网络安全协议与信任体系构造

国家信息化教授征询委员会委员

沈昌祥　院士

目前互联网不可信任的主要原因：

- 协议安全性差，源接入地址不真实，源数据难标识和验证。
- 没有完整的信任体系构造，难以实现可信接入和端点安全保护；顾客、控制、管理三大信息流难以实现安全可信。

一、IPv6 的安全挑战

- 下一代互联网是基于IPv6的网络
- IPv6相对于IPv4的主要优势是：扩大了地址空间、提升了网络的整体吞吐量、服务质量得到很大改善、安全性有了更加好的确保、支持即插即用和移动性、更加好地实现了多播功能。
- 巨大的地址空间使全部终端都使用真实地址。是信任接入的基础。
- 真实IP地址访问和全局顾客标识是建设可信任互联网的根本。

- IPv6的安全特征是其主要特点之一。IPv6协议内置安全机制，并已经原则化。

- IPSec提供如下安全性服务：访问控制、无连接的完整性、数据源身份认证、防御包重传攻击、保密、有限的业务流保密性。

- IPv6并不能彻底处理互联网中的安全问题，更大规模接入和应用，更快的速度会增长安全风险
- 对存在的安全风险必须做仔细地研究。

引入扩展头可能存在安全性问题

- 一般情况下扩展头只有在包的终点才干作相应处理，但在有些处理中获取源路由就能形成 IP 欺骗攻击。

ICMPv6存在重定向和拒绝服务攻击的可能

- 伪装最终一跳路由，给访问者发重定向包；
- 用不同的源或目的MAC地址发邻居祈求包实现欺骗；
- 反复地址检测和邻居发觉Dos攻击

移动IPv6可能存在的安全问题

- 节点移动需要经常向MN的本地代理和CN发送绑定更新报文可能被重定向。

- 高层应用和操作系统的漏洞隐患，影响网络安全连接。

二、骨干网络可信任的体系构造