博格科技股份有限公司

Vista資訊保護產品開發

●計畫執行目標

運用Windows Vista建的RMS Client，係針對Windows Vista作業系統中的Office、Acrobat PDF、AutoCAD、與Pro/E等應用軟體，進行機密資料保護的措施，架構於「微軟E-DRM平台」，提供文件加解密、功能控制、權限設定、防抓圖軟體、動態浮水印、佈署等功能模組。

●新產品簡介

※支援Windows Vista的應用軟體：於Windows Vista作業系統中的Office、Acrobat PDF、AutoCAD、與Pro/E等應用軟體，作者直接於應用軟體設定權限。

※多種控制許可權：文件的控制許可權包括查看（View）、修改（Modify）、複製（Copy）、列印（Print）、程式存取（Programming Access）、另存新檔(Save As）、螢幕拷貝（PrtSc）、離線瀏覽、期限等。可設定期限，期限到期時則文件失效。

※離線瀏覽：機密的文件離開公司網路後，仍然可以在一定時間內查看。可設定離線之租期期間，每隔多久就需要連線到授權伺服器以取得授權。

※Policy功能：使用者只可挑選其部門合適的Policy。

※動態浮水印：開啟文件時，應用軟體動態地加上開啟者的使用者名稱與開啟日期時間之浮水印，嚇阻文件被列印、照相偷拍，以及稽核外漏文件。在文件加密時，可以設定是否加浮水印，浮水印可以設為固定浮水印和動態浮水印，動態浮水印包括人員、電腦名稱、開啟日期時間等。

※抑制各種抓圖、錄畫面軟體盜取機密文件：無複製權限者，無法使用軟體抓取機密文件的畫面。可於伺服器新增加待抑制軟體之黑名單，自動生效。

●計畫創新重點

「Vista資訊保護產品開發」的商品化內容與創新之重點如下：

※應用軟體功能控制：採用Hook技術以控制Windows Vista作業系統中的Office、Acrobat PDF、AutoCAD、與Pro/E等應用軟體之功能，包括功能選單、工具列、快速鍵等，以限制機密文件之列印、儲存、複製編輯等功能。

※抑制各種抓圖、錄畫面軟體盜取機密文件: 採用Hook技術以抑制Windows Vista各種抓圖、錄畫面軟體盜取機密文件的動作，可於伺服器新增加待抑制軟體之黑名單。

※動態浮水印: 採用Hook技術以將Windows Vista文件加上螢幕與列印之動態浮水印，以稽核透過照相、列印方式外洩機密文件。

●公司研究發展能量及研究發展制度之效益說明

對公司的研發能量及制度效益如下：

※協助本公司開發Windows Vista之機密資料保護技術。

※協助本公司更深化在資安解決方案之研發能力，使產品線更完整。

※本公司的研發人力及資金，在本計畫執行後，將大幅成長。

※建立我國中小企業或育成中心企業技術升級與產品轉型的開發模式。

●人才培訓及運用效益

在培訓方面，透過微軟新技術發表，進而要求研發人員開始學習新技術領域(DRM For Vista)，並試著透過研習課程研究開發在既有平台的新技術功能增值。

在技術方面，透過微軟新技術方法，開發的DRM For Vista的資訊安全機制，將一般通行於網頁的機密性網頁，或是限制閱讀性網頁透過新技術給予網頁加密保護。

在運用方面，透過參與微軟新技術與新產品的發表會介紹已開發完成的產品增值功能介紹，進而達成技術交流與廣宣目的。

●產學研各界之技術移轉及合作效益說明

目前無此部份。

●新產品創造之技術效益及市場效益說明

對企業、政府機關而言其具體效益如下：

※資訊使用者無法洩漏機密文件：使用者即使將業務、研發、行銷、財務、法務等機密資料，再傳給別人，別人因無法取得授權而無法再開啟機密資訊，即使用者無法再發佈機密資訊給別人，完全確保企業資訊的安全。

※離職員工無法帶走公司的重要資料：離職員工即使將機密資料帶走，因無法取得授權而無法再開啟這

些機密資訊。

※解決人員異動、與權限異動頻繁的問題：當人員異動、或企業權限政策變動時，可隨時「改派權限、回收（Recall）權限」，已經發行（Distribution）到使用者端電腦中的文件，權限管理員只要更改文件所套用的權限設定，就可以隨時重新設定、或回收（Recall）其使用權限。

※鼓勵研發投資：可以鼓勵企業於智慧財產上做更多的投資與創新研發。

BorG DRM (博格企業資訊保全系統)通過微軟公司【Works With Windows Vista】認證 (ID為13310816)，認可與 Windows Vista 的相容性。

●計畫完成後對提升我國產業水準及競爭優勢說明

對國內產業發展之影響如下：

1. 將對國內企業及政府部門對於資訊保全的方式，進行改變升級。
   ◆ 傳統資訊保全方式：
   在檔案中加上讀取密碼或編輯密碼。
   但取得檔案密碼後檔案就可能被散佈出去！
   ◆ 新一代資訊保全方式：
   文件發佈者可以決定使用者、使用範圍及有效時間。機密文件即使被非法外洩，該機密檔案亦無法被開啟！
2. 可以解決目前企業及政府部門對於資訊保全上所面臨的難題。
   A. 資訊使用者非法洩漏機密文件。
   B. 離職員工帶走公司機密資料。
   C. 人員異動、與權限異動頻繁的問題。
   D. IT人員利用職務之便竊取機密資料。
3. 企業不需要實施禁業條款等不合理的管理制度。
   藉由資訊保全技術於企業當中的自動保護運作，企業不需要實施禁業條款等不合理的管理制度，仍然可以保護企業資訊的安全，間接地可以提昇員工士氣。
4. 無形中可以鼓勵企業勇於智慧財產上做更多的投資。
   對國內產業發展之關聯性方面，因為導入E-DRM（企業資訊保全）系統，可以保障企業於業務、研發、行銷、財務、法務等機密資料的安全，無形中可以鼓勵一般企業於智慧財產上更安心地投資，間接促進產業升級。

●專案執行重要心得

藉由此項研發的新技術領域與研發團隊一同構思，達成與其他相關產品的開發團隊群做技術交流。

在技術方面，由於Windows Vista基於安全上的考慮，會抑制嘗試控制應用軟體功能程式的執行動作，因此在開發團隊多次的開會後實測，終於突破技術瓶頸，達到資訊保護的目的。

突破技術瓶頸：

1. Hook 與加解密程式整合
2. Word 開啟多個加密檔案,重覆 Hook 的問題
3. 阻擋拖曳的動作,Word,Excel,PowerPoint,Adobe Reader OK.

解法:

在開始拖曳之前，先限制滑鼠的可移動範圍，待拖曳動作完成後，再釋放可移動範圍。

Word 存檔時幫 user 加密的程式完成：

1. 由於目前沒有辦法得知 word create file 的 handle 值,所以即使 Hook 到存檔的 api，也不知道 word 是寫入那個檔案，所以再搭配 word automatick object，利用 beforesave 的事件得知存檔動作，再搭配 hook api，在存檔後呼叫加密程式。
2. 由於加密的程式的 dll 檔目前直接由 hook 程式呼叫仍有問題,所以暫時是以 .Net 寫成一個 exe ,供 hook 程式以 shell execute 的方式呼叫。