<<无线局域网安全分析与防护>>

图书基本信息

书名：<<无线局域网安全分析与防护>>

13位ISBN编号：9787811333879

10位ISBN编号：7811333872

出版时间：2009-1

出版时间：哈尔滨工程大学出版社

作者：李贤玉，吴小华 著

页数：195

前言

个人通信的目标，就是使人们能够在任何时候和其他任何人进行任意的通信联系，自由地享用网络提供的多种业务。

宽带无线IP技术将目前最热门的两大技术——IP技术和无线通信技术有机地融合起来，并顺应宽带化的发展趋势，为移动主机或移动终端提供方便、快捷、高速的Internet接入服务，以适应人们对高速网络和多媒体通信业务不断增长的需求。

无线局域网（wireleSs Local Area Network，WLAN）不仅支持移动计算，而且具有灵活性、快捷性及可扩展性等优点。

以无线局域网为基础，基于Internet的宽带无线接入网络结构如下图所示。

它主要由移动终端（Mobile Teminal，MT）、无线接入点（Access Point，AP）及无线接入服务器（Wireless Access Server，WAS）等设备组成，其中移动终端MT可在网中任意移动，无线接入点AP可实现包括越区切换在内的小区管理、对移动终端MT的管理及桥接功能，无线接入服务器WAS可实现无线接入终端的网间漫游管理。

从固定接入Internet到移动无线接入Internet，宽带无线IP技术为世界网络环境带来了全新的观念和巨大的冲击。

<<无线局域网安全分析与防护>>

内容概要

《无线局域网安全分析与防护》从无线局域网的组成和应用环境出发，结合Internet系统的体系结构，按照密码学的基本原则对无线局城网iEEE 802.11标准的安全机制，结合相应的安全技术原理的论述，进行了深度分析，指出了现有的无线局域网IEEE 802.11标准自身的安全防护机制和常用无线局域网的安全策略所存在的安全缺陷或漏洞，为便于说明问题，《无线局域网安全分析与防护》介绍了一些常见的、针对这些安全缺陷和漏洞的攻击方法和技术，旨在通过这些缺陷分析来说明无线局域网络目前存在的潜在安全隐患，并且提出较好的无线局域网络安全解决方案，以促进网络安全管理员给出更好的网络防护方案，加强无线局域网络的安全防护意识和能力。
近几年来，随着无线技术的迅猛发展，无线局域网（WLAN）得到了广泛的应用。
无线局域网由于其自由组网快捷、使用方便和成本低等优势而备受青睐。
但是其通信内容因具有公开性而极易被攻击者获得，因此无线局域网的安全问题变得十分突出。

<<无线局域网安全分析与防护>>

书籍目录

章节摘录

入侵检测可分为实时入侵检测和事后入侵检测两种。
实时入侵检测在网络连接过程中进行，系统根据用户的历史行为模型、存储在计算机中的专家知识以及神经网络模型对用户当前的操作进行判断，一旦发现入侵迹象立即断开入侵者与主机的连接，并收集证据和实施数据恢复。
这个检测过程是不断循环进行的。
而事后入侵检测由网络管理人员进行，他们具有网络安全的专业知识’根据计算机系统对用户操作所做的历史审计记录判断用户是否具有入侵行为，如果有就断开连接，并记录入侵证据和进行数据恢复。
事后入侵检测是管理员定期或不定期进行的，不具有实时性，因此防御入侵的能力不如实时入侵检测系统。
入侵检测的方法分为4类，其详细描述如下。
（1）基于用户行为概率统计模型的入侵检测方法。
这种入侵检测方法是基于对用户历史行为建模以及在早期的证据或模型的基础上，审计系统实时地检测用户对系统的使用情况，根据系统内部保存的用户行为概率统计模型进行检测’当发现有可疑的用户行为发生时，保持跟踪并监测、记录该用户的行为。
系统要根据每个用户以前的历史行为，生成每个用户的历史行为记录库，当用户改变他们的行为习惯时，这种异常就会被检测出来。
（2）基于神经网络的入侵检测方法。
这种方法是利用神经网络技术来进行人侵检测。
因此，这种方法对用户行为具有学习和自适应功能，能够根据实际检测到的信息有效地加以处理并做出入侵可能性的判断。
但该方法还不成熟，目前还没有出现较为完善的产品。
（3）基于专家系统的入侵检测技术。
该技术根据安全专家对可疑行为的分析经验来形成一套推理规则，然后在此基础上建立相应的专家系统，由此专家系统自动进行对所涉及的入侵行为的分析工作。
该系统应当能够随着经验的积累而利用其自学习能力进行规则的扩充和修正。

版权说明