

防范网络窃听的安全技术

访问控制

决定开放系统环境中允许使用那些资源,在什么地方适合阻止未授权访问的过程叫访问控制,其一般目标是对抗涉及计算机或通信系统非授权操作的威胁,对于网络窃听的防范来讲,涉及到的主要内容有非授权使用,泄露,修改,破坏等。进行访问控制(图 2)的目的是防止对信息系统的非授权访问和非授权使用系统资源。访问控制机制一般由一个访问控制方案,如访问控制列表方案和为该方案向 ADF(访问控制判决功能)提供 ADI(访问控制判决信息)的支持机制组成。涉及到访问控制的基本实体是发起者和目标,实现功能指访问控制执行功能(AEF)、访问判决功能(ADF)

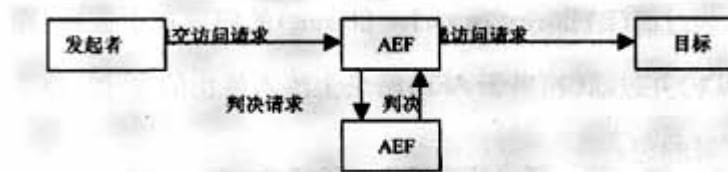


图 2 访问控制策略图

其中,发起者代表访问或试图访问目标的人和基于计算机的实体。在系统中,基于计算机的实体代表发起者。目标代表被试图访问或由发起者访问的,基于计算机或通信的实体。例如,目标可能是 OSI 实体、文件或系统。访问请求代表构成试图访问部分的操作和操作数。正如 ADF 所决定的那样,AEF 确保只有对目标允许的访问才由发起者执行。当发起者请求对目标进行特殊访问时,AEF 就通知 ADF,需要一个判决来作出决定。

为了作出判决决定,给 ADF 提供了访问请求(图 3)(作为访问请求的一部分)和以下几种信息:发起者 ADI,目标 ADI,访问请求 ADI。

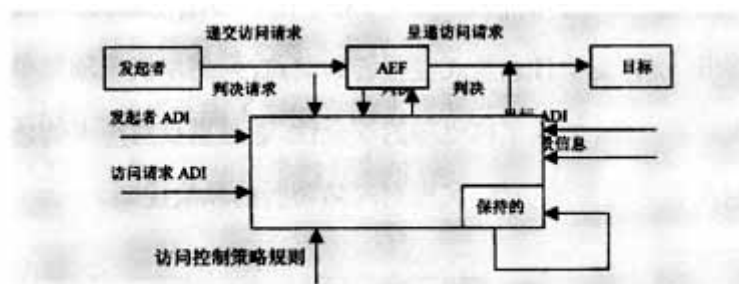


图 3 ADF 示意图

ADF 的其他输入信息是访问控制规则和用于解释 ADI 或策略的必要上下文信息,上下文信息包括发起者的位置、访问时间或使用中的特殊通信路径。基于这些输入,及以前判决中保留下来的 ADI 信息,ADF 可以作出允许或者禁止发起者试图对目标进行访问的判决,并传递给 AEF,然后 AEF 允许将访问请求传递给目标或采取其他合适的行动。

防止对声卡、麦克风的非授权使用

防范网络窃听,防止对电脑的声卡和麦克风的非授公使用,其主要方法是加

入控制软件对电脑声卡的工作状态进行动态监测，其控制软件由如下模块组成：身份识辨模块，启动和关闭麦克风模块，报警启动和安全日志模块。

通信端口的访问控制

实施网络窃听对外进行通连时，必然要使用一个工作端口，因而对可以工作端口进行控制。工作端口控制部分应该由以下几个模块构成：网络合法端口判决模块。网络端口锁定或解锁模块，启动报警和安全日志模块。

通过包过滤来访问控制

包过滤(IPFiltering or packet filtering)的原理在于监视(相当于 ADF)并过滤(相当于 AEF)网络上流入流出的 IP 包，拒绝发送可疑的包。

与加密性服务的交互

加密性服务的目的是确保信息只是对授权者使用。就防范网络窃听方面来讲，主要隐藏本机的信息不被外部可能存在的威胁准确地定位，通过加密等技术手段来完成。

建立工作日志

通过对网络窃听防范的安全模型的分析，不同的事件有不同的风险度，根据其不同风险度，在工作日志的实现过程中进行分类成不同的安全等级保存起来。

防范网络窃听及实现原理

防范网络窃听的模型(图 4)，对于用户终端电脑，为解决安全性低，没有安全日志及入侵报警的弱点，采用单机电脑加单机防火墙的方法，加强单机电脑的安全性，通过重点对声卡的访问控制及实时报警的功能，实现对网络窃听的风险控制。



图 4 网络窃听防范模型

用动态安全发现和静态安全风险相结合的方法来实现，静态分析主要是对系统漏洞进行检测和评估，即先于入侵者发现漏洞并进行弥补，从而进行安全防护，由于网络环境比较复杂，一般利用工具针对网络层、操作系统层等进行漏洞检查，由于网络是动态变化的，故漏洞检测与评估定期进行。网络漏洞检测通过模拟攻击者的角度，攻击方法结合漏洞知识进行扫描和检测。由于静态的防护机制仍可能被渗透和突破，所以在网络中选取节点进行实时入侵检测的测试，进行主动的防护机制，在静态防护机制失效前检测到攻击活动、恶意行为或误操作，并及时做出响应。通过静态和动态检测的配合，就能够实现防范网络窃听和网络的安全的风险的有效的控制。

结束语

随着网络技术及国内网络的基础设施的发展,网络多媒体的飞速发展和迅速普及,如网络电话、语音邮件、网络会议的逐步应用,特别是微软公司开发出的下一代办公软件 Office P,已经将语音输入功能嵌入到软件里,随着 Office XP 的推出和普及,更多的电脑将会装上麦克风。另外,笔记本电脑所占的市场份额正在逐渐扩大,使用网络窃听实现的使用范围大大增加。不久的将来,网络窃听的使用将会更加常见,因此,对防范网络窃听技术的研究具有重要的信息安全意义。