Intelligent Information Management, 2009, 1-5
doi:10.4236/iim.2009.11001 Published Online July 2009 (http://www.scirp.org/journal/iim)

The Analysis and Amendment of Security System in 3G

Min ZHAO, Ling SHI
Computer Department, East China University of Science and Technology, Shanghai, China

Abstract: This paper analyses security mechanism and authentication, key agreement protocol of 3G system amply, puts forward a amelioration scheme. This scheme assures security communications without credible VLR. This paper analyses ameliorative protocol and resolves the security communications problem between MS and HLR.

Keywords: 3G Security, 3G Security Structure, 3G authentication and key agreement protocol Security arithmetic

3G 系統安全體制分析與協議改進

趙　敏，史　令
華東理工大學 計算機系 200237

摘　要：本文對 3G 系統安全體制和認證、密鑰分配協議進行了詳細分析，提出了對協議的改進方案，從而保證有不完全可信 VLR 參與的保密通信，並對改進方案進行了分析，解決了 MS 到 HLR 之間的通信安全問題。

關鍵詞：3G 安全，3G 安全體制，3G 認證與密鑰協商，安全算法

1. 引 言

在第三代移動通信系統中，除了傳統的話音業務外，電子商務、電子貿易、網路服務等新型業務將成為 3G 的重要業務內容。目前，2G 網路已經投入了大量資金和設備，廢棄 2G 網路在一種新的安全體制之上開發 3G 網路是不現實的作法。移動通信中 3G 網路與 2G 網路的共存是目前移動通信向 3G 過渡必然要經歷的階段。因此，3G 網路要繼承 2G 網路，無法改變建立在對稱密碼安全體制之上的 2G 安全體制。從 1996 年起，歐洲電信標準學會著手開發 3G 移動系統，並逐漸由 3GPP 取代，其目的是制定一個全球統一的移動應用規範。3G 安全的設計宗旨是在 2G 安全的基礎上有所提高，以提供新的安全性能與服務。因此，在移動通信系統中，資訊的加密仍將採用對稱密碼體制，為實現資訊的加密傳輸，通信雙方必須首先進行身份認證，協商會話密鑰[1]。在現有 2G 網路中引入 3G 接入設備和網路實體時,要在儘量不改變原有 2G 網路實體的基礎上,實現與現有 2G 網路的交互，使移動網路能為雙模式手持設備用戶提供通過使用 SIM 卡或 USIM 卡在 2G 和 3G 網路的接入和服務[2]。

3G 安全體制不是端到端的安全機制, 給密級較高的應用帶來困難。比如, 如果 VLR 在一個不被信任的網路域中，由於在 3G 系統中它可以獲取通信所需的 CK 和 IK 的，這樣對 VLR 而言，就沒有什麼秘密可言。

2. 3G 安全體制

3G 的安全目標是: 保證由用戶產生的或與用戶相關的資訊能夠得到充分保護，防止被誤用或盜用；保證由服務網路或歸屬環境提供的資源和業務能夠得到充分保護，防止被誤用或盜用；保證標準化的安全特徵至少應有一個可以在世界範圍的基礎上輸出的加密

演算法；保證安全特徵被充分的標準化，以確保世界範圍內互操作與不同的服務網路之間的漫遊；保證提供給用戶和業務供應者的保護級別比現代固定和移動網路提供的高；保證 3GPP 安全特徵、機制和實現能被擴展和加強[3]。

3G 安全體制的總體結構分為 3 個層面和 5 個部分：

⑴ 網路接入安全：提供安全接入 3G 服務網的機制，並抵禦無線鏈路攻擊。這一部分功能包括：用戶身份保密、認證和密鑰分配、資料加密和完整性等。認證過程也融合了加密、完整性保護等措施。

⑵ 網路域安全：保證網內信令的安全傳送並抵禦對有線網路的攻擊。

⑶ 用戶域安全：主要保證對移動台的安全接入，包括用戶與智慧卡間認證、智慧卡與終端的認證及其鏈路的保護。

⑷ 應用域安全：使用戶域與服務提供商的應用程式間能夠安全的交換資訊。

⑸ 安全特性的可視性及可配置能力：主要指用戶能獲知安全特性是否在使用以及服務提供商提供的服務是否需要以安全服務為基礎[4]。

加密和完整性保護是實現安全通信的核心，認證與密鑰分配是實現安全通信的重要保證。3G 系統的安全體制是建立在 2G 的基礎上，GSM 及其他 2G 系統中已被證明是必須和穩健的安全元素將繼續被採用，3G 還將改進 2G 中的安全弱點，最終提供全新的安全性能和業務。3G 相關安全協議很多，本文針只對其中的核心部分，認證與密鑰分配協議進行分析與改進。

3. 3G 認證與密鑰分配協議分析與改進

3G 安全系統定義了一些安全演算法，下面只介紹本文所用到的安全演算法：

f1=>MAC：產生消息認證碼；

f2=>XRES：用於消息認證中計算期望回應值；

f3=>CK：產生加密密鑰；

f4=>IK：產生完整性密鑰；

f5=>AK：產生匿名密鑰；

3G 認證與密鑰分配由 f1~f5 實現。

3G 規範中 UMTS 鑒權過程是建立在每個用戶唯一的用戶鑰匙 K 的基礎上的，K 存儲在 USIM 和用戶環境歸屬 AuC 中。MS：移動站；AKA：認證與密鑰分配；UE：用戶終端；HLR：歸屬位置寄存器；VLR：訪問位置寄存器；HE：本地環境；AV：認證向量，AV=RAND||XRES||CK||IK||AUTH ； XRES=f2(K ，RAND)；CK=f3(K，RAND)；IK=f4(K，RAND)；AUTH=SQN ⊕ AK||MODE||MAC；MODE：移動性管理標識；MAC=f1(K，SQN||RAND||MODE)。

3.1 協議過程分析

認證協定分為以下幾個步驟：

⑴ MS➔VLR：IMSI||HLR；

⑵ VLR➔HLR：IMSI；

⑶ HLR➔VLE：認證向量 AV；

⑷ VLR➔MS：RAND||AUTH；

⑸ MS➔VLR：RES

首先 VLR 收到 MS 的註冊請求，MS 發送用戶自己的 IMSI 和 HLR 資訊給 VLR；

VLR 接收到該請求後，將 IMSI 轉發給 MS 的 HLR；

HLR 接到 IMSI 後產生 SQN，RAND，按照上述公式計算認證向量 AV，併發送給 VLR；

VLR 接收到 AV 後，將解析到的 RAND 和 AUTH 轉發給 MS；

MS 接收到認證請求回應後，計算 XMAC= f1(K，SQN||RAND||MODE)，比較是否等於 MAC，如果不同，則向 VLR 發送拒絕認證消息並放棄該過程。接下來檢測 SQN 是否在合理的範圍內，如果不在合理範圍內，就向 VLR 發送“同步失敗”消息，放棄該過程。如果上面檢測都通過了，MS 計算 RES、CK 和 IK，並將 RES 發送給 VLR；

VLR 接收到 RES 後，與 XRES 比較，如果 RES 與 XRES 相同，認證成功，否則認證失敗。協定流程如圖 1 所示。

3.2 安全性分析

前面已經提到 MS 與 HLR 之間共用一個密鑰 K，該密鑰的安全是 3G 安全體制的基本保障。因為 3G 安全體制建立在對稱密碼體制基礎上，所以對稱密鑰的安全顯得尤為重要。

⑴ 認證安全分析：我們已經知道，3G 安全認證是雙向認證，MS 需要認證 HLR，VLR 需要認證 MS。

VLR 接收到來自 HLR 的認證向量中包含了期望 MS 產生的應答 XRES=f2(K，RAND)。若 MS 是合法用戶，在接收到 VLR 返回的 RAND 後，只有合法的

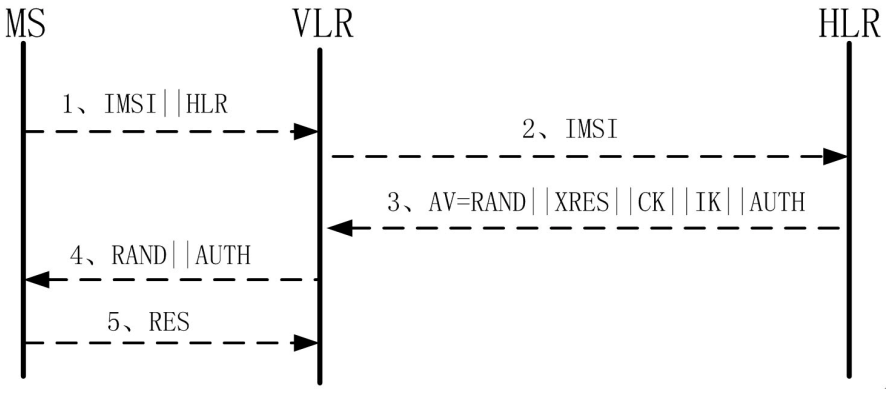

圖 1. 認證與密鑰分配過程
Figure 1. Authentication & key distribution process

MS 才能計算出 RES=f2(K, RAND), 且 RES=XRES。因為 K 由 MS 和其歸屬的 HLR 所掌握，所以別人無法計算得出 RES。這樣, 就實現了 VLR 對 MS 的認證。

MS 對 HLR 的認證是通過消息認證碼 MAC 來實現的。MS 接收到 VLR 轉發的來自 HLR 的 MAC=f1(K, SQN||RAND||MODE)，計算 XMAC=f1(K，SQN||RAND ||MODE)，在保證 SQN 的正確性前提下，MAC=XMAC，則認證成功。因為對稱密鑰 K 在 HLR 也掌握，隨意只有合法的 HLR 才能計算出與 MS 計算得到相同的 MAC 值，這樣就實現了 MS 對 VLR 和 HLR 的認證。

⑵ 加密和完整性密鑰每次會話都更新

MS 與 VLR 之間每次通信均採用不同的密鑰 CK 與 IK。由於每次通信前的認證選擇了不同的認證向量, 保證每次通信採用的 CK 和 IK 是採用不同的亂數得到的。而每次使用的消息認證碼 MAC 是由不斷遞增的序列號 SQN 作為其輸入參數之一, 保證了認證消息的新鮮性，從而確保密鑰的新鮮性，但在一次會話建立後直到該會話結束 CK 與 IK 不會改變。

⑶ 資料完整性

通過在消息中包含哈希值來進行完整性驗證。在認證和密鑰分配過程中，通信雙方協商了完整性密鑰 IK，通過 IK 可以保證資料沒有被修改。

⑷ MS 與 VLR 之間的密鑰分配安全性

VLR 接收到來自 HLR 的認證向量中包含了加密密鑰 CK 與完整性密鑰 IK，合法用戶在收到正確的亂數 RAND 後，能正確產生 CK=f3(K，RAND)，CK 與 IK 未在無線介面中傳輸，確保了密鑰的安全性。也就是說，CK 與 IK 在 HLR 和 MS 端分別產生，由於有共用密鑰 K，所以雙方產生的 CK 和 IK 是一致的。

3.3 協議改進

從上面分析可以看出, 目前 3G 通過在 MS 和 HLR 共用密鑰, 達到 MS 與 VLR 之間加密通信。也就是說, MS 可以用與 VLR 之間協商的 CK 和 IK 進行加密通信，但無法從 3G 安全協議本身保證從 VLR 和 HLR 之間的安全通信，VLR 和 HLR 之間的安全通信是通過網路域的保密措施來保證的, 3G 協議本身並未對次進行定義。

3G 的認證與密鑰分配協議在假定 HLR 與 VLR 之間安全的前提下，實現了用戶終端對網路 HLR/VLE 的認證和網路對用戶的認證，同時也實現了在 UE 與 VLR 之間的密鑰分配。從協議上看，3G 認證與密鑰分配協議不是一種端到端的安全協議, 在 VLR 和 HLR 之間是通過網路域安全來保證的。

如果第三方在 VLR 和 HLR 之間對資訊進行竊取，就可以獲取 HLR 傳送給 VLR 的認證向量 AV，從而可以獲取 CK 和 IK。這樣，MS 的加密資料對入侵者而言就沒有秘密可言。

針對上述分析，有兩種方案進行改進：

⑴ 對可信的 VLR 而言，增加 HLR 與 VLR 之間的共用密鑰 K2；

通過增加 HLR 與 VLR 共用密鑰，實現 HLR 和 VLR 之間重要資訊的加密傳輸，保證了傳輸資訊的機密性，使第三方無法獲取認證向量 AV，保證通信的安全[5]。

本方法解決了在 VLR 和 HLR 之間的安全傳輸問題，雖然這可以用網路域的安全方案給予解決，但本方案從 3G 協議本身入手，解決了第三方竊取通信資

料的問題。

⑵ 對不完全可信的 VLR 而言，利用 MS 與 HLR 之間共用的密鑰 K 進行加密通信，VLR 只作轉發工作，這適用於密級較高的應用。

從圖 1 可以看出，在 VLR 和 HLR 之間部分傳輸資料對不可信 VLR 是敏感的，比如：認證向量 AV。如果不希望 VLR 見到敏感資料, 可以利用共用密鑰 K 進行處理。假設對稱加密演算法為 E(●)；對稱解密演算法為 D(●)；

① MS➔VLR：IMSI||HLR；

② VLR➔HLR：IMSI；

③ HLR➔VLE：E(K，AV)||XRES；

④ VLR➔MS：E(K，AV)；

⑤ MS➔VLR：RES

注：AV= RAND|| AUTH

在改進協議中，HLR 利用與 MS 共用的密鑰 K 對 AV 加密處理，並計算 XRES，把 E(K，AV)||XRES 傳送給 VLR。由於 VLR 無法掌握密鑰 K，也就無法掌握認證向量 AV。VLR 把 E(K，AV)轉發給 MS，由於 MS 掌握密鑰 K，所以可以得到認證向量 AV。從 AV 中可以獲取 RAND 和 AUTH, MS 計算得到 CK 和 IK 用於加密通信, 計算 RES= f2(K, RAND)返回給 VLR。VLR 比較 XRES 與 RES，如果相等就認證成功。此過程見圖 2。

此方法解決了如果在 VLR 不可信的基礎上, 如何保證端到端的資料加密通信。第三方或不可信的 VLR 無法獲取敏感通信資料。

安全性分析：

加密通信過程中，用密鑰 CK 進行加密，完整性驗證用密鑰 IK。CK 和 IK 由 RAND 和共用密鑰 K 產生, 而 K 只有 MS 和 HLR 掌握, 所以只有 MS 和 HLR 能夠產生正確的 CK 和 IK，從而保證通信安全。

假設，建立會話後進行後續通信的資料為 Data，對稱加密演算法為 E(●)；對稱解密演算法為 D(●)；MS 把 Data 進行對稱加密結果 E(CK，Data)||HLR 發送給 VLR，VLR 轉發給 HLR。HLR 利用 CK 進行解密得到 Data。這樣，在通信線路中傳輸的為密文，從而確保安全。

假設某個 VLR 不可信, 由於它無法計算得到加密密鑰 CK，從而無法得到加密通信資料 E(CK，Data)的明文 Data, 資料就可以安全通過 VLR 到達 HLR 了。

假設竊聽者在通信線路上截取通信資料，與 VLR 一樣，它也無法計算得到加密密鑰 CK，也無法獲取通信資料的明文。

該協定繼續沿用了 3GPP 標準中該協議的安全特性：對 MS 和 HLR/VLR 進行雙向認證；在認證過程中進行密鑰分配和協商；資料完整性驗證等。

此協定中，只是把 VLR 作為通信資料轉發站來看，VLR 和任何想截獲通信資料的第三方都無法得到通信資料明文，從而有效的防止了第三方竊取和 VLR 不可信的問題，但這會增加一些計算量，對通信效率有所影響。對密級較高的通信，損失一些速度而保證安全也是可取的。

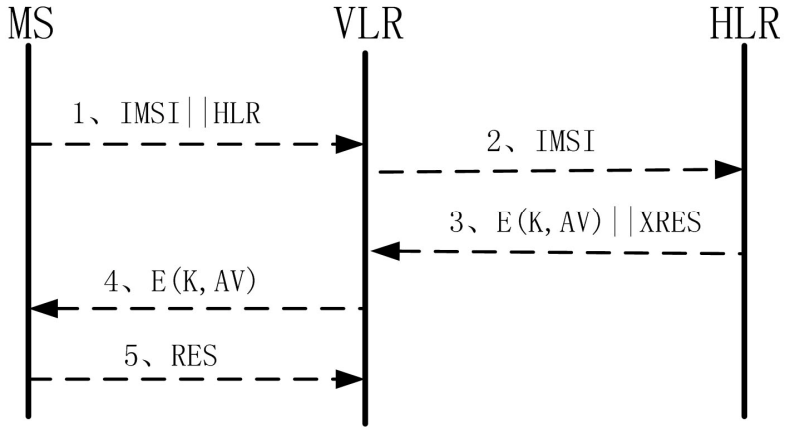

圖 2. 改進的認證與密鑰分配協定

Figure 2. Improved authentication & key distribution agreements

4. 結論

目前 3G 相關的協議和標準正在不斷完善過程中，本文從理論角度提出瞭解決在不完全可信 VLR 參與情況下安全通信的問題。目前 3G 系統中 HLR 和 VLR 之間網路傳輸的安全特性定義在網路域的安全協定中，本文從 3G 協議本身出發，提出了建立在對稱密碼機制基礎之上結合 3GPP 相關協議的安全認證與密鑰分配協議的新思路。

該安全協議有如下特點：

繼承 3G 認證與密鑰分配協議的優點，不損害原有協議安全性；

從協議自身增強 VLR 與 HLR 之間的通信安全性；能夠抵抗中間人攻擊。

REFERENCES

[1] Zhu li-qi, Huang ben-xong. improvement and formal analysis of 3G authentication and key distribution protocol. Electronics Engineers, 05/2004(In Chinese) (朱裏奇，黃本雄. 3G 認證和密鑰分配協議的形式化分析與改進. 電子工程師, 5/2004).

[2] Liu zi-long, lu Zheng-xin, huang zhai-lu. 2G and 3G mobile network system security and user authentication. Telecommunications technology, 02/2002(In Chinese)(劉子龍，盧正新，黃載祿. 2G 與 3G 移動網系統安全性及用戶鑒權. 電訊技術, 2/2002).

[3] Li xiang, 3G Security Architecture. Telecommunications Technology, 10/2002(In Chinese)(李翔. 3G 的安全體系結構. 電信技術, 10/2002).

[4] Lin de-jing, lin bai-gang, lin de-qing. research and analysis of 3G system-wide network security. ZTE Technology. 02/2003 (In Chinese)(林德敬，林柏剛，林德清. 3G 系統全網安全體制的探討與分析. 中興通訊技術, 2/2003).

[5] Liu dong-shu, wei bao-dian, wang xin-mei. improvement of the 3G authentication and key distribution protocol. Journal of Communication, 05/2002(In Chinese)(劉東蘇，韋寶典，王新梅. 改進的 3G 認證與密鑰分配協定 通信學報. 5/2002).

