家庭網路簡易監控機制

謝文恭
中國文化大學資訊管理研究所
(11114)**台北市陽明山華岡路** 55 **號**
wgshieh@faculty.pccu.edu.tw

黃鈞鴻
中國文化大學資訊管理研究所
(11114)**台北市陽明山華岡路** 55 **號**
g8914028@ms2.pccu.edu.tw

摘要

本文針對一般家庭中以資訊家電為主的家庭網路，提出一個簡單、易於使用、可負擔而安全的家庭網路監控方法。相較於企業網路，大眾化的家庭網路雖然沒有企業網路來得有規模，但其所含蓋的範圍卻直接影響我們的日常生活。因此，以簡單可靠為前題，在成本與技術的考量下，本研究應用 Hashing **與低成本的對稱加密等技術，提出簡易的監控機制，讓在遠端的使用者可以安全的使用無線或有線的裝置來監視與控制家中的資訊家電。**

關鍵詞：資訊家電、家庭網路、資訊安全

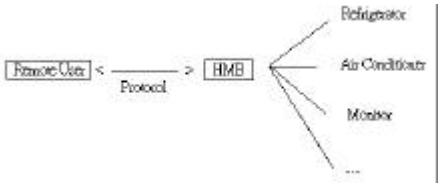
一、緒論

家庭網路與個人行動裝置的興起將是今年資訊界最熱門的話題，尤其是整合上網能力的資訊家電，更是未來家電的主流。家庭網路環境，包括了許多的具有上網能力的設備，彼此以有線或無線的傳輸方式與裝置溝通。因此，為了保障個人的隱私與機密資料，需要確保家庭網路設備的安全管理以及資料的傳輸保密。

一般家庭中以資訊家電為主的家庭網路，其網路環境與企業的網路環境並不相同，需要保護資料的性質與重要程度也有所不同，相對所應負擔的成本也有所不同。例如使用者希望在遠端控制家中冰箱的溫度、打開家中的冷氣或監看家中環境情況，諸如此類的需求，所需之安全保護不外乎是防止外人入侵家庭網路非法監控，或保護外傳之家中即時影像或聲音的隱私。其所付出之成本與企業網路所需付擔之資訊安全成本，自不應相提並論。

因此，本文針對大眾化家庭網路遠端監控之需求，考慮簡單、可負擔而安全的家庭網路監控機制(如圖 1.1)**。圖中之** Home Manager Broker(HMB)**與遠端使用者應用軟體，透過預設協定**(protocol)**，應用** Hashing **與低成本的對稱加密等技術，來提供簡易的安全機制，讓在遠端的使用者可以安全的使用無線或有線的裝置來監視與控制家中資訊家電。更明確的說，本研究乃應用** Mohammad Peyravian and Nevenko Zunic**[11]所提出的密碼傳遞時的保密方式，並修改其認證過程中訊息交換的協定，作為安全監控的機制。**

圖 1.1 **家庭網路環境**



(**資料來源:本研究整理**)

本文以下將於第二節探討相關的文獻，第三節比較家庭網路與企業網路不同之處，第四節提出我們的安全保護機制並於第五節加以評估，最後提出結論與未來研究方向。

二、文獻探討

(一) 資訊家電

根據美國國家半導體公司 (National Semiconductor Corporation)**對資訊家電所提出的定義[9]：**

針對特定用途且具互動的資訊存取功能

的設計，可負擔而易於使用的裝置。而資訊家電最主要的特色是具功能性、品質穩定、可靠性及易於使用性。

由 Roy Want[13]等對資訊家電裝置的調查，認為裝置的功能是為了特定的目的所發展出來的，它可增加使用者的效率，節省使用者的時間，如洗衣機和洗碗機就是一個例子。但獨立的裝置可不像桌上型電腦一樣具有通訊、處理資訊、展示的能力，一方面電腦成本太高，另一方面使用者只需要幾個簡單的功能，並不需要用到運算能力強、具大量儲存能力的電腦來控制。因此，一種具有 Low Power、high-performance CPUs、可提供特定功能與資訊存取能力的裝置被發展出來，稱之為"資訊家電(Information Appliance)[13]。

另外，資訊家電，根據 IDC(International Data Corporation)的解釋，一項資訊家電產品應包括三項特性：低價、容易操作、上網能力。包括網路電視、線上遊樂器、網路螢幕電話、可上網的掌上型設備等都被 IDC 歸類於資訊家電的範圍之內。

(二) 家庭網路

一般傳統的家庭網路利用家中電話線或網路線，讓家中多台電腦和附屬裝置之間能傳送、接收資料。但隨著通訊科技的進步，家庭網路變得不再是那麼單純，其所含蓋的範圍除了一般的家用電腦外，尚包括了具有連網與控制能力的家庭設備，也就是一般所稱的資訊家電。

方便、容易使用可說是資訊家電的精神，這樣才能符合真正的需要。為此特性與消費習慣，家庭網路對設備使用的簡易性與價格相當的敏感。因此，家庭網路技術均以能妥善利用家庭中現有設備而成之家庭網路為主，包括電話線(Phone Line)、纜線(Cable)等。另外，隨著寬頻網路的來臨，多媒體影音的資料傳輸，利用目前的佈線是不足以因應的，新一代的傳輸技術如 USB2.0-(Universal Serial Bus)、Power Line、IEEE1394(Institute of Electrical and Electronic Engineers)、HiperLAN/2、802.11X、Bluetooth、HomeRF 等家庭連網技術[7]，在未來家庭網路中也佔一定的重要性角色。

(三) 資訊家電的應用

就目前資訊家電的應用方向，可分為下列四種類別[13]：

(1) Home Use
(2) Office Use
(3) Mobile professionals
(4) Specialist occupations

雖類別區分、應用方向不同，但皆強調無線通訊的能力，並可隨時隨地連接 Internet 和 WWW(World Wide Web)。就目前現有的產品包括了電子書、全球定位裝置、具上網能力的電話、WebTV、Wireless Based PDA、Embedded Web Servers、Smart rooms、Wearable computers 等。

結合多樣化的資訊家電產品，整合了多樣化的服務，資訊家電在家庭網路的應用可分為下列幾個方向[1]:

(1) 多人同時連網
提供家庭多台上網機上網，包括了無線連網技術的結合，不需要複雜的接線施工，即可讓家中的多台上網機輕鬆連線，共享網路資源。
(2) 能源與儀表管理
結合電力、水力、瓦斯等家庭能源的管理機制，使用者可直接透過能源儀表裝置了解目前家庭能源使用狀況，而電力公司、水力公司則可透過家庭網路裝置了解目前能源的使用刻度，結省人力抄表的成本，且更為精準。
(3) 保全服務
家庭防盜系統、火警警示系統與保全業的安全防護結合，提供使用者更安全的居住環境。
(4) 設備監視與控制服務
提供家庭設備的狀況及使用狀態，對於使用者外出時，可隨時地透過遠端服務來對資訊家電做控制或修正的動作。
(5) 病患與老人看護服務結合網路攝影機查看家庭目前的現狀，更可結合醫療服務網，提供病患或老人看護服務。

資訊家電在這股網路熱潮下創造了非常多的商機，相對地為了符合未來市場的需求，

勢必須面臨更多整合設計上的挑戰。

(四) 家庭網路安全相關研究

目前對於家庭網路安全主題的研究，逐年的增加，而研究的範圍包括了家庭網路的無限傳輸協定、手持式裝置的通訊安全與遠端控制的機制探討，提供了不同方向的思考。在這整理了幾個相關性的研究主題，如表所示。

Securing the handheld environment –An Enterprise Perspective**[10]**	主要討論手持式電腦的安全、未來手持式裝置的安全的特色。
A Comparison of Security in HomeRF versus IEEE802.11b**[8]**	主要為探討 HomeRF 與 IEEE802.11b 標準的差異與安全性。
Wireless Lan Security**[4]**	主要為無線網路安全的探討。
Web-Enabled Information Appliances for Broadband Residential Networks**[2]**	提供一個遠端控制家中的烤麵包機的機制。
A User Interface System for Home Appliances with Virtual Network Computing**[6]**	使用 VNC 的機制監控家庭設備。
Connecting Your Home LAN to the Internet –Securely**[3]**	對家庭網路安全性的探討與保護措施。

與上表中研究主題不同的是，本研究並非針對所有家庭網路探討，而是針對簡單大眾化的家庭網路之監視與控制，提出一個滿足安全、可靠、可負擔的作法，並使用簡易的加密方式，來確保家庭網路監控的安全。

三、家庭網路與企業網路不同之處

根據 HomeRF Working Group **[5]**對網路市場的報告(May 9,2001)指出，目前網路使用市場大致可分為四塊(圖 3.1):

(1) Personal Connectivity

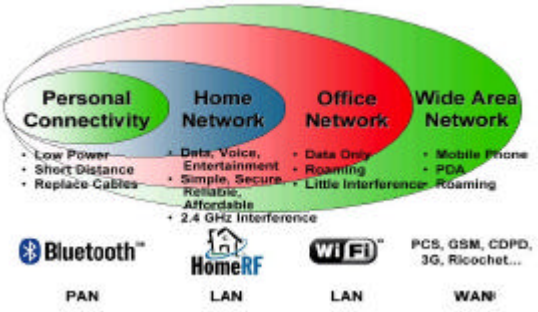
(2) Home Network

(3) Office Network

(4) Wide Area Network

其中 Personal Connectivity 主要是以個人攜帶方便為主，強調 Lower Power、Short Distance、Replace Cables 等。Home Network 主要為在資料、語音與娛樂上的應用，強調簡單、安全、可靠、可負擔的，並提供 2.4GHZ 的傳輸。而在 Office Network 大部份使用於資料的傳輸、網路資料的瀏覽、少許的資料互動。

圖 3.1 網路使用市場狀況表



(資料來源:ken Haase**[5]**)

家庭網路與企業網路雖可視為一個 Lan 的網路環境架構，但兩者確有截然的不同，不論在使用對象、傳輸媒介、使用裝置、應用範圍、成本、安全的考量上都有很大的差異。

(一) 家庭網路與企業網路之比較

以下為家庭網路與企業網路的簡單比較:

(1) **家庭網路**

- 家庭網路使用對象為家庭成員
- 傳輸媒介為電話線、電力線等
- 使用裝置為資訊家電，如可上網的冰箱、冷氣、烤箱等
- 家庭網路服務包括上網機、控制家電設備、監視、看護、保全
- 家庭網路一般來說設備成本較低，網路環境較為單純

- 特定功能性，品質穩定，容易使用

(2) 企業網路

- 企業網路使用對象，對內是企業員工
- 傳輸媒介為網路線、wireless 網路等
- 使用裝置為 PC 與其週邊設備，如印表機、掃瞄器等
- 企業網路一般常使用於對資料的存取與交換
- 企業網路設備一般來說設備成本高，網路環境架構較複雜
- 需有完善的規劃，操作需具專業的能力
- 電腦處理運算能力強，具有儲存裝置，安全控管與維護成本高

	家庭網路	企業網路
使用對象	家庭成員	公司、SOHO
使用媒介	電話線、電力線	網路線
使用裝置	上網的冰箱、冷氣、烤箱	印表機、掃瞄器
功能性	簡單	複雜
使用性	簡單	複雜
穩定性	較佳	佳
運算能力	低	高
維護成本	低	高

(二) 家庭網路與企業網路面臨的安全威脅

網路的使用雖有其便利性，但在安全與隱私上，網路技術所帶來的網路安全危機，將造成許多企業機構或家庭網路遭受病毒或駭客趁機而入。根據上述的比較結果，不同的網路環境與裝置，相對的在安全威脅考量上也有所不同。

(1)企業網路的安全威脅

- Interception
  企業網路受到竊聽，資料被非法複製、偷竊。
- Interruption
  企業資料受到破壞，檔案系統遭到刪除，侵犯了可獲得性。
- Modification
  企業檔案或程式遭到非法的修改，受到間接的影響。
- Fabrication
  企業系統被植入偽裝程式或被冒充之使用者，非法竊取資料或修改資料

(2) 家庭網路的安全威脅

- Authentication
  家庭網路的認證機制遭受到非法使用者的破壞並入侵，非法取得家庭網路的使用權限，危害家庭的安全。
- Integrity
  家庭網路遭受入侵，資訊家電設備遭受未允許的修改控制，如家庭冰箱遭 Hacker 修改溫度設定，導致食物損壞等。
- Availability
  家庭網路遭受惡意攻擊，無法連接資訊家電。資訊家電雖然在需要的時間內無法連接控制，以安全的考量上，家庭並無受到安全的威脅，只是在需要的時間內無法使用。
- Confidentiality
  家中外傳之監視、影音資訊被中途複製盜用，妨害隱私及家庭安全。

(3)家庭網路現有保護方案

由於家庭網路與企業網路受到的安全威脅不同，保護的價值也不同，相對的在成本考量上也有所差異，因此滿足安全的機制也有所差異。

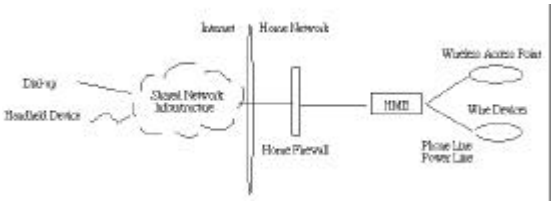
目前現有的產品中，已經有滿足的方式，但硬體的成本過高，非一般家庭使用者可接受。

四、保護

本研究將針對家庭網路的安全威脅，提出一個簡單的安全機制，讓使用者可對家庭網路中的設備進行監控的動作。所謂的監控包括了控制與監視。控制指的是對家中的資訊家電設備做控制的動作，而監視指的是透過家庭網路攝影機來察看目前家中的現況，包括了聲音與影像的傳輸。

本文考慮之家庭網路的環境如下所示，家庭網路中有一個 HMB(Home Management Broker)的控制器，透過 HMB 來管理所有家庭網路中的設備，提供了權限控制與監控保護的機制。其中在 HMB 之前有個 Home Firewall，是選擇性可有可無的裝置，其可為簡單的軟體或是硬體防護，主要功能是替家庭網路過濾一些基本的攻擊與入侵動作，為家庭網路做第一層的基本把關。

圖 4.1 資訊家電遠端監控



(資料來源:本研究整理)

HMB 則提供了下列兩個權限控制與監控保護的機制，為家庭網路做第二層的保護。

(一) 權限控制

家庭成員可依不同的需求設定自己有權限控制的設備。所謂的權限控制是指對資訊家電的控制權限。透過 HMB，來設定使用者對資訊家電的控制權限，讓適當的使用者做適當的事，如圖所示。

圖 4.2 HMB 權線控制機制

(資料來源:本研究整理)

使用者使用除了使用 HMB 建立帳號、密碼與設定控制權限，並由 HMB 產生使用者密碼訊息摘要(idpw_digest = hash (使用者 id, 使用者密碼 pw))存入 HMB 中。HMB 並不儲存使用者的密碼，只儲存使用者及其密碼的訊息摘要(idpw_digest)，以保護密碼的安全。

(二) 監控保護

本研究應用 Mohammad Peyravian and Nevenko Zunic[11]所提出的密碼傳遞時的保密方式，並修改其認證過程中訊息交換的協定，作為安全監控的機制。

使用者在 client 端對 HMB 執行遠端監控，client 與 HMB 驗證協定說明如下:

(1) 使用者輸入 userid(id)、request、password(pw) 到 client 端，client 計算 idpw_digest =hash (id ,pw)， 並比對 idpw_digest 與預先儲存的 idpw_dugest, 若符合則作下一步。

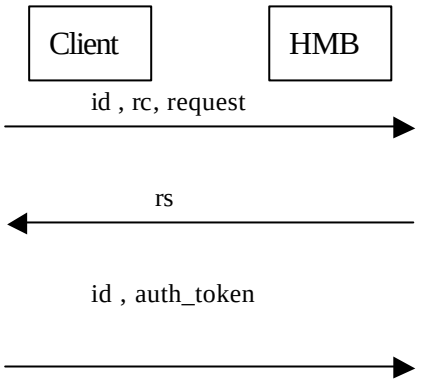
(2) client 端產生一個 random values(rc)並送出 id、request、rc 到 HMB，HMB 驗證 request 是否為可接受的控制，如可接受則做下一步的動作。

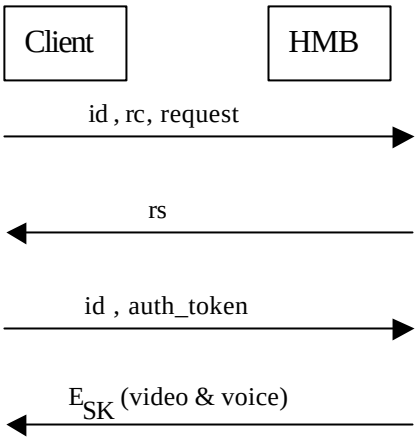
(3) HMB 產生一個 random values(rs)並把它回傳給 client 端。

(4) Client 端產生“ one-time “ auth_token values
auth_token=hash(idpw_digest,rc,rs,request)

(5) Client 端送出 id 和 auth_token 到 HMB，HMB 檢查 auth_token, 方法為 HMB 自行計算 auth_token, 並與所收到之 auth_token 比對，若符合則做下一步。

(6) HMB 檢查使用者權限，並執行可接受的控制動作。





針對外傳之家中即時影像或聲音的隱私部份，本文建議採用 Stream Cipher 的方式來保護聲音與影像傳輸的隱密性。使用者 client 端與 HMB 的監控動作，其方式如下說明:

(1) 使用者輸入 userid(id)、request、password(pw) 到 client 端，client 計算 idpw_digest =hash (id ,pw)， 並比對 idpw_digest 與預先儲存的 idpw_dugest, 若符合則作下一步。

(2) client 端產生一個 random values(rc)並送出 id、request、rc 到 HMB，HMB 驗證 request 是否為可接受的控制，如可接受則做下一步的動作。

(3) HMB 產生一個 random values(rs)並把它回傳給 client 端。

(4) Client 端產生“one-time“ auth_token values，auth_token = hash (idpw_digest ,rc, rs,request)。

(5) Client 端送出 id 和 auth_token 到 HMB，HMB 檢查 auth_token, 方法為 HMB 自行計算 auth_token, 並與所收到之 auth_token 比對, 若符合則做下一步。

(6) HMB 檢查使用者權限，並執行可接受的控制動作。HMB 針對外傳之聲音與影像使用簡易 stream ciphers 加密 (例如使用 polyalpha- betic 方式[12])，並採用 SK = hash (idpw_digest , auth_token)為 session key，將影音密文(E_{SK}(video & voice))傳送至 client 端。

在監視方面，使用 stream ciphers 加密傳送的好處是加密速度快、不需要等待，適合大資料量的影像、聲音等封包的傳輸，雖然有較易破解的缺點，但每次加密的 random session key 不一樣，可提高保密性，對家庭網路的監視需求來說是足夠的。由於本文方法不需網路傳送加密金鑰，且使用者從未傳送密碼或其訊息摘要， HMB 也不儲存使用者的密碼，只儲存使用者密碼的訊息摘要，成本低卻又保障了外傳之家中即時影像或聲音的隱私安全。

五、評估

由於需要保護的資料價值不同，相對的保護資料所需的成本也就不同。針對一般家庭的使用者而言，本研究所提出的家庭網路簡易監控模型，不論是成本上、功能上、安全上皆能滿足一般家庭網路使用者的需求。歸納下列幾點:

(1) 易於使用:

使用者在第一次使用該控制裝置時需直接在 HMB 上輸入 id 與 password 並設定權限，使用者即可使用該裝置對家庭網路設備進行監控的動作。當使用者需遠端監控家庭網路時，只需在 client 端輸入 id、request 以及 password，其餘動作皆可由 client 與 HMB 來完成，極為簡便。

(2) 安全的:

Client 及 HMB 裝置內皆無使用者的密碼，只有使用者及其密碼的訊息摘要。而傳輸協定當中，亦不傳送使用者密碼或其訊息摘要，確保使用者密碼的安

全。對家中外傳的影音資訊，亦做適當之簡易加密，且加密金鑰(session key)是隨機的，每次不一樣，更不需網路傳送加密金鑰。因此，雖然採用簡易快速的stream cipher加密，亦能符合保護大眾化家庭網路安全的需求。

(3) 可負擔的:

使用訊息摘要及簡易的加密方式來保護家庭網路的監控安全，成本遠比現有的產品來的低廉，不但簡單、速度快、功能性佳，更是一般家庭網路使用者可負擔的。

六、結論

本文針對大眾化家庭網路，提出一個簡單、可負擔而安全的家庭網路監控機制。透過預設協定(protocol)，應用 Hashing 與低成本的對稱加密等技術，提供了簡易的監控機制，讓在遠端的使用者可以簡單安全的使用無線或有線的裝置來監視與控制家中資訊家電。

但隨著資訊家電的增多，每個家電皆有其特殊的功能與獨立運作的特性，就目前而言，並無完整功能性的整合，且有諸多不便。因此，如何讓家電設備能有效溝通並在功能上做互動性的整合，並提供資訊家電整合性的管理機制，以提升使用的便利性，確保居家生活安全，為未來推展家庭網路最重要的一環，也是我們未來的研究方向。

七、參考文獻

[1] 曾曉晴，"網路家電之發展趨勢分析",財團法人資訊工業策進會資訊市場情報中心，3月 2001 年。

[2] Fatima Ahmed and Yan Jiao, "Web-Enabled Information Appliances for Broadband Residential Networks," http://cs.spsu.edu/YES/YES5.6.PDF.

[3] Andrew S. Baker, "Connecting Your Home LAN to the Internet – Securely, " March 27, 2001, http://www.sans.org/infosecFAQ/homeoffice/home_LAN.htm

[4] Cisco Systems, "Overview Wireless LAN Security - The Growth of Wireless LANs," Wed.Apr.2001, http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm.

[5] Ken Haase, "HomeRF Wireless Voice, Data and Streaming Media for the Broadband Internet Home," general Chair, HomeRF Working Group Public Seminar, May .2001.

[6] Hasedawa and Nakajima, "A User Interface System for Home Appliances with Virtual Network Computing, "Distributed Computing Systems Workshop, 2001 International Conference, 2001.

[7] HomeRf Working Group, "Quality of Service in the Home Networking Model, HomeRF Working Group," White Paper, 2000, http://www.homerf.org/data/tech/HomeRF_QoS_whitepaper.pdf.

[8] HomeRf Working Group," A Comparison of Security in HomeRF versus IEEE802.11b," White Paper, 2001, http://www.homerf.org/data/tech/security_comparison.pdf.

[9] National Semiconductor, The Age of Information Access - National Semiconductor Embraces the Emerging Information Appliance Market, A National Semiconductor White Paper, March 2001, http://www.national.com/appinfo/solutions/files/ia_wht_2.pdf.

[10] Palm Inc, "Securing the handheld environment – An Enterprise Perspective," 2001, http://www.palm.com/pdfs/securing_env.pdf

[11] Mohammad Peyravian and Nevenko Zunic, "Method for Protecting Password Transmission," Computer & Security, 2000,Vol.19, No.5, pp466-469.

[12] Charles P. Pfleeger, Security in Computing - Second Edition, Prentice Hall PTR, 1996.

[13] Roy Want and Gaetano Borriello, "Survey on Information Appliances," IEEE Computer Graphics and Applications, May/June.2000.