可信網路接入認證在移動終端上的實現
Access Authentication Mechanism for Trusted Network Implement on Mobile Terminals

吳昊 Hao Wu, 鐘章隊 Zhang-dui Zhong
北京交通大學軌道交通控制與安全國家重點實驗室
hwu@bjtu.edu.cn, zhdzhong@bjtu.edu.cn

摘要

傳統無線標準第三代合作夥伴計畫（3rd Generation Partner Project, 3GPP）、無線區域網路（Wireless Local-Area Network, WLAN）、全球微波互聯接入（Worldwide Interoperability for Microwave Access, WiMAX）中的安全機制對用戶接入認證、業務傳輸安全提供了保障，但由於應用服務提供者和IP網路本身的開放性和安全漏洞，導致來自應用層面的安全威脅無法應對。本文提出一種移動網路可信接入認證模型，通過對移動台的安全狀態進行評估，來指導網路側網元設備對移動台實施動態的網路訪問控制和應用服務限制，並根據安全狀態評估結果輔助移動台及時進行自身安全相關的更新、升級，從而給移動網路和移動台都提供了增強安全的手段，並提供了一種防止病毒或者蠕蟲在網路中快速蔓延的方法。

關鍵字：可信網路、接入認證、移動。

Abstract

The security mechanism of traditional wireless standard, such as 3GPP (3rd Generation Partner Project), WLAN (Wireless Local-Area Network), WiMAX (Worldwide Interoperability for Microwave Access), provides the ensure of user access authentication, service transmission security, but due to the openness and secure weakness of the application service provider and IP network, it leads to the secure threat from the application layer can not be solved. This paper presents a trust access authentication model in mobile networks, through the evaluation of mobile station' s secure status, the network side equipments limit the mobile station to act dynamic network control and application service, and they also help mobile station update itself according to the secure evaluation results. Therefore, it provides the mobile network and mobile station secure-enhance means, and also provides the way to prevent the virus and the worm from spreading rapidly in the network.

Keywords: Trust Network, Access Authentication, Mobile.

1 緒論

隨著無線資料網路的普及，越來越多的人開始使用移動終端設備享受網路服務，分組資料業務逐漸取代傳統電路業務，移動運營商網路趨於IP化。傳統標準3GPP、WLAN、WiMAX中的安全機制對用戶接入認證、業務傳輸安全提供了保障，但由於應用服務提供者和IP網路本身的開放性和安全漏洞，導致來自應用層面的安全威脅（如病毒、駭客攻擊、用戶資訊盜用等）層出不窮，傳統的安全機制對這些安全威脅無法應對。

來自運營商核心網內部的安全威脅容易得到有效管理，而對於從接入網接入核心網的移動台而言，其安全管理相對困難得多。移動台因為資源有限導致防護能力較低，其作業系統漏洞或安全應用未及時更新，很容易導致病毒入侵，而且移動台數目眾多、分佈範圍廣泛、移動性強，一旦其感染病毒並成為病毒傳播的源頭，運營商從網路側很難在保證安全和為用戶提供高品質服務之間作出合適的選擇。

本論文將提出一種可信網路接入認證在移動終端上的實現方法，相對於有線網路，由於移動網路中的移動性、漫遊、小終端處理能力有限，故可信網路接入認證方法必須作一定的改動，才能保證移動終端安全的接入網路，進一步保證移動網路的安全。

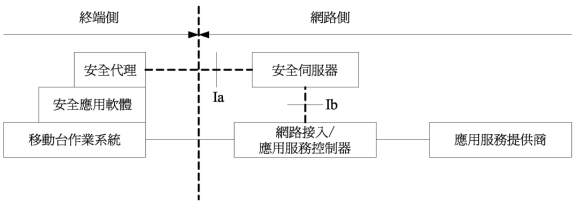
2 移動網路可信接入認證模型

本文中提出的移動網路可信接入認證模型實際上是可信網路接入認證模型在移動網中的一個應用。該模型是一個應對不安全移動台對移動網路所造成的潛在威脅的系統，它通過對移動台的安全狀態進行評估，來指導網路側網元設備對移動台實施動態的網路訪問控制和應用服務限制，並根據安全狀態評估結果輔助移動台及時進行自身安全相關的更新、升級，從而同時給移動網路和移動台都提供了增強安全的手段，並提供了一種防止病毒或者蠕蟲在網路中快速蔓延的方法。圖一描述了移動網路可信接入認證模型。

從圖中可以看出，移動網路可信接入認證模型主要包括四個實體：移動台側的安全代理、網路側的安全伺服器、網路側的網路接入控制器和應用服務控制器。安全代理和安全伺服器構成了該模型的核心。

安全代理和安全伺服器通過Ia介面進行通信。同時，安全伺服器通過Ib介面和PLMN中的其他網元通

信，通過它們之間的通信和交互，網路側提供對移動台的控制功能。



圖一　移動網路可信接入認證模型

安全代理負責收集移動台的安全相關資訊，對其進行處理，並和安全伺服器進行通信。從安全代理的功能可以看出，它是可信網路接入認證模型中可信網路收集部分和可信代理用戶端部分的功能集成；安全伺服器通過安全代理收集到的安全狀態資訊來評估和判斷移動台的安全狀況和安全等級，以及移動台的安全狀況是否被允許訪問網路和申請各種應用服務。從安全伺服器的功能上來看，它是可信網路接入認證模型中可信代理伺服器部分和可信屬性驗證部分的功能集成。

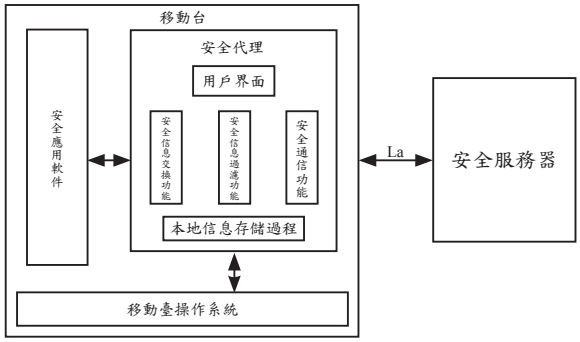
當安全伺服器收到安全代理發來的安全狀態資訊後，進行相關的評估，如果安全伺服器根據分析認為移動台不夠安全，安全伺服器會指示網路訪問控制器或應用服務控制器，對移動台的網路訪問和應用訪問作適當的控制，安全伺服器也會將對移動台的控制情況通知給安全代理。

如果有適合移動台進行自身作業系統升級的補丁、元件或者安全相關應用軟體的更新時，安全伺服器會通知安全代理協助移動台進行相應的升級或者更新，這些更新或者補丁、升級包都在安全應用軟體伺服器和移動台作業系統伺服器上，並由這些伺服器提供升級、更新服務，這些伺服器的擁有者一般是移動台作業系統生產商和移動台安全應用軟體生產商，可以把它們稱為應用服務提供商。

安全伺服器對於移動用戶的網路訪問控制和應用服務控制，通過對用戶所使用的移動台的控制來實現。其基礎資訊來源是安全代理向安全伺服器發送的安全狀態資訊和移動用戶已經在移動資料網路中申請或定制的各種服務。對於已經安裝安全代理的移動台，當移動台連接到資料網路時，安全代理的功能同時啟動。當某個移動台接入到網路，但是安全伺服器卻沒有收到移動台安全代理發送來的安全狀態資訊，此時無法評估移動台的安全狀態，可根據不同情況來做相應的處理。如果用戶要使用的是非緊急業務或優先順序別較低的業務，安全伺服器將不發送相應的控制消息給網路接入控制器，此時可以默認移動台被禁止訪問移動資料網路或Internet的任何資源，以此來保證網路的安全；如果用戶要使用緊急業務或優先順序別比較高的業務，則可以讓網路接入控制器將移動台發出的所有報文重定向到專用的安全設備處理，例如，重定向到反病毒閘道先進行過濾，然後再向報文的目的地轉發。另外，由於需要安全代理傳送一些移動台的一些安全狀態資訊給網路側的安全伺服器，此時，若是被攻擊者所知道，在還沒更新之前就會被入侵。因此，安全代理和安全伺服器之間的通信應該給予某種特定的安全通道，以保障移動台安全狀態諮詢不會被攻擊者截獲，安全代理和安全伺服器都可以選擇是否建立安全通道，通過在互相開始通信時發送安全通道建立消息來實現。本文暫不研究具體的安全通道建立方法。

3 安全代理的功能結構

移動台側安全代理的功能結構如下圖二所示。



圖二　安全代理的功能結構

從上圖可以看出，移動台側的安全代理主要包括的功能有：安全資訊交換功能、安全資訊過濾功能、安全通信功能、用戶介面以及本地資訊存儲功能。各部分功能的具體介紹如下：

(1)安全資訊交換功能：安全代理收集來自移動台的安全狀態資訊。這裏的安全狀態資訊包括：移動台安全事件、移動台作業系統版本和補丁資訊、安全應用軟體的日誌資訊、移動台用戶ID、移動台ID、遺留在移動台中的網路病毒蹤跡等。此外，安全資訊交換功能還要將安全伺服器發來的安全狀態更新資訊和指令，通過安全代理和移動台作業系統和安全應用軟體之間的介面，提供給移動台作業系統和安全應用軟體的補丁、升級資訊，並輔助其進行更新、升級。

(2)安全資訊過濾功能：安全代理按照本地或者安全伺服器發來的策略，處理和組織移動台安全狀態資訊，將篩選過濾後的資訊上報給安全伺服器。同時接受安全伺服器發來的安全更新命令和指示、移動台安全評估等級、移動台網路訪問受限等資訊，篩選後即時通知給移動台用戶或者生成本地安全報告／日誌供移動台用戶主動查詢。

(3)安全通信功能：是負責和安全伺服器之間進行互認證，協商、建立安全的安全狀態評估消息傳輸通道，保證與安全伺服器之間進行可靠的安全狀態相關消息傳輸。

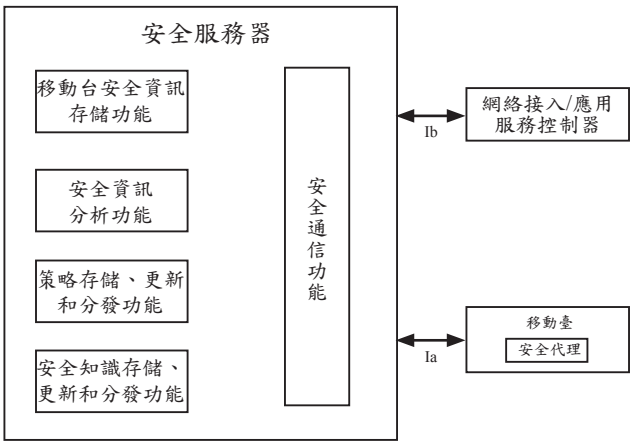
(4)用戶介面：是指提供移動台用戶和安全代理之間進行資訊交互的功能，為用戶提供即時資訊的提示或者接受用戶對安全代理報告／日誌的查詢。

(5)本地資料庫：用於存儲安全代理涉及的安全相關資訊、日誌和各種策略。當移動台關機或者掉電後，安全代理獲得的終端側和網路側的安全相關資訊不會丟失。

通過上述對安全代理功能結構的描述可以看出，該功能結構不僅能夠實現終端側與網路側的安全相關資訊交互，而且還方便了用戶即時瞭解移動網路可信接入認證系統正在如何對移動台進行控制，用戶也可以主動地向安全代理查詢目前移動台的安全狀態。

4 安全伺服器的功能結構

安全伺服器是一個邏輯的概念，由5個功能模組構成，每個功能模組都可以是一個物理設備。安全伺服器的功能結構如下圖三所示。



圖三　安全代理的功能結構

從上圖可以看出，網路側的安全伺服器主要包括的功能有：移動台安全資訊存儲功能；安全資訊分析功能；策略存儲、更新和分發功能；安全知識存儲、更新和分發功能；以及安全通信功能。各部分功能的具體介紹如下：

(1)安全通信功能：負責在安全伺服器和安全代理、網路接入控制器／應用服務控制器之間建立安全可靠的傳輸通道，保證傳輸消息的一致性、完整性和機密性。

(2)移動台安全資訊存儲功能：可以包含一個安全資料庫，用於存儲移動台安全代理向安全伺服器上報的安全狀態資訊和安全伺服器對移動台安全等級的評估結果以及目前正在執行的移動台控制策略。在該安全資料庫的結構中，可以用國際移動用戶標識（International Mobile Subscriber Indentity, IMSI）來唯一標識一個移動用戶，用國際移動終端設備標識（International Mobile station Equipment Indentity, IMEI）來唯一標識一個移動終端，還可以有相關的資料庫表來記錄移動台IMEI、移動用戶IMSI以及安全代理ID三者之間的當前和歷史的聯繫。

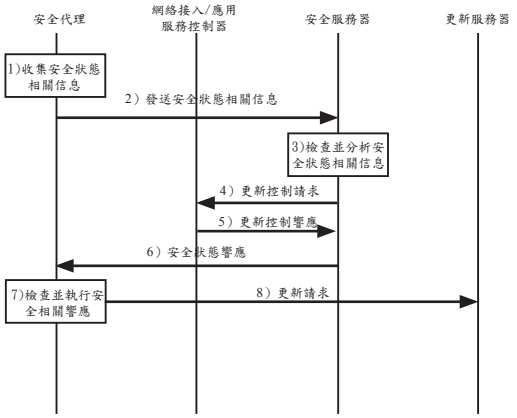
(3)安全資訊分析功能：安全伺服器根據本地的安全策略和安全知識，利用移動台安全代理上報的安全狀態資訊來分析和評估單個移動台的安全等級。

(4)策略存儲、更新和分發功能：策略包括面向系統控制的策略和安全分析評估策略。策略應該事先定義完善並存儲在安全伺服器中，可以通過安全伺服器的通信功能將策略分發給安全代理、網路接入控制器和應用服務控制器以指導它們的行為。

(5)安全知識存儲、更新和分發功能：安全知識包含所有網路側提供的知識和資訊。安全知識包括各種網路安全威脅及其應對方法，移動台補丁、升級報資訊和資源位址，移動台安全應用軟體更新升級資訊和資源位址，安全代理各個版本資訊和下載位址等等。大部分的安全知識應該由移動台作業系統生產商、移動台安全應用軟體生產商和第三方安全研究機構提供。安全知識用於指導移動台進行安全相關的更新、升級，並作為參考資訊用於安全伺服器分析和策略管理單元對安全策略的制定。

5 對移動台進行評估控制的過程

當有移動台想要接入移動網路時，首先要和網路進行身份認證，身份認證通過後，移動台上的安全代理將主動收集移動台的安全狀態相關資訊併發送給網路側的安全伺服器，安全伺服器評估這些安全狀態相關資訊，並對移動台的接入作出判決。具體流程如圖四所示。



圖四　對移動台進行評估控制過程

(1)安全代理收集移動台的安全狀態相關資訊。

(2)安全代理將收集的安全狀態相關資訊發送給網路側的安全伺服器。

(3)安全伺服器收到安全代理發送來的安全狀態相關資訊後，首先檢查其有效性，然後根據資訊的內容和自己本地存儲的移動台安全策略進行分析，判斷目前移動台的安全狀態等級。

(4)如果安全伺服器認為需要對移動台的網路訪問控制／應用訪問控制策略進行更新，則發送控制資

訊給網路訪問控制／應用訪問控制設備，對移動台的網路接入／應用接入按照策略進行控制。如果安全伺服器認為移動台的安全狀態符合安全策略，則不發送控制資訊，移動台接入狀態不進行更新。

(5)如果步驟4的網路訪問控制／應用訪問控制策略要求移動台接入狀態進行更新，則網路訪問控制器／應用訪問控制器需要向安全伺服器回饋控制更新的執行結果。

(6)安全伺服器向安全代理發送安全狀態資訊評估響應，通知安全代理目前移動台的安全評估結果。該回應中還可以包含安全代理生成和發送安全狀態相關資訊的策略、安全代理收集整理移動台安全相關資訊的策略等資訊。如果安全伺服器認為移動台不需進行安全更新，則安全代理不對移動台的策略進行更新；如果安全伺服器認為移動台需要進行安全更新，安全狀態資訊評估回應中還要攜帶安全更新的獲取位址和移動台進行安全更新的策略。

(7)安全代理收到安全狀態資訊評估回應後進行有效性檢查，然後使用其中的資訊更新安全代理的本地資訊和策略。

(8)如果安全狀態資訊評估回應中指示移動台需要安全更新，則安全代理按照回應中的資訊和策略協助移動台進行安全更新。這裏的安全更新也包括安全代理自身的升級和更新。

上述過程中，4、5、7、8是可選步驟，不一定每次都會執行，當移動台安全狀態不符合安全策略，則執行4、5、7、8。當移動台按照安全代理的指示進行成功更新，並通過安全伺服器的安全狀態資訊驗證後就可以安全地接入到該網路。

6 總結及展望

本文給出了可信網路接入認證模型在移動網路實現的具體方案。包括對移動網路中安全伺服器的功能以及結構的詳細描述，對移動臺上安全代理的功能以及結構的詳細描述，以及移動網路和移動台之間進行認證的具體流程。本文的研究還處於理論研究階段，需要開展和探討的工作還有許多，後續工作主要包括：

(1)需要做開源實現來驗證本文的可信網路接入認證方法的合理性，在此過程中需要對認證體系結構中各個介面運行的協定進行詳細定義。

(2)對於用戶接入時的效率以及如何提高終端安全（即具體的修補策略）還需要具體定義和描述。

致謝

本論文得到國家自然科學基金——鐵道聯合資助重點專案（60830001）及軌道交通控制與安全國家重點實驗室（北京交通大學）開放課題基金（SKL2008K007）資助。

參考文獻

[1] 林闖、彭雪海，*可信網絡研究*，計算機學報，2005，5月，pp.751-758。

[2] 楊義先、忸心忻，*無線通信安全技術*，北京：北京郵電大學出版社，2005，5月，pp.74-300。

[3] 薑楠、王健，*移動網絡安全技術與應用*，北京：電子工業出版社，2004，2月，p.79。

[4] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz Ed., "*Extensible Authentication Protocol (EAP),*" Internet Engineering Tast Force RFC3748, June, 2004.

[5] IEEE Std 802.1x-2001, "*IEEE Standards for Local and Metropolitan Area Network: Port Based Network Access Control[S],*" 2001.

[6] TPM Main Part1 Design Principle, "*Specification Version 1.2[Z],*" TCG Specification.

作者簡歷

吳昊（**Hao Wu**），女，1973年出生，北京交通大學現代通信研究所，副教授／博士。2000年畢業於哈爾濱工業大學電子與通信工程系，獲通信與電子系統博士學位。目前研究方向主要為移動通信、資訊安全。

鐘章隊（**Zhang-dui Zhong**），男，1962年5月出生，北京交通大學現代通信研究所所長、教授、博士生導師。長期從事軌道交通無線通信移動通道理論與關鍵技術、軌道交通無線網路理論與技術、軌道交通通信網路和資訊網路測量理論與技術等方向的研究。