Previous surveys and research by other groups have found that the majority of crimes have been committed by insiders (62.9% according to [1]); with average financial losses by an insider attack amounting to US$2.7 million, as compared to $56,000 from an outsider. Admittedly, however, the trends from the surveys find the financial losses for both insider and outsider attacks to be decreasing.

A study completed by the National Threat Assessment Centre (NTAC) and the Computer Emergency Response Team at Carnegie Mellon University (CERT/CC) concluded seven common findings among insider threats to the Banking and Finance Industries [2]. These findings were based on studies of 26 previous insider attacks. The study also found that information on insider attack cases were limited since many companies do not report attacks, possibly due to fear of negative publicity or increased liability [2, 13]. These limitations make it difficult to establish estimates, and amend problems by finding solutions to common attacks. However, the seven findings made by the paper concluded that:

Finding 1: Most incidents required little technical sophistication.
Most insider attacks were not technically sophisticated or complex and exploited vulnerabilities in the business rules or organisation's policies rather than those in its information system or network [2]. Of the cases that did manipulate/attack the information systems, most used legitimate commands (87%), were completed by authorized users (78%) and exploited systemic vulnerabilities in applications, for example, business rule checks (70%). Furthermore, another 26% of attacks were completed on another person's account, which was gained access to via unattended computers, poor password practices or social engineering [2].

Finding 2: Perpetrators Planned their Actions
81% of attacks were planned in advance and in 85% of the cases other individuals, such as co-workers and family, had knowledge about the attacks and often also stood to gain from the attack. About one third of the attacks showed noticeable signs of planning, such as stealing administrative level passwords or copying information. Preparatory incident-related behaviours included planning discussions with competitors or co-conspirators and the construction of logic bombs.

Finding 3: Financial gain motivated most perpetrators.

Most insiders were motivated by financial gain (81%); however, other motives included revenge (23%), desire for respect (15%), dissatisfaction with the company (15%) and stealing of proprietary information (19%). In 27% of attacks, the insider had multiple motives.

Finding 4: Perpetrators did not share a common profile

Insiders came from varying different positions and experience. Insiders also ranged in age (18 – 59 years), included both male and female (42% female), and were of varying race and ethnic background. One commonality, however, was that most insiders were single (54% single, 31% married). Few of the insiders were considered difficult to manage (15%) or untrustworthy (4%), and only 26% of insiders had been previously reported due to concerning behaviour before the incident.

Finding 5: Incidents were detected by various methods and people

Attacks were detected by people both internal and external to the company, including customers, supervisors and IT staff. Most detection was discovered by non-security personnel (61%), and was generally done so through manual procedures (61%) such as customer complaints and manual account audits. After detection, 74% of the insiders were exposed through detection logs.

Finding 6: Victim organisations suffered financial loss

Nearly all the Banking and Finance organisations attacked by insiders incurred financial loss (91% suffered losses, 30% of the cases had losses in excess of US$0.5 million), or suffered losses to multiple aspects of the firm. Another 91% of the firms had at least one adverse impact on the organisation, such as damage to business operations (30%) and the organisation's reputation (26%). All the cases studied involved attacks on the organisation's data, with only 22% of these attacks affecting the security of the information systems. 78% of cases involved modification and/or deletion of data.

Finding 7: Perpetrators committed acts whilst on the job.

Most incidents occurred at the workplace and during normal business hours (83% from physically within the organisation's building, and 70% during normal working hours). Only 30% of the incidents occurred through remote access, with 57% of these attacks occurring from both workplace and home.

Based on these findings, the study proposed eleven proactive strategies that will help mitigate the threats posed by insiders [2]. These strategies are:

- Train staff about security and acceptable use policies.
- Ensure system access is disabled timely and completely following an employee termination.
- Establish formal grievance procedures as an outlet for insider complaints.
- Create a reporting process when a colleague notices or suspects concerning behaviour.
- Enforce comprehensive password policies and computer account management practices.
- Use configuration management practices to detect logic bombs and malicious code.

- Monitor system log activity.
- Establish and monitor procedural and technical controls for system administrators and privileged system functions.
- Provide layered security for remote access.
- Monitor compliance with backup procedures and testing recovery processes.
- Ensure procedures are in place to disable temporary employee and contractor access as thoroughly as those for permanent employees.

3. TRUSTED COMPUTING AND INSIDER THREATS

In this section we apply Trusted Computing to insider threats, and view if and how Trusted Computing can mitigate insider threats based on the eleven proactive strategies outlined by [2]. To be objective, we also discuss how Trusted Computing may even aid future insider attacks.

3.1. Strategies for Preventing Insider Attacks using Trusted Computing

Prevention of insider attacks aims to avert insider attacks from occurring in the first place. This means that mechanisms must be in place to deter or prevent common forms of insider attacks. The following presents three prevention strategies where TC may limit insider threats based on the findings of the NTAC/CERT study.

3.1.1. Use of configuration management practices to detect logic bombs and malicious code.

In several cases studied in [2], malicious software was inserted into the organization's information systems and was used to damage programs and data or steal information. This malicious software included logic bombs, keyloggers, viruses, and deliberate back-doors in the software created by member(s) of the organization.

One of the key TC objectives is data integrity [2]. Therefore TC contains mechanisms that check the integrity of both the Operating System and software to ensure that they have not been tampered with or that any malicious applications (such as logic bombs or key loggers) have been added to the environment.

Through the application of TC, these attacks can possibly be mitigated using two TC hardware components: "Secure I/O" and "Curtained Memory". Note that further study into each insider attack regarding malicious applications must be conducted before the effectiveness of each of these components can be assessed. With the limited information provided by the study, we only speculate that these components will help to protect against malicious software attacks.

Secure I/O can be used to prevent malicious software from tampering with, or recording data, which is coming directly from the keyboard or being displayed on the screen, such as key logging software and screen grabbers. One finding made by the CERT study found that 26% of insiders used others' accounts to commit attacks. Access to these accounts was primarily through poor password practices; however, stealing of passwords is another common approach.

Secure I/O ensures that the input and output of a computer are not tampered with or recorded by ensuring I/O data is fed directly through hardware and is also encrypted while in transit to prevent 'sniffing' on the transmission line [4]. Secure I/O can also protect against esoteric attacks, since it can determine whether a user is physically present by checking input from the secure hardware. This prevents a script or application from trying to impersonate a user [4].

Nine percent of reviewed cases found that insiders attacked software or used scripts to complete an attack. Depending on the script or type of attack, damage can be caused by accessing the memory location of a program and altering that program to function differently or cause a malfunction. Curtained Memory ensures that any programs (trusted and untrusted) cannot access the allocated memory of another program, thereby preventing access to runtime code and data being used by the program. Curtained memory prevents malicious applications such as Trojan horses, viruses or logic bombs from accessing other running applications, thereby preventing 'damage' to the software and data of that application. The advantages of Curtained Memory in preventing malicious applications maybe limited, however, depending on the implementation of the application by the insider. For example, if the logic bomb is a script for an application (such as a SQL Stored Procedure), since the script is run within the memory space of that application, Curtained Memory becomes redundant for this attack. Therefore, further information about each attack using malicious applications is required, and these prevention methods should only be used to supplement a more thorough monitoring procedure setup by the organization.

3.1.2. Data Protection from Stealing

Although not strictly a strategy outlined by the CERT paper, one of the key advantages that TC can provide is data protection [5]. Though this is primarily focused at preventing outsiders from accessing sensitive data or secrets, we can extend this to insider threats [2].

Data protection can help by preventing insiders from stealing data, such as Intellectual Property, which accounts for 19% of the cases studied in [2]. Sealed Storage on a TP can be configured to prevent data being transferred from an approved computer to another (trusted or untrusted). If it is transferred to an unapproved computer, the unapproved computer is unable to read the data since it does not hold the correct decryption key stored within the TPM [4]. This key is derived from various software and hardware components on the original computer, allowing the data to only be read on the computer it originated from [4]. This prevents insiders stealing the data, by transferring it onto another computer (or storing it on media to be read on another computer).

3.1.3. Providing security for Remote Access

Approximately one third of the cases studied [2] involved remote access. Several of these remote attacks involved stealing sensitive or IP data [2].

TC provides remote data protection (similar to data protection), which is achieved by limiting the accessibility of sensitive data to remote clients. This limits the ability of the insider to steal sensitive data while accessing remotely.

Data protection via remote access can firstly be achieved via TC during remote attestation. Remote attestation occurs between the TP client and server to verify that the user and platform are running in a valid, authorized and trusted state, and also that the system is running the require software. This ensures information is not being passed to an unauthorized and untrusted computer which may be used to steal the data. However, this assumes by default that the insider's computer is an untrusted machine and is not running the correct software environment. Once data is decrypted on a trusted computer, data protection as outlined in Section 3.1.2 applies, preventing the data from being transferred onto another unauthorized and untrusted computer.

TC can also help when considering layered security for remote systems. Layered security allows us limit the level of information accessibility based on the level of trust of the client platform, therefore is similar to a role-based security system. In the case of TC, layered security can be achieved during remote attestation when a computer's software state is being checked. The client must disclose an identity (TPM identity), that discloses various trusted verification details (although not necessarily the user's identity), and this allows the computer's software state to be categorized within a layer or role. Based on this state, when the remote client calls for data and the decryption key the remote server can only pass it a limited set of data. That is, the remote server can remove access to all sensitive data if the computer is in a relatively untrusted state, such that users cannot access sensitive data remotely. Any machines accessing remote data from outside the organization's network can therefore be considered untrustworthy, and passed only a limited set of data. This was recommended by the CERT paper.

Again this application of TC to provide security remote access is dependent on the actions of the insider in the first place; meaning insider attacks via remote access must be studied further to gain knowledge of how features like remote attestation can help. For example, if the insider attacks the organization remotely through simple valid commands, rather than stealing data, then TC and remote attestation cannot help, since these are considered, from the perspective of a TP, as legitimate commands. Furthermore, the advantages that mechanisms like remote attestation brings could act as a "double-edged sword", and aid insiders in performing attacks (See Section 3.5.1).

3.2. Strategies for Detecting Insider Attacks using Trusted Computing

Detection relates to the detection of insider threats either when the insider is performing the attack, or after the attack has been performed.

3.2.1. Monitoring System Log

As part of the TC Specification, a TP system contains a monitoring or reporting tool located in the TPM that is responsible for ensuring a proper boot sequence for the computer. This is not specifically designed to record user actions; rather this Section proposes an extension to the existing specification.

Using the TPM, it possible to maintain application and network level records based on the actions involving the TPM. The TPM is involved with any remote attestation (network level) and application execution (application level). Due to this functionality the TPM can provide application-level logging, which can provide detailed information regarding data access, modifications and deletions which can facilitate auditing and monitoring. At a minimum, and as outlined by the

CERT findings, the TPM can record the computer account (i.e. who is logged in), IP address and actions taken. Such logging can only occur if an extension to the TPM is made, since at present the TPM has no functionality to achieve this.

3.3. Limitations of Trusted Computing to Insider Attacks

The remaining strategies outlined by the study require the organisation to implement some procedures within its human resources department to mitigate and prepare for insider threats, which require little or no technology. For example, the creation of a "reporting process when a colleague notices or suspects concerning behaviour" is completely non-technical and requires the organisation to setup a process which is known and can be anonymously used by staff within the company's culture.

How company policies and procedures are implemented to mitigate insider threats is out of the scope of this paper, and we shall not expand further on this. We do, however, emphasise the importance of people over technology when dealing with insider threats.

3.4. Learning more about Insider Threats

Section 3.2 outlined possible applications of TC to prevent and detect insider threats, Section 3.3 indicated that even with TC, insider threats can by no means be averted; both these Sections have been derived from the research completed by CERT/NTAC in [2]. Our paper however, provides limited detail with regard to each of the insider attacks, and is primarily focussed at presenting general findings regarding insider attacks. As a result, this paper requires further information regarding each insider attack, to provide a more comprehensive use of TC which may mitigate insider threats.

The approach to determining where TC can be applied should start by categorising attacks in technical and non-technical approaches as well as legitimate and illegitimate means. TC generally cannot prevent most non-technical and legitimate attacks since TC is designed to prevent attacks from outsiders, which are typically attacks by illegitimate and computerised means. In fact the technology is designed to be simple and easy to use, as to not limit apparently legitimate users from completing their functions.

Research should focus on attacks through technical and illegitimate means, particularly attacks involving the use of computer networks and data protection. It must be noted that although most applications of TC will be derived from technical and illegitimate attacks, attacks of the opposing categories should still be studied since there are some situations, such as stealing data (which is considered non-technical), that TC can be used to prevent.

Once categorised, details should be drawn up regarding the specifics of the attack; for example, attacks involving logic bombs should be studied in depth to determine how the logic bomb was planted, how it was detonated and how it affected company data (e.g. deleted a software application).

Using the details derived from the previous step we can determine if attacks could have been averted through TC from the perspective of prevention and detection. That is, “could we have stopped it?”, and “how can we detect it if it is to happen again?” In applying TC, we must also be wary of future changes to the TC Specification. At present, TC is an extremely premature technology undergoing several changes, and at the time of writing the author has found several changes and conflicts regarding technologies and features outlined by previous versions of TC Specifications.

3.5. Trusted Computing Aiding Insider Attacks

To provide an objective view on TC and Insider Threats, we discuss situations where TC may also aid an insider complete an attack.

3.5.1. Increasing number of Attacks through Remote Access

One of the key advantages of TC is that greater trust, and therefore confidence, can be established between a remotely accessing client and server. That is, through remote attestation a remote server can have greater confidence in the client not being an attacker logging on an untrusted machine to perpetrate harm on the system, if their computer meets the characteristics and software state determined by the remote server. With increased confidence an organisation could possibly expose more sensitive operations and features remotely.

Such an infrastructure that remotely exposes more functionality, allows an insider a greater opportunity to undertake their attacks without “worrying about somebody watching over his shoulder” [2]. Therefore the proportion of insider attacks could increase significantly due to the increased availability to perform insider attacks from a remote location.

4. DISCUSSION

Trusted Computing aims to protect standard everyday client computers from external and outside threats, such as hackers and Trojan horses. By protecting a user’s machine and data, and by providing a mechanism to measure and transmit the trustworthiness of a client machine to a third party, TC is able to extend this protection to servers, such as the servers of an e-commerce business. This paper takes the features of TC, which are predominantly designed for protection from external threats, and applies them to insider threats, in order to determine if TC can aid the ‘fight’ against internal threats also.

To focus this paper we consider insider threats to the Banking and Finance Sector (although these findings can be applied to many industries), and use the eleven proactive strategies outlined in the CERT/NTAC study to evaluate the effectiveness of TC to insider threats in this sector. Effectiveness is determined by checking if features of TC can be applied to the proactive strategy, in such a way that it can meet the strategy totally or partially.

Using the proactive strategies as evaluation criteria, we find that TC has limited uses against insider threats, and is more suited to protecting against external threats than internal ones. From initial findings and research of the CERT/NTAC study, only three of the eleven criteria can be partially fulfilled from the features provided by TC. Furthermore, these three criteria require further research in each of the insider cases, to establish how TC can be more effectively applied.

Therefore, TC cannot alone prevent, detect or mitigate insider threats; however, it can provide the technology and features to supplement existing means of preventing insider threats.

Insider threats are generally caused through exploitation of vulnerabilities in the systems of an organisation [2]. These vulnerabilities maybe technical such as flaws in the software or networks, or maybe due to weak or lax policies that do not provide sufficient overlap of tasks or auditing and monitoring. According to Finding 1 of the CERT/NTAC study, in most cases it is the latter. Therefore the onus is on the organisation is to establish good procedures and practices through education and constant evaluation of existing systems, rather than apply technology (including TC), to limit insiders from attack the information systems. For example, the organisation must establish good practices with regard to passwords, such that insiders cannot easily guess passwords and allow insiders to perpetrate harm from another's account. TC is limited against preventing attacks of a non-technical nature, since these attacks require limited computer usage and typically use authorized, legitimate commands, which TC cannot (and should not, by design) prevent. For example, according to Finding 6 of the CERT/NTAC study, all insider cases affected data of the organisation. Although TC provides an ideal solution to protecting data, it cannot prevent an insider modifying data if they have proper authorization to do so, and are using trusted hardware and software to access that data.

As a further note, vulnerabilities of organisations vary significantly due to different experiences, backgrounds and industries. This means insiders of those organisations would attack each system differently. For example, a logic bomb can be implemented in different ways such as to exploit a flaw in the network of one company, and exploit a software flaw in another company. This example outlines that although TC can limit some categories of attacks (such as viruses); there are several cases within those categories that TC cannot stop. This emphasises again that each organisation should be responsible for discovering vulnerabilities with their own systems before it can be exploited, since no technology can provide protection against attacks on vulnerabilities that are not known in the first place.

In stating that TC is limited in several cases, we should not detract from the features and advantages that the technology can bring, particularly to data protection. Data security is a major problem in several organisations, particularly when insiders have legitimate access to the information, and steal it to pass to a competitor, which represents a considerable proportion of insider attacks (19% according to [2]). Furthermore, these features will be available 'pre-packaged' without further setup on the organisation's behalf, if TC becomes ubiquitous and accepted.

We must also be wary of the features that TC can provide that may aid insider attacks. In particular, remote access, which at present represents fewer than 30% of the cases studied, but will inevitably increase. As organisations' infrastructures develop further and as businesses expand worldwide, the need for flexibility within remote access becomes more significant. This gives an insider more opportunity to attack the organisations' systems. This is particularly true for the Banking and Finance industry. Therefore procedures and security must be provided to prevent these remote internal attacks. Further research into current remote access insider attacks will allow us to determine if TC can help in this respect.

TC should act as supplement to existing practices and procedures to prevent insider attacks. Although it can prevent only a few cases of insider threats, we consider this to be better than preventing nothing.

5. CONCLUSIONS

- The features of Trusted Computing provide limited protection with regard to preventing insider threats in the Banking and Finance Sector.
- The features of Trusted Computing are more suited to the protection of data, which represents 19% of insider attacks.
- Improvements to practices, procedures and discovery of vulnerabilities should be the main focus of organisations to stop and limit insider threats.
- Further in-depth research into the insider cases studied in the CERT/NTAC study should be undertaken in order to establish where Trusted Computing features can be more constructively applied to prevent common insider attacks.
- Trusted Computing has the potential to aid insider attacks, particularly through remote access.
- Trusted Computing should supplement existing practices and procedures to prevent insider attacks.

REFERENCES

[1] Shaw, E.D., K.G. Ruby, and J.M. Post, *The Insider Threat to Information Systems*. 1999, Political Psychology Associates Ltd.

[2] Randazzo, M.R., et al., *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*. 2004, CERT

National Threat Assessment Center.

[3] Wikipedia. *Threat*. 2005 [cited 3 October 2005]; Available from: http://en.wikipedia.org/wiki/Threat.

[4] Schoen, S., *Trusted Computing: Promise and Risk*. 2003.

[5] Pearson, S., *Trusted Computing Platforms: TCPA Technology in Context*. 2002: Prentice Hall PTR. 352.

[6] Safford, D., *The Need for TCPA*. 2002, IBM Research.

[7] Anderson, R.H. (1999): *Research and Development Initiatives Focused on Preventing, Detecting and Responding to Insider Misuse of Critical Defense Information Systems*. National Security Research Division.

[8] *Trusted Computing Group*. 2005 [cited; Available from: https://www.trustedcomputinggroup.org/home.

[9] Anderson, R. *'Trusted Computing' Frequently Asked Questions*. 2003 [cited; Available from: http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html.

[10] Pearson, S., *Trusted Computing Platforms, the next Security Solution*. 2002, Hewlett Packard.

[11] *Is Trusted Computing Friend or Foe?* 2005 [cited; Available from: http://www.tomshardware.com/howto/20051005/index.html.

[12] *High Growth Industry Profile*. 2005 [cited 6 October 2005]; Available from: http://www.doleta.gov/BRG/Indprof/Financial_profile.cfm.

[13] *Tenth Annual CSI/FBI Computer Crime Survey*. 2005, Computer Security Institute.