第4卷第1期　　空 军 工 程 大 学 学 报(自然科学版)　　Vol.4 No.1
2003年2月　　JOURNAL OF AIR FORCE ENGINEERING UNIVERSITY(NATURAL SCIENCE EDITION)　　Feb. 2003

无线局域网中的信息安全保护与漫游管理

孙树峰，　贺　樑，　石兴方，　顾君忠
（华东师范大学 计算机系，上海　200062）

摘　要：分析了无线局域网中目前常用的802.11协议的安全特性及不足，提出了一种改进的动态WEP加密，重点讨论了基于多种安全策略的ESMP，论述了在不同无线接入点之间用户的漫游管理。

关键词：安全策略；动态WEP；ESMP；漫游
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009－3516(2003)01－0050－04

1999年9月，IEEE－SA标准推出了2.4 G上的11M 802.11b标准和5 G上的54 M 802.11a标准。自此，无线局域网已经成为新的市场热点，由于它的方便性及快速盈利性，使得越来越多的公司或组织开始组建无线网络。无线网络具有如下优势：一是可移动性，它提供了不受线缆限制的应用，用户可以随时上网；二是容易安装、无须布线，大大节约了建网时间；三是组网灵活，即插即用，网络管理人员可以迅速将其加入到现有网络中，并在某种环境下运行；四是成本低，特别适合于变化频繁的工作场合。但随着时间的发展，无线网络正暴露出越来越多的安全问题。据美国Gartner发表的有关企业WLAN导入的安全方面的调查报告表明，因企业在采取WLAN系统时都未采取适当的安全措施，到2002年底，30%的企业将被数据泄漏等严重安全问题所困扰。据介绍，现在有50%以上的企业已采用或正计划采用WLAN。RSA Security在英国伦敦进行的一项调查也表明，67%的WLAN毫无安全可言。

1　802.11协议的安全措施

1.1　ESSID

通讯前，所有的移动节点必须和无线接入点AP(Access Point)建立连接，这要求移动节点和AP配置为具有相同扩展服务集标识ESSID(Extended Service Set Identifier)，是无线局域网最基本的安全措施。然而这种安全措施是十分有限的，许多无线网卡能自动搜索周围环境中的AP和AP的ESSID参数同时，为方便用户，很多无线网卡和AP都提供了ANY这个保留关键字来使得网卡能够自动连接到附近信号最好的AP，但方便性带来了安全的隐患，如果需要增强无线网络的安全性，就需要关闭这个关键字。

1.2　MAC地址过滤

MAC地址过滤需在AP设备的永久性存储器中存放一组用户的MAC地址列表，只有列表中用户可访问对应的AP。这对AP数量不多的无线局域网系统比较适合。它也是比较脆弱、麻烦的安全手段，因为许多无线网卡支持通过重新配置的方法来改变网卡的MAC地址；另一方面，很多厂商为方便用户常把网卡的MAC地址印刷在无线网卡背面的标签上。非法入侵者可以从无线电波中截获数据帧，从而分析出合法用户的MAC地址，进而修改自己的地址，伪装成合法地址以访问网络，这就使得网络的安全遭到破坏。

1.3　静态WEP加密法

在802.11中有一个对数据基于共享密钥的加密机制，称为“有线等效保密WEP”(Wired Equivalent Privacy)的技术，WEP是一种基于RC－4算法的40 bit或128 bit加密技术。移动用户端和AP可以配置4组

收稿日期：2002－08－28
基金项目：国家863信息安全(863－104－03－02)课题资助(2001AA143060)
作者简介：孙树峰（1969－），男，山东济宁人，讲师，博士生，主要从事系统分析与集成，网络系统的安全等研究；
顾君忠（1949－），男，教授，博士生导师，主要从事智能数据库、信息安全和CSCW等研究.

WEP 密钥,加密传输数据时可以轮流使用,这允许加密密钥动态改变,但密钥只能是 4 组中的一个,其实质上还是静态 WEP 加密。同时,AP 和它所联系的所有移动用户都应使用相同的加密密钥,使用同一 AP 的用户也使用相同的加密密钥,带来的问题是:若其中一个用户的密钥泄漏,其他用户的密钥也无法保密了。

2000 年 10 月,WEP 被发现存在安全漏洞,根据理论分析[1],我们可写出破解 WEP 加密技术的算法,破解算法简化如下:

```
RecoverWEPKey(CurrentKeyGuss,KeyByte)
  Counts[0...255]=0
  for each packet→P
      if Resolved(P.IV)
          Counts[SimulateResolved(P,CurrentKeyGuess)] + =Weight(P,CurrentKeyGuess)
  for each SelectMaximalIndexesWithBias(Counts)→ByteGuess
      CurrentKeyGuess[KeyByte] = ByteGuess
      if KeyByte = KeyLength
          if CheckChecksums(CurrentKeyGuess)
              return CurrentKeyGuess
      else
          Key = RecoverWEPKey(CurrentKeyGuss,KeyByte + 1)
          if Key = Success
              return Key
      return Failure
```

2　改进的安全技术

针对目前无线局域网上存在的安全漏洞,我们提出了在无线局域网中采用动态 WEP 数据加密技术和 RADIUS 用户认证相结合的全方位多层次的信息安全保护解决方案。

动态 WEP 它能够给不同的用户分配不同的基于会话的 WEP 加密密钥,使得窃听者即使分析出密钥,也无法利用此密钥来分析出数据。动态 WEP 的实施需要和 RADIUS 认证服务器结合在一起,因为动态密钥的分配需要和用户绑定在一起,在用户的身份认证通过后,AP 会通过一个随机算法生成一个动态的 WEP 密钥,此密钥通过 RADIUS 认证服务器分配给客户端设备,客户端设备将使用此密钥和 AP 保持通讯连接,当用户离开此 AP 服务范围并再次进入,或者一个预定的会话超时后,此用户将需要重新进行一次身份的认证,此时密钥被改变,用户将使用新的密钥保持与无线网络的通讯。

对于每一个客户端,都将分配到两个密钥,其中一个是特殊的用于广播的密钥,这个密钥不会被改变,而是在 AP 端被预设后分配给客户端。改进的信息安全保护方案可以分两步来实现[2].

1)用户和无线接入点之间的认证过程。认证前 AP 组群和其移动台上都必须安装一特殊的 WLANA1 算法。当移动台或无线网卡(Supplicator)欲接入网络时,首先向接入点 AP 发出连接请求,AP 收到连接请求后产生一随机数 RAND,并把此随机数发送给提出请求的用户。同时,AP 和移动台分别把此随机数 RAND 和移动用户的注册的有关信息进行本地运算,进而产生认证密钥 Kc。然后,移动用户向 AP 发送自己计算出的 Kc,AP 则将用户送来的 Kc 与本地计算出的 Kc 进行比较,若二者一致,则相互认证成功,用户即可接入网络。如果两者计算出的 Kc 不相等,用户将被拒绝访问网络。对于每一次认证过程计算出的 Kc 均不相同。

2)传输数据的加密过程。传输数据过程中,AP 和其认证过的用户之间使用相同的但不断改变的 WEP 密钥来加密信息。一般地,WEP 密钥应每 5 s 更换一次。生成的密钥算法称 WLANA2 算法,生成的密钥具有实时动态性,其中包含 WEP 密钥的同步机制。系统中,我们采用了一种伪随机的密钥生成方法,即动态 WEP 密钥是大量的、预先配置的、存储在 RADIUS 认证服务器的数据库中。相比而言,这种方法虽然缺乏真正的动态随机性,但易于实现和控制,对于用户不太多的小型系统比较适合。

3　安全策略

安全策略[3]是一种处理安全问题的管理策略的描述,是一个组织关于安全事务的一个规划、实施的办

法。安全策略的设计与开发是提高网络安全状态的第一步。在系统中,我们把安全体系分为三个等级,每一级都提供了不同的安全层次和用户访问权限。

最低的安全等级称为"基本安全级",在这一层次上仅提供了网络的 ESSID 参数认证。在网络管理员许可的情况下,任何用户只要使用无线设备在周围扫描电磁波,即可获取附近 AP 设备的 ESSID,也可由用户手工输入网络的 ESSID 或自动选择信号最强的 AP 后,就可以访问网络了。

第二级的安全等级称为"中安全级",安全策略需要验证移动台的 ESSID 参数、对移动台的 MAC 地址进行过滤、对用户名和口令的验证、对传输的数据采用静态 WEP 进行加密。其中对用户名和口令的验证是作为可选项出现的,亦即当移动用户登录网络时,他的用户名和登录口令必须和已注册的相一致。作为安全策略的一部分,在移动用户和 AP 之间传递的数据报必须经过 64 bit 或 128 bit 静态 WEP 的加密。

第三级的安全等级称为"高安全级",在安全策略中除了采用不断变化的动态密钥来取代被所有用户共享的静态 WEP 密钥外,还利用 RADIUS 服务器对每一用户进行身份的认证。具体地讲,它首先要求移动台的 ESSID 要和网络(或 AP)的 ESSID 设为相同,然后把用户的 MAC 地址和存储在 AP 的 MAC 列表中的地址进行比对,通过后再强制对移动用户的身份进行认证,认证完成后利用 RADIUS 服务器产生的动态密钥对传输的数据加密。为了解密,双方要就加密使用的 WEP 密钥达成一致(同步),同时为了管理这些 WEP 密钥,需要复杂而有效的算法和数据库系统。

4 可扩展的安全管理平台 ESMP(Extensible Security Management Platform)

可扩展的无线安全管理平台 ESMP 不是采用现有的某一安全技术开发的,而是容纳了各种安全手段对无线传输的信息进行保护,并对现有的及今后出现的安全措施实行"即插即用"更重要的是该系统实现全面地多层次信息安全保护,对无线网卡、用户和 AP 设备进行全面地认证、监管和保护,可以随着无线安全技术的不断发展而提升自身的安全性能。

4.1 ESMP 的层次结构

整个 ESMP 系统从层次上可以分成 4 个层面:

第一层:无线设备管理层。对整个网络中的无线设备进行有效地管理和控制,包括设备的硬件扫描以监控设备的工作状态;设备的软件扫描和锁定,放置非法用户修改设备中的配置;设备的认证锁定,让设备在投入使用或者更换时进行系统认证。

第二层:用户漫游管理层。即对漫游用户或非漫游用户的管理,对用户进行统一管理,配置用户的权限、了解用户的状态,定义用户的安全策略,划分用户组群等。

第三层:系统监控层。对可能出现的安全问题进行全面的预警,从非法用户的入侵到对非法用户的跟踪,险境机制,日志管理维护等。

第四层:统一数据管理层。要实现一个成功的安全系统,必须能够对用户数据和安全的数据进行统一管理,通过统一的平台处理可以把可能存在的安全隐患在一个界面上显示出来,减少由于疏忽而造成的损伤,很多安全问题往往是起源于一个小小的管理漏洞。

4.2 ESMP 的子系统及其功能简介

整个 ESMP 系统从功能上可以分为以下几个子系统:

用户管理子系统(User Management Subsystem)。对整个系统中的用户进行集中管理,对用户应用安全策略、给用户分配有关权限等。让合法用户平滑进入网络,将非法用户拒之系统以外。

无线设备管理子系统(AP Management Subsystem)。实时监控网络中的无线设备,将设备的变化和数据库中的数据保持同步,从而达到配置和获取无线设备中的安全属性的功能,并添加系统中新的无线设备。

无线设备群组管理子系统(AP Group Management Subsystem)。以组群为单位管理系统中的设备,可简化系统中安全策略的应用。把不同局域网中的多个 AP 或单一局域网中的某些 AP 分成组群,并将其配置成具有相同安全级别的一个单元,管理员就可以以组群为单位方便地管理局域网中的所有 AP。

安全策略分析与管理子系统(Security Policy Analysis and Management Subsystem)。根据系统中搜集的当前信息来对整个系统环境进行分析,找出系统安全策略中的问题和提升安全的解决方案。对系统中的安全策略进行统一管理,系统中不仅包含预定义的安全策略,同时还允许网络管理人员自己定制安全策略。

日志管理和预警子系统(Log Management and Warning Subsystem)。将系统中发生的各类事件记录下来,供系统其它部分跟踪报警以及作为安全记录留档,并根据日志数据库,显示非法用户侵入系统的时间、地

点或入侵者的 MAC 地址等信息。

漫游管理子系统(Roaming Management Subsystem)。对漫游用户进行有效管理和组织,为系统能够控制漫游用户并及时更新漫游用户的信息提供手段。

5 无线漫游管理

无线电波在传播过程中会不断衰减,导致 AP 的通讯范围被限定在一定的范围之内。这个范围被称为"Cell"。当网络环境存在多个 AP,且它们的互相小区有一定范围的重叠时,无线用户可以在整个 WLAN 覆盖区内移动,无线网卡能够自动发现附近信号强度最大的 AP,并通过这个 AP 收发数据,保持不间断的网络连接,称为无线漫游。

在无线环境中,合法用户允许在不同 AP 之间漫游,一般可将这些 AP 的 ESSID 配置为相同。当无线用户发现原来所连接 AP 信号变弱时,它会扫描附近邻居 AP 的信号强度,一旦发现邻居 AP 的信号质量比目前所连 AP 的信号好时,它就会通过新的 AP 发出连接认证请求,网络通过 RADIUS 认证代理(Proxy)路由此用户的认证请求到归属服务器(Home Server),由归属服务器完成对用户的认证。若认证通过,则新的 AP 允许用户访问并接纳用户,则移动用户成功地从一个 AP 漫游到另一个 AP。有关移动用户的注册信息和安全信息必须有效地存储在归属服务器的用户数据中心(中央数据库)。

实际上,漫游管理模块的任务是管理和控制移动用户,这包括用户的身份信息、访问权限和用户的位置信息。因此,在系统中我们采用了智能数据库来完成这一任务,它嵌入在 RADIUS 服务器中。具体讲,认证中心 AuC(Authentication Center)负责对移动用户的身份作出鉴别,归属位置数据库 HLD(Home Location Database)负责记录移动用户的登录点 AP,访问位置数据库 VLD(Visitor Location Database)负责记录移动用户当前所连接的 AP, VLD 是用户临时存储信息的分布式数据库,安全策略数据库 SPD(Security Policy Database)决定了移动用户通过 AP 访问网络的方式和传输数据的加密形式。

6 结论

无线网络的安全和管理是一个不断改善的过程,最终的安全是要实现设备和平台的互动性,通过安全管理平台"消除设备的不一致性,填补设备的安全漏洞,保护信息的完整性"。需要从无线网卡的认证和识别、用户的身份认证和授权及无线接入点 AP 保护等方面提供全方位的信息安全保护,从身份认证、数据保密和系统监控等角度完成对无线网卡、移动用户和传输数据的全面控制、管理及监测和预警。ESMP 安全平台将各种安全手段或措施整合为系统的安全策略,可以根据管理员的实际应用需要选取不同的安全策略,更重要的是该系统可以随着无线安全技术的不断发展而提升自己的安全性能,达到保护无线局域网安全的目的。

参考文献:

[1] Nikita Borisov, Ian Goldberg, David Wagner. Security of the WEP algorithm [J/OL]. URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, 2001-02.

[2] Xavier Lagrange, Philippe Godlewski, Sami Tabbane. Reseaux GSM [M]. 北京:电子工业出版社, 2002.

[3] IETF's RFC 2196. Site Security Handbook [S]. URL: http://www.ietf.org/rfc/rfc2196.txt.

(编辑:姚树峰)

Information Security and Roaming of Mobile on Wireless LAN

SUN Shu-feng, HE Liang, SHI Xing-fang, GU Jun-zhong

(Computer Science Dep. East China Normal University, Shanghai 200062, China)

Abstract: This paper analyzes the security character and the defects about the common used 802.11 agreement, proposes a principle of improved dynamic WEP encryption. The extensible security management platform based on security policies of wireless LAN is presented and discussed. The roaming of mobile unit between APs is simply introduced in the end.

Key words: Security Policy; Dynamic WEP; ESMP