12-3-2012

The Mobile Execution Environment: A Secure and Non-Intrusive Approach to Implement a Bring You Own Device Policy for Laptops

Peter James
Edith Cowan University

Don Griffiths
Curtin University

DOI: 10.4225/75/57b55a80cd8db
10th Australian Information Security Management Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

THE MOBILE EXECUTION ENVIRONMENT: A SECURE AND NON-INTRUSIVE APPROACH TO IMPLEMENT A BRING YOUR OWN DEVICE POLICY FOR LAPTOPS

Peter James[1] and Don Griffiths[2]
[1]School of Computer and Security Science, Edith Cowan University
Perth, Western Australia
[2]School of Information Systems, Curtin Business School, Curtin University
Perth, Western Australia
[1]pjames@securesystems.com.au; [2]don.griffiths@cbs.curtin.edu.au

Abstract
Bring Your Own Device (BYOD) has become an established business practice, however the practice can increase an organisation's information security risks. The implementation of a BYOD policy for laptops must consider how the information security risks can be mitigated or managed. The selection of an appropriate secure laptop software configuration is an important part of the information security risk mitigation/management strategy. This paper considers how a secure laptop software configuration, the Mobile Execution Environment (MEE) can be used to minimise risks when a BYOD policy for laptops is implemented.
In this paper the security and business risks associated with the implementation of such a policy are identified and discussed before giving an overview of a range of laptop software configuration options suitable for the implementation of a secure BYOD policy. The design objectives and security requirements of the MEE are enumerated and its key features described. For each identified risk, the MEE features that mitigate/manage the risk are presented. The paper concludes by considering the type of work for which the MEE is most suited and also how the security features of the MEE can be enhanced when the MEE forms part of a secure portable execution and storage environment.

Keywords
BYOD, information security, portable execution environments, hardened operating system.

INTRODUCTION

The Bring Your Own Device (BYOD) approach has emerged through recognition that employees were using their own (more sophisticated) laptops to perform work, either in the workplace or at home. The recent accelerated adoption of the BYOD paradigm can also be attributed to an organisational need to both introduce human resource (HR) polices that attract and retain talented employees, and contribute to the containment of information technology (IT) infrastructure costs. This paper will consider the implementation of a secure BYOD policy for laptops using a simple, yet secure laptop software configuration called the Mobile Execution Environment (MEE).

The purchase of sophisticated and technologically advanced laptops for home and private use has created a workforce that has high expectations of the capabilities of the laptops furnished by their employer. Accordingly, the requirement to furnish and maintain laptops to a growing percentage of employees who need a laptop, and to refresh the laptop fleet on a regular basis, has increased organisational IT costs. From a HR and financial perspective (typically key organisational business drivers), the introduction of a BYOD policy for laptops has a number of advantages (Paul, 2009; PWC, 2012) as it:

- ***Empowers employees:*** Selecting your own laptop (and operating system) can instil a sense of loyalty to the organisation and hence contribute to ownership of corporate objectives and strategy.
- ***Allows for flexibility:*** An employee has the same platform for both professional and private computing potentially enabling work to be more readily performed (as required) outside of the office. For mobile workers and teleworkers a single platform for both professional and private activities can contribute to the concept of a more agile workforce.

- ***Delivers infrastructure cost savings:*** Often the BYOD policy is implemented through an allowance which the employee can supplement if desired, possibly resulting in the purchase and use of a more superior and powerful laptop than would otherwise be used if the employer furnished the laptop. As the user owns the laptop he/she is more inclined to keep the laptop in a good state of repair resulting in lower costs for an organisation's break/fix support team. Also the "technology savvy" employee is more likely to upgrade to a new more powerful model using their own money more often than the typical three year replacement cycle of most organisations.

These perceived HR and financial advantages are accelerating the transition to BYOD particularly where an organisation is conducting projects using activity based working and/or is allowing staff to telework. There are, however, a number of security and business risks that need to be considered before a BYOD policy for laptops is introduced. The selection of a secure laptop software configuration can mitigate or manage some of these risks. In this paper a secure laptop software configuration is modelled and presented as consisting of the following three components:

1. ***Professional computing environment:*** The set of software applications provided by the employer to allow an employee to conduct work. The professional computing environment executes within the computing delivery software.
2. ***Computing delivery software:*** This software facilitates the execution of the professional computing environment and separates it from personal/private software; examples of computing delivery software are a remote desktop client, a browser or a virtual machine. The computing delivery software executes on the platform software.
3. ***Platform software:*** The software that manages and makes available the capabilities of the laptop hardware; examples of platform software are operating systems and type 1 hypervisors.

An appropriate selection of computing delivery software and platform software can provide the basis for a secure laptop software configuration. In this paper the MEE (a secure laptop software configuration) is presented and discussed as a suitable laptop software configuration to counter a set of identified security and business risks associated with implementing a BYOD policy for laptops. To enable the reader to appreciate the laptop software configurations that can be selected a number of the popular computing delivery and platform software components are outlined. The design of the MEE is discussed and an assessment of how the MEE security features mitigate or manage the identified security and business risks is given. The style and type of work most suited to the use of the MEE is outlined, and finally limitations of the MEE are highlighted and the use of a secure portable execution and storage environment that addresses the limitations is outlined.

SECURITY AND BUSINESS RISKS

A risk assessment should be performed before the implementation of any new IT initiative that involves the processing of sensitive corporate data, particularly if the processing is to occur outside of the boundary enforced by the organisation's security policy. The introduction of a BYOD policy for laptops without full consideration of the information security risks will inevitably result in breaches of confidentiality of sensitive corporate information (Markelj and Bernik, 2012). High speed broadband, coupled with the secure laptop software configurations available, is allowing organisations to implement secure remote access architectures that achieve an appropriate level of information security when employee owned laptops are used to process sensitive corporate data.

The following set of risks has been identified as those that need to be considered before the implementation of a BYOD policy for laptops. Each risk is presented without any consideration given to the laptop software configuration that can be used to mitigate or manage the risk. For each risk its impact on confidentiality, integrity and availability is identified:

Corporate Data Becomes Resident on the Laptop: When an employee owned laptop is used for both professional and private purposes it is possible that the laptop will have corporate data stored on it. This corporate data may be intentionally stored or inadvertently stored due to the actions of the user or the standard processing actions of the laptop software configuration (Jones et al, 2008). As the laptop is employee owned it will be used for private and social activities where it could be vulnerable to loss or theft, possibly resulting in unauthorised access to corporate data. Also a laptop fault may require warranty/service work to be performed by the supplier, possibly resulting in the laptop supplier having unauthorised access to any sensitive corporate data residing on the laptop and allowing for the possibility of the supplier to embed malicious software. This risk could result in a breach of data confidentiality and/or system integrity.

Personal Laptop Use Affects the Integrity of the Professional Computing Environment and Data: An employer furnished laptop is provided to an employee on the basis that it is used predominately for professional purposes, with possibly some private use. However, a BYOD laptop policy will result in the laptop being used for a range of personal activities as the employee owns the laptop. Such personal activities may result in the installation of software packages and data that could affect the integrity of the professional computing environment and/or corporate data stored on the laptop. Software and data integrity issues including damage to configuration settings and corruption of software and data could also result in the laptop not being available to perform work, impacting productivity. This risk will impact software and data integrity, and could impact laptop availability.

Laptop Not Available for Work: When a laptop is used for private purposes it may be subject to handling that impacts its physical and/or logical capabilities resulting in damage that prevents the laptop being available for professional work. Also an employee owned laptop is unlikely to be locked (i.e. prevented from installing application software) and/or configured to run with minimum user privileges. An unlocked and/or privilege high laptop may therefore allow software to be installed for private use that may conflict with, and/or prevent the operation of, the professional computing environment resulting in the laptop not being available for work. Further, if the employer provides a break/fix support capability yet allows employees to select any laptop they desire then there may be delays with the support team addressing laptop issues due to the team's inability to have the necessary skills and knowledge in all the different laptops and OS' that have been selected. Similarly, allowing an employee to select any laptop/OS may result in a selection that is functionally new to the user causing both a learning curve that impacts productivity and a lack of technical experience to resolve laptop issues when they occur. Finally, as identified in the risk above, if the integrity of the professional computing environment is compromised through private use the laptop may not be available for work. This risk will impact laptop availability.

Malicious Software (Malware) Becomes Resident on the Laptop: Malware can be introduced through numerous sources; some of the most popular sources include a browser, email, portable storage media and application software (Symantec, 2012; Sophos 2012). A laptop used for private and professional use could be more susceptible to malware (due to the private use) than a locked and/or low privilege employer supplied laptop. Although anti-virus and anti-malware software is now a standard feature of a laptop purchase, increasingly such software is unable to keep pace with the complexity and growing number of malware/viruses. Malware allows cyber attacks to be launched. Such attacks can result in the loss of sensitive corporate data. This risk could result in a breach of data confidentiality, impact software and data integrity, and impact laptop availability.

Private Use Affects Productivity: As a user's personal application software suite will be installed on a BYOD laptop there may be the temptation to use the laptop for non-work activities (during a working day), resulting in reduced productivity from the employee. Although this risk is not a direct security risk, this business risk could contribute to the security risks (identified above) occurring.

The computing delivery and platform software options identified below are designed to counter many of the aforementioned risks. This paper considers the MEE as a combined implementation of a professional computing environment, computing delivery and platform software that addresses all the identified security and business risks in a non-intrusive way (i.e. the laptop software configuration that is provided by the MEE neither intrudes upon nor interferes with the personal/private software).

LAPTOP SOFTWARE CONFIGURATION OPTIONS

As identified above, in this paper the laptop software configuration is defined as a set of software components which are modelled diagrammatically in Figure 1.

The professional computing environment is the set of software applications provided by the employer to enable the employee to conduct work. The applications may consist of commercial off the shelf packages and/or bespoke software.

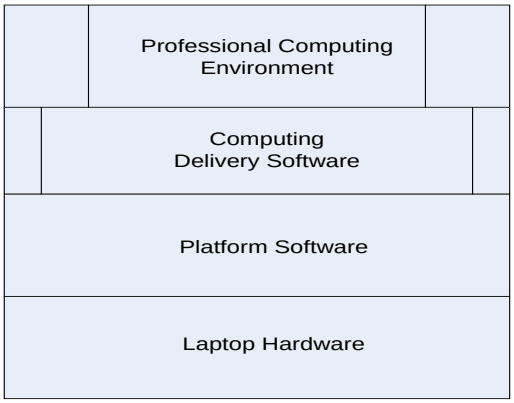

Figure 1: Conceptual Model of Software Components forming the Laptop Software Configuration

Computing delivery software is based upon thin client (3Com, 1999), virtualisation (VMware, 2006) or zero client (David, 2002) technology and the most popular examples include:

- ***Browser:*** A browser is designed to allow the retrieval, presentation and creation of information across a network and therefore, depending upon the work to be performed, can provide an ideal computing delivery model to access an application (that forms part of a professional computing environment) located on a remote server.
- ***Remote Desktop:*** The standard terminal server application provided with most operating systems is used to connect to a corporate server to access the professional computing environment. Like the browser all processing is performed remotely and therefore no corporate applications have to be installed on the laptop. Remote desktop has traditionally been a popular delivery model for remote computing.
- ***Desktop Virtualisation:*** Virtualisation can be achieved either through installing a virtual machine (VMware, 2006) containing an image of the 'professional computing environment' on the laptop, or alternatively installing a virtual machine client (Rouse, 2011a) that connects to a corporate server that is hosting the virtual machine containing an image of the 'professional computing environment'.
- ***Application Hosting or Streaming:*** Application hosting software (Citrix, 2011) makes an application (in the professional computing environment) available on the laptop but the application is actually installed in a virtual machine that is either downloaded from a server or executed directly on the server. Conversely, application streaming software (Citrix, 2011; Rouse 2011b) has an application installed on a server which is streamed to the laptop in full or in part as required. In both cases the laptop user is unaware the application is not installed locally.

The above computing delivery software options allow the laptop to act either as a terminal to access a server over a network or as a networked workstation, if the network is the Internet then a secure protocol (e.g. virtual private network or hyper text transfer protocol secure) would be used to protect data transmission. Each computing delivery option has advantages and disadvantages and therefore selection will depend upon a number of different factors including, bandwidth of communication technology, information security, the type of work performed and the employer's software, hardware, communications and technical support infrastructure. To enable any of the above computing delivery options to be implemented one of the following platform software options could be utilised:

- ***Laptop Operating System (OS):*** The selected computing delivery model can be installed on to the laptop OS.
- ***Type 1 Hypervisor:*** A type 1 hypervisor (VirtualComputer, 2012) runs directly on the laptop hardware (instead of the laptop OS). The type 1 hypervisor acts as a virtual machine manager, i.e. it allows a number of virtual machine images to execute. A hypervisor as the platform software replaces the laptop OS as the laptop bootable software. The user can then utilise private or professional virtual machine images as required.

- ***Dual Boot:*** The dual boot option requires the installation of two OS' (each in a separate partition) on the laptop HDD; one for professional use and the other for private use. When the laptop is powered on the user selects which OS to load and execute.
- ***Secure Portable Execution Environment (secure PEE):*** A secure PEE (James, 2008) is an execution environment (e.g. a highly portable OS and set of applications) contained on an external attachable device (e.g. a USB thumb drive). When the external attachable device is plugged into the laptop and is set as the first boot device it loads the secure PEE. The secure PEE requires no access to the laptop HDD and uses only the processor and memory of the laptop. Depending upon how the secure PEE is packaged it can be considered to be platform software or a combined platform and computing delivery software.

Like the computing delivery software options the selection of the platform software will be dependent upon a number of factors. The MEE is an example of a secure PEE that can be packaged with any of the computing delivery software options (identified above) to provide a secure laptop software configuration that can be uploaded from portable storage media onto a laptop.

The dual boot platform software option is similar to the portable PEE option, the difference being that the computing delivery software and professional computing environment is installed on the laptop HDD together with the private operating system and applications, albeit each professional/private environment in a separate partition. Hence, the dual boot option makes the professional computing environment accessible and therefore potentially vulnerable when the private operating system and applications are executing.

A key difference between the MEE and the other single operating system and type 1 hypervisor platform software options is that only software applications forming part of the MEE can be utilised whilst the MEE is executing, access to private data/applications on the laptop HDD is not possible. The MEE effectively separates private from professional computing whilst the MEE is executing.

MEE – FEATURES AND FUNCTIONALITY

The MEE is part of an on-going research project to develop secure portable execution and storage environment (secure PESE) devices (James, 2008) to support secure remote computing. The goal of the MEE is to provide a simple hardened secure PEE that can be executed from a secure PESE device. A detailed description of the design of the MEE is given in James and Griffiths (2012).

An outcome from the research project is that the MEE can be imaged onto a standard USB thumb drive and used as a laptop software configuration to support a secure BYOD policy for laptops. As a laptop software configuration, the MEE consists of the professional computing environment, computing delivery software and platform software that is up loaded from a thumb drive onto a laptop and executed.

MEE Project Business and Operational Objectives

A project development goal was to build the MEE from freely available open software. The following business and operational objectives were defined to direct both the selection of open software and the development of the MEE:

1. Enable the rapid development of the MEE.
2. Be bootable from a USB storage device.
3. Ability to run on the widest variety of laptops without additional driver installation.
4. Support a wide range of application software.
5. Have acceptable licensing conditions.
6. Be easy to use.
7. Provide the basis to separate the professional computing environment from the personal/private software applications.

Following a comprehensive review of a number of open software operating systems the 'live CD' version of Ubuntu (Ubuntu, 2012), the commercially supported Linux distribution was selected. Table 1 presents the rationale for the selection of Ubuntu by showing conformance to the business and operational objectivess of the MEE project.

Table 1: Rationale for Selection of Ubuntu

Business/Operational Objective	Ubuntu Based MEE
Enable the rapid development of MEE.	Ubuntu is a commercially supported Linux distribution that is professionally packaged and structured such that the MEE could be constructed to a tight development schedule.
Be bootable from a USB storage device.	The 'live CD' version of Ubuntu can be ported to, and executed from, portable USB attachable storage media.
Ability to run on the widest variety of laptops without additional driver installation.	Ubuntu is considered to be one of the most portable Linux distributions (Lifehacker, 2009).
Support a wide range of application software.	Due to its commercial support Ubuntu has one of the widest ranges of application software (Vaughan-Nichols, 2012).
Acceptable licensing conditions.	The Linux Gnu licence allows a distribution to be configured for commercial use provided the kernel is not changed.
Easy to use.	Ubuntu provides an easy to use and configurable user interface.
Provide the basis to separate the professional computing environment from the personal/private software applications.	As Ubuntu can be tailored, configured and then imaged onto a portable USB storage device it can be booted to provide a professional computing environment that is separate to the personal/private software held on the laptop HDD.

MEE Security Requirements

The MEE was developed as part of a secure PESE device project which was designed to satisfy the following teleworking/remote working security model attributes (James, 2011):

- Protect data transmitted over a network.
- Ensure only authorised access to the teleworker's computing environment is achieved.
- Protect the confidentiality of data processed by the teleworker.
- Prevent temporary data and data remnants (created through data processing) being accessed by an unauthorised user.
- Protect the integrity of the teleworker's computing environment and stored data from malicious software and/or user induced damage.
- Protect the confidentiality and integrity of any software and data stored on a portable storage device.
- Ensure the availability of the teleworker's computing environment.

Using the teleworking security model attributes as a basis the project defined and allocated the following set of security requirements to the MEE:

1. Prevent the storage of corporate data on laptop HDD.
2. Prevent the user from installing software.
3. Prevent the user from performing privileged/administrator actions.
4. Prevent the laptop HDD being accessed.
5. Limit the introduction of malware.

Certain security requirements (e.g. "prevent the user from installing software" and "prevent the laptop HDD being accessed") can be considered to conflict with the BYOD HR objective of empowering and trusting users. However, satisfying these security requirements in the MEE provides a secure and elegant approach to separating professional and personal computing activities on the one laptop. As outlined in a later section of this paper, the MEE may not be appropriate for all BYOD laptop users but for a particular category of worker the MEE provides a secure solution to implement a BYOD policy for laptops.

MEE Design

An MEE development goal was to construct the MEE with minimal or no software changes, and in particular avoid Ubuntu kernel changes. This development goal was achieved through making configuration changes to the desktop manager, specific application configuration settings and operating system configuration changes; no kernel changes were necessary. The key features of the MEE that enable it to be a secure laptop software configuration are:

Simple Desktop: In its most basic form, the MEE has only a browser and remote terminal client available; all other applications have been removed/disabled. Upon booting the MEE the user is presented with either the simple desktop interface or a default application. From the desktop the user can only access applications that are packaged with the MEE; no command line access is possible.

Single Unprivileged User: The MEE has a single user. The user has no privileges, other than those required to configure the MEE to print and access a network. The user is unable to switch to a more privileged role.

No Access to Laptop HDD: A user of the MEE is neither able to access the laptop HDD nor mount a volume/partition on the HDD.

Data Storage: The thumb drive containing the MEE provides a volume/partition for user data storage and also a separate partition to keep application settings and virtual memory (N.B. it is possible to select to not store virtual memory on the thumb drive as continuous writes to the drive can reduce the life of the flash storage). The user data partition is configured as the first partition on the thumb drive and formatted as a FAT-32 file system, allowing the user to access the data partition when the thumb drive is plugged into a PC running Microsoft Windows.

Secure Browser: The MEE browser has been configured to reduce the opportunities for malware to exploit the browser. A detailed description of the design of the secure browser is given in Griffiths and James (2010).

Utilising the Capabilities of a Secure PESE Device: The MEE is designed to exploit the security features of the Secure Systems' Mini Silicon Data Vault (Secure Systems, 2012); a secure PESE device. In particular, the MEE is designed to utilise the SDV's secure partitioning, authentication and encryption capabilities (James and Griffiths, 2012). The utilisation of the SDV features by the MEE provides a secure remote computing solution to protect highly sensitive corporate data when it is processed outside the secure corporate environment. When installed on a secure PESE device the MEE writes all temporary data to the device and the MEE is protected by a secure partition, strong authentication and encryption. The MEE as part of a secure PESE solution is considered later in this paper.

Table 2 presents a requirements conformance matrix, mapping the MEE features developed to address the MEE security requirements.

Table 2: Requirements Conformance Matrix

MEE Security Requirement	MEE Feature That Satisfies Requirement.
Prevent the storage of corporate data on laptop HDD.	No access to the laptop HDD is possible.
Prevent the user from installing software.	Simple locked down desktop and single unprivileged user prevents the installation of software.
Prevent the user from performing privileged/administrator actions.	Single unprivileged user.
Prevent the laptop HDD being accessed.	No access to the laptop HDD is possible.
Limit the introduction of malware.	Simple locked down desktop and single unprivileged user and secure browser limits the opportunity for malware to attack or become embedded in the MEE.

THE MEE AS A SECURE LAPTOP SOFTWARE CONFIGURATION

The MEE is a laptop software configuration that enables the packaging of the professional computing environment, computing delivery software and platform software into a single separate loadable execution environment. Ubuntu provides the platform software component of the MEE. In its simplest configuration the MEE provides a browser and remote desktop as computing delivery software, although any computing delivery software that can execute on Ubuntu can be installed. The professional computing environment is either installed as part of the MEE or installed on a remote server and accessed remotely through the MEE computing delivery software. The MEE provides a solution to achieve a secure BYOD laptop policy as it mitigates/manages the identified BYOD security and business risks, as follows:

Corporate Data Becomes Resident on the Laptop: The MEE provides a completely separate execution environment for professional work and the processing of corporate data. The MEE prevents access to the laptop HDD and therefore it is not possible for sensitive corporate data to become stored on the laptop HDD; only the laptop processor and memory are used by the MEE. The laptop can be used for private and personal activities without concern that corporate data may be resident on the laptop. If there is a need to store corporate data and organisational policy allows for external storage of data then the data can be stored on the user data partition of the MEE thumb drive or alternatively on another external storage device.

Personal Laptop Use Affects the Integrity of the Professional Computing Environment and Data: As the MEE provides the professional computing in a separate bootable execution environment, personal use of the laptop will not affect its integrity. The MEE thumb drive will not be plugged into the laptop when the laptop is being used for personal computing. The separation of personal and professional computing activities on a laptop limits the possibility of deliberate or accidental damage to the professional computing environment.

Laptop Not Available for Work: Lack of laptop availability will not prevent work being performed as the MEE thumb drive can be booted and used from any available PC or laptop.

Malware Becomes Resident on the Laptop: Any malicious software resident on the laptop HDD cannot attack the MEE as the MEE prevents access to the laptop HDD; the MEE is a completely separate system that boots and loads from a thumb drive. The MEE's small set of fixed applications and the lack of a privileged user capability reduce the possibility that any malware introduced during professional work can successfully attack or become embedded in the MEE.

Private Use Affects Productivity: The MEE provides a separate execution environment and only includes applications that form the professional computing environment. When the MEE is executing the user is not able to access and use private application software.

CONCLUSION

In this paper the MEE has been proposed as a secure laptop software configuration to support the implementation of a secure BYOD policy for laptops. However the MEE should only be considered to be part of a security solution when implementing such a policy. Appropriate security policy and procedures, training and awareness, network auditing and need to know access controls should all be considered as an integral part of a BYOD policy (Valli, 2012).

The use of the MEE as a laptop software configuration for a BYOD policy is particularly suited to teleworkers involved in transaction oriented processing, e.g. remotely based customer support or back office business functions. Whilst transaction oriented processing may not require highly qualified knowledge workers the increasingly sophisticated nature of the work is necessitating that policies like BYOD and teleworking are implemented to attract and retain appropriately skilled personnel. Transaction oriented processing typically involves a continuous stream of activities that are performed consecutively. Each activity requires the worker to be completely focussed on the activity until its conclusion. Transaction oriented processing is characterised by a fixed set of repetitive activities and hence requires a professional computing environment consisting of a (small) suite of dedicated software applications. There should be no requirement for a laptop software configuration, used for transaction oriented processing, to be changed by the worker nor should access to personal software applications be necessary as the worker is likely to be processing a continuous stream of transactions. The MEE therefore provides a suitable laptop software configuration for remotely based transaction oriented processing as it provides a dedicated professional computing environment that is separated from personal software applications. The provision of the MEE on a thumb drive provides a solution for organisations where highly sensitive data is not processed but where security of data is still an important consideration.

As a secure laptop software configuration the MEE:

1. Prevents sensitive data residing on a laptop HDD.
2. Prevents personal activities affecting the integrity of the professional computing environment.
3. Allows work to be performed if the laptop is not available.
4. Limits the opportunity for any malware to become embedded on the laptop HDD;
5. Limits the occurrence of private activities whilst work is being conducted.

These five capabilities of the MEE provide a secure and non-intrusive solution for the implementation of a BYOD laptop policy. The MEE does, however, have limitations which include:

1. No mechanism to protect the integrity of the MEE on a thumb drive.
2. No authentication mechanism or access controls to prevent unauthorised access and use.
3. No encryption so the MEE and any data stored on the thumb drive can be read and copied.

These limitations are a consequence of installing the MEE on a standard thumb drive. The MEE was developed as part of a secure PESE project. A secure PESE provides security functionality that complements, and integrates with the MEE. When used with a secure PESE, the MEE is protected by a secure partition, access controls, authentication and encryption; these secure PESE security mechanisms address the above limitations. Many of the features of a secure PESE are not necessary unless highly sensitive data is being processed.

REFERENCES

3Com (1999). The Net Impact of Thin Clients – Technical Brief, 3Com Corporation, September 1999, Retrieved July 2012 from URL: http://www.pulsewan.com/data101/thin_client_basics.htm.

David, B. (2002). Thin Client Benefits, Newburn Consulting, Version 1b, March 2002, Retrieved July 2002 from URL: http://www.thinclient.net/pdf/Thin_Client_Benefits_Paper.pdf.

Griffiths, D. and James, P. (2010). Fireguard – A Secure Browser with Reduced Forensic Footprint, Journal of Network Forensics, Vol. 2, Issue 2, Summer 2010.

James, P. (2008). Secure Portable Execution Environments: A Review of Available Technologies, *6th Australian Information Security Conference*, December 2008, Edith Cowan University, Perth.

James, P. (2011). Are Existing Security Models Suitable for Teleworking?, *9th Australian Information Security Conference*, December 2011, Edith Cowan University, Perth.

James, P and Griffiths, D. (2012). A Hardened Mobile Execution Environment to Enable Secure Remote Working. Unpublished.

Jones, A., Valli, C., Dardick, G., & Sutherland, I. (2008). The 2007 Analysis of Information Remaining on Disks offered for sale on the second hand market. Journal of Digital Forensics, Security and Law, Vol. 3, Issue 1, 2008.

Lifehacker, (2009). Five Best Live CDs, Lifehacker, February 2009, Retrieved July 2012 from http://lifehacker.com/5157811/five-best-live-cds.

Markelj, B. and I. Bernik (2012). Mobile Devices and Corporate Data Security, Journal of Education and Information Technologies, Vol. 6, Issue 1, 2012.

Paul, A. (2009). Bring Your Own Computer Policies, The Generation V, November 2009, URL: http://www.thegenerationv.com/2009/11/bring-your-own-computer-byoc-policies.html.

PwC (2012). Bring your own device: Agility through consistent delivery, Price Waterhouse Coopers LLP 2012, URL: http://www.pwc.com/en_US/us/increasing-it-effectiveness/assets/byod-1-25-2012.pdf.

Rouse, M. (2011). Client-based Virtual Machine, SearchVirtualDesktop TechTarget, November 2011, Retrieved July 2012 from http://searchvirtualdesktop.techtarget.com/definition/Client-Based-Virtual-Machine.

Rouse, M. (2011). Application Virtualisation, SearchVirtualDesktop TechTarget, November 2011, Retrieved July 2012 from http://searchvirtualdesktop.techtarget.com/definition/app-virtualization.

Secure Systems, (2012). Mini Silicon Data Vault, 2012, Retrieved July 2012 from URL: http://www.securesystems.com.au/secure-systems-mini-sdv.html.

Symantec, (2012). Internet Security Report 2011 Trends, Symantec Corporation, April 2012, URL: http://www.symantec.com/threatreport/

Sophos, (2012). Sophos Threat Report 2012 – Seeing the Threats Through the Hype, Sophos Ltd. Retrieved July 2012 from URL: http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx.

Ubuntu, (2012). Ubuntu Documentation - LiveCD, Canonical Limited, Retrieved July 2012 from URL: https://help.ubuntu.com/community/LiveCD.

Valli, C. (2012). Bring Your Own Disaster, Secau – Security Research Centre seminar, Edith Cowan University, Joondalup, WA, 22nd March 2012.

Vaughan-Nichols, S. (2012). Ubuntu 12.04 vs. Windows 8: Five points of comparison, ZDNet, May 2012, Retrieved July 2012 from URL: http://www.zdnet.com/blog/open-source/ubuntu-12-04-vs-windows-8-five-points-of-comparison/10900.

VMware, (2006). Virtualization Overview, VMware White Paper, VMware Inc. Retrieved July 2012 from URL: http://www.vmware.com/pdf/virtualization.pdf

VirtualComputer, (2012). Type-1 vs. Type-2 Client Hypervisor, Retrieved July 2012 from http://www.virtualcomputer.com/type-1-vs-type-2-hypervisor.