Watch Your Money：A Solution to Protect Your Android from Sending Unknown SMS Messages

廖緯玲[1] 陳世仁[2] 蘇育生[3] 許富皓[4] 吳敏豪[5]
[1,4,5]中央大學資訊工程系
[2]資策會
[3]中央大學前瞻科技研究中心
hsufh@csie.ncu.edu.tw

摘要

由於 Android 對於敏感應用程式介面 (Application Programming Interface, API)是用權限機制來做管理與限制，所以這些惡意軟體想要存取這些敏感 API 的話，只要在 AndroidManiflest.XML 檔案當中揭露它所需要的權限或是動態的在程式碼中宣告後，就可以一直使用，直到它被解除安裝為止，也因此簡訊 (Short Message Service, SMS) 惡意軟體可以利用這種機制，在使用者不知道的情況下，擅自寄送簡訊，造成使用者財務損失。當使用者安裝含有這個類型的惡意軟體後，它會讓手機發送出付費簡訊，而且使用者無法查覺此惡意行為，因此造成使用者財務上的損失。本篇論文所提出的方法是藉由分析簡訊木馬發送簡訊的行為，並設計出防止簡訊被濫發的機制 — Taurus。Taurus 以動態監控的方式，透過記錄使用者輸入的內容與即將要發送出去的簡訊內容和接收方的電話號碼做比對，來確認簡訊是否使用者發送。若兩者比對不成功，則 Taurus 會向使用者發出通知訊息，讓使用者確認是否要發送此簡訊，一旦曾經被拒絕發送的應用程式和簡訊又再次重新發送，Taurus 就會判定其為惡意行為並中止其執行，阻止其發送簡訊。

關鍵詞：SMS Trojans, SMS malware, SMS Zombie, 簡訊木馬, SMS 木馬

1. 前言

隨著科技進步，傳統手機逐漸被智慧型手機取代，智慧型手機猶如一台非常輕薄的電腦，可以隨意在手機內安裝應用軟體，有別於一般傳統手機，它們功能豐富，擁有很強的應用擴展性，操作簡單便利，並且能替代個人電腦處理辦公事務與其他事務，體積輕薄短小攜帶方便，加上隨時隨地上網功能讓它廣受大眾喜愛。

目前智慧型手機的作業系統主要有：Android、iOS、BlackBerry OS、Windows Phone 與 Symbian 等，由於 Android 是最受歡迎的行動平台，因此很容易成為攻擊者的焦點。趨勢科技指出基於 Android 平台的惡意軟體在 2012 年已經有 35 萬個，預計到 2013 年底惡意軟體的數量將成長四倍，將會到達百萬個以上[1]。在這些惡意軟體中，有一部份的惡意軟體是以謀取利益為主要目標，這類型的惡意軟體所使用的方法是利用簡訊來獲取利益，所以被稱為簡訊木馬。他們會假冒知名 Android 遊戲，透過讓使用者免費下載的方式流傳，一旦使用者安裝這些知名 Android 遊戲，它會讓手機發送出付費簡訊或自動向電信業者發出訂購高資費服務的簡訊，讓使用者付出鉅額的電信服務費用。

針對以上問題，本篇論文提出一個解決機制為 Taurus。Taurus 的設計構想來自於當使用者使用手機傳送簡訊時，會輸入簡訊內容後再傳送出去。但簡訊木馬在發送簡訊時，並不會由手動輸入內容，而是使用預設的內容或是經由網路下載的內容當成簡訊內容。因此，我們透過紀錄使用者輸入的文字與即將要傳送出去的簡訊內容做比對，如果相符的話，表示的確是使用者所發送出去的簡訊，Taurus 接著會檢查接收方的電話號碼，接收方的電話號碼必須是由使用者輸入或是手機內聯絡人的電話，如果簡訊內容或電話號碼中的其中一個不相符的話，則很可能是由簡訊木馬所發出的簡訊，Taurus 跳出通知訊息通知使用者，讓使用者確認是否需要發送這封簡訊。

另外 Taurus 會記錄被使用者發送與拒絕發送簡訊的 App 名稱、接收者電話號碼和簡訊內容，並將被使用者拒絕發送的簡訊視為不安全的內容，一旦不安全的簡訊內容又想再次發送的話，Taurus 會判定此行為為惡意行為，跳出警告訊息通知使用者並且阻止其寄送簡訊。

在接下來的章節中，我們會在第二章介紹 Android 相關的知識與簡訊惡意軟體的種類與行為；第三章介紹 Taurus 的系統設計與實作；第四章介紹實驗分析；第五章結論；第六章未來研究方向。

2. 背景知識介紹與文獻探討

2.1 簡訊惡意軟體的種類與特性

一般而言，惡意程式的主要有三種目的，第一洩漏受害者隱私資料，包括受害者位置資訊、信用卡資料、照片等；其次是控制受害者的手機，以作為散播惡意軟體到其他手機的跳板；最後則是謀取利益，在受害者不知情下，傳送付費簡訊、撥打色情電話等，讓受害者付出鉅額通訊費用。

根據卡巴斯基(Kaspersky)[2]在 2012 年 11 月表示，超過一半的惡意軟體裡，都被檢測出含有簡訊木馬(SMS Trojans)，這些惡意軟體利用受害者的手機帳號，傳送付費簡訊，藉此獲取利潤。

2.2 簡訊木馬

簡訊木馬[3]跟 Trojan Horse 很像，基本上沒有複製與散佈自己的機制，因此攻擊者通常把這些簡訊木馬包裝成有趣的應用程式，如行事曆與遊戲等，以免費的方式吸引手機使用者下載安裝，一旦使用者安裝受感染的應用程式後，他們的手機就被感染了。當使用者啟動含有簡訊木馬的惡意軟體，這些應用程式就會開始自動寄送付費簡訊到特定的號碼，而使用者完全無法查覺手機正在寄送付費簡訊，等到使用者收到電話費用賬單後才驚覺手機可能安裝到惡意軟體，雖然不是使用者自己發送出去的簡訊，但使用者仍需為此付出高昂的電話費用。到目前為止，簡訊木馬對於網路罪犯來說，仍然是最簡單快速又輕鬆的賺錢方法。

簡訊木馬還會結合殭屍(Bot)病毒，變形成為簡訊殭屍 (SMS Zombie)，簡訊殭屍取得受害者的手機資訊和隱私資料後，將這些資訊用簡訊的方式發送給攻擊者，攻擊者則利用這些資訊來控制受害者的手機。在 2012 年 7 月，TrustGo[4]發現 SMSZombie 透過網路論壇散佈，在中國大陸約有五十萬隻手機遭受 SMSZombieA 感染，這是首次發現的 SMS Zombie。當使用者下載並安裝含有 SMSZombieA 的 App 後，該 App 會要求使用者安裝額外的檔案，使用者同意後，這些含有惡意程式的檔案就會被添加進去，一旦手機受到 SMSZombieA 的感染後，SMSZombieA 會嘗試取得管理者的權限，讓使用者無法手動將它移除，此外它還會攔截與銀行或財務相關的 SMS 訊息並且將訊息轉送給攻擊者[5]。

2.3 垃圾簡訊殭屍網路

垃圾簡訊殭屍網路 (SMS spam botnet) 是攻擊者用來發送大量的垃圾簡訊的方式，一旦使用者安裝並且啟動這個類型的惡意軟體，該惡意軟體會持續的跟 command-and-control (C&C) server 連線，取得目標手機的電話號碼和垃圾簡訊的內容後，接著利用受害者的手機來自動發送垃圾簡訊，受害者的手機也會定期的傳送報告給 C&C server。

Android 垃圾簡訊殭屍網路在 2012 年 12 月被 Cloudmark[6]發現，Symantec 檢測出 Android.Pikspam[7]。Android.Pikspam 攻擊的流程，首先使用者會收到通知中獎或免費下載知名遊戲的 App 的垃圾簡訊，如果使用者相信簡訊內容，並且點擊該簡訊內的 URL 連結，就會從第三方網站上面下載含有垃圾簡訊惡意軟體的 App 到手機內，這個惡意軟體會隱藏自己並且安裝合法的 App，讓使用者看到合法的廣告軟體，藉此來欺騙使用者相信這是安全的 App。

2.4 增加 Android 平台安全的機制

Android 的特點是開放原始碼，在 Android 平台下廠商或一般使用者可以自行開發軟體給用戶安裝，而權限機制設計，是為了讓未事先權限的 App 無法存取相關的隱私資訊或手機功能。這些 App 必須在它的 AndroidManiflest.XML 檔案或是在程式中動態宣告所需要的權限。若使用者接受並安裝該程式，這些 App 即取得其宣告的權限，直到它解除安裝為止。

Rubin Xu 等人[8]提出利用重新包裝 App 的方式，將 user-level sandboxing 和 policy code 放入 App 內，用來監控 App 的行為。當 App 違反 policy 時，像是 App 嘗試想要瀏覽使用者的敏感資訊，或連線到惡意的 IP 位址時，即便該 App 有宣告相關的權限，Aurasium 仍會顯示訊息讓使用者知道並處理，不過在檢查寄送簡訊時，Aurasium 只有檢查簡訊的電話號碼是否為 premium-rate number，沒有對簡訊內容做檢查，而且惡意軟體為了躲避監控，會想辦法不讓其被重新包裝。

2.5 惡意軟體偵測

自從 2006 年 3 月 Amazon.com 推出雲端運算(Cloud Computing)服務後，雲端運算開始蓬勃發展，至今已推出許多服務，讓使用者能夠存取服務軟體及資料，而無需了解雲端的基礎設施與架構，於是 Chris Jarabek 等人[9] 提出結合雲端運算服務來偵測惡意軟體。ThinAV 主要有二個元件：客戶端(client)與伺服器(server)。客戶端主要功能是將需要掃描的 App 檔案傳送到伺服器；伺服器主要的功能是將客戶端傳送過來的 App 檔案上傳至雲端的第三方掃描服務(Third-party Scanning Services)，使用第三方掃描服務檢查該 App 是否為惡意軟體，並且在掃描完成後，通知客戶端掃描的結果。ThinAV 所使用到的第三方掃描服務包括：VirusTotal Service、VirusChief Service、Kaspersky Service 和 ComDroid Service。ThinAV 提供一個在 Android 上使用的輕量級的掃描系統，不會佔用 Android 太多資源，不過 ThinAV 的偵測率是依賴第三方的掃描服務，且網路快慢也會影響到整體的效能。

Asaf Shabtai 等人[10]提出 Andromaly，是藉由修改應用程式架構所設計出的 Host-based 惡意軟體偵測系統，透過機器學習(Machine Learning)的方式訓練檢測模型，Andromaly 利用安裝在手機上的應用程式來持續不斷監控與收集手機內各式各樣的特徵和事件(CPU 的消耗、經由 Wi-Fi 所傳送封包的數量、執行的 process 數量和電池的用量)，將這些特徵和事件產生相對應的威脅評估(thread assessment, TA)，用來檢測手機上的可疑活動，並通知使用者檢測的結果。

3. Taurus 系統設計與實作

第一隻簡訊木馬 Trojan-SMS.AndroidOS.FakePlayer 是由卡巴斯基所發現，根據該研究指出[11]，當使用者啟動含有簡訊木馬的 App 後，該簡訊木馬會自動的發送三封簡訊到俄羅斯，而我們將該簡訊木馬反組譯後發現，其簡訊內的電話號碼與內容，是由簡訊木馬所提供，不會經過使用者輸入以及經由使用的通訊錄來取得相關內容，因此 Taurus 利用這個特性來運作。

3.1 系統架構

Taurus 主要是防止簡訊木馬隨意的發送簡訊的機制。我們從兩方面進行，首先取得並記錄使用者使用輸入法 (Input Method Editors, IMEs) 所輸入的內容，其次用記錄下的內容來比對簡訊內容，此外也會記錄被使用者拒絕發送的 App 名稱、接收方的電話號碼和簡訊內容，Taurus 一旦發現曾經被拒絕發送的應用程式和簡訊又再次被發送，就會判定此為惡意行為，接著將該可疑的程序殺掉，阻止其發送簡訊。如圖 1 所示，Taurus 主要由六個元件所組成，其分別為 Input Component、Write Component、Monitor Component、Service Component、Alert Component 和 SQLite。Input Component 是負責取得使用者輸入的內容，Write Component 是負責記錄的工作，Monitor Component 是負責取得簡訊內容，Service Component 是負責將記錄的檔案內容或白名單與黑名單的資料與簡訊內容互相比對的工作。當 Taurus 判斷有情況發生時，Alert Component 是負責通知使用者，SQLite 是儲存白名單和黑名單的地方。

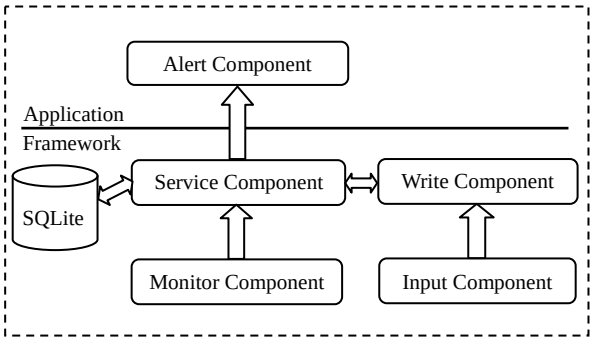

圖 1 Taurus 組成元件

首先由 Input Component 取得使用者輸入的內容後，再將使用者輸入的內容傳給 Write Component 處理，Write Component 將 Input Component 傳遞過來的內容加密，再將加密過的內容記錄在檔案中。當手機想要傳送簡訊時，Monitor Component 將會負責攔截即將要傳送出去的簡訊，並將此簡訊交由 Service Component 處理。接下來 Service Component 會先取得 Write Component 所產生的檔案並且與 Monitor Component 傳送過來的簡訊內容做相互比對，若兩者內容相同則比對成功，表示確實是由使用者發送，接著完成發送簡訊動作，相反的，如果兩者內容不相同或檔案不存在則為比對不成功，Service Component 會依照比對不成功的結果再進一步與白名單和黑名單的資料比對，如果與白名單的內容比對成功的話，表示此封簡訊內容為安全的內容，Taurus 會讓此封簡訊發送；如果與黑名單內容比對成功，表示此封簡訊為不安全的簡訊內容，Service Component 會將發送簡訊的程序刪除，阻止其發送簡訊，並交由 Alert Component 顯示警告訊息通知使用者；如果以上皆非，則依照比對的結果呼叫 Alert Component 向使用者顯示不同的訊息。

Alert Component 主要的工作是通知使用者。經過 Service Component 比對後產生的結果有三種不同的通知內容，分別為未知的簡訊內容、未知的電話號碼和警告等內容；當比對結果被判斷為惡意行為時，Alert Component 顯示警告的訊息，告知使用者此為惡意行為，系統已中止發送簡訊的訊息；當比對結果為未知的簡訊內容時，Alert Component 顯示未知的簡訊內容通知訊息，提醒使用者目前有簡訊將要傳送，讓使用者確認是否要發送此簡訊；當比對結果為未知的電話號碼時，Alert Component 顯示未知的電話號碼通知訊息，提醒使用者目前有簡訊將要傳送，讓使用者確認是否要發送此簡訊。

3.2 白名單與黑名單

白名單與黑名單的作用是用來輔助 Taurus。當 App 嘗試傳送簡訊時，Taurus 會先去確認該 App 的記錄檔案是否存在，如果不存在，就會尋找在白名單或黑名單內是否有相同的簡訊內容，存在白名單內的簡訊內容被認為是安全的，而存在黑名單內的簡訊內容則被認為是不安全的。

白名單的內容主要是儲存使用者曾經發送出去的簡訊內容，儲存內容包括 App 的 package name、電話號碼、簡訊內容與發送時間。如果使用者想要轉寄一封發送過的簡訊給其它電話號碼的話，因為使用者並沒有使用輸入法輸入簡訊內容，而在白名單內存在著一筆相同簡訊內容資料，接收方的電話號碼為使用者輸入或為手機內聯絡人電話或該電話號碼存在於白名單內，這封簡訊內容會被 Taurus 視為安全的內容，而將它發送出去。

黑名單的內容主要是儲存使用者曾經拒絕發送的簡訊內容，其儲存的內容與白名單相同，如果 App 想要再次發送存在於黑名單內的簡訊的話，該行為會被 Taurus 判定為惡意行為，Taurus 會將該 App 用來發送簡訊的程序殺掉，阻止其發送簡訊。

3.3 Taurus 的資料

Taurus 使用到三種資料，分別為記錄檔案、白名單與黑名單，所有的資料都是先經過 Advanced Encryption Standard (AES)加密後才儲存。記錄檔案

與白名單內的資料，我們保存 24 小時，在 24 小時之後，Taurus 將會自動清除所有存在於系統中的記錄檔案和白名單的內容，黑名單的資料則不清除，以便用來協助識別不安全的訊息內容。

3.4 Taurus 的限制

Taurus 藉由使用者使用輸入法輸入的方式進行判斷，可以確保發送出去的簡訊都是經由使用者輸入的，不過由於手機提供使用者可以不經過輸入法輸入的方式，譬如使用複製貼上或轉寄簡訊等功能，使用這些功能，Taurus 就無法藉由使用者輸入方式來取得內容，且在白名單或黑名單內沒有資料的話，Taurus 會顯示傳送簡訊的通知訊息，交由使用者決定。

4. 實驗結果

本實驗所使用的 App 樣本皆從網路[12]下載，樣本的選擇是以具有簡訊木馬的特徵為主要的篩選條件。實驗主要是測試手機內的 App 非經由使用者透過鍵盤輸入簡訊內容且嘗試寄出簡訊時，Taurus 是否能如預期的通知使用者，當使用者拒絕傳送簡訊時，而該 App 想再次傳送簡訊時，Taurus 是否能阻止簡訊傳送。本次實驗都是使用 Android 模擬器來模擬手機設備。實驗畫面如圖 2 所示，我們在 Android 模擬器上安裝含有簡訊木馬的 App 後，開啟並執行時此 App 時，可以發現此 App 嘗試自動寄送簡訊時，Taurus 顯示通知訊息通知使用者。當使用者拒絕發送此封簡訊，而該 App 又嘗試寄出簡訊時，Taurus 顯示警示訊息通知使用者，如圖 3。

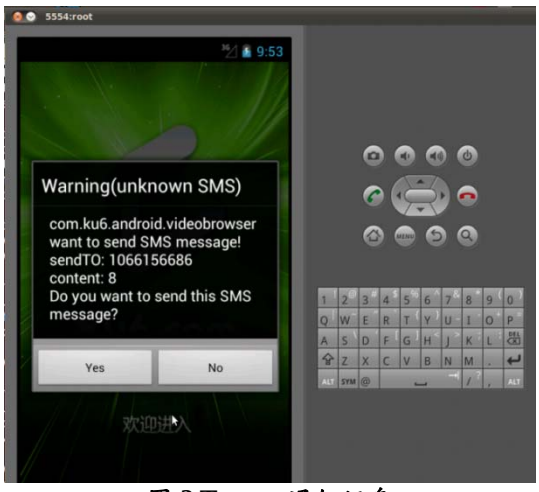

圖 2 Taurus 通知訊息

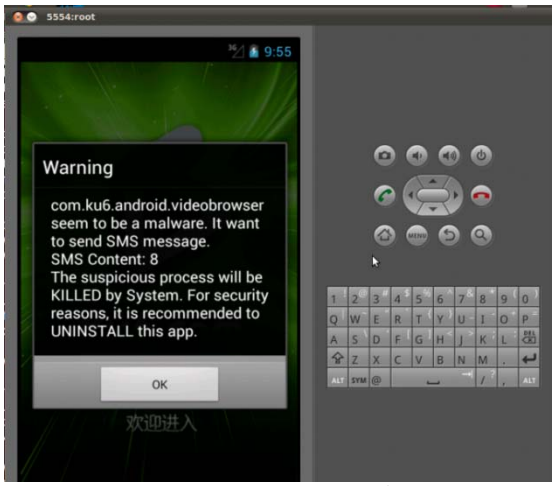

圖 3 Taurus 警告訊息

5. 結論

目前 Android 對於權限控管的方式以資訊揭露為主，一旦使用者安裝 App 後，形同使用者同意該 App 使用宣告的權限，App 便可在使用者不知道的情況下隨意使用發送簡訊的權限，造成使用者財務損失。

本論文提出藉由使用者輸入的內容來確認簡訊是否為使用者發送，如由非使用者發送，即便該 App 有發送簡訊的權限，使用者仍然可以阻止其發送簡訊，讓使用者能夠確實掌握簡訊的發送，避免手機淪為發送垃圾簡訊的工具，減少使用者財務上的損失，而且 Taurus 在執行過程對使用者而言是通透的，所以使用者不會感覺到 Taurus 的存在。

6. 未來研究方向

由於 Taurus 是屬於 Framework 層的保護機制，如果簡訊木馬是屬於 Linux 核心層的話，就有可能會繞過 Taurus 的檢查，未來可將 Taurus 加到 Linux 核心層，讓簡訊的保護能夠更加完善。

誌謝

本研究接受中央大學前瞻科技研究中心之計畫編號：1021062-2 和財團法人資訊工業策進會之計畫編號：10214011 的部分經費補助。

參考文獻

[1] 趙郁竹, "趨勢科技：Android 惡意 App 數量今年將達 140 萬 ", http://www.bnext.com.tw/article/view/cid/0/id/26045, January 8, 2013

[2] Ken Presti, "Kaspersky: SMS Trojans Account For Over Half Of Smartphone Malware ", http://www.crn.com/news/security/240012810/kaspersky-sms-trojans-account-for-over-half-of-smartphone-Malware.htm, February 2012.

[3] Pablo Ramos, "Don’t pay high phone bills: SMS Trojans can trick you via premium-rate numbers", http://www.welivesecurity.com/2012/11/29/android-sms-trojan-tricks-you-into-premium-rate-calls/, November 29, 2012.

[4] TrustGo Security Labs, "New Virus SMSZombie.A Discovered by TrustGo Security Labs", http://blog.trustgo.com/SMSZombie/, August 15, 2012.

[5] Shane McGlaun, "500,000 Android users in China infected with SMSZombie", http://www.slashgear.com/500000-android-users-in-china-infected-with-smszombie-20243293/, August 20, 2012.

[6] Andrew Conway, "Android Trojan Used To Create Simple SMS Spam Botnet", http://blog.cloudmark.com/2012/12/16/android-trojan-used-to-create-simple-sms-spam-botnet/, December 16, 2012.

[7] Pikspam: An SMS Spam Botnet, http://www.symantec.com/connect/blogs/pikspam-sms-spam-botnet, December 20, 2012.

[8] R. Xu, H. Saïdi, and R. Anderson, “Aurasium:Practical policy enforcement for android applications,” *In 21st USENIX Security Symposium. USENIX*, 2012.

[9] Jarabek, Chris, David Barrera, and John Aycock. “ThinAV: truly lightweight mobile cloud-based anti-malware,” *In 28th Annual Computer Security Applications Conference. ACM*, 2012.

[10] Asaf Shabtai, Uri Kanonov, Uuval Elovici. "“Andromaly”: a behavioral malware detection framework for android devices." *Journal of Intelligent Information Systems* 38.1 2012. pp. 161-190.

[11] Denis Maslennikov, “Mobile Malware Evolution: An Overview, Part 4”, http://www.securelist.com/en/analysis/204792168, March 22, 2011

[12] contagio mobile, http://contagiominidump.blogspot.tw/, Accessed:July 1 2013.