Regular Paper

Communications of the CCISA
Vol. 26 No. 3 Aug. 2020

藉由智慧音箱竊取隱私之攻擊演示

李建賢[1*]、孫沛靖[2]、吳介騫[3]
[1,2,3]國立高雄科技大學電腦與通訊工程系
[1]0651010@nkust.edu.tw、[2]0651092@nkust.edu.tw、[3]jcwu@nkust.edu.tw

摘要

近年來，智慧音箱的產品逐漸成熟與普及。由於智慧音箱的語音助理一直在聆聽用戶下指令以便啟動服務，這將導致資訊安全上有漏洞。我們發現：小米智慧音箱上連接埠的 root 簽入密碼，不是沒有設定、就是以特定的方式設定，以至於可以利用系統指令來存取。當我們以 root 簽入系統後，可以將惡意軟體注入小米智慧音箱系統中，以此達成：在麥克風被設定為關閉的情況下，竊聽用戶與語音助理的對話、並竊取用戶隱私資料。我們演示了三個攻擊場景，分別是：竊聽、魚叉式釣魚、以及被動式釣魚。最後，根據所演示的攻擊，我們分為對於廠商、及用戶，提出建議的緩解方法。

關鍵詞：智慧音箱、語音助理、隱私

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 26 No. 3 Aug. 2020

Demonstration of Privacy Stealing Attack via Smart Speakers

Jian-Xian Li[1†], Pei-Jing Sun[2], Jieh-Chian Wu[3]
[1,2,3] Department of Computer and Communication Engineering, National Kaohsiung University of Science and Technology, Kaohsing City,Taiwan R.O.C.
[1]0651010@nkust.edu.tw、[2]0651092@nkust.edu.tw、[3]jcwu@nkust.edu.tw

Abstract

Recently, the product of smart speakers becomes mature and popular. Since the voice assistant of the smart speaker is always listening to users' commands to issue services, it leads to security vulnerabilities. We find that the login password for root access to the UART ports of the XIAOMI smart speakers is either not configured or configured by certain pattern which can be accessed by using system commands. After login as root, we can inject malware into XIAOMI smart speakers so that we can eavesdrop on conversations between user and voice assistant to perform privacy stealing attack, even when users turn off the microphone. We demonstrate three attack scenarios including eavesdropping, spear phishing, and passive phishing. Finally, we propose mitigations to such attacks for both manufacturers and user.

Keywords：Smart Speaker、Voice Assistant、Privacy

† Corresponding author.

壹、前言

近幾年人工智慧與物聯網技術快速發展，加上語音個人助理技術的成熟，因此用戶利用語音控制物聯網的設備也逐漸普及，進而出現了智慧音箱等產品。隨著智慧音箱市場的擴大，Amazon、Google、Apple 等廠商各自發布了針對英語語系的智慧音箱[22]；而針對亞洲比較多使用中文的用戶，小米、阿里巴巴等廠商也各自推出了中文語系的智慧音箱[22]。因為智慧音箱支援的語系滿足各種語言的需求，使用智慧音箱的用戶在全球逐漸成長。

許多智慧音箱的控制是經由音箱中的語音助理進行處理，因此智慧音箱中的語音助理安全性、與隱私性等問題是必須注意的[10][11][13]，然而大多數的智慧音箱的用戶並沒有考慮到智慧音箱的安全及隱私問題[10][17]。

1.1 智慧音箱的資安風險

根據文獻[13]指出：智慧音箱的使用環境，不單單只會使用在家庭環境中，而是漸漸擴展到辦公室與工作室等環境，因此如先前的研究[7][13][14][16][17][18][20]所示，代表著智慧音箱的安全性與隱私問題，需要更加的重視。大多的智慧音箱的安全隱私問題的源頭是：智慧音箱的麥克風[14][17]、及語音助理[7][8][20]。其中，智慧音箱的語音助理，需要用戶利用喚醒詞喚醒才能啟動語音助理的服務[16]，因此智慧音箱在等待喚醒詞時，麥克風是一直處於聆聽狀態中，使得用戶與語音助理交談過程隨時都可能被竊聽[18]。雖然智慧音箱的麥克風可以被使用者關閉，但是攻擊者仍然能透過遠端打開智慧音箱的麥克風，同時關閉麥克風啟用的顯示燈號，直接對受害者進行靜音式的竊聽，使得用戶難以察覺[19]。至於關閉麥克風的方式可從硬體、或軟體方式達成。根據文獻[12]指出：對於用戶比較安全的麥克風關閉方式是利用硬體方法來啟動的。反之，若智慧音箱提供軟體方式來關閉麥克風，則存在較高的資安風險。

用戶與智慧音箱的使用流程與互動，使得很多用戶的個人信息經由智慧音箱，傳送至官方伺服器的後端[14][16]。因此當攻擊者針對智慧音箱進行：封包嗅探[18]、重新導向[15]、語音釣魚[15]等方式的攻擊，就可能取得個人敏感信息[20]。駭客技術研究組織 SRLabs 在文獻[4]中提到智慧音箱中的語音助理的問題：攻擊者可以透過廠商開放的標準介面[15]，使智慧音箱變成智慧間諜，並且能利用語音釣魚來騙取用戶的敏感訊息，例如：密碼、及詳細個資，導致用戶的個人敏感信息洩漏與曝光。而且攻擊者發動這些相關竊取個人信息的攻擊時，可能是在用戶並無察覺的情況下進行的，因此若用戶長時間使用智慧音箱，容易造成用戶的個人敏感信息洩漏的威脅。

1.2 智慧音箱的資安弱點

根據[9][14][19][20][21]文獻指出：智慧音箱經常使用的連接埠為通用非同步收發傳輸器（Universal Asynchronous Receiver/Transmitter，UART）介面的連接埠，而該連接埠很容易從設備主機板上找到。因此，攻擊者可透過物理方式連接到該連接埠後，進入智慧音箱系統進而取得 root 訪問的權限。一旦獲得 root 訪問權限，攻擊者就可以從遠端訪問、注入攻擊、並安裝惡意軟體。文獻[19]指出：雖然攻擊者必須透過物理方式才能取得 root 訪問的權限，是一個主要的資安防禦機制，但是當智慧音箱被使用於旅館房間等不固定用戶的環境下，而攻擊者扮演第三方的智慧音箱販賣者或維修人員時，即可透過物理方式攻擊智慧音箱[14]。

許多智慧音箱資安的文獻研究對象是：英語語系 Amazon 的音箱，如文獻[14][19]。而本論文則是以中文語系的小米智慧音箱為研究對象，我們發現市售的小米智慧音箱存在著漏洞，且我們也證實此漏洞對於用戶可造成威脅。根據我們所知：關於小米智慧音箱的資安問題目前並未被揭露，因此在本論文中，我們專注於小米智慧音箱的隱私資安問題進行研究，並提出防護的解析。在研究分析中，我們假設：攻擊者可以透過物理方式接觸到智慧音箱，因而攻擊者可利用 UART 介面漏洞攻擊智慧音箱設備，並開啟智慧音箱的後門，使攻擊者由遠端進入系統，控制智慧音箱中的語音助理。本論文實作了智慧音箱可能存在著被竊聽、魚叉式釣魚、被動式釣魚等隱私洩漏的風險，並討論防護的方法。

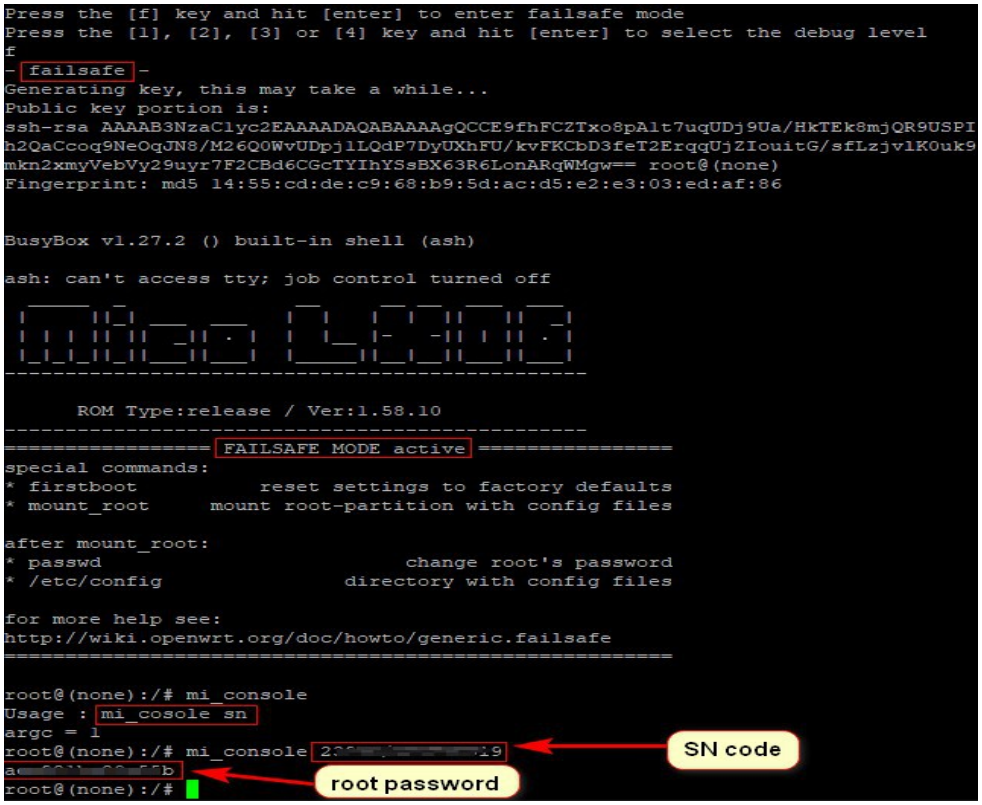
本論文架構分為五章，第一章是前言，將探討現有的研究文獻與研究背景；第二章詳細說明本研究中發現智慧音箱的資安漏洞與相關的攻擊技術；第三章為結合智慧音箱漏洞與相關技術，進行語音助理竊取隱私的攻擊演示及結果說明；第四章是依據本研究的實驗結果，提出防護的分析，以及給予廠商與用戶的防護建議；最後於第五章提出關於本研究的結論。

貳、智慧音箱之資安漏洞與攻擊技術

2.1 UART 介面資安漏洞

我們發現了小米智慧音箱中存在著：UART 介面免密碼即可取得 root shell 的資安漏洞，並申請了美國 MITRE 之通用漏洞揭露（Common Vulnerabilities and Exposures，CVE）資料庫的兩項漏洞，該漏洞編號為：CVE-2020-8994[1]、及 CVE-2020-10263[3]。隨後小米廠商在新版本的音箱系統中新增了 UART 介面登入時的密碼驗證，但我們發現：在開機程序時啟動安全模式後，執行特定命令並輸入產品的序號（SN 碼），即可取得 root shell 的密碼，如圖一所示。其中，產品的序號是黏貼在智慧音箱的底部。我們也以此發

現另外申請了 CVE 資料庫漏洞，其漏洞編號為：CVE-2020-10262[2]。當我們透過上述的 UART 介面漏洞取得 root shell 之後即可：查看、編輯、或執行智慧音箱系統內所有服務程序，進而控制語音助理。



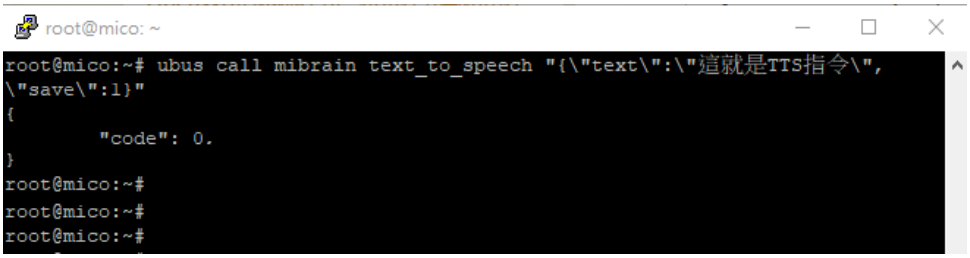
圖一：取得 root shell 的密碼截圖

2.2 控制語音助理

我們經由 UART 介面資安漏洞取得 root shell 後，即可透過指令來：控制語音助理發話、查看用戶語音指令及音箱發話紀錄、錄製用戶語音、聽取特定用戶語音中的喚醒詞（wake-up word）、以及在顯示麥克風關閉燈號下開啟麥克風。茲分述如下。

2.2.1 控制語音助理發話

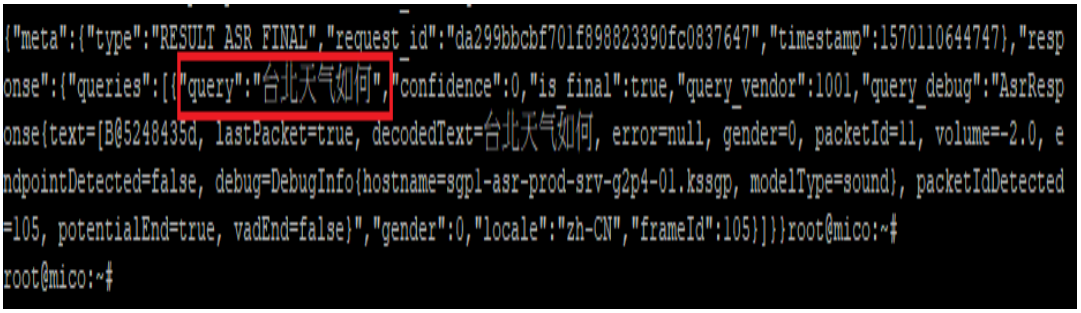
藉由控制「文字轉語音（Text-to-Speech，TTS）」技術[6]，能將任意文字串轉換成合成的語音，來控制語音助理的發話朗讀。圖二是使用小米智慧音箱之文字轉語音（TTS）的範例指令。



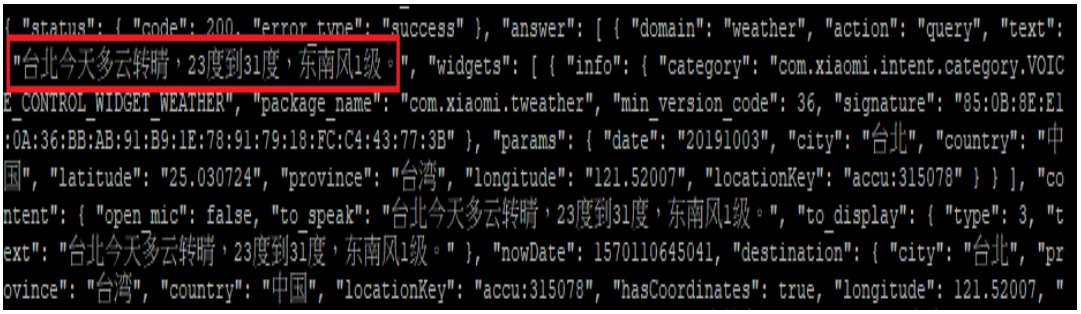
圖二：使用 TTS 的指令截圖範例

2.2.2 查看用戶語音指令及音箱發話紀錄

當智慧音箱中的語音助理聽取用戶語音下達的指令後，會透過自動語音識別（Automatic-Speech-Recognition，ASR）[5]功能，能將語音轉換為文字，並記錄於 log 日誌檔中，該檔案的副檔名為 ASR。此外，語音助理答覆的文字訊息，也會記錄在 log 日誌檔中。因此，查看 log 日誌檔即可查看用戶的語音指令及音箱發話紀錄。例如，用戶喚醒語音助理後下達了詢問「台北天氣如何」，而語音助理答覆「台北今天多雲轉晴，23 度到 31 度，東南風 1 級」，以上兩筆語音轉成的文字皆紀錄於：服務程序當中用戶下達指令的 log 日誌檔、及語音助理答覆用戶的 log 日誌檔，如圖三、及圖四所示。由於本論文是以中文語系的智慧音箱進行研究，我們發現：用戶若以英文下達指令，則該智慧音箱執行自動語音識別（ASR）的結果是錯誤的。



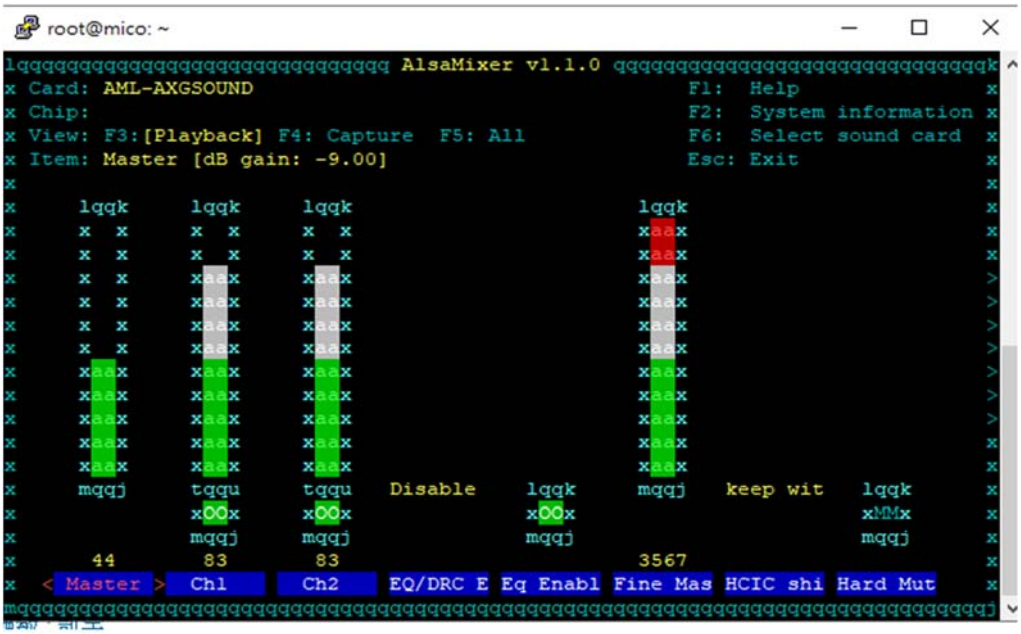
圖三：用戶 log 日誌檔截圖範例



圖四：語音助理答覆的 log 日誌檔截圖範例

2.2.3 錄製用戶語音

小米智慧音箱裡的作業系統，使用的是 Linux，所以智慧音箱中所使用到的服務，大多都是使用 Linux 系統服務。由於智慧音箱裡本身就有麥克風陣列的硬體，首先我們透過：進階 Linux 聲音體系（Advanced Linux Sound Architecture，ALSA）來控制音效卡。ALSA 是 Linux 中的音訊體系結構，提供了應用層的 API，如圖五所示。使用該 API 可以完成對底層音訊硬體的控制。我們透過查看系統中裝置設定，發現語音助理在運作的過程中會占用麥克風陣列裝置，因此當我們需要錄取受害者回話時，須先取得麥克風陣列裝置的使用權，而再透過執行相關指令與設定參數，即可利用智慧音箱中的麥克風陣列執行錄製用戶語音。



圖五：智慧音箱系統中的 ALSA API 介面

2.2.4 聽取喚醒詞

智慧音箱中的語音助理是透過喚醒詞來喚醒語音助理，而我們發現智慧音箱系統接收到喚醒詞後會執行一個服務程序，來完成後續的動作。在這個服務程序中，我們發現：當智慧音箱聽取到喚醒詞，此服務會先執行答覆用戶，使用戶知道喚醒語音助理有喚醒成功，再對用戶進行錄音收取語音指令，然後再將用戶下達的命令回傳至官方伺服器，來完成後續的服務。其中，服務程序聽取用戶語音命令的指令如圖六所示。此外，我們發現：此服務的程序中，有個關閉此服務程序的指令。因此，若在用戶對語音助理下達命令時，執行關閉此服務程序的指令，將會使語音助理不再答覆用戶原會答覆的話。

```
root@mico:/# ubus call pnshelper event_notify '{"src":1,"event":0}'
{
        "code": 0
}
root@mico:/#
```

圖六：語音助理聽取用戶指令

2.2.5 關閉麥克風燈號顯示下開啟麥克風

雖然用戶可能會在談論到敏感的話題時有所警覺，並能透過智慧音箱上的按鍵將智慧音箱的麥克風關閉，同時透過智慧音箱上的指示燈顏色確認麥克風已經關閉，關閉時的靜音顯示燈號如圖七所示，以此防止智慧音箱聽取敏感資訊。然而我們在禁用麥克風的服務程序當中，發現小米智慧音箱關閉麥克風的方式，是透過軟體的方式將其麥克風關閉的，其關閉指令如圖八所示。因此，攻擊者可以執行開啟麥克風的指令，並將指示燈設為關閉麥克風模式的顏色，使受害者無法察覺麥克風已被開啟。

圖七：智慧音箱上的靜音燈號

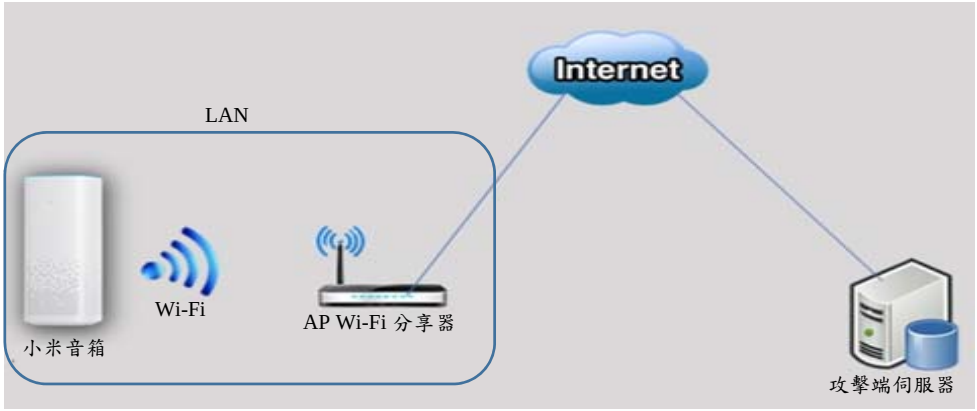
```
root@mico:/# /etc/init.d/pns mic_off
{
        "code": 0
}
root@mico:/#
```

圖八：麥克風關閉指令

參、語音助理竊取隱私之攻擊演示

3.1 系統架構

本攻擊演示之系統架構，如圖九所示，分為：攻擊端及受害端，茲分述如下。



圖九：攻擊演示架構圖

攻擊端（Attacker）是伺服器，其軟硬體設備為：一台桌上型電腦（搭載 Ubuntu 18.04 作業系統）、Apache HTTP 伺服器、PHP7.0、以及 FTP 檔案伺服器。

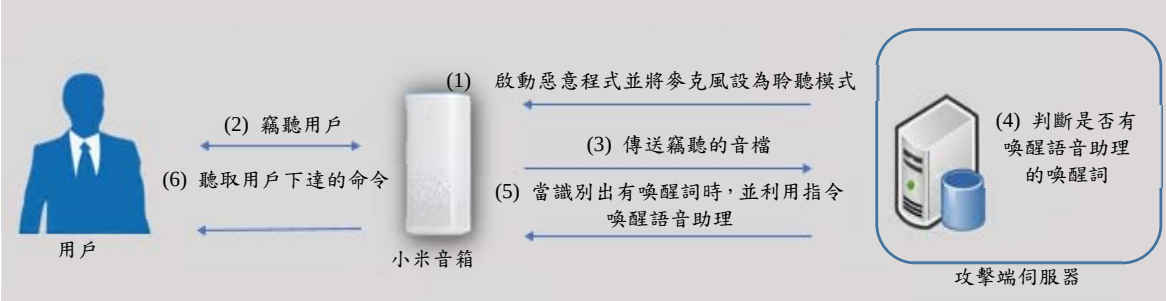
受害端（Victim）是刷機後小米音箱系統，其安裝的軟體為：Linux mico 4.9.61 作業系統、eavesdrop.sh 竊聽惡意程式、Voice_Spear_Phishing.sh 魚叉式語音釣魚惡意程式、及 Voice_Phishing.sh 被動式語音釣魚惡意程式。

以下將分別演示：竊聽、魚叉式語音釣魚、及被動式語音釣魚之攻擊。

3.2 竊聽攻擊演示

3.2.1 流程

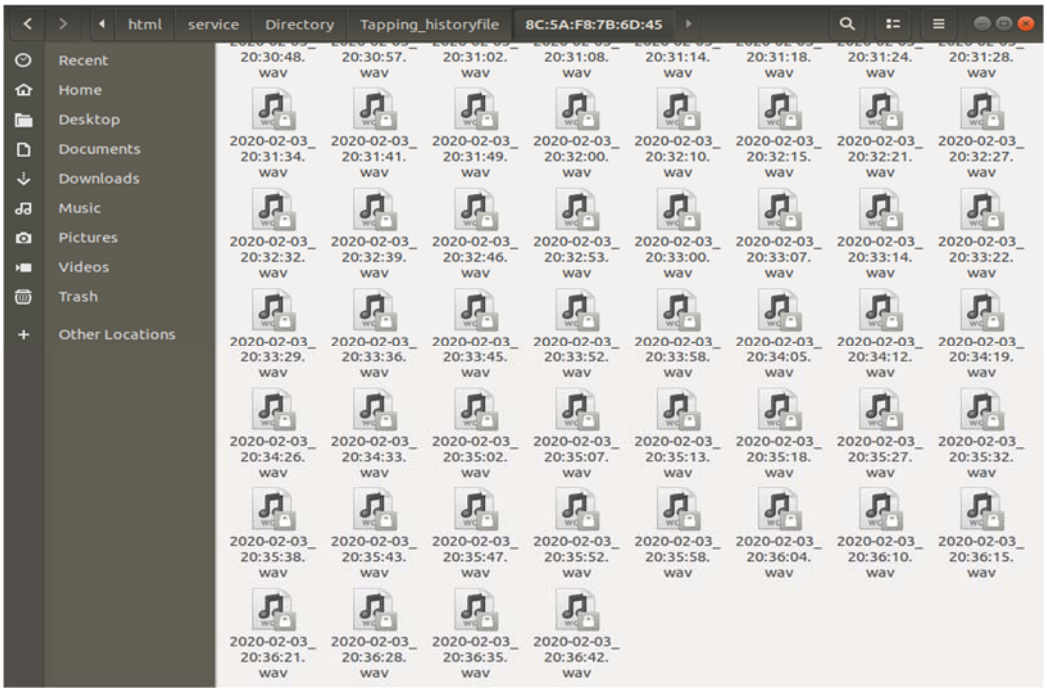
攻擊者先將竊聽的惡意程式寫入智慧音箱系統中，當觸發惡意程式後，此惡意程式會先將麥克風啟動為聆聽狀態，再利用 PS 指令查詢當前執行中的程序，並找到占用麥克風陣列的程序且將其停用之後，即可取得麥克風陣列的使用權。接者，透過錄音相關指令將受害者的語音錄製，並以串流的形式回傳至攻擊者伺服器中，攻擊者伺服器則將回傳的錄音檔進行語音識別，判斷受害者是否有喚醒語音助理的動作，如果識別出受害者喚醒語音助理的喚醒詞時，伺服器立即利用指令喚醒語音助理，藉此可達到：受害者毫無察覺之下的竊聽，其攻擊演示流程如圖十所示。



圖十：竊聽攻擊演示流程圖

3.2.2 結果

攻擊者啟動竊聽的惡意程式後，受害者的智慧音箱會連續錄取周遭環境的聲音，並將此錄取聲音的音檔以串流方式回傳至攻擊端伺服器，而受害者無從察覺自己已被竊聽。即使受害者啟動智慧音箱的麥克風禁用功能，攻擊者依然可進行竊聽。其中，攻擊端伺服器接收到竊聽的音檔範例如圖十一所示。

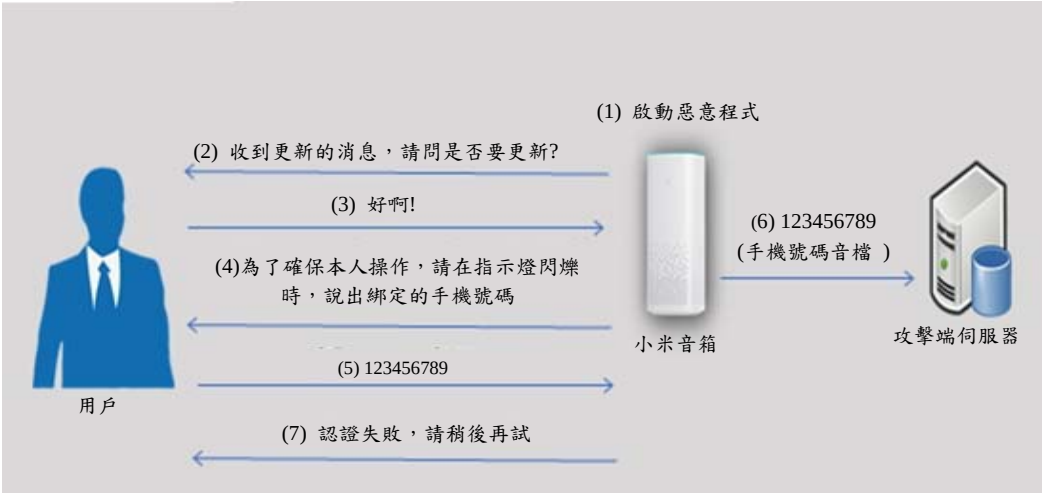


圖十一：攻擊端伺服器接收到竊聽的音檔範例

3.3 魚叉式釣魚攻擊演示

3.3.1 流程

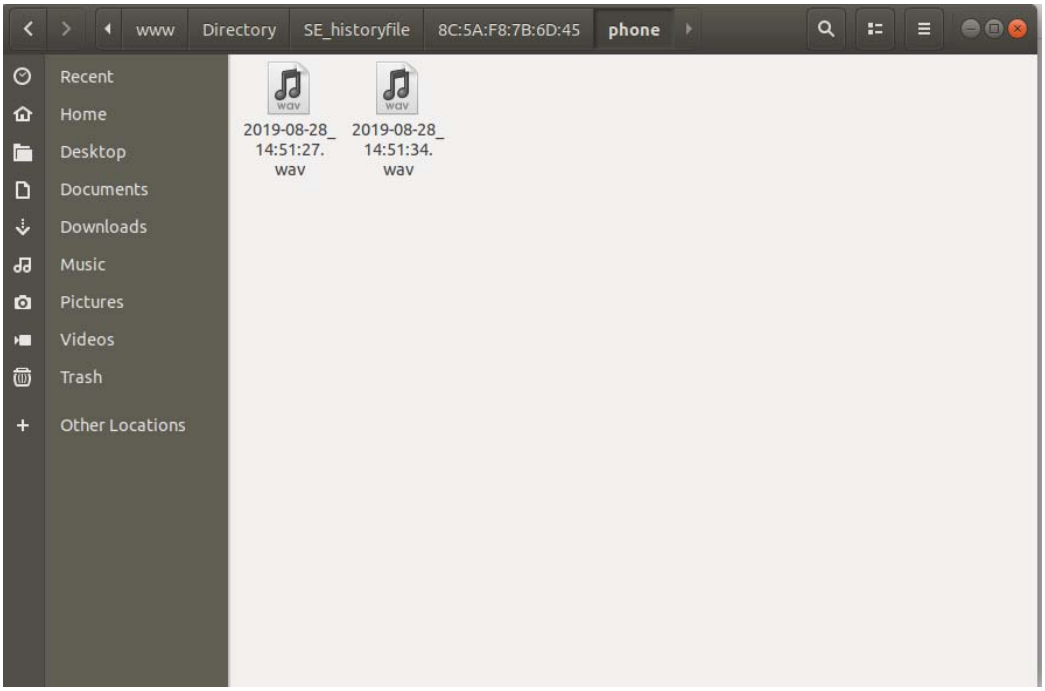
攻擊者先將文字轉語音（TTS）指令、擷取自動語音識別（ASR）關於用戶與語音助理對話的 log 日誌檔內容之程式、與錄音的相關指令寫入惡意程式，並注入受害者的智慧音箱系統中。當惡意程式被觸發後，利用文字轉語音（TTS）指令使音箱中的語音助理提出：系統升級的請求、或是安全認證請求來向受害者進行互動，並透過自動語音識別（ASR）對話 log 日誌檔的內容擷取出受害者的答覆，進行判斷受害者是否同意更新，當受害者同意更新時，再次利用文字轉語音（TTS）指令，讓語音助理以確認身分為由向受害者要求密碼或是個人資料，同時藉由錄音相關指令錄製受害者的回覆，並將錄音檔傳回至攻擊端伺服器。過程中為了降低受害者起疑，我們錄完受害者回覆後，利用文字轉語音（TTS）指令讓語音助理答覆：「驗證失敗，請稍後再試」，如圖十二所示。



圖十二：魚叉式釣魚攻擊演示流程圖

3.3.2 結果

當攻擊者執行受害端的惡意程式後，而受害者誤以為是官方系統所提出的升級請求或安全認證時，便將密碼或個人資料告訴智慧音箱中的語音助理，並被傳送到攻擊端的伺服器，其中，被錄下的受害者個人資料音檔範例如圖十三所示。

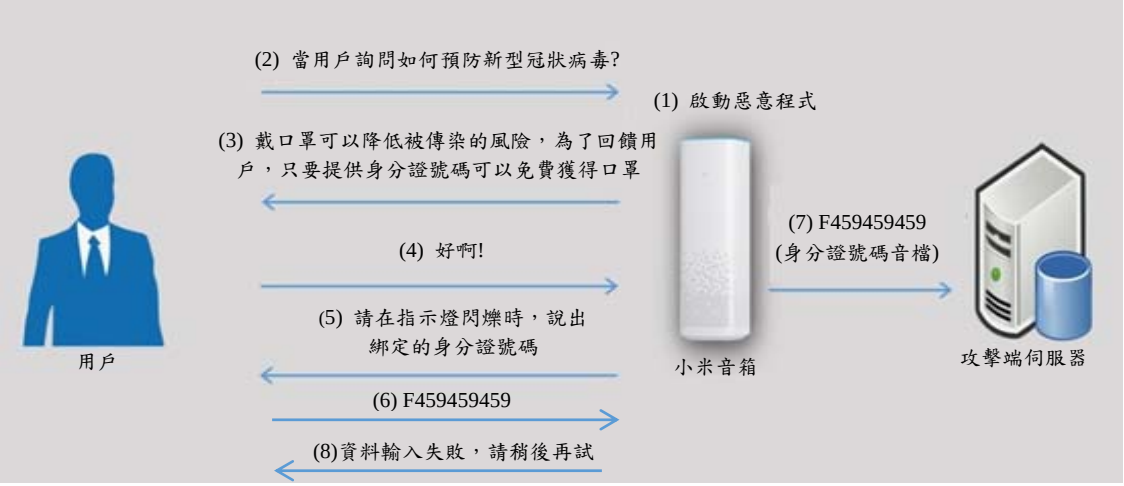


圖十三：攻擊端伺服器接收到錄下受害者個人資料音檔範例

3.4 被動式釣魚攻擊演示

3.4.1 流程

攻擊者先將文字轉語音（TTS）指令、擷取自動語音識別（ASR）關於用戶與語音助理對話的 log 日誌檔內容之程式、中斷語音助理回話指令、以及錄音的相關指令寫入惡意程式，並注入受害者的智慧音箱系統中。當攻擊者啟動此惡意程式時，此惡意程式會先等待受害者對語音助理詢問關於時事的問題，例如：「如何防護避免新型冠狀病毒的感染」。惡意程式透過自動語音識別（ASR）對話 log 日誌檔中的內容，擷取出來與攻擊者設定的關鍵字，例如：「新型冠狀病毒」，並進行比對。如果比對的結果是相同，則立即中斷語音助理的答覆，並透過文字轉語音（TTS）指令，讓語音助理發話答覆造假的訊息，例如：「可以獲得免費口罩」為誘引，向受害者要求須先取得相關個資才可取得口罩，同時透過錄音相關指令錄製受害者的回覆，再將錄音檔傳回攻擊端伺服器。同時，為了降低受害者起疑，我們錄完受害者回覆後，利用文字轉語音（TTS）指令讓語音助理答覆：「資料輸入失敗，請稍後再試」，並完成此攻擊，以上流程如圖十四所示。

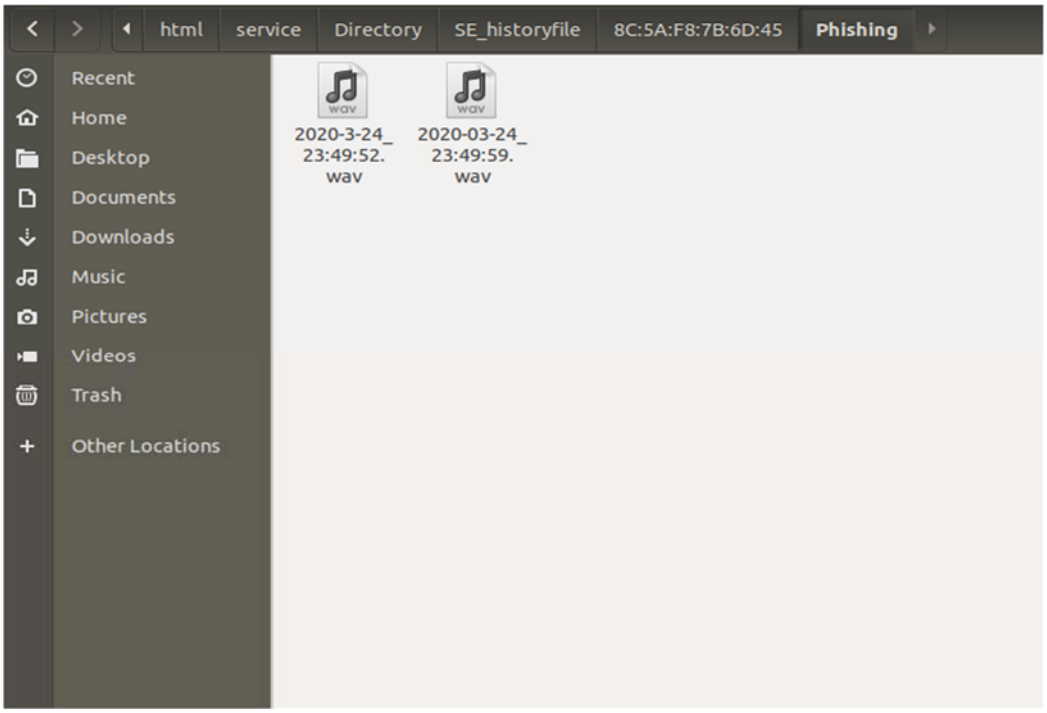


圖十四：被動式釣魚攻擊演示流程圖

3.4.2 結果

攻擊者執行受害端的惡意程式後，當受害者詢問關於目前的時事，例如：「如何防護避免新型冠狀病毒的感染」，如圖十五所示，則攻擊者利用文字轉語音（TTS）指令，使語音助理說出造假訊息並以可獲得免費口罩為誘引，誘使受害者為了取得免費口罩，因此將相關個資告訴語音助理，並藉此錄下受害者的回覆傳回攻擊端的伺服器，其中，被錄下的受害者個人資料音檔範例如圖十六所示。

圖十五：用戶對語音助理的詢問 log 日誌檔範例



圖十六：攻擊端伺服器接收到錄下受害者個人資料音檔範例

3.5 智慧音箱影響與防護

以上攻擊方式，可以證明智慧音箱存在著資安的風險，使用戶暴露在被竊聽與竊取個人敏感資料等風險中。而釣魚攻擊能夠成功達成騙取的原因，主要為用戶對於智慧音箱回復的正確性深信不疑，以及對於智慧音箱廠牌的信任，所以用戶會輕易的相信語音助理的任何回話。因此我們認為：智慧音箱中語音助理，應該具備足夠保護機制，例如，不宜提供軟體的方式來關閉智慧音箱中的麥克風，應以硬體方式來關閉麥克風較佳。

肆、防護分析與建議

首先我們分析：基於智慧音箱硬體、智慧音箱系統軟體的資訊安全防護，以及用戶的資安意識，也分別提出防護建議。最後，我們總結提出：廠商、及用戶的防護建議。茲說明如下。

4.1 防護分析

4.1.1 基於智慧音箱硬體的資安防護分析

基於智慧音箱硬體的安全防護，我們建議：可透過具有內含安全隔離區的處理器，進而保護智慧音箱中用戶的個人隱私數據、語音助理的麥克風以及系統加解密和身分認證等安全金鑰。透過硬體層面斷開軟體與硬體的聯繫，使得攻擊者就算進入智慧音箱系統，也無法執行竊取隱私相關攻擊，藉此可有效保護用戶的隱私安全。

語音助理接收用戶語音指令的麥克風是智慧音箱中較為敏感的硬體設備，雖然廠商有設計可讓用戶關閉麥克風的功能，但根據我們的實驗可證實，關閉麥克風功能為軟體方式的關閉，使的攻擊者仍可透過惡意指令進行控制麥克風開啟。因此我們建議：智慧音箱廠商在設計麥克風關閉功能時應以硬體方式進行，如同 Google 品牌的智慧音箱是透過硬體開關來控制麥克風的，如圖十七紅框所示。直接使用硬體開關的方式來控制麥克風元件的電源，以此確實關閉麥克風，避免攻擊者透過惡意指令進行更動。

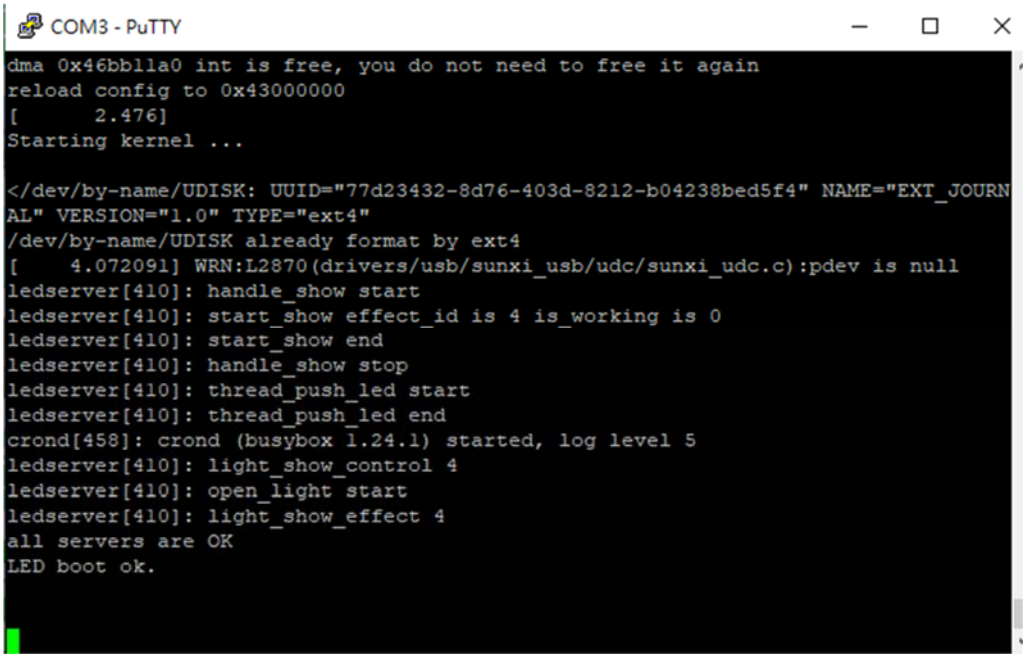
圖十七：Google 品牌智慧音箱麥克風開關

4.1.2 基於智慧音箱系統軟體的資安防護分析

基於智慧音箱系統軟體的資安防護方面，根據我們的研究，攻擊者可透過連接埠以

root 權限進入系統。此問題能夠透過系統的設計解決，最直接的解決方法，可將使用 UART 介面的連接埠登入介面進行關閉。因此當攻擊者透過使用 UART 介面的連接埠進入系統時，只能查看系統資訊與啟動的介面，如圖十八所示，進而防護攻擊者植入惡意的軟體。另外，廠商可在系統中，建立軟體更新的機制，隨著威脅和漏洞的發現，廠商能夠即時修改和升級系統的安全性。

此外，關於智慧音箱連線網路的服務連接埠，應更加注重管控。應關閉或封鎖非官方的服務連接埠，防止攻擊者透過該服務連接埠進行攻擊；而當透過官方的服務連接埠進行網路連線時，應透過金鑰加密的認證，來進行安全連線。同時，存放金鑰的資料區，也必須透過加密方式加以保護。



圖十八：關閉使用 UART 介面的連接埠的登入介面

4.1.3 用戶的資安意識分析

隨著相關智慧家庭的資安事件頻繁的發生，藉此我們可以發現：除了產品本身存在著資安漏洞外，用戶的操作方式與觀念也是造成資安事件發生的主因之一。因此，用戶更應該具備基本的資安意識。尤其在智慧家庭中，常見帶有麥克風元件的智慧音箱設備等等應更加注意。而用戶與智慧音箱互動時，應注意：不能太過於信任於智慧音箱，當智慧音箱提出要求索取用戶較於隱密的數據或不合理的操作時，需更加三思。應該透過廠商來進行求證。在我們的實驗中證實了：可以透過物理方式，將惡意軟體植入智慧音箱系統中，而外表與使用上並無任何異常，所以用戶購買智慧音箱時，需更加注重產品的來源，切勿購買非官方販售的產品。

4.2 防護建議總結

4.2.1 廠商防護建議

本論文建議廠商的防護方式為：(1) 將連接埠和 root 權限關閉，並且加裝安全晶片；(2) 禁止開啟非官方通訊管理功能服務的埠口；(3) 只提供硬體方式來關閉智慧音箱上的麥克風；(4) 加強宣導民眾購買途徑之正當性；(5) 提供資料的查證。

4.2.2 用戶防護建議

本論文建議消費者的防護方式為：(1) 不要購買非官方廠商販售的智慧音箱，因為可能會有由第三方的更改智慧音箱系統的機會；(2) 避免在使用智慧音箱過程中，透漏過多個人財務以及其他敏感資訊，如果智慧音箱提到需提供密碼與個人資料之需求時，應至官方進行查證。

伍、結論

本論文分析目前智慧音箱中存在的安全與隱私的問題，進而針對中文語系的小米智慧音箱設備提出並實作了三種攻擊方式，分別可造成的資安攻擊效果為：竊聽及騙取用戶個人資料。其中的竊聽攻擊，可透過攻擊智慧音箱的麥克風，進行環境的錄音，即使用戶關閉智慧音箱的麥克風，攻擊者仍然可以在關閉麥克風燈號顯示之下開啟麥克風，並讓用戶在毫無察覺之下進行竊聽。至於騙取用戶個人資料的攻擊，可分別使用魚叉式語音釣魚、或是被動式的語音釣魚方式達成。本論文演示的魚叉式語音釣魚，是仿造官方系統提出需更新或安全認證需求，藉此竊取用戶密碼與個人資料；而演示的被動式語音釣魚，則是等待用戶詢問目前相關時事，藉由仿造語音助理給予假訊息，並誘使受害者答覆個人資料，藉此竊取用戶的個人敏感資料。

我們證明了目前市售小米智慧音箱設備存在著資安問題，而且這些攻擊方式將會真實的威脅到目前正在使用智慧音箱設備的用戶，因此我們也針對這些攻擊方式，向廠商與用戶提出建議實施的防護方法，我們期望能夠降低對於擁有智慧音箱的用戶所面臨的風險。

參考文獻

[1] CVE-2020-8994: Common Vulnerabilities and Exposures, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8994.(2020/02/14).

[2] CVE-2020-10262: Common Vulnerabilities and Exposures, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10262.(2020/03/10).

[3] CVE-2020-10263: Common Vulnerabilities and Exposures, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10263.(2020/03/10).

[4] Smart Spies: Alexa and Google Home expose users to vishing and eavesdropping: Security Research Labs, https://srlabs.de/bites/smart-spies/.

[5] Speech recognition: Wikipedia, The Free Encyclopedia., https://en.wikipedia.org/w/index.php?title=Speech_recognition&oldid=949143164.(2020/4/4).

[6] Speech synthesis: Wikipedia, The Free Encyclopedia., https://en.wikipedia.org/w/index.php?title=Speech_synthesis&oldid=949282784.(2020/4/5).

[7] W. Candid. "A guide to the security of voice-activated smart speakers An ISTR Special Report". (2017/11).

[8] P. Cheng, I.E. Bagci, J. Yan and U. Roedig, editors. "Smart Speaker Privacy Control - Acoustic Tagging for Personal Voice Assistants". *IEEE Workshop on the Internet of Safe Things*; 2019.

[9] I. Clinton, L. Cook and S. Banik. "A survey of various methods for analyzing the amazon echo". The Citadel, *The Military College of South Carolina*. 2016.

[10] F. Eoghan and B. Juanita, editors. "She Knows Too Much – Voice Command Devices and Privacy". *2018 29th Irish Signals and Systems Conference (ISSC)*; 21-22 June 2018.

[11] B. Eric. Is There An Echo In Here? What You Need To Consider About Privacy Protection: Forbes Legal Council; 2017, https://www.forbes.com/sites/forbeslegalcouncil/2017/09/18/is-there-an-echo-in-here-what-you-need-to-consider-about-privacy-protection/#72f7d9fa38fd.

[12] M. Ford and W. Palmer. "Alexa, are you listening to me? An analysis of Alexa voice service network traffic". *Personal and Ubiquitous Computing*, vol.23,issue.1,pp.67-79. 2019.

[13] L. Hart. "Smart speakers raise privacy and security concerns". *Journal of Accountancy*, vol.225,issue.6,pp.70. 2018.

[14] C. Jackson and A. Orebaugh. "A study of security and privacy issues associated with the Amazon Echo". *International Journal of Internet of Things and Cyber-Assurance*,

vol.1,issue.1,pp.91-100. 2018.

[15] D. Kumar, R. Paccagnella, P. Murley, E. Hennenfent, J. Mason, A. Bates, et al., editors. "Skill Squatting Attacks on Amazon Alexa". *27th USENIX Security Symposium*; 2018.

[16] J. Lau, B. Zimmerman and F. Schaub. "Alexa, are you listening?: Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers". *Proceedings of the ACM on Human-Computer Interaction*, vol.2,issue.CSCW,pp.1-31. 2018.

[17] J. Lau, B. Zimmerman and F. Schaub, editors. ""Alexa, Stop Recording": Mismatches between Smart Speaker Privacy Controls and User Needs".

[18] J.-s. Lee, S.-y. Kang and S.-j. Kim. "Study on the AI Speaker Security Evaluations and Countermeasure". *Journal of the Korea Institute of Information Security and Cryptology*, vol.28,pp.1523-37. 2018.

[19] B. Mark. Alexa, are you listening? , https://labs.f-secure.com/archive/alexa-are-you-listening/?fbclid=IwAR3iSLzk2PauTFxarV2wM0MzCn0Dbjd82Spoe7kRQiAgqLJpL2Cf1KN1oMQ. (2017/8/1).

[20] Y. Park, H. Choi, S. Cho and Y.-G. Kim. "Security Analysis of Smart Speaker: Security Attacks and Mitigation". *Computers, Materials and Continua*, vol.61,pp.1075-90. 2019.

[21] G. Shawn, G. Brett and G. Kanwalinderjit, editors. "Future Security of Smart Speaker and IoT Smart Home Devices". *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*; 2019 2-3 March 2019.

[22] X.-T. Xiao and S.-I. Kim. "A Study on the User Experience of Smart Speaker in China - Focused on Tmall Genie and Mi AI Speaker". *Journal of Digital Convergence*, vol.16,issue.10,pp.409-14. 2018.

[作者簡介]

李建賢、及孫沛靖，現為國立高雄科技大學電腦與通訊工程系大學部學生，其研究領域為：資訊安全。

吳介騫為美國南加州大學電機工程博士，現為國立高雄科技大學電腦與通訊工程系副教授，其研究領域為：行動通訊系統、光纖網路、及資訊安全。