黑暗首爾（Dark Seoul）資訊安全事故（2013-03-20）及其防禦方法初論

樊國楨[1]、韓宜蓁[2]、季祥[3]

[1]臺灣網站防護協會
[2]中國文化大學資訊管理學研究所
[3]趨勢科技股份有限公司

中華民國一〇二年十一月十五日

摘要

2013年03月20日，使用擦拭磁碟開機主引導記錄（Master boot record，簡稱MBR）之攻擊方法，致使韓國三家廣播電視網與三家銀行金融網及二家保險公司，共超過48,000部伺服機、電腦以及提款機無法啟動的資訊安全事故，彰顯防禦「禍起蕭牆之內」的資訊安全威脅之攸關性。根基於已納入（資訊）安全內容自動化協定（Security Content Automation Protocol，簡稱SCAP）1.2版的應用範疇之屬性基存取控制（Attribute Based Access Control，簡稱ABAC）的「可信賴計算基底之內部威脅的保護（Trusted Computing Based Insider Threat Protection，簡稱TCBITP）之標準化的進程，闡明其實作框架供相關人士參考。

備考：本文部分內容已刊登於「網路通訊國家型科技計畫簡訊」，第57期，頁24-31，2013-11。

關鍵詞：

1. 屬性基存取控制(Attribute Based Access Control)。
2. 基本輸出入系統(Basic Input / Output System)。
3. 主引導記錄(Master Boot Record)。
4. 安全內容自動化協助(Security Content Automation Protocol)。
5. 可信賴計算基底之內部威脅的保護(Trusted Computing Based Insider Threat Protection)。

一、前言：

「初戰即是終戰，首戰就是決戰」，2013年03月20日下午14:00時起，韓國受擦拭磁碟開機之主引導記錄（Master boot record，簡稱MBR）的攻擊，留下了前述網路攻防情境之印記[1]，表1.1是其惡意程式組件的簡述。

表1.1：2013-03-20韓國資安事故惡意程式組件簡述

組件（Component）	目的（Purpose）	文件大小	編譯日期
Dropper Trojan（母體木馬）	安裝MBR Wiper	418KB	2013年3月20日
MBR Wiper（MBR刪除程式）	擦拭磁碟中的MBR	24KB	2013年1月31日
Remote-Access Trojan（遠端存取木馬）	提供駭客存取之後門程式（Backdoor）	46KB	2013年1月26日

說明：1.MBR：Master boot record（主引導紀錄）。

2.資料來源：Sherstobitoff, R., I. Liba and J. Walter（2013） Dissecting Operation Troy Cyberspionage in South Korea, McAfee, 2013-03-20。

韓國政府於2013年4月10日正式公布前述於2013年03月20日造成KBS韓國廣播公司、MBC文化廣播公司、YTN韓聯社電視臺三家廣播電視網與新韓（Shin Han）、農協（Nong Hyup）、濟州（Jeju）三家銀行金融網及二家保險公司，共超過48,000部伺服機、電腦，以及提款機無法啟動之調查報告[2]，係遭受入侵Ahn Lab.與ViRobot等資訊安全的修補（Patch）伺服機，使用如先進持續攻擊（Advanced Persistent Threat，簡稱APT），針對前述8家已完成滲透其內部所有電腦之機構，發動如表1.1所示的軟體更新重寫MBR之標的進行攻擊[1]。

針對前述資訊系統內部威脅之保護（Insider Threat Protection，簡稱ITP）的標準化已有初步成果，規範基本輸出入系統（Basic Input / Output System，簡稱BIOS）完整性（Integrity）之標準草案與使用公開金鑰基礎架構的攸關BIOS完整性量測之屬性基存取控制（Attribute Based Access Control，簡稱ABAC），以及其通訊協定均已進行實作[3~5]；根基於此，分別在第2節與第3節闡明2013年03月20日韓國發生的資安事故與其能提供適當之防禦的可信賴基底（Trusted Computing Based，簡稱TCB）之ITP（簡稱TCBITP）[1,3~7]，第4節是本文的結論。

二、韓國資安事故-特洛伊行動：

此次攻擊代號稱作黑暗首爾（Dark Seoul）的攻擊，資安廠商稱它為特洛伊行動（Operation Troy）。表面上看起來為摧毀電腦主機的資料，實際上是一個秘密間諜活動的結論，其網路攻防情境，依前表1.1所示之多種類別惡意程式組件之特定用途進行攻擊[1]，並推測順序為：

1. 2013年1月26日藉由遠端存取方式在受攻擊單位內部直接製作木馬程式。

2. 2013年1月31日，具有銷毀MBR能力之惡意程式被製作並潛伏在眾多系統中。

3. 受害組織是被駭客透過魚叉式網路釣魚（Spear phishing）方式，植入遠端控制木馬程式（Remote Access Trojan，RAT）。推估是在3月20日前發生，更可能是事件爆發前幾周才正式入侵。

4. 3月20日，攻擊發生的前幾個小時，編譯Dropper病毒植入程式。

5. Dropper病毒植入程式分散於各個受害組織的系統中，在幾分鐘內的執行將主開機紀錄（MBRs）摧毀（發生時間為3月20日，首爾當地時間下午2:00左右）。

母體木馬(The dropper Trojan)

母體木馬主要用來下載的衍生的惡意程式，破壞系統的MBR。藉由修補程式管理伺服機（patch management server），假裝佈署一個偽冒的更新而散佈開來的。

這一支木馬程式於3月20日在攻擊當天系統被破壞前的幾個小時被編譯，因此很不容易透過現有的防毒軟體予以偵測阻攔。一般認為駭客在3月20日之前已能夠自行進出目標環境。因為不可能一次對30,000以上的用戶進行社交工程攻擊。有了最初的受害者電腦系統受到感染，讓駭客有機會能進一步存取其他系統。

MBR刪除程式(MBR wiper)

MBR刪除程式皆於1月31日被編譯。Wiper本身是小型檔案（24KB）由母體木馬載入攻擊環境中，母體木馬418KB，於攻擊當天被編譯。

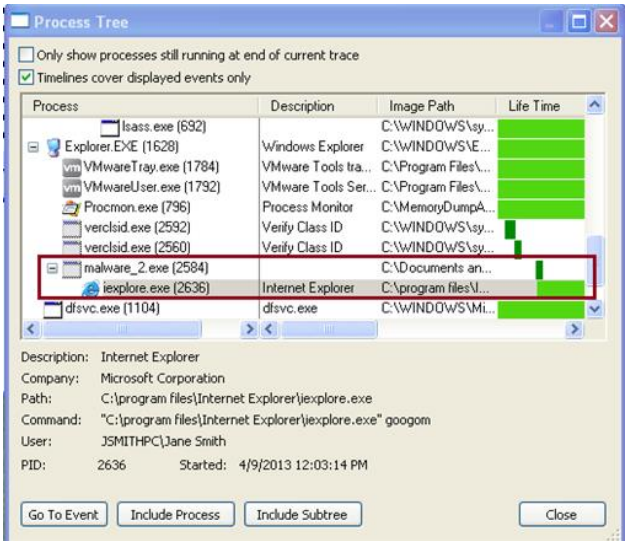
執行該惡意程式後，主要的母體木馬（9263e40d9823aecf9388b64de34eae54）衍生建立了名為AgentBase.exe的MBR刪除程式。檔案被放置在受感染用戶的應用程式資料文件夾中，會自動執行，並立即開始倒數計時以摧毀系統，使目標電腦無法正常開機啟動。該檔案大約在攻擊發生前兩個月被編譯。

主要母體惡意程式在3月20日攻擊當天，首爾時間上午04點07分被編譯。並且於首爾時間下午02:00執行安裝Wiper，摧毀了MBRs。一旦母體惡意程式執行時，目標電腦作業系統在幾分鐘之內被刪除。因此，這些惡意程式可能是先部屬但未執行，直到駭客希望的時間點發動攻擊摧毀這些目標電腦。

遠端存取的木馬程式(The remote-access Trojan)

駭客使用不易被管理員發現的遠端存取木馬程式攻擊內部伺服器，再利用這受控制的內部伺服器將Wiper組件分發至數千台PC。遠端存取木馬程式檔案大小為46KB，於1月26日被編譯，也就是在MBR Wiper發動前五天被編譯。

駭客在抹除電腦系統前，其實就已進入了目標環境。遠端存取木馬程式經由魚叉式網路釣魚活動被傳遞到內部PC，木馬立即在註冊表中修改屬性，以允許遠端連接到系統。駭客還存取了這些系統中其他內部資源。如圖2.1，該木馬被設計在Internet Explorer中執行，發動前隱藏在Internet Explorer的實體，並且在發動時自我關聯到正在執行中的處理程序。



資料來源：Sherstobitoff, R., I. Liba and J. Walter（2013） Dissecting Operation Troy Cyberspionage in South Korea, McAfee, 2013-03-20。

圖2.1：「進程監視器」顯示遠端存取木馬在Internet Explorer產卵的實體。

摧毀目標

間諜惡意程式具有破壞電腦系統的能力；2013年3月20日，惡意程式攻擊毀壞了韓國數以萬計的電腦系統。如果在敵手蒐集情報後，再將軍事網路突然抹除毀滅，這對受害者來說更是嚴重的損失與損害。3月20日“黑暗首爾（Dark Seoul）”事件，就是明顯的實例，在電腦系統遭受MBR抹除之前，3Rat木馬已取得存取權限[1]。

```
HANDLE __cdecl WipeAndReboot()
{
  unsigned int DriveNum; // esi@1
  struct _PROCESS_INFORMATION ProcessInformation; // [sp+8h] [bp-544h]@5
  struct _STARTUPINFOA StartupInfo; // [sp+18h] [bp-534h]@5
  int LLDiskInstance; // [sp+5Ch] [bp-4F0h]@1
  int v5; // [sp+53Ch] [bp-10h]@1
  int v6; // [sp+548h] [bp-4h]@1

  v5 = dword_10025840;
  LLDisk_CTOR(&LLDiskInstance);
  v6 = 0;
  DriveNum = 0;
  do
  {
    if ( LLDISK_OpenDisk((int)&LLDiskInstance, DriveNum) )
    {
      LLDISK_Wipe(&LLDiskInstance);
      LLDISK_Wipe2((DWORD)&LLDiskInstance);
    }
    ++DriveNum;
  }
  while ( (signed int)DriveNum < 4 );
  memset(&StartupInfo.lpReserved, 0, 0x40u);
  ProcessInformation.hProcess = 0;
  ProcessInformation.hThread = 0;
  ProcessInformation.dwProcessId = 0;
  ProcessInformation.dwThreadId = 0;
  StartupInfo.cb = 68;
  CreateProcessA(0, "shutdown -r -t 0", 0, 0, 1, 0, 0, 0, &StartupInfo, &ProcessInformation);
  v6 = -1;
  return LLDISK_CloseDisk((HANDLE *)&LLDiskInstance);
}
```

資料來源：Sherstobitoff, R., I. Liba and J. Walter（2013） Dissecting Operation Troy Cyberspionage in South Korea, McAfee, 2013-03-20。

圖2.2：用來抹除MBR之惡意程式的功能函數。

在韓國歷年的駭客攻擊事件中，將所發現行為明顯不同的子活動進行分類與比對發現以下六個情資[1]：

- 木馬程式幾乎都使用相同來源之原始碼，進行增加功能修改後即可發動攻擊。
- 木馬程式幾乎都用ZIP加上密碼封裝後傳遞
- 在惡意程式之編譯路徑中，使用一致的資料夾或檔案命名原則（例如，*Troy, Work,…*等）。
- 所有的變種程式都使用相同的網際網路聊天室（Internet Relay Chat，簡稱IRC）殭屍網路通訊管道與加密方法。
- 2009至2013年之間，所有惡意程式中都發現了軍事相關用語。
- 分別於2009~2010年與2012~2013年的活動，都使用相同字串模糊技術。

由此看來，3月20日攻擊發生之前，駭客確已進行與此次攻擊相關的韓國國內間諜活動，並獲得攻擊目標之相關情報，以開展進一步攻擊；其攻擊一直是隱藏之間諜活動，

駭客在抹除電腦系統前，就已擁有系統環境內安全軟體運行的知識，讓他們從3月20日之前，襲擊中使用的一些變種程式，看起來就像是防毒軟體的更新元件。

駭客於3月20日事件之前，透過使用各種自行撰寫的惡意工具，指揮隱匿攻擊行動持續了數年之久；至少是自2009年開始就有的一個長期國內間諜工作[1]。此攻擊行動之惡意程式皆修改自相同之原始碼，試圖滲透某些韓國的特定目標。它是基於在惡意程式編譯路徑字串中，被頻繁使用的"*Troy*"單詞。這些攻擊之首要犯罪嫌疑人組織-「新羅馬網軍團隊」，在他們的程式碼中頻繁的使用羅馬和古羅馬術語。事件之前之惡意程式組件，彼此有相近與一致性的檔案屬性，使其能夠將它們鏈接到遠端管理工具3Rat樣本可追溯至2010年3月20日，以及客戶端使用相同的屬性。透過事先存取受害者的網路，駭客能夠上傳MBR Wiper組件，並散播出去。它也可以被稱為"10 Days of Rain"，該行動是特洛伊行動的副產品；此外，在這些攻擊中，亦發現了惡意程式"隱蔽性特洛伊（Concealment Troy）"的蹤跡[1]。

以上所述之攻擊，通常會發生在四個階段：

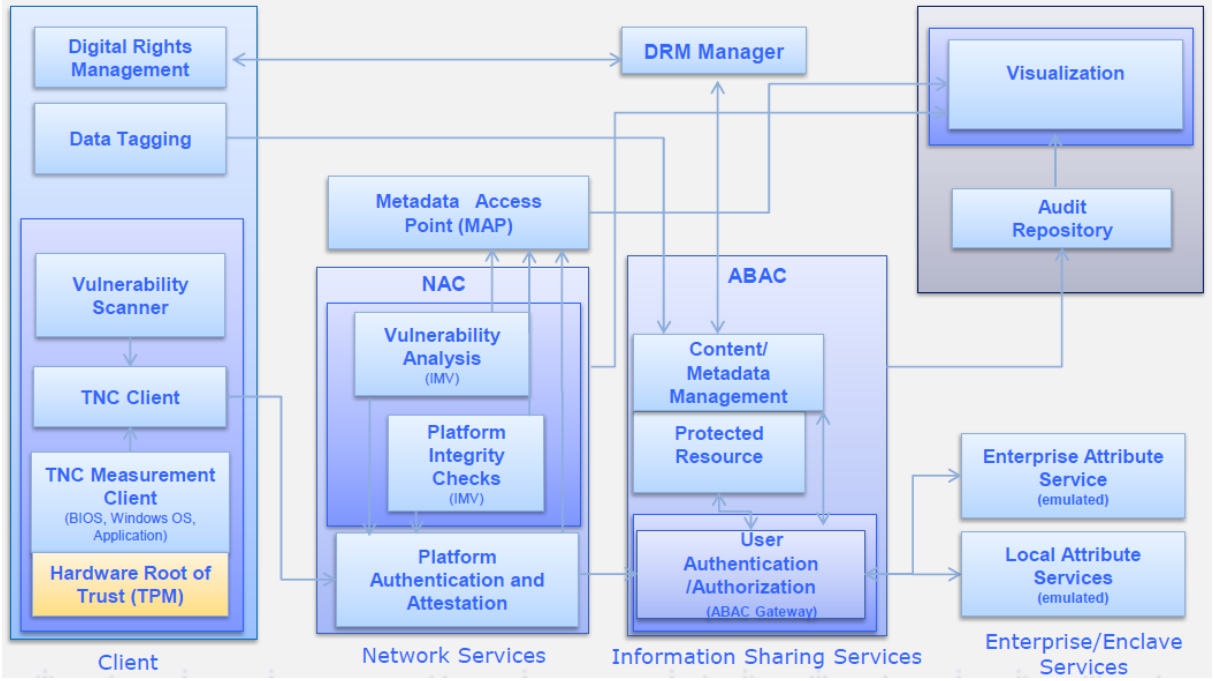
- 經由"水坑（Watering Hole）攻擊"進行初步危害，這將導致內部系統遭受攻擊（在2009年的情況）。（駭客放置了一個零時差剌探利用（zero-day exploit）在軍事社交網站上）。後來的情況也很可能用魚叉式網路釣魚，讓攻擊能更迅速地獲得正確目標。
- 惡意程式會自動在目標系統上執行偵察，以尋找感興趣的文件檔案。惡意程式也可以沿著感興趣的檔案目錄列表，刮除密碼與登錄訊息。
- 當駭客對某些資料感興趣，可以從受感染的系統要求目錄內容。可以選擇性回傳所需的特定檔案。
- 竊取之文件透過HTTPS加密通道，傳輸到駭客的伺服機。

此次韓國遭受長期潛伏攻擊的真實意圖，在於試圖剌探和破壞韓國軍方與政府活動。大部分的木馬惡意程式都是基於相同的源程式碼，用來設計這些特殊的變種惡意程式，如bs.dll與payload.dll，這將會發現整個惡意程式家族的一致性。駭客自2009年以來試圖設置具有摧毀目標能力之MBR Wiper組件，就像在"黑暗首爾（Dark Seoul）"事件中所見的。他們從一開始就已經認定特洛伊行動，就是聚焦於蒐集韓國軍事目標情報。

三、網路端點安全與TCBTIP：

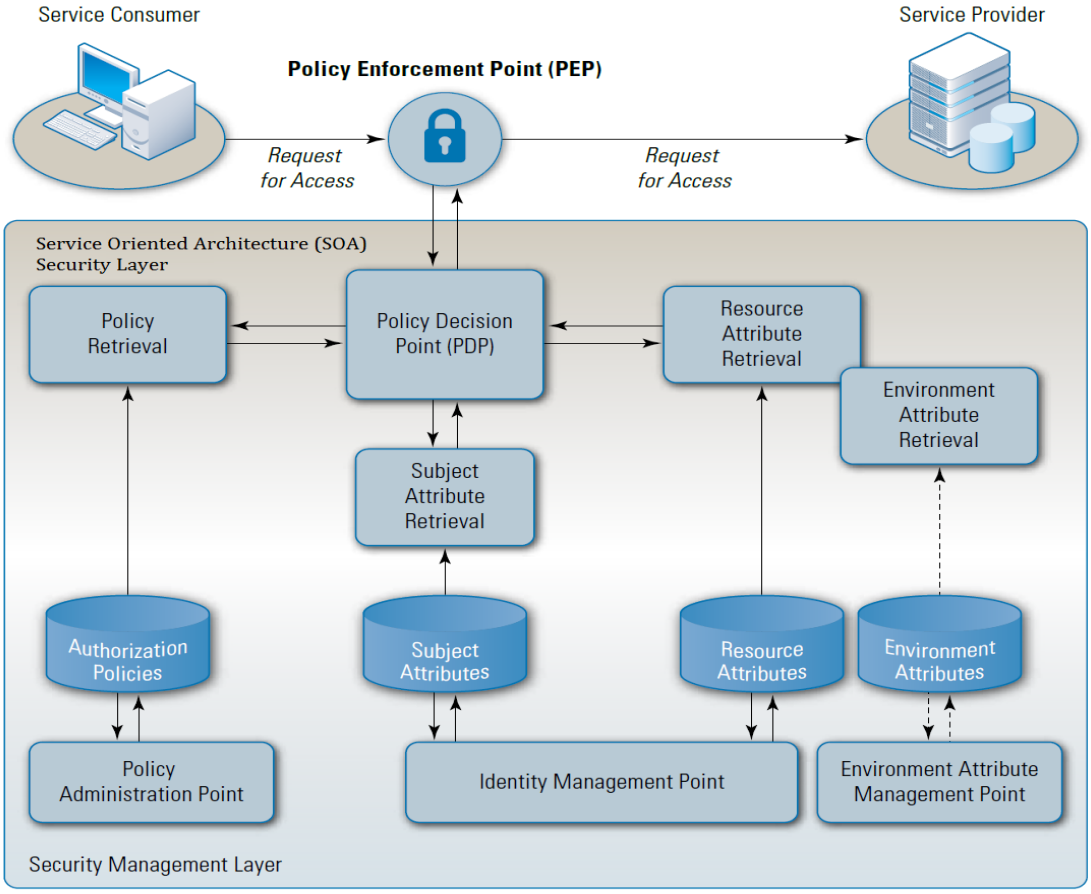
結合密碼學技術，使用雙重識別與根基於安全內容自動化協定（Security Content Automation Protocol，簡稱SCAP）及其之安全自動化資料信賴模型（Trust Model for Security Automation Data，簡稱TMSAD）以及可信賴網路接取（Trusted Network Connect，簡稱TNC）等標準[8~10]，經由精細化（granular）的存取控制與BIOS之完整量測，保護MBR等資訊系統底層資料的正確性以防止類似表1.1的攻擊之可行性是TCBTIP之標的；圖3.1及圖3.2分別是其高階架構以及屬性基於存取控制（Attribute Based Access Control

，簡稱ABAC）授權樣型之示意說明，圖3.3是BIOS完整性架構的示意說明。



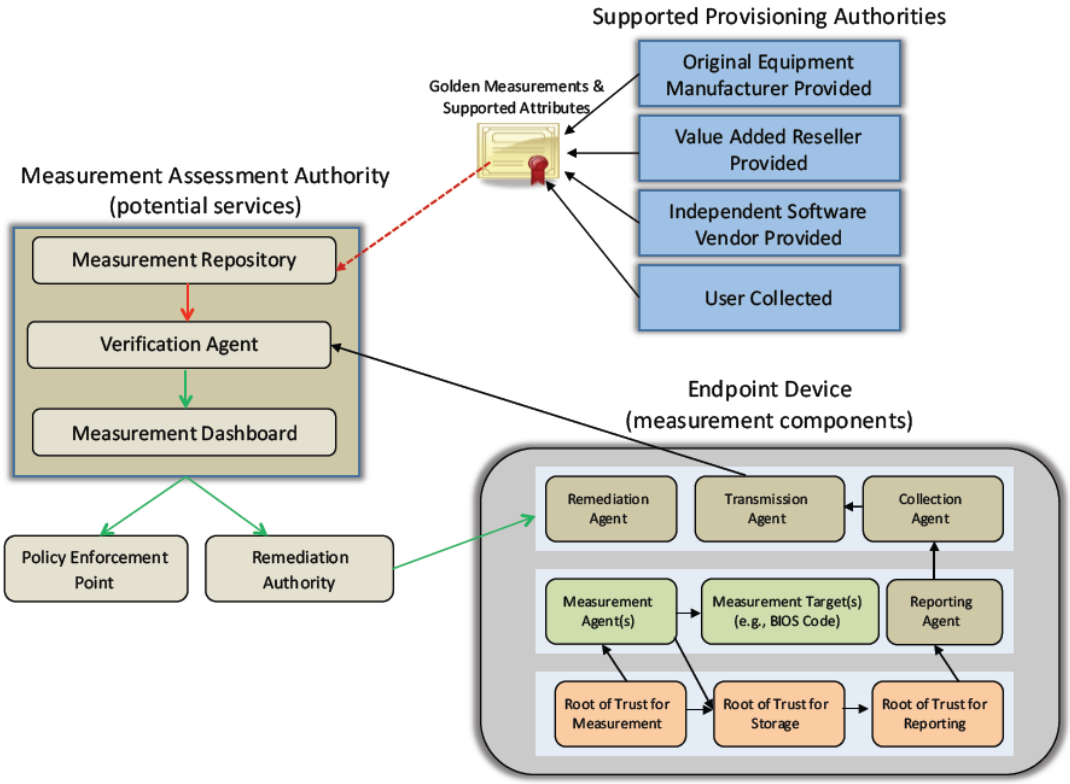
資料來源：Leslie Andresen (2011) Trusted Computing Based Insider Threat Protection, 2nd Annual NSA Trusted Computing Conference & Exposition (Presentation), 2011-09-20。

圖3.1：TCBITP高階架構



資料來源： DoD/IC SOA Security Reference Architecture: IAnewsletter, Vol. 14, No. 3, Summer 2011, Figure 1, page 16, http://iac.dtic.mil/iatac/ (2012-06-23)。

圖3.2：屬性基存取控制(Attribute Based Access Control，簡稱ABAC)授權(Authorization)樣型(Pattern)



資料來源：Regenscheid, A. and K. Scarfone (2011) BIOS Integrity Measurement Guidelines (Draft), NIST Special Publication 800-155 (Draft), Figure 1, page 8, December 2011。

圖3.3：基本輸出入系統(Basic Input/Output System，簡稱BIOS)完整性(Integrity)架構(Architecture)

簡言之，TCBITP經由裝置識別類（Device Identity Class，簡稱DIC）與使用者識別類（User Identy Class，簡稱UIC）之鑑別機制，再經由精細至內儲於TCB的諸如MBR之屬性，使用內嵌式的公開金鑰基礎建設（Public Key Infrastructure，簡稱PKI）以查證及確認ABAC之完整性，已提昇面對表1.1的攻擊時之防護能力[3~9]。

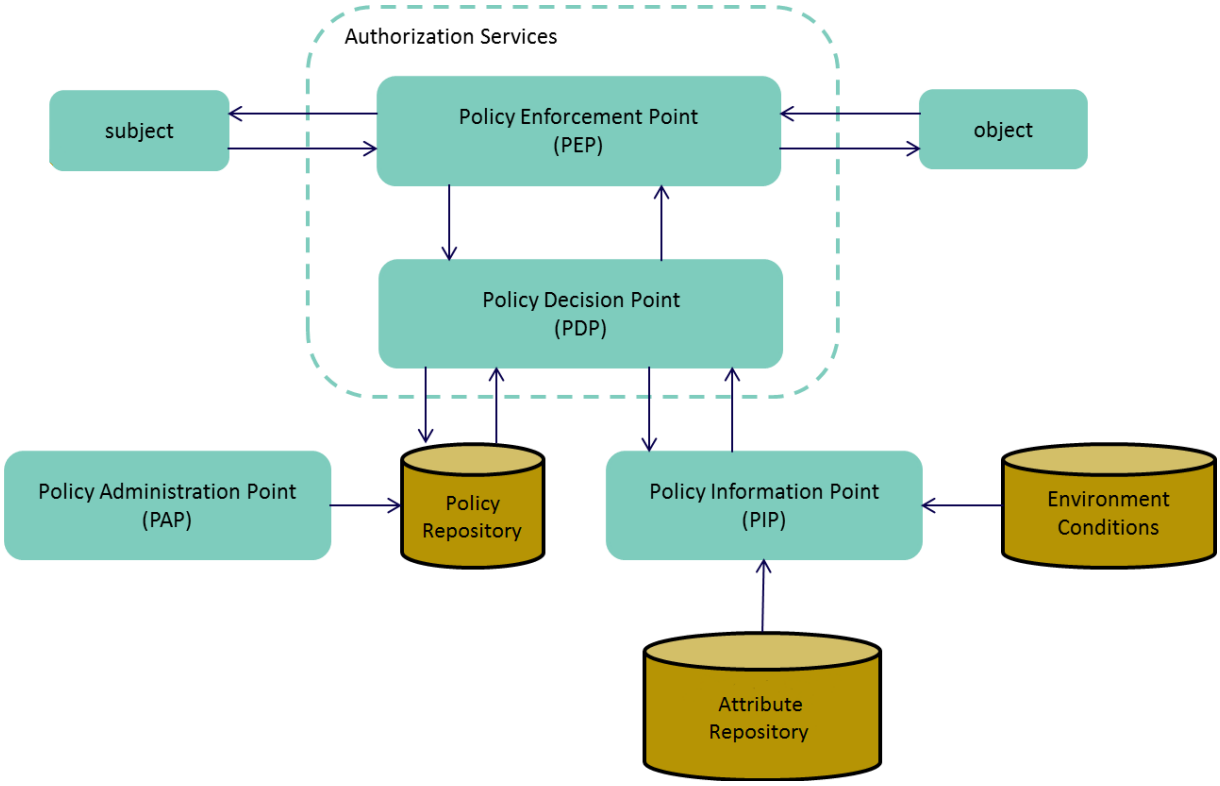
四、結論：

由於網路之普及與系統程式功能的日益強大，帶給使用者許多效益，但是伴隨而來之網路攻擊的情境亦更形嚴峻，各種攻擊手法充斥著社會，這些攻擊不僅會導至資安事件或毀損資訊系統，甚至癱瘓整個網路[1]。

能有效防護惡意程式碼之資訊安全護理（Healthcare）是一個富於創造性的研究領域。歷經從國家脆弱性資料庫（National Vulnerability Database，簡稱NVD）之產品（Product）到SCAP1.2版之實作，已證實其有效性[5~12]；為落實TCBITP，於可信賴網路接取（Trusted Network Connect，簡稱TNC）的存取控制機制（Access Control Mechanism，簡稱ACM）[10]，ABAC提出擴增TNC之如圖4.1所示之PDP（Policy Decision Point）與PEP（

Policy Enforcement Point)，增加PAP(Policy Administration Point)及PIP(Policy Information Point)，表4.1是TCBITP取徑的組件表列，期能有效管理前述MBR等之安全性[5~12]；TCBITP的實作尚在開展之中，是否如TPM1.0般：「起而未行」，還是隨著TPM2.0的問市以及SCAP之逐漸普及而融入資安技術中？尚待驗證，惟如何簡化其使用介面，應具攸關性。

TCBITP根基於數位簽章與SCAP及TNC以及TPM，圖4.2是其作業之簡要說明[3,6,8~15]；以更新MBR為例，若設定環境屬性為離線，時間屬性為分成20階段，每階段30分鐘，分批更新，則面對「黑暗首爾」的攻擊時，能提高其防禦之有效性；囿於篇幅，有興趣的讀者可以參閱參考文獻「3,6,9,10,12」。

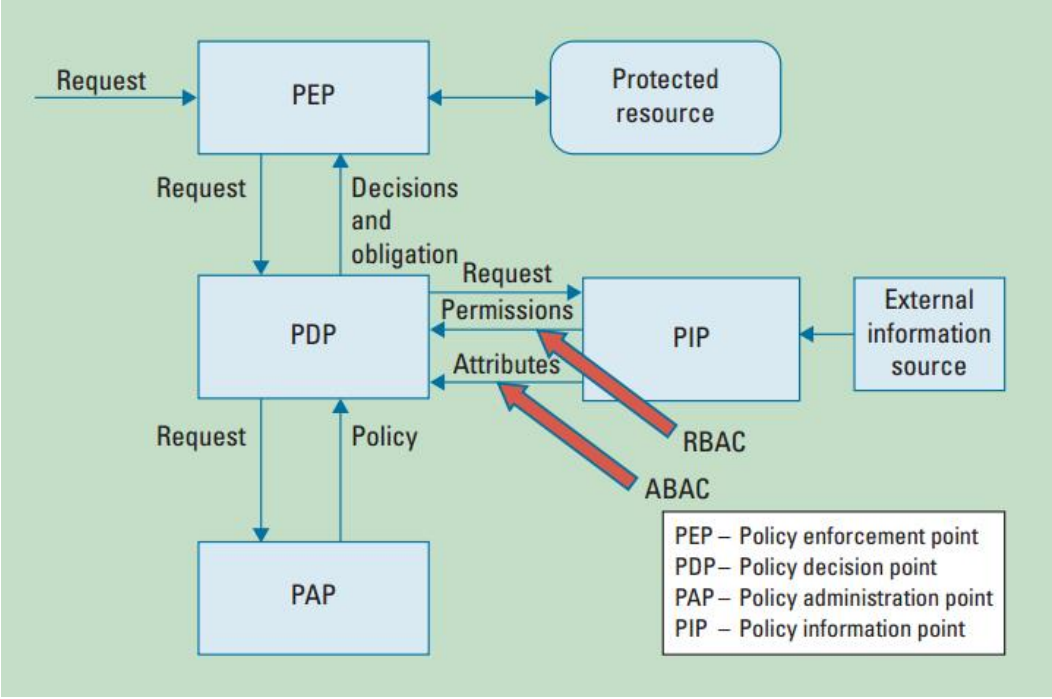


資料來源：Hu, C. V. et al. (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations, NIST Special Publication 800-162, Figure 5, Page 15, Jan. 2014。

圖4.1：屬性基存取控制（Actribute Base Access Control，簡稱ABAC）之存取控制機制

表4.1：可信賴基底之內部威脅的保護(Trusted Computing Based Insider Threat Protection，簡稱TCBITP)之取徑表列：

1.可信賴平台模組(Trusted Platform Module，簡稱TPM)。
2.安全內容自動化協定(Security Content Automation Protocol，簡稱SCAP)。
3.可信賴網路接取(Trusted Network Connect，簡稱TNC)。
4.安全自動化資料信賴模型(Trust Model for Security Automation Data，簡稱TMSAD)。
5.網路存取控制(Network Access Control，簡稱NAC)。
6.屬性基存取控制(Attribute Based Access Control，簡稱ABAC)。
7.態勢感知(Situational Awareness)。



說明：1. ABAC經由RBAC（Role-Based Access Control）執行識別、環境、時間、資源、觸點、定址（例：MBR）、適當性等屬性規範。

2. ABAC使用布林函數（Boolean Function）決定是否准許使用者（u）在客體（o），在特定之環境（e）下執行其所欲的作業（op）之規則集（$Rules$），A（）代表使用者預存的屬性函數：

$$\{\text{允許（grant）、拒絕（Deny）}\} \leftarrow \text{決策（decision）}\ (A(u) \times A(o) \times A(e) \times Rules \times op)$$

3. 資料來源：http://www.csrc.nist.gov/project/abac（2014-03-11檢索）

圖4.2：屬性基存取控制作業示意說明

當SCAP已納入雲端運算資訊安全控制措施且日本（2002年06月起）、中國大陸（2007年04月起）等均已進行其實作之此時[11]，在2013年至2016年的國家資訊與通信安全發展方案中，我國NVD及SCAP以及TCBITP等之工作計畫，是具攸關性的議題，宜進行深入之分析與探討，再制定適當之行動方案。

參考文獻：

[1] Sherstobitoff, R., I. Liba and J. Walter（2013） Dissecting Operation Troy Cyberspionage in South Korea, McAfee, 2013-03-20。

[2] 吳啟文（2013）政府資通安全威脅趨勢及防護策略（簡報資料），第 23 屆全國資訊安全會議，2013-05-23（A.M.09:15~10:05）。

[3] Regenscheid, A. and K. Scarfone (2011) BIOS Integrity Measurement Guidelines (Draft), NIST Special Publication 800-155 (Draft), December 2011。

[4] DoD/IC SOA Security Reference Architecture: IAnewsletter, Vol. 14, No. 3, Summer 2011。

[5] Leslie Andresen (2011) Trusted Computing Based Insider Threat Protection, 2nd Annual NSA Trusted Computing Conference & Exposition (Presentation), 2011-09-20。

[6] Unal, D. and M.U. Caglayan (2013) A formal role-based access control model for security policies in multi-domain mobile networks, Computer Networks, Vol.57, No.1, pp.300~350。

[7] Enders, R. and H. Schwarz (2013) Network Endpoints and Attribute Based Access Controls, May 2013 Whitepaper and Presentation Submissions, ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) (http://www.ics-cert.us-cert.gov/(2013-10-19 檢索)。

[8] http://nvd.nist.gov/(2013-10-19 檢索)。

[9] Booth, H. and A. Halbardier (2011) Trust Model for Security Automation Data 1.0 (TMSAD), NIST Intergency Report 7802 September 2011。

[10] 樊國楨與黃健誠 (2013) 下一世代網路(Next Generation Network，簡稱 NGN)安全標準初探之三：可信賴網路接取(Trusted Network Connect，簡稱 TNC)，網路通訊國家型科技計畫簡訊，第 54 期，頁 38~47。

[11] 樊國楨、黃健誠與朱潮昌 (2013)資訊安全管理與脆弱性評分系統初探，電腦稽核，第 27 期，頁 79~101。

[12] Cooper, D. etal. (2011) BIOS Protection Guidelines, NIST Special Publication 800-147, April 2011。

[13] Hu, C. V. et al. (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations, NIST Special Publication 800-162,Figure 5, Page 15, Jan. 2014。

[14] E.J. Coyne, T.R. Weil (2013) ABAC and RBAC: Scalable, Flexible, and Auditable Access Management, IEEE IT Professional, May/June 2013 (reviews tradeoffs and characteristics of role based and attribute based approaches)。

[15] D.R. Kuhn, E.J. Coyne, T.R. Weil (2010) "Adding Attributes to Role Based Access Control", IEEE Computer, June, 2010, pp. 79-81 (discusses revisions to RBAC standard being developed to combine advantages of RBAC and ABAC approaches)。