调研·计划·开发

* 调研
* 哪些信息需要加密？

传输通道（账号，视频）

《计算机网络攻击与防范策略》——王芳芳

* 如何加密？

严密性，加密的信息只有信息源端和目的端能够解码，读取信息内容。

完整性，信息开始传输时，将其封装，加密，整个过程没有拆卸信息，保证了传输信息前后的完整性。

身份验证，信息传输前，对信息的数据来源进行认证，确保计算机的真实身份和信息的来源的安全健康。

反重发性，每个数据包唯一，以此保证攻击者捕获的数据包不能重发或重用。

* 常见攻击手段？

安全漏洞攻击、木马攻击、网络欺骗、网络监听

* 如何防攻击、防病毒？

防火墙技术、病毒防护、网络入侵检测

参考《探讨网络安全传输通道技术》——宁福旺

TCP/IP由四个层次组成：网络接口层、网络层、传输层、应用层。

网络接口层

通用的安全协议有两个：PPTP 和L2TP。它们主要在远处访问VPN 上起作用。

1. PPTP 的封装

将用户数据，TCP 或UDP，IP 进行绑定，封装，然后传输给PPP。



2. L2TP 封装

L2Tp封装分两个阶段：初始L2TP封装阶段和IPSec封装阶段。

阶段 1 ：初始 L2TP 封装

阶段 2 ： IPSec 封装



网络层

在网络层实现安全传输通道的技术主要体现在IPSec规范上，它是将安全机制引入TCP/IP网络的一系列标准，主要包括安全协议、安全联盟、密钥管理和安全算法等。IPSec是主机之间、安全网关之间以及主机与安全网关之间数据安全的保证。它支持多种方式的 VPN 访问，包括 ExtraNet VPN访问，IntraNet VPN 访问 和 VPN 远程访问。网络层的安全协议增加了主机或进程的数据通道的安全性。

|  |  |
| --- | --- |
| IPSec 规范 | |
| 安全协议 | 1.保护一个完整的 IP 载荷  2.保护某个 IP 载荷的上层协议 |
| 安全联盟 | 1.联系安全服务/密钥与要保护的通信数据  2. 联系远程通信实体与要交换密钥的 IPSec 数据传输 |
| Internet 密钥交换 | 在 IPSec 的通信双方之间建立起共享的安全参数和验证过的密钥 |

传输层

在传输层能够实现安全传输通道的协议是安全套接层协议（ SSL ），它需要以可靠的传输服务为基础。它主要由SSL 记录协议和SSL 支持协议两部分组成。

|  |  |
| --- | --- |
| SSL 协议 | |
| SSL 记录协议 | 主要处理应用程序提供的信息的分段、信息压缩、信息的数据认证和加密 |
| SSL 支持协议 | 用来对数据进行认证和加密的密钥可以通过 SSL 的握手协议来协商 |

应用层

安全数据通道主要在主机之间或进程之间，但对于传输文件的安全性不同需求无法满足。如果需要区分具体文件的不同的安全性要求，那就需要依附于于应用层的安全性。应用层的安全服务，最突出特点就是能安全的灵活处理单个文件，继而保证文件传输的安全性和完整性。