TCP_IP学习笔记:TCP_IP的安全性 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022_TCP_IP_E5_AD_A6_E4_c101_142298.htm TCP/IP的层次不同提供的安全性也不同，例如，在网络层提供虚拟私用网络，在传输层提供安全套接服务。下面将分别介绍TCP/IP不同层次的安全性和提高各层安全性的方法。 一、Internet层的安全性 对Internet层的安全协议进行标准化的想法早就有了。在过去十年里，已经提出 了一些方案。例如，“ 安全协议3号(SP3) ”就是美国国家安全局以及标准技术协 会作为“ 安全数据网络系统(SDNS) ”的一部分而制定的。“ 网络层安全协议(NLS P) ”是由国际标准化组织为“ 无连接网络协议(CLNP) ”制定的安全协议标准。“ 集成化NLSP(I-NLSP) ”是美国国家科技研究所提出的包括IP和CLNP在内的统一 安全机制。SwIPe是另一个Intenet层的安全协议，由Ioannidis和Blaze提出并实 现原型。所有这些提案的共同点多于不同点。事实上，他们用的都是IP封装技术。 其本质是，纯文本的包被加密，封装在外层的IP报头里，用来对加密的包进行In ternet上的路由选择。到达另一端时，外层的IP报头被拆开，报文被解密，然后 送到收报地点。 Internet工程特遣组(IETF)已经特许Internet协议安全协议(IPSEC)工作组对IP安 全协议(IPSP)和对应的Internet密钥管理协议(IKMP)进行标准化工作。IPSP的主 要目的是使需要安全措施的用户能够使用相应的加密安全体制。该体制不仅能在 目前通行的IP(IPv4)下工作，也能在IP的新版本(IPng或IPv6)下工作。该体制应 该是与算法无关的，即使加密算法替换了，也不对其他部分的实现产生影响。此外，该体制必

须能实行多种安全政策，但要避免给不使用该体制的人造成不利影 响。按照这些要求，IPSEC工作组制订了一个规范：认证头(Authentication Hea der，AH)和封装安全有效负荷(Encapsulating Security Payload，ESP)。简言之， AH提供IP包的真实性和完整性，ESP提供机要内容。 IP AH指一段消息认证代码(Message Authentication Code，MAC)，在发送IP包之前，它已经被事先计算好。发送方用一个加密密钥算出AH，接收方用同一或另一 密钥对之进行验证。如果收发双方使用的是单钥体制，那它们就使用同一密钥；如果收发双方使用的是公钥体制，那它们就使用不同的密钥。在后一种情形，AH 体制能额外地提供不可否认的服务。事实上，有些在传输中可变的域，如IPv4中 的time-to-live域或IPv6中的hop limit域，都是在AH的计算中必须忽略不计的。 RFC 1828首次规定了加封状态下AH的计算和验证中要采用带密钥的MD5算法。而与 此同时，MD5和加封状态都被批评为加密强度太弱，并有替换的方案提出。 IP ESP的基本想法是整个IP包进行封装，或者只对ESP内上层协议的数据(运输状 态)进行封装，并对ESP的绝大部分数据进行加密。在管道状态下，为当前已加密 的ESP附加了一个新的IP头(纯文本)，它可以用来对IP包在Internet上作路由选择。 接收方把这个IP头取掉，再对ESP进行解密，处理并取掉ESP头，再对原来的IP包 或更高层协议的数据就象普通的IP包那样进行处理。RFC 1827中对ESP的格式作了 规定，RFC 1829中规定了在密码块链接(CBC)状态下ESP加密和解密要使用数据加 密标准(DES)。虽然其他算法和状态也是可以使用的，但一些国家对此类产品的进 出口控制也是不能不考虑的因素。有些国家甚至连私用加密都要限

制。 AH与ESP体制可以合用，也可以分用。不管怎么用，都逃不脱传输分析的攻击。人 们不太清楚在Internet层上，是否真有经济有效的对抗传输分析的手段，但是在 Internet用户里，真正把传输分析当回事儿的也是寥寥无几。 1995年8月，Internet工程领导小组(IESG)批准了有关IPSP的RFC作为Internet标 准系列的推荐标准。除RFC 1828和RFC 1829外，还有两个实验性的RFC文件，规定 了在AH和ESP体制中，用安全散列算法(SHA)来代替MD5(RFC 1852)和用三元DES代替DES(RFC 1851)。 在最简单的情况下，IPSP用手工来配置密钥。然而，当IPSP大规模发展的时候，就需要在Internet上建立标准化的密钥管理协议。这个密钥管理协议按照IPSP安全条例的要求，指定管理密钥的方法。 因此，IPSEC工作组也负责进行Internet密钥管理协议(IKMP)，其他若干协议的标准化工作也已经提上日程。其中最重要的有： IBM 提出的 “ 标准密钥管理协议(MKMP) ” SUN 提出的 “ Internet协议的简单密钥管理(SKIP) ” Phil Karn 提出的 “ Photuris密钥管理协议 ” Hugo Krawczik 提出的 “ 安全密钥交换机制(SKEME) ” NSA 提出的 “ Internet安全条例及密钥管理协议 ” Hilarie Orman 提出的 “ OAKLEY密钥决定协议 ” 在这里需要再次强调指出，这些协议草案的相似点多于不同点。除MKMP外，它们都要求一个既存的、完全可操作的公钥基础设施(PKI)。MKMP没有这个要求，因为它假定双方已经共同知道一个主密钥(Master Key)，可能是事先手工发布的。SK IP要求Diffie-Hellman证书，其他协议则要求RSA证书。 1996年9月，IPSEC决定采用OAKLEY作为ISAKMP框架下强制推行的密钥管理手段， 采用SKIP作为IPv4和IPv6实现时的优先选择。目前已经有一些厂

商实现了合成的 ISAKMP/OAKLEY方案。 Photuris以及类Photuris的协议的基本想法是对每一个会 话密钥都采用Diffie-Hellman密钥交换机制，并随后采用签名交换来确认Diffie --Hellman参数，确保没有“ 中间人 ”进行攻击。这种组合最初是由Diffie、Oos chot和Wiener在一个“ 站对站(STS) ”的协议中提出的。Photuris里面又添加了一 种所谓的“ cookie ”交换，它可以提供“ 清障(anti-logging) ”功能，即防范对 服务攻击的否认。 Photuris以及类Photuris的协议由于对每一个会话密钥都采用Diffie-Hellman密 钥交换机制，故可提供回传保护(back-traffic protection，BTP)和完整转发安 全性(perfect-forward secrecy，PFS)。实质上，这意味着一旦某个攻击者破解 了长效私钥，比如Photuris中的RSA密钥或SKIP中的Diffie-Hellman密钥，所有其 他攻击者就可以冒充被破解的密码的拥有者。但是，攻击者却不一定有本事破解 该拥有者过去或未来收发的信息。 值得注意的是，SKIP并不提供BTP和PFS。尽管它采用Diffie-Hellman密钥交换机 制，但交换的进行是隐含的，也就是说，两个实体以证书形式彼此知道对方长效 Diffie--Hellman 公钥，从而隐含地共享一个主密钥。该主密钥可以导出对分组 密钥进行加密的密钥，而分组密钥才真正用来对IP包加密。一旦长效Diffie-Hel lman密钥泄露，，则任何在该密钥保护下的密钥所保护的相应通信都将被破解。 而且SKIP是无状态的，它不以安全条例为基础。每个IP包可能是个别地进行加密 和解密的，归根到底用的是不同的密钥。 SKIP不提供BTP和PFS这件事曾经引起IPSEC工作组内部的批评，该协议也曾进行过 扩充，试图提供BTP和PFS。但是，扩充后的SKIP协议版本其实是在BTP和PFS功能 的提供该

协议的无状态性之间的某种折衷。实际上，增加了BTP和PFS功能的SKIP 非常类似于Photuris以及类Photuris的协议，唯一的主要区别是SKIP(仍然)需要 原来的Diffie-Hellman证书。这一点必须注意:目前在Internet上，RSA证书比其 他证书更容易实现和开展业务。 