Pandora's Email Box? An Exploratory Study of Web-Based Email Forgery Detection and Validation.

Richard Boddington
School of IT, Murdoch University
Perth, WA 6150, Australia.
r.boddington@murdoch.edu.au
Tel: +61 893602801 Fax: +61 89360 2941

Grant Boxall
School of IT, Murdoch University
Perth, WA 6150, Australia.
gwunta@hotmail.com
Tel: +61 893602801 Fax: +61 89360 2941

Jeremy Ardley
Dalton Pty Ltd
Forensic Information Analysts
jeremy@ardley.org
Tel: +61 8 6280 0008

ABSTRACT

Web based email systems may be a source of pristine digital evidence because of the perceived difficulty of client tampering with messages stored inside the email account. We demonstrate that such assumption is wrong in the case of Windows Live Hotmail[®1]. Windows Live Mail[®1] synchronises message on client-side computers with the Hotmail[®] server, benefiting users wishing to synchronise their email accounts and personal devices. However, this synchronisation opens an exploit for wrongdoers to tamper with existing email messages and attachments as well as facilitating the insertion of fabricated messages. The exploit process enables persistent storage of tampered and fabricated messages on the Hotmail[®1] server. The exploitation favours both account owners and wrongdoers who gain unauthorised access of others' accounts. Even if tampering were suspected, we anticipate some difficulties in validating messages to determine their reliability and relevance. We predict, with trepidation, that the exploit process will become commonplace and pose greater challenges to the cyber forensics examiner and

---

[1] Hotmail[®], Windows Live Hotmail[®] and Windows Live Mail[®] are the registered trademarks of Windows Corporation.

legal practitioner during investigations and legal proceedings. Regrettably, the exploit complements the existing arsenal of tools for email forgery. More ominously, it provides opportunity for traceless injection of illicit material/malware onto any machine synchronised with the Hotmail® account.

Keywords Digital evidence, evidence validation, Windows Live Mail®, email tampering, web-based email exploitation.

1. INTRODUCTION

Covert attacks to gain control over other users' web-based email accounts for a range of illegal and unethical purposes is not a new or uncommon phenomenon (Florencio & Herley, 2007). Use of email systems to promulgate the spread of malicious software capable of breaching privacy, disabling individuals' computers and networks, and a myriad of scams, are unwelcome but well-entrenched phenomena (Sunner, 2005). Bogus email messages created with little technical skill can override email identity checking process, providing anonymity for the miscreants and when delivered can have disastrous outcomes for victims of such ploys (Levi & Koc, 2011). A significant vulnerability is poor password security measures used by email providers, aggravated by weak user passwords, which in turn facilitates, if not actually encourages exploitation of this essential communications medium (Craddock, 2011; Preibusch & Bonneau, 2010).

The ability to access others' email accounts allows intruders to create, delete, transmit, move and copy messages but little else. An intruder, or account holder wishing to modify an existing email message for some improper purpose may be able to export messages, modify them but then find it impossible to reinsert the emails into web-based accounts. It was considered difficult, if not impossible, to modify web-based email messages stored on vendors' servers without direct access to the server by means other than the web page (Ardley, 2011).

We became aware of a current criminal case[2] during which the defendant suggested the possibility of the complainant tampering with messages received by the complainant from the defendant in a Hotmail® web-based email account. The suggestion was this was done as a means to implicate the defendant in a criminal activity. Initially, the proposition seemed improbable because of perceived technical difficulties in editing message content and was dismissed by the prosecution team of cyber forensics experts as being technically beyond the ability of the average home computer user without advanced programming skills. Nevertheless, the defence, forensics team considered it was possible with an unknown but probably low level of difficulty, and further research would help to identify and test simple processes allowing authorised and unauthorised tampering of Hotmail® messages to succeed.

---

[2] While the case is *sub judice* we are not permitted to identify the court or parties involved.

In this paper, we show that Windows Live Hotmail® messages can be modified with a modicum of skill and that simple processes do exist to overcome export/import issues as well as obliterating traces of modification used in these processes. We observed that it was a relatively simple process to access and modify Hotmail® messages by a non-technical forger using Windows Live Mail® (WLM); an unannounced vulnerability we contend existed since 2007. The processes we tested confirmed that it in some instances, it was possible to produce near perfect forgeries. We will demonstrate that a Windows Live Hotmail® account can be synchronised with WLM by the account holder but unlike the Hotmail® account, WLM can be used to alter existing messages and insert fabricated messages into the Hotmail® account stored on the Hotmail® server.

Reliance on Hotmail® messages as unadulterated digital evidence is questionable, and confirmation of the WLM exploit means that some form of validation is required. If tampering evidence on the forger's computer were purged, it is likely that the Hotmail® server would provide the only possible means to detect and verify message tampering and fabrication. However, reliance on Internet Service Providers to provide full historical records of their client's Hotmail® communications may prove disappointing to law enforcement agencies seeking confirmation of tampering and fabrication because of insufficient message logging. We note, for example that in contrast to its European and American counterparts, Australia does not require Internet Service Providers to maintain detailed logs of its users' Internet activities including email messaging. Australia does not presently possess powerful legislative standards such as the European Telecommunications Standards Institute requiring service providers to retain significant sets of data on their clients that assist law enforcement in investigating crime and seeking exculpatory evidence to eliminate the innocent from their investigations (Attorney-General's Department, 2010).

Australia's Telecommunications (Interception and Access) Act 1979 permits service providers to provide telecommunications data, including email data, to law enforcement agencies and telecommunications data and related information kept for billing and other business purposes (Attorney-General's Department, 2010). Australian federal and state government laws do not mandate service providers to retain Internet data (e.g. SMTP records or mail client access other than authentication) and email providers are unlikely to record email logs for any length of time or hold sufficient data to validate suspect email messages. This apparent lack of data available from service provider logs to assist examination was further incentive to undertake our study to see what other evidence of tampering the WLM exploit might provide.

Notwithstanding legislation empowering law enforcement agencies to obtain email records from email vendors in criminal investigations, it is not always so straightforward in civil cases. In a 2008 civil trial (Alexander, 2008) a

Mississippi district court upheld the defendants' right to seek the quashing of a court order by the other party seeking detail of the email accounts of the defendants' employees. The court ruled that the relevant statute the third party, the email vendor, may not disclose such information in civil matters (Alexander, 2008).

We foresee that evidence obtained by forensics examiners from Windows Live Hotmail® server logs that hitherto provided authoritative views on message antecedents and attributes might no longer be relied upon *per se*. Although email communications exploitation through a broad range of attacks has been present since its creation, we anticipate that WLM, while offering many benefits to its users, may be one of a number of applications inadvertently nurturing email forgery in a variety of forms.

Although at the time of writing were unable to find any scientific literature on the WLM vulnerability or other exploits, we thought it prudent to publish and make aware those responsible for law enforcement and the courts that the integrity of web-based emails should not be taken at face value. We suggest that some means of validating email messages be applied when circumstances dictate or ideally, as a matter of standard forensics practice. We have also engaged with Microsoft via appropriate channels and received a reply that stated they were aware of the functionality of the application but that it was essential to, *". . . provide a more complete service to customers wanting email synchronized across multiple devices"*, but Microsoft was unaware of the exploitation process *per se* (Ardley, 2011, pp. 3-4).

Of concern to us was whether email messages could be tampered with and fabricated messages could be inserted into a target Hotmail® account using WLM. If so, certain criteria must establish alteration of the message content, the message headers and the message attachments as well as insertion of fabricated messages. It was necessary to establish that these changes would persist in the Hotmail® account linked to the server, not solely in the WLM account after an extended period[3]. To establish a proof of concept, we required certain conditions that would confirm conclusively the WLM exploit process, namely:

1. Message content could be altered.
2. Message headers could be altered.
3. Message attachments could be altered.
4. Fabricated messages could be inserted.

This paper looks specifically at the current version of Windows Live Hotmail®, and the vulnerability of email messages for tampering. Time did not permit us to

---

[3] An arbitrary eight week-period would demonstrate stability and persistence of the tampered messages on the Hotmail® sever over an extended period.

undertake similar, detailed examinations using other web-based email applications, notably Gmail™, Yahoo 7 Mail®, AOL Mail[4] or Outlook®[5], but the results observed from exploratory examinations of these applications leads us to suspect that they too were vulnerable to tampering via WLM, and in the case of Outlook®, through the simple 'drag and drop' migration process.

In this paper, we outline the history and nature of Hotmail®, Windows Live Hotmail® and WLM. We define and describe the process of the WLM exploit and the extent to which it can be used to modify Hotmail® message content, headers and attachments. We describe how we tested the proof of concept and the outcomes, and how we compared the modifications with original email data. We also highlight the challenges to validating messages facing the cyber forensics practitioner

2. SUMMARY OF HOTMAIL™ AND WINDOWS LIVE MAIL®

Hotmail®, one of the pioneering web-based emails, was made available to the public free of charge in 1996 (Craddock, 2010a). In 2004, Hotmail® was moved onto a system using Windows Server and Windows SQL Server® and more recently upgraded to the latest version of SQL server (Craddock, 2010a). In 2007, Microsoft released a beta version of its free email application WLM to replace Outlook Express® on Windows XP® and Windows Mail® on Windows Vista®[6]. WLM incorporated the DeltaSync®[5] protocol enabling users to synchronise Hotmail® and other email accounts with WLM (LeBlanc, 2007a, 2007b; Sierra, 2010). By 2010, Hotmail® accounts synchronised with WLM offered users synchronicity between their PC email client, their browser, and their phone (Craddock, 2010b). There is evidence that Outlook® has had a functional synchronisation for some time, perhaps preceding 2007 using WebDav (LeBlanc, 2007b).

When installed on a user's computer under Vista® or Windows 7®, WLM typically creates a default directory named Windows Live Mail under the Microsoft folder in the nominated user's Users folder. Users are able to add email accounts by using the menu feature in WLM, provided they add the email account name and password. Folders under Hotmail® accounts are created in WLM, most usually, Inbox, Draft, Sent items, Junk email and Deleted items. This is very similar to some IMAP email-clients such as Thunderbird that provide similar directory structures and individual files.

---

[4] Gmail is owned by Google Incorporated. Yahoo 7 Mail® is owned by Yahoo. AOL Mail is owned by AOL Incorporated.

[5] Outlook® is a registered trademark of Microsoft Corporation.

[6] These applications and operating systems are registered trademarks of Microsoft Corporation.

3. THE PROCESSES INVOLVED IN THE WLM EXPLOIT

Unlike its predecessors, Outlook Express® and Windows Mail®[7], which stored messages in less accessible formats and obscure folders, WLM folders are readily visible using Windows Explorer, for example, and each message can be opened, viewed, modified and saved using Notepad, and other text editing software. More remarkable is that when WLM is running, it is also possible to drag and copy email messages from any of the message folders to the desktop, edit the message in various ways, and drag the message back into WLM. This feature is not obvious to users and we do not believe it was intended to be part of the normal use of the application. It seemed likely that tampering of email messages could occur because of the way WLM stored messages from Hotmail® accounts on the client machine and these messages would be migrated to the vendor server. If so, these changes were expected to persist server-side and may assist in detecting tampering.

The account holder may access the Hotmail® account either by direct access to the Hotmail® account held on the server or by installing WLM and synchronising with the Hotmail® account as shown in Figure 1a. Opening the Hotmail® account by web access does not permit the user to tamper and insert a fabricated message into the account. However, accessing the Hotmail® account through WLM facilitates exploitation and allows the account holder to alter existing sent and received messages for a variety of reasons.

Figure 1b presents an alternative scenario is when an attacker gains access to the account holder's computer and uses WLM to access the Hotmail® server and tamper with or insert messages.

A remote attack is shown in Figure 2 where the attacker has the account holder's account name and password. The attacker is able to access the Hotmail® server by synchronising through WLM and tamper with and insert messages.

---

[7] Outlook Express®, Outlook 2011® and Windows Mail® are registered trademarks of Microsoft Corporation.
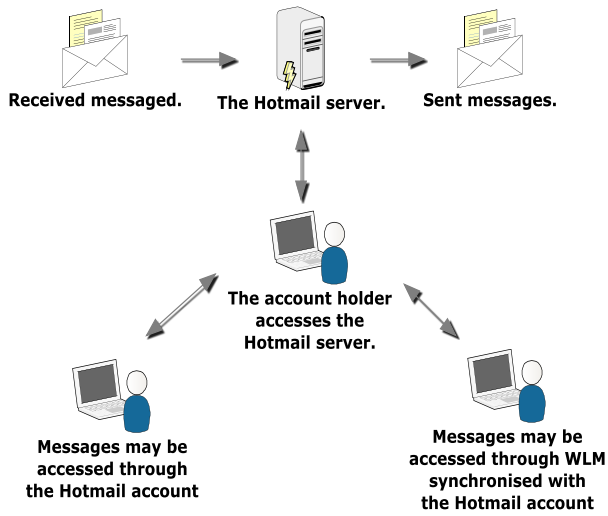
Figure 1a. The account user accesses the Hotmail® server by direct access to the email account or uses WLM to synchronise and access the account.
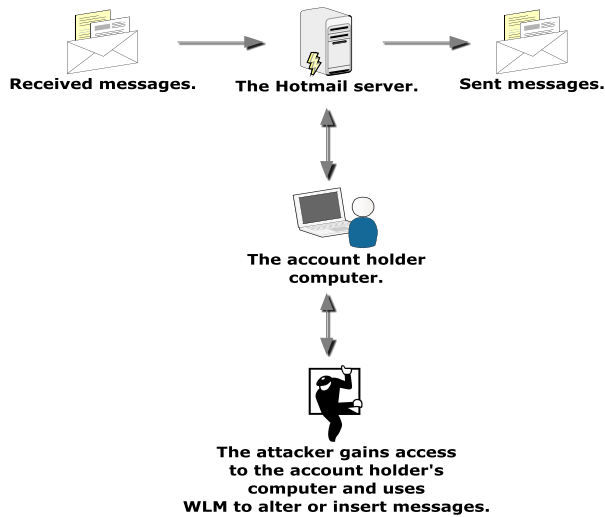
Figure 1b. An attacker gains access to the account holder's computer to tamper with or insert messages.

Received messages.   **The Hotmail server.**   **Sent messages.**

The account holder computer.

The attacker uses a remote computer to gain access through WLM to the account holder's email on the Hotmail server.
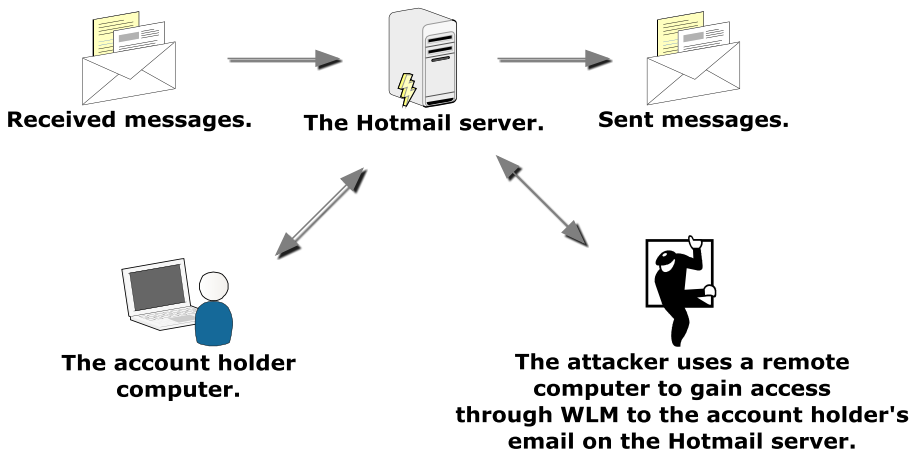
Figure 2. An attacker on a remote computer using WLM to synchronise with the account holder's account on the Hotmail® server to tamper and insert messages.

Figure 3 illustrates how WLM on an account holder's computer synchronises with the Hotmail® account held on the Hotmail® server. The Hotmail® account is added to WLM using the account name and password. The WLM account is opened on the account holder's computer and a message selected for tampering is dragged from WLM by the 'drag and drop' facility and placed on the desktop and the original message in the account is deleted to conceal the forgery. The extracted message may be edited using a text editor such as Notepad then saved and dragged back into the account in WLM. The account is manually or automatically synchronised with the Hotmail® server and the tampered message remains in the Hotmail® account.
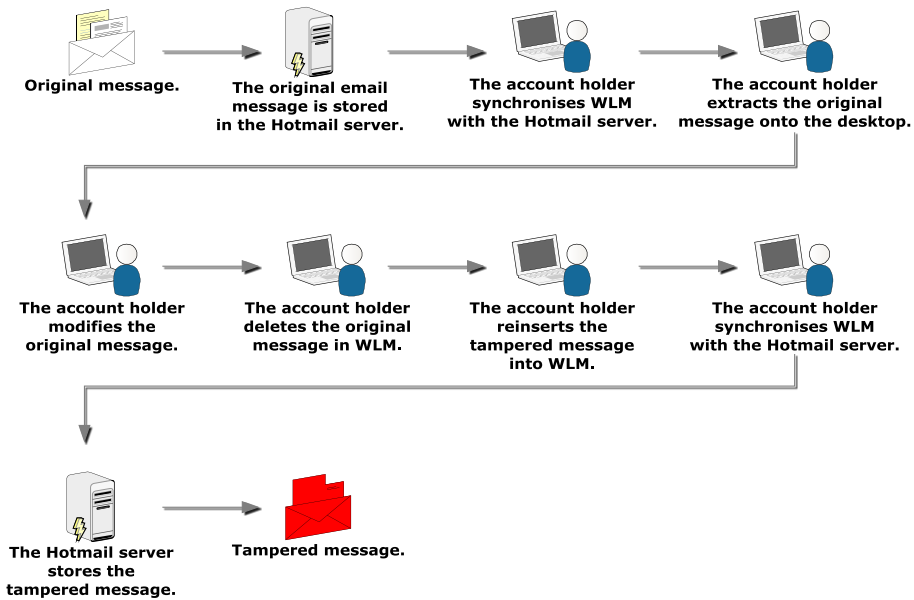
Figure 3. The sequence of events showing an account holder altering an existing email message.

Similarly, in the event an attacker hijacks the account holder's computer or initiates an attack from another computer, the attacker has the ability to access the account holder's account through the WLM exploit either on the account holder's computer or on the attacker's computer, as shown in Figure 4. The process of message tampering and insertion is identical with the process illustrated in Figure 3.
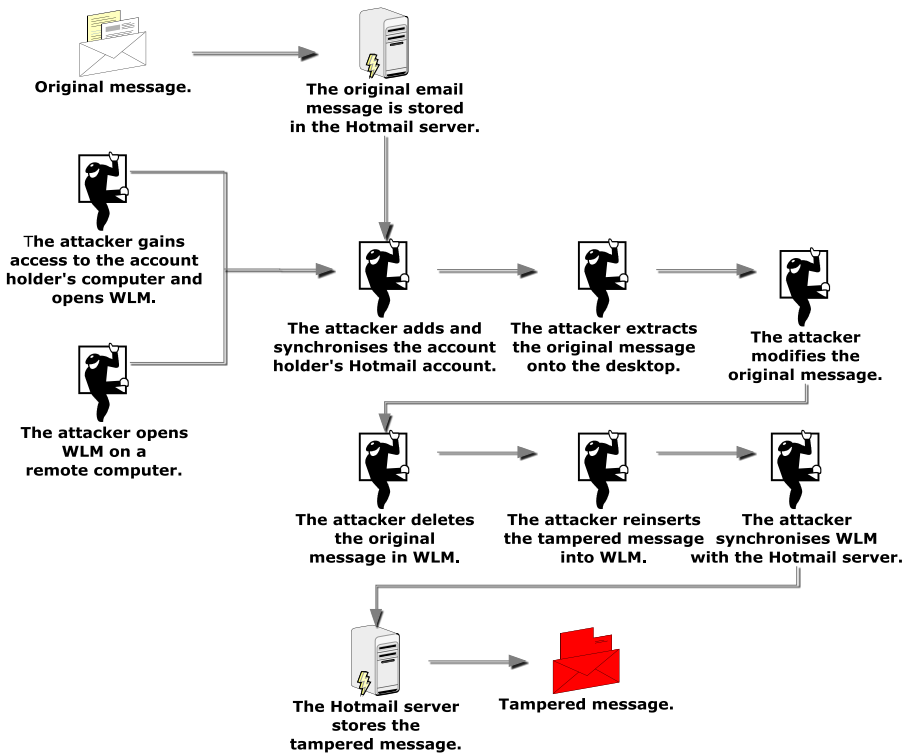
Figure 4. The sequence of events showing an attacker altering a message in account holder's account.

In the first two instances, evidence artifacts of tampering are confined to the account holder's computer and the Hotmail® server. In the remote attack, evidence of tampering would be located on the attacker's computer and the Hotmail® server; server-side is dependent on appropriate server logs and retention periods of those logs.

We discuss the issues of evidence location and characteristics in Section 8.

4. APPLICATIONS USED AND PROCESSES UNDERTAKEN TO TEST THE PROOF OF CONCEPT

For the proof of concept, we used a desktop computer running Windows 7 Home Premium® operating system and Windows Live Mail 2011® email application[8]. For ease of reference, we called this computer the 'editing computer'. A second computer, the 'independent computer', compared and checked the outcomes obtained by the 'editing computer'. Identical operating system and email

---

[8] Windows 7 Home Premium® operating system is the registered trademark of Microsoft Corporation.

application were installed on the 'independent computer' as were used on the 'editing computer'. The use of the 'independent computer' would ensure that results observed on the 'editing computer' could be verified independently. The computer mouse was used to transfer twelve candidate message files (.eml) from the Hotmail® account in WLM onto the 'editing computer' desktop and vice versa using a 'drag and drop' technique. Notepad was used to edit the extracted files and message files in the WLM folders present on the 'editing computer' directory.

A Windows Live Hotmail® account was created using the 'editing computer' for testing the processes and efficacy of message tampering. The account was populated with messages sent from other Windows Live Hotmail®, Gmail™, Yahoo 7 Mail®, AOL Mail, and POP3/SMTP accounts created specifically for the study on a separate computer. Email messages were sent from the Hotmail® account on the 'editing computer' to the other email accounts. These processes would enable later study of the characteristics of the tampered messages and fabricated messages located in the respective Inbox and Sent items folders on the 'editing computer'.

WLM was installed and opened on the 'editing computer' where tampering and fabrication of messages would occur. The Hotmail® account previously created for the purpose of the study was synchronised successfully with WLM on the 'editing computer' and we noted confirmation during the account synchronisation, that the mail server was an HTTP server implementing DeltaSync® version 2.0.0. We observed the same version of DeltaSync® was installed during the installation of WLM on the 'independent computer'.

The study commenced with attempts to copy and modify email messages in the Inbox and Sent items folders on the 'editing computer' by dragging twelve prepared messages from each folder to the computer desktop to see whether tampering of the message content, headers and attachments were possible. Notepad was used to change headers and message content and then the messages were reinserted into the respective message folder, in some instances with the original message extant, in others with the message previously deleted. Observations would determine whether these processes resulted in persistence of the migrated file remaining in each message folder. On completion of each tampering process, hashes were taken of each file for later comparison during our study into the persistence of the messages in the Hotmail® account and the Hotmail® server. WLM was closed and the computer rebooted to determine whether the tampered messages persisted in the folders.

We then studied the viability of tampering with extracted messages by substituting original image and text file attachments with previously prepared messages to facilitate the substitutions on the 'editing computer'. We used Notepad to alter and insert the fabricated scripts into original messages, two in the Inbox folder and two in the Sent items folder. Once the substitution was completed, the messages were reinserted into their original folders onto the

'editing computer' using the 'drag and drop' process. We then manually synchronised WLM with the Hotmail® server.

To test whether fabricated messages could be inserted into WLM and synchronised with the Hotmail® server, we used twelve messages from a different Hotmail® account which we dragged to the 'editing computer' desktop then inserted them into the Inbox and Sent items folders of WLM, which was then synchronised with the server. Four of the messages contained image file attachments and the remaining four messages contained text file attachments.

We also wished to observe whether the tampered and fabricated messages inserted into the WLM folders would synchronise and remain on the Hotmail® server. WLM was manually synchronised after each insertion and the 'editing computer' shut down and rebooted, WLM was opened and observations made of the presence and characteristics of the tampered and inserted messages to determine their persistence in WLM. This process was repeated by using a WLM account on the 'independent computer' to see whether the tampered message would populate WLM and to observe the characteristics of the messages. To determine whether the files had synchronised with the Hotmail® server, we used the 'editing computer' and the 'independent computer' and opened the Hotmail® account to see whether the tampered files were present and observe their characteristics. We assumed that an eight week-period would be sufficient to confirm that the tampered files persisted on the Hotmail® server.

To gain more information about the DeltaSync® synchronisation process, namely, the characteristics of the message metadata recorded on the Hotmail® server, we simulated conditions of the DeltaSync® synchronisation as closely as possible. DeltaSync® is not freely available for use separate from Microsoft products[9] and we were unable to identify the type of metadata stored on the Hotmail® server. Consequently, we used the UNIX utility *rsync* as the nearest known approximation to DeltaSync® to simulate and investigate the server-side actions.

The X-Ways Forensics[©10] analysis tool was used to locate and examine the folder and email message files and obtain file hashes for comparison and event reconstruction purposes. This provided confirmation of changes to tampered messages and proof of reinsertion into WLM and the Hotmail® control account; physical examination of the computer directories providing more complete file attributes and antecedents.

Forensics images were taken of the 'editing computer' after the tampering was completed and the WLM synchronisation with the Hotmail® server completed, to observe and obtain the characteristics of the WLM folders and messages for signs

---

[9] Note: DeltaSync® has been reverse engineered at the client side.

[10] X-Ways Forensics is the copyright of X-Ways Software Technology AG.

of tampering. Searches of tampering events and migrated message files were also made to see if any typical evidence artifacts were available to the forensics examiner.

These tests were replicated using a 'third computer' with Windows XP® with Service Pack 2 installed and a compatible version of WLM. This would allow us to compare results obtained on the 'third computer' with the 'editing computer'.

Section 5 provides details of each examination and our observations so that the reader may also repeat the examinations themselves.

5.   TESTS OF WLM BEHAVIOUR DURING MESSAGE TAMPERING

Question 1: Do tampered and inserted messages synchronise with the Hotmail® server and persist server-side for an extended period?

Test 1A:	Eight tampered messages and four fabricated messages were created on the 'editing computer' and were inserted into WLM then synchronised with the Hotmail® server. The messages were hashed for later comparison and WLM was closed. Testing for synchronicity was carried out on the 'independent computer' using Windows 7® and WLM 2011, by accessing the messages in WLM and the Hotmail® account. This would determine whether the tampered and fabricated messages persisted on the Hotmail® server when accessed by the 'independent computer'.
Outcome 1A:	Complete and permanent synchronisation of the tampered messages was observed. All tampered files were synchronised and hash values were found to be identical. The tampered messages persisted in the WLM account and on the Hotmail® server for a period of eight weeks.
Test 1B:	We attempted to replicate the DeltaSync® synchronisation process on a server to identify the nature of the metadata synchronised between the server and WLM. This involved using a server to simulate what occurs on the Hotmail® server after synchronisation with WLM using Microsoft's DeltaSync®, running a similar application, rsync to simulate DeltaSync® as close as possible, to identify the type of metadata synchronised.
Outcome 1B:	The rsync test showed that unlike Windows, which provides three distinct types of temporal metadata (created, modified and accessed), rsync preserves last modification time but

loses last access time. Modification is a combined creation and modified time, while accessed is displayed as an access time. Consequently, server-side metadata and logging is not expected to provide as much temporal metadata as stored in the WLM message folders. We recognise there are applications freely available that are capable of falsifying file metadata to assist camouflage client-side emails[11].

Question 2: Does WLM support the process of altering email message content?

Test 2:   We added the Hotmail® account to WLM on the 'editing computer'. Twelve email messages from the WLM Inbox and Sent items folders were dragged onto the desktop. Each message was opened on the desktop with Notepad, the original message content was deleted and a substituted with a different message. Using Notepad, the message was then saved and reinserted into WLM. WLM was synchronised with the Hotmail® server, closed and the computer rebooted.

Outcome 2:   WLM does support the process of altering message content. The tampered messages persisted in the WLM account and on the Hotmail® server for a period of eight weeks. These results were confirmed by accessing the Hotmail® server by the 'independent computer'.

Question 3: Does WLM support the process of altering email message headers?

Test 3:   Twelve email messages were dragged to the desktop of the 'editing computer' and Notepad was used to view and modify the message headers. The messages were then reinserted into their respective folders on the 'editing computer'. WLM was closed and the computer rebooted.

Outcome 3:   WLM does support the process of altering message headers, notably message name, message timestamps, IP and SMTP data. The tampered messages persisted in the WLM account

---

[11] For example, see:
http://www.techrepublic.com/search?q=http%3A%2F%2Fwww.techre public.com%2Farticle%2Fbuild-your-skills-learn-to-manipulate-file-time-stamps-in-windows%2F5034280.

and on the Hotmail® server for a period of eight weeks. These results were confirmed by accessing the Hotmail® server by the 'independent computer'.

Question 4: Does WLM support the process of altering email message attachments?

Test 4:
During tests 2 and 3, we observed that it was possible to remove and modify message content script and presumably possible to remove message attachment script. We wished to confirm whether it was possible to replace the original attachment script with script from substitute attachments, specifically, picture image (.jpg) and Word 2010®[12] document files. To do so, we prepared four similar emails to the original sent and received messages so that we could simplify the substitution process by having available attachment data of the same format as the target message. We would then transfer that image and text file data by copy and paste into the original message using Notepad on the 'editing computer'. WLM was closed and the computer rebooted.

Outcome 4:
WLM does support the process of deleting message attachments and substituting different attachments; notably text and image files. The tampered messages persisted in the WLM account and on the Hotmail® server for a period of eight weeks. These results were confirmed by accessing the Hotmail® server by the 'independent computer'.

Question 5: Does WLM support the insertion of fabricated messages?

Test 5A:
Using a template from a different Hotmail® account and mimicking the header and formatting of existing sent and received messages, four fresh messages were created and saved to the 'editing computer' desktop. The messages were then inserted into the Inbox and Sent Items folders of WLM, which was then synchronised with the server.

Test 5B:
We created a fabricated text message in Notepad and saved it on the desktop as an email message (.eml) to see whether the fabricated message could be dragged into WLM and synchronise with the Hotmail® server.

---

[12] Word 2010® is a registered trademark of Microsoft Corporation.

Outcomes 5A/B: WLM does support the process of inserting fabricated messages. The tampered messages persisted in the WLM account and on the Hotmail® server for a period of eight weeks. These results were confirmed by accessing the Hotmail® server by the 'independent computer'.

Identical outcomes were observed using the 'third computer' running Windows XP® with Service Pack 2 and a compatible version of WLM.

6. OTHER OBSERVATIONS

During the course of the study, we recorded observations of additional details regarding tampering and insertion processes that provide an insight into the exploit process.

Altering and creating message contents

Using Notepad on the 'editing computer' during Test 2 to alter message content and save the files was a straightforward process only requiring the user to identify the message content and then substituting the new message by typing or pasting new text and saving the file. Identification of the message content in the original message was the first step so that it could be removed or altered, and with a little practice and intuition, might be considered that a task a novice user could complete successfully. Figure 5a shows a portion of the message script opened in Notepad with the message content 'No attachment' clearly displayed. Figure 5b illustrates the message content replaced with the word 'substituted'. The file is saved in Notepad and dragged back into the WLM folder. These messages remained in the same form when viewed on the 'independent computer' when viewed in WLM and the Hotmail® account. All tampered messages appeared authentic with no evidence of tampering inside the message script.

Messages remaining on the 'editing computer' desktop were deleted and the Recycle Bin emptied. Recovery of erased messages was possible using the forensics recovery tool and would be of potential evidentiary value in verifying tampering.

Altering and creating message names, timestamps and other header data

During Test 3, the process of identifying the relevant timestamps within the extracted messages required some testing on the 'editing computer' to ensure that all relevant data was changed. This was important, as tampering would be evident if all temporal data, typically three date sets in the header, did not match and the reinserted file showed the original date and time in the folder view. Initially, some reinsertion attempts did fail because of difficulties identifying the header data; for example, Hotmail® headers are different from Gmail, Yahoo etc. Perseverance and practice rewarded our efforts in identifying critical dates and times ensuring they were consistent with the original message format. These messages were

reinserted and did move to the intended new time-based order in the message folders in accordance with the changed dates and times. The files retained their position and format throughout the eight-week period.

```
Subject: HMYM
Date: Tue, 21 Jun 2011 21:35:43 +1030
Importance: Normal
MIME-Version: 1.0

--_111aeb1e-485e-4493-8cac-6ea1ab3de7ef_
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

No attachment
=
--_111aeb1e-485e-4493-8cac-6ea1ab3de7ef_
Content-Type: text/html; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
<html>
<head>
<style><!--
.hmmessage P
{
margin:0px=3B
padding:0px
}
body.hmmessage
{
font-size: 10pt=3B
font-family:Tahoma
}
--></style>
</head>
<body class=3D'hmmessage'><div dir=3D'ltr'>
No attachment<br>
</div></body>
</html>=
--_111aeb1e-485e-4493-8cac-6ea1ab3de7ef_--
```

Figure 5a. Original 'sent' message with the string, "No Attachment" visible in two locations.

```
Subject: Tampered message
Date: Mon, 20 Jun 2011 23:31:46 +1130
Importance: Normal
MIME-Version: 1.0

--_111aeb1e-485e-4493-8cac-6ea1ab3de7ef_
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

substituted
=
--_111aeb1e-485e-4493-8cac-6ea1ab3de7ef_
Content-Type: text/html; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
<html>
<head>
<style><!--
.hmmessage P
{
margin:0px=3B
padding:0px
}
body.hmmessage
{
font-size: 10pt=3B
font-family:Tahoma
}
--></style>
</head>
<body class=3D'hmmessage'><div dir=3D'ltr'>
substituted<br>
</div></body>
</html>=
--_111aeb1e-485e-4493-8cac-6ea1ab3de7ef_--
```

Figure 5b. Original message replaced with the tampered 'sent' message. The string "substituted" visible at the same locations. Note the date/time and message name changes.

Changing the message name was a simpler process to master and it was possible to change all message names, which retained their status after reinsertion. Figure 6a shows the original message name 'ORIGINAL.docx', whereas Figure 6b shows the altered message name changed to 'SUBSTITUTED DOCUMENT.docx'.

Changing IP and SMTP data was a straightforward process although a forger would have to ensure that the altered data would enhance the forgery. For example, if a fabricated IP address was inserted this might reveal tampering and defeat the purpose of the forgery. If an attacker manipulated a message the metadata stored locally, the Modified, Accessed, Created times will change and be identifiable to a forensic examiner. Specifically, those metadata would differ from the header information that is contained in the message when they should be in close approximation of one another.

From our observations, we identified and analysed groups of evidence artifacts created during the tampering processes on the 'editing computer'. This included locating evidence of tampering and the use of the WLM exploit on the 'editing computer'. From the outset, it was evident that WLM logs, while a possible source of 'tamper evidence' may not always be available for examination if the forger removed traces of the application's presence on a computer used to complete the tampering or fabrication. Similarly, effective erasure of email messages edited on the host computer desktop would leave little for the forensic examiner to use.
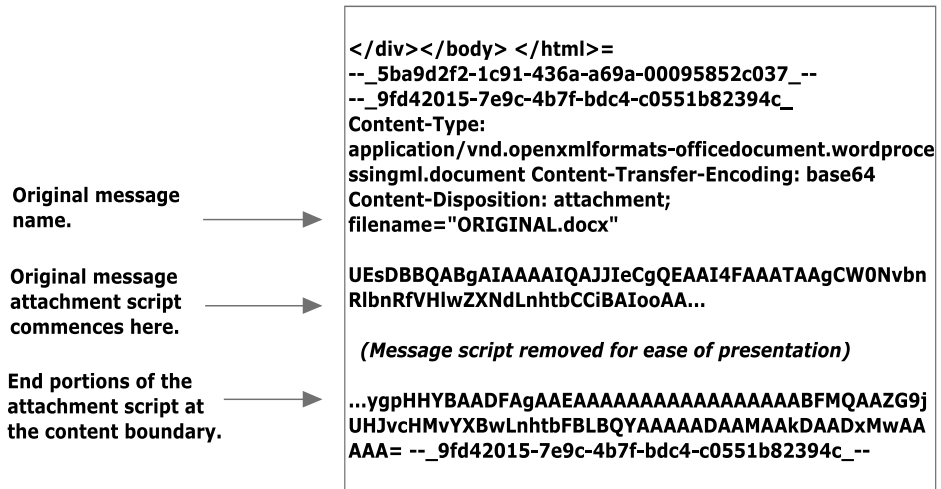
Original message name.

Original message attachment script commences here.

End portions of the attachment script at the content boundary.

</div></body> </html>=
--_5ba9d2f2-1c91-436a-a69a-00095852c037_--
--_9fd42015-7e9c-4b7f-bdc4-c0551b82394c_
Content-Type:
application/vnd.openxmlformats-officedocument.wordproce
ssingml.document Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="ORIGINAL.docx"

UEsDBBQABgAIAAAAIQAJJIeCgQEAAI4FAAATAAgCW0Nvbn
RlbnRfVHlwZXNdLnhtbCCiBAIooAA...

(Message script removed for ease of presentation)

...ygpHHYBAADFAgAAEAAAAAAAAAAAAAAAAABFMQAAZG9j
UHJvcHMvYXBwLnhtbFBLBQYAAAAADAAMAAkDAADxMwAA
AAA= --_9fd42015-7e9c-4b7f-bdc4-c0551b82394c_--

Figure 6a. Original message showing text attachment script before alteration.

Altered message name.

Substitute attachment data inserted here.

End portion of the substitute attachment script at the content boundary.

</div></body> </html>=
--_5ba9d2f2-1c91-436a-a69a-00095852c037_--
--_9fd42015-7e9c-4b7f-bdc4-c0551b82394c_ Content-Type:
application/vnd.openxmlformats-officedocument.wordproces
singml.document Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="SUBSTITUTED
DOCUMENT.docx"

UEsDBBQABgAIAAAAIQAJJIeCgQEAAI4FAAATAAgCW0NvbnR
lbnRfVHlwZXNdLnhtbCCiBAIooAA...

(Message script removed for ease of presentation)

...DmR/2scgEAAMICAAAQAAAAAAAAAAAAAAAAAEgrAABkb2
NQcm9wcy9hcHAueG1sUEsF
BgAAAAMAAwACQMAAPAtAAAAAA==
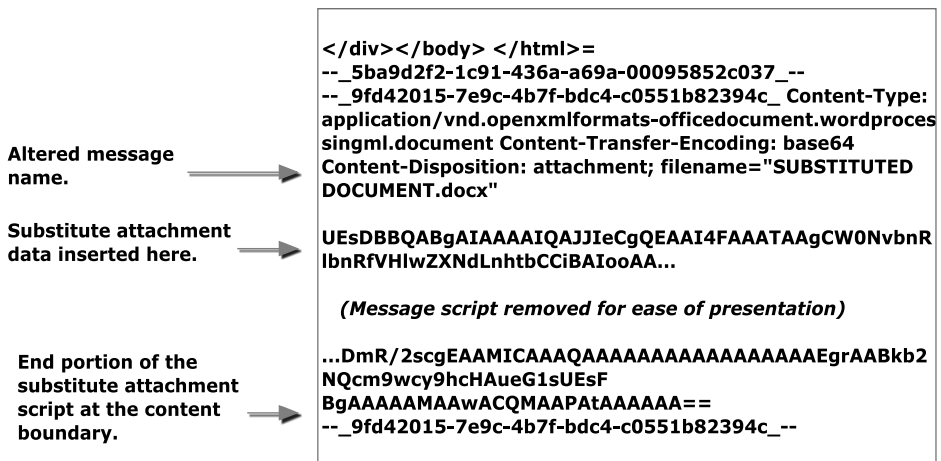**--_9fd42015-7e9c-4b7f-bdc4-c0551b82394c_--**

Figure 6b. Tampered message with the document attachment script removed and replaced with a substitute document script.

We assume, based on the rsync test and the persistence of messages retained on the Hotmail® server, that the server would retain creation/modified metadata when the message was synchronised on the Hotmail® server. Whether the metadata would provide meaningful corroboration would require checking the metadata under legislative power or court order. This metadata may be the best means of authenticating messages timestamps by comparing them with server-side timestamps. That is, of course, provided the message was still stored on the server and whether correlating the timestamps was possible to provide meaningful analysis.

It appears the messages headers scripts are persistent and remain with the message irrespective of synchronisation with the server. How reliable are the message header timestamps and can they be taken at face value? Even if the message were authentic, the timestamps may be inaccurate because of a range of delays and transmission faults. Comparing the sent message header with the received message header would provide a means of triangulating the most reliable dispatch and receipt times. Comparing the messages with the server timestamps is also conditional on the correct interpretation of the timestamps. Even if they do conflict with the message timestamps, it may suggest tampering or some other event. The difficulty is the last accessed time is not overly helpful and the creation/modified timestamp metadata identified in the rsync test does not provide a log of original creation or modified events. However, the creation/modified metadata used to compare the message timestamps would establish message authenticity.

Deleting and substituting message attachments.

Removing original attachments (Word 2010 documents and image files) from messages stored on the 'editing computer' and replacing them with substitute attachments initially appeared more challenging and time-consuming than replacing message and header scripts. Study of the attachment required confirmation of the start and end of the attachment scripts. Once located the attachment boundaries were identified it was a straightforward process to remove original scripts using Notepad. Figure 6a is a segment of an original message viewed in Notepad showing the start and end boundaries of the attachment script - a Word 2010® document in this instance. Once removed, it was possible to copy and paste the substitute attachment script from a previously prepared message attachment into the tampered message. Figure 6b shows a segment of the substituted attachment script (Word 2010®) inserted into the message. Comparison of the hash values of all messages and attachments reinserted into WLM showed they maintained all their file characteristics.

Ability to alter messages in the directory folder

In a separate test using the 'editing computer', we noted that the WLM exploit did not support attempts to open and alter messages located in the computer directory

folders that were visible using Windows Explorer®13. While fabricated messages could be inserted and existing messages could be opened using Notepad, the messages did not synchronise with WLM and did not appear in the folders when viewed with WLM. None of these messages synchronised with the Hotmail® server because of the local synchronisation that only synchronises messages when WLM is run.

Ability to create fabricated messages

Test 5 showed that it was possible to create and insert fabricated messages by two different processes: by creating an email message, and by changing the file extension of a text document to .eml format. Both processes provide the means to include malicious code into the message script and pose security threats to unwary recipients unprotected by malware filters.

7. SUMMARY OF FINDINGS

Our ability to manipulate and insert messages through WLM into the Hotmail® server established proof of concept of the exploit. Study of these processes showed that the exploit could be used for message tampering and the insertion of malicious code. Test 1 confirmed that the tampered messages with altered messages content persisted on the Hotmail® server for the trial period of at least eight weeks.

Tests 2, 3 and 4 show that WLM permits tampering through a simple 'drag and drop' message migration using a simple text editor. We observed the process failed repeatedly when attempting to tamper messages in the computer folder directory housing WLM files. Tampering with message content is a relatively simple process requiring relatively little knowledge. Changing file headers and removing and substituting attachments requires more knowledge, but no advanced computer skills.

Test 5 confirmed the ability to create and insert fabricated messages into WLM and synchronise those messages with the Hotmail® server through two different processes. The process of creating a fabricated message mimicking a genuine email required some practice, but was helped by using message templates matching message formatting to other email applications and not considered an insurmountable challenge to novice forgers. The process of changing file extensions to .eml was uncomplicated but their format was readily recognisable as fabricated messages. Of security concern is that this process permits the inserting of 'zero-day' code into a target computer.

Time did not permit us to trial similar examinations with Gmail™, Yahoo 7 Mail® and AOLmail applications beyond some initial account creation in WLM and basic proof of concept trials. Preliminary trialing did confirm that tampering

---

13 Windows Explorer® is a registered trademark of Microsoft Corporation.

was achieved to the same degree as with our earlier examinations of Hotmail®. Outlook 2010® appeared to present a similar opportunity for a similar process to be exploited.

There may be other applications, such as Mozilla Thunderbird that enables message tampering with similar results as WLM. We leave that to further research to clarify the possibility but consider it worthy of mention at this time. Similar attacks may be feasible against Gmail using IMAP.

8. IMPLICATIONS FOR DIGITAL EVIDENCE ANALYSIS AND RELIABILITY

Having established the vulnerability of various web-based email applications to tampering, we can envision serious third-party injection attacks. Consider a government official with home and office internet access. The attacker injects malware with appropriate social engineering tags inserted into the message and is synchronised to the investigator's account as we have described previously. Custom code ('zero day') can pass virus scans and is later run by the investigator as a trusted programme potentially compromising the official's home and office network.

In another scenario, a vengeful, disgruntled client seeks to implicate a business provider and tampers with an existing email from the provider to discredit the latter. If the provider has no record to contradict the forgery, it may be burdensome if not impossible to support a counter-claim, for as we have shown, there may be a paucity of tampering evidence.

A tampered email message could have serious implications for its victim as well as potential benefits for the forger. We assert that Hotmail® messages tendered as evidence should not be accepted at face value if there were even the slightest doubts over their integrity; yet some form of validation is required. Validation requires confidence about inferences drawn from the evidence, in particular, verification of the domain where the evidence is created, processed and transferred (Boddington, Hobbs & Mann, 2008). As Boddington et al., (2008) assert, not only the validity of the evidence files but examination of the application and operating programs must be available for examination. Simply assuming an email message is authentic and relates to a critical date and time, without seeking some reasonable validation can be disastrous. Such expediency or inattention to detail, as Dardick (2010) points out, may involve faulty reasoning that fails to prove that the facts support the conclusions and only those conclusions. It was important to see whether forgeries and fabricated messages could be detected though.

A potentially rich source of evidence is the directory folder and WLM but a perceptive forger may well deep erase traces of WLM, or it may be unavailable if the 'editing computer is not located or its existence unknown. We assume, based on the rsync test and the persistence of messages retained on the Hotmail® server,

that the server would retain creation/modified metadata when the message was synchronised on the Hotmail® server. Whether the metadata would provide meaningful corroboration would require checking the metadata under legislative power or court order. This metadata may be the best means of authenticating message timestamps by comparing them with server-side timestamps, which depends on the message still being stored on the server and whether correlating the timestamps provides meaningful information to assist analysis.

What concerns us, and should certainly be heeded by those with a vested interest in seeking the truth, is that while tampering may be suspected, the metadata available to support or refute assertions as to the message integrity may be scarce in cases where attempts have been made to camouflage the alterations. Government and private organisations often have in place email security and pre-forensics strategies that record all received, sent and deleted messages on their own servers. This would seem to be a wise precaution, because such strategies do save deleted messages for use in future investigations. Having an original message to compare with a tampered message may be a sound validation process. Otherwise, if an original message is no longer available there is nothing to challenge a tampered or fabricated message linked to the server with a wrongdoer exploiting an external Hotmail® account.

Further research would be helpful to understand more fully, what useful server-side evidence is available to the forensic practitioner. Equally important would be a reliable, formal validation template to help the forensics practitioner examine suspect messages. Given the large number of email clients in use, the question of email aggregation playing a role in this type of exploit should also be considered. The WLM exploit may be prevented by administration through one of the other email clients, and since the exploit deals with the messages maintained on the account holder's computer and their synchronization to the Hotmail® server, this raise the question of whether this can be bypassed by using another client. While the main focus of this paper is on WLM and how it stores messages, these other aspects warrant further consideration.

9. CONCLUSIONS

The results of this study may well have implications for cyber forensics examiners and legal practitioners preparing cases involving email evidence. We have shown that WLM facilitates forgery and requires little computer skill to fulfill improper or mischievous aims. Validation of email messages should be undertaken whenever there is a suspicion of, or claim of tampering is implicit. This requires access to email message metadata server side and from likely venues where WLM was used to undertake tampering.

This confirmation of the WLM process to edit and exploit web-based emails persuaded us to bring this to the attention of law enforcement authorities. We hope it will assist forensics examiners in considering the possibility of message tampering in future cases and perhaps review some existing and previous cases

where incorrect assumptions were made regarding the authenticity of email-based digital evidence.

Assuming the server side messages are stored in some sort of database (and a reasonably complex one we assume), the problem could be fixed by removing updates to message bodies and attachments within the server side database, so that when synchronisation occurs, only the entire email can be removed or deleted, rather than updated. The implications of the WLM exploit process should be considered by Microsoft and fixed.

Civil, criminal and internal disciplinary cases involving emails are not novel and occur with increasing sophistication. We predict cases of tampering will come to public note more often in the future. Pandora's email box is now opening and legal cases relying on email evidence should be cognisant of the danger of assuming the obvious. Prudence suggests circumspection of the circumstantial.

AUTHOR BIOGRAPHIES

Mr. Richard Boddington holds a B.Sc (Hons) 1st Class and is undertaking Ph.D. research in digital evidence validation at Murdoch University, Australia where he teaches and researches information security and cyber forensics. He has a police and security intelligence background and provides cyber forensic analysis and expert testimony for the legal fraternity in a range of civil and criminal cases.

Mr. Jeremy Ardley has a B.Sc in Physics and Computer Science. He has 30+ years' experience in information capture, analysis, presentation, and advice to decision makers. He now works as a Forensic Information Analyst, interpreting forensic evidence and advises legal teams on technical evidence as well as acting as an expert witness.

Mr. Grant Boxall is a third year student completing a B.Sc, majoring in Business Information Systems, Cyber Forensics and Computer Science at Murdoch University where he is also completing a postgraduate certificate in Business Administration. He has a background in database programming, data analysis and application development.

ACKNOWLEDGEMENTS

REFERENCES

Alexander, A. (2008). JT Shannon Lumber Company, Incorporated versus Gilco Lumber Incorporated. Mississippi: United States District Court, Northern District of Mississippi, Delta Division.

Ardley, J. (2011). *Personal communication with Microsoft: Live Mail (Hotmail) functionality.* (Affidavit). Perth, Australia.

Attorney-General's Department. (2010). *Carrier-carriage service provider data set consultation paper.* Retrieved April 17, 2012, from http://images.smh.com.au/file/2010/07/23/1710367/Secret-Document.PDF?rand=1279847709475

Boddington, R. G., Hobbs, V. J., & Mann, G. (2008). Validating digital evidence for legal argument. Paper presented at the SECAU Security Conferences: The 6th Australian Digital Forensics Conference, Perth, WA.

Craddock, D. (2010a). A short history of Hotmail. Retrieved April 17, 2012, from http://windowsteamblog.com/windows_live/b/windowslive/archive/2010/01/06/a-short-history-of-Hotmail.aspx

Craddock, D. (2010b). Hotmail now supports push email, calendar, and contacts with Exchange ActiveSync, *Inside Windows Live*.

Craddock, D. (2011). Hey! My friend's account was hacked! Retrieved April 17, 2012, from http://windowsteamblog.com/windows_live/b/windowslive/archive/2011/07/14/hey-my-friend-s-account-was-hacked.aspx

Dardick, G. S. (2010). Cyber forensic assurance. Paper presented at the 8th Australian Digital Forensics Conference.

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. In: WWW. *Proceedings of the 16th International Conference on World Wide Web*, New York, American Computer Magazine.

LeBlanc, B. (2007a). Introducing Windows Live Mail. Retrieved April 17, 2012, from http://windowsteamblog.com/windows/b/windowsexperience/archive/2007/05/07/introducing-windows-live-mail.aspx

LeBlanc, B. (2007b). Microsoft Outlook Connector beta now available. Retrieved April 17, 2012, from http://windowsteamblog.com/windows/b/windowsexperience/archive/2007/06/11/microsoft-office-outlook-connector-beta-now-available.aspx

Levi, A., & Koc, C.K. (2001). Inside risks: Risks in email security. *Communications of the ACM*, *44*(8): 112.

Preibusch, S., & Bonneau, J. (2010). The Password Game: Negative Externalities from Weak Password Practices. In Alpcan, Buttyán, and Baras (Eds.), *Decision and Game Theory for Security*. Heidelberg, Springer-Verlang. 6442: 192-207.

Sierra, P. (2010). What draws people to Windows Live Mail and other email applications? *Inside Windows Live*.

Sunner, M. (2005). Email security best practice. *Network Security*, *2005*(12): 4-7.