[文章编号] 1007- 7405(2001)03- 00238- 09

·综 述·

IPv6 互联网信息安全的有关问题研究

刘年生[1], 郭东辉[2], 刘瑞堂[2], 吴伯僖[2]

(1. 集美大学生物工程学院, 福建 厦门, 361021; 2. 厦门大学技术物理研究所, 福建 厦门, 361005)

[摘要] 简要介绍了基于 IPv6 互联网的安全机制, 并对 IPv6 所支持的主要密码算法的安全性进行了讨论和分析; 着重论述了 IPv6 的密钥管理; 并针对我国的 IPv6 互联网信息安全的建设提出了一些建议.

[关键词] IPv6; 信息安全; 加密算法

[中图分类号] TP 393.8 [文献标识码] A

0 引言

网络和信息深刻地影响人们的生活、工作等各个方面, 因而信息安全将影响到社会所有的成员, 尤其在个人隐私、军事情报和国家机密等方面显得更为突出和重要. 而现实中又存在着各种各样的网络安全威胁, 包括伪装 (欺骗)、窃听、非法接入、篡改、抵赖、伪造、拒绝服务、设置后门和传播病毒等等, 它们直接针对信息系统的信息保密性、完整性、可控性和可用性; IPv6 (Internet Protocol Version 6, 即下一代互联网 IPng) 协议将取代现行的互联网通讯协议 (即 IPv4 协议) 而成为 21 世纪主要的计算机网络第 3 层协议[1], 它同样是基于 OSI (Open System Interconnect) 模型的, 这样在开放的系统互联环境下实现信息保密就更加困难; 所以国内外都十分关注 IPv6 互联网信息系统的安全性[2~5].

1 IPv6 的安全机制

随着互联网规模和应用范围的不断扩大, 原 IPv4 中缺乏网络安全性的问题日渐显露出来, 于是 IETF (Internet Engineering Task Force) 根据市场和商业对网络层安全性的需求起草制定了一些 IP 安全标准, 特别是针对 IPv6, 逐步建立起网络层安全机制, 包括安全结构、安全协议和实现方式.

1.1 IPv6 的安全结构

[收稿日期] 2000- 11- 08

[基金项目] 国家自然科学基金项目 (69886002); 福建省自然科学基金项目 (A0010019).

[作者简介] 刘年生 (1967-), 男, 讲师, 现为厦门大学技术物理研究所在职博士生, 从事人工智能、网络通讯等方面研究.

IPv6 的安全体系是吸收了 IPv4 的安全经验和教训，根据网络发展的实际需要而逐步改进发展起来的，在网络层上增强了安全性操作，在 RFC2401、2402 和 2403[6~8] 中定义了 IPv6 的安全体系结构，它是由安全变量、机制、控制和管理等构成的，其概念如图 1 所示，它在网络层中增设了安全协议机制，采用原 OSI 分层封装协议机制，与传输层和数据链路层（即网卡接口层）相连，并通过新增安全变量与网络系统管理进行通讯，因此从网络管理的角度来看，如果在管理信息结构（SMI）、管理信息库（MIB）和管理协议（MP）等方面都引进和增加了安全管理的标准化模块，而且每个节点都支持这一安全管理体系结构，则可实现节点之间网络层安全的可互操作性.

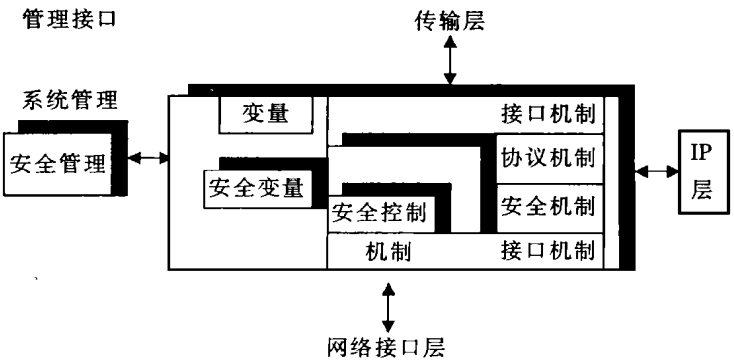

图 1　IPsec 体系的概念模型

IP 的安全体系主要用于 IP 数据报的认证和加密，其目的是为了保证 IP 层数据信息的完整性、机密性、可控性和可用性. 它的安全机制是按模块化设计进行的，如图 2 所示；从图 2 中可看到安全协议 ESP（Encapsulating Security Payload）和 AH（Authentication Header）与密码算法相分离，是按照安全关联的理论进行设计的；这样，IPv6 的安全性并不依赖于某一特定的认证算法或加密算法，便于将来可用一种功能更强的安全算法替代旧的算法，便于安全算法的扩展. 但是这种 IP 安全机制也存在一些安全方面的局限性，如缺乏对业务特性的分析服务和无法支持拒绝服务等.

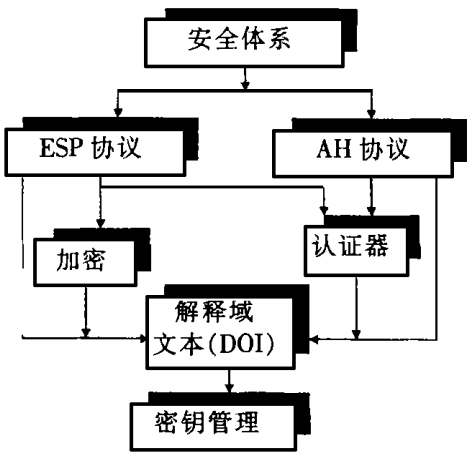

图 2　IPsec 的模块化结构

1.2　IPv6 的安全协议

在图 2 中，IPv6 的加密与认证主要依赖于 ESP 协议和 AH 协议；其中 ESP 协议主要提供 IP 数据报的完整性检验和保密性服务；而 AH 协议主要提供 IP 数据报的完整性检验和认证服务. 这两个协议既可以分别单独使用，也可以共同使用；如果共同使用，则可以向那些需要特别的信息认证、完整性检验和加密服务的用户提供增强性安全服务. 用户可以使用 IPv6 报头格式（如图 3 所示）中的两个扩展安全报头：AH 报头和 ESP 报头；AH 和 ESP 报头格式分别如图 4 和图 5 所示，它们在 IPv6 Next Header 域中的取值分别为 51 和 50. AH 协议还可以根据其所采用适当的加密算法和密钥管理，来提供发送端确认服务，例如：采用公称数字签名算法（如 RSA 法）就可

Version(4)	Traffic class(8)	Flow Label(20)
Payload Length(16)	Next Header(18)	Hop Limit(8)
Source Address(128)		
Destination Address(128)		

图 3　IPv6 的报头格式

以提供发送端确认服务. AH 报头一般位于 IPv6 的扩展报头 Hop-by-Hop header 之后, 而在 Destination header 之前. ESP 报头则可位于 IP 报头之后、上层传输层报头之前的任一位置, 因此, 用户可根据自己的需要利用 ESP 对整个 IP 数据进行加密, 或仅对传输层数据如 TCP 和 UDP 数据包进行加密; 对于前者来说可采用隧道模式, 而对于后者则应为传输模式. ESP 也能根据所使用的加密算法提供数据来源认证和无连接的完整性验证; 它还提供反应答服务、序列完整性检验服务和有限业务流服务. 当 ESP 和 IP 协议共同使用时, 一般 AH 报头放在 ESP 报头之前, 这样对用户而言可能更为有利, 多数用户期望能对数据报提供较强的完整性验证、认证服务、保密服务和数据来源认证服务, AH 报头的位置能清楚地标明哪些数据信息是经过认证的, 在进行 ESP 解密之前就可检测和拒绝应答已被篡改过的或坏的信息包.

Next Header (8)	Length (8)	Reserved (16)
Security Parameters Index (32)		
Authentication Data (varable number of 32-bit words)		

图 4 AH 的报头格式

Security Parameters Index (32)		
Initialization Vector (32)		
Payload Data		
…Padding	Pad Length (8)	Payload Type (14)

图 5 ESP 的报头格式 (采用 DES-CBC 算法时)

1.3 IPsec 的实现方法

IPsec 既可以直接在主机上实现端对端的保密通信, 也可以在网关上如防火墙、路由器中实现信息的链路加密传输或信息的节点加密传输[2,9]. 当然, 端对端的保密通信更符合用户的安全要求, 它可保证单个用户之间或单个用户对多个用户之间的通讯安全; 而在防火墙和路由器中实现 IPsec, 则可构筑起专用虚拟网络, 保证路由安全, 对防火墙内侧的数据信息则没有加密保护.

2 IPv6 密码算法的安全性分析

1949 年 Shannon 所发表的《Communication Theory of Secrecy System》一文为私钥密码系统建立了理论基础, 使得密码学从一门技巧变成一门科学; 到了 1976 年, Diffiee 和 Hellman 的《New Directions in Cryptography》开创了公钥密码学的新纪元, 出现了许多新的加密算法. 在 IPv6 这种开放系统互联的环境下, IPsec 机制将 AH 和 ESP 协议与其所用的加密 (或认证) 算法相隔离, 即所用的加密 (或认证) 算法具有独立性. 尽管 IPsec 安全机制将 AH 和 ESP 协议与其所用的加密, 认证算法相融离, 但实际 IPsec 的软硬件实现必然要用到一些具体的密码算法; IPsec 安全机制与密码算法两者之间是密不可分的, 这是因为: 一方面采用不同的密码算法, AH 和 ESP 协议某些功能如发送端确认服务就可能没有; 另一方面密码算法的安全性直接关系到 IP 信息包的保密强度; 所以对 IPv6 的安全性来说, 所采用的密码算法就显得非常重要, 特别是密码算法的安全性方面. 下面就对 IPv6 所支持的主要几种密码算法的安全性进行具体的探讨与分析.

2.1 认证算法

在 AH 协议中规定必须支持 HMAC (″message authentication codes″ mechanism based on cryptographic hash functions.) 与 MD5 (或 SHA-1) 结合的算法[7], 在 ESP 协议中规定必须支持

DES-CBC 算法[8]，以及 HMAC 与 MD5（或 SHA-1）结合的算法[10]；因此首先分析一下 MD5 和 SHA-1 等认证算法的安全性，然后再分析包含 DES-CBC 在内的加密算法的安全性.

2.1.1　MD5 算法

MD5 算法[11]是由麻省理工学院教授 Rivest 设计的，从原 MD4 Hash 函数算法改进而成的. 该算法是通过对明文进行填充和分块（512 bit）、然后对第一块明文用预定义的逻辑函数、常数和初始寄存数进行四轮、每轮 16 回的杂凑运算，每轮输出 128bit 作为下一轮的寄存数；对其它明文块则引用上一轮的寄存数依次进行类似的运算处理. 最后产生 128bit 的指纹或信息摘要，用于信息认证. 这种 Hash 函数的设计不基于任何数学难解问题和密码体制，只依赖于求两个具有相同 Hash 值的消息在计算上不可行性. 对穷举攻击法、生日攻击法和中间攻击法等具有较强的抗破译能力，具有较高的实际安全性. 如采用穷举攻击法寻找一个具有给定 Hash 值的计算困难性为 2^{128}，用处理能力为 10^9 个消息/秒的计算机需时 1.07×10^{22} 年，如用生日攻击法，利用相同的处理能力计算机则需时 585 年. 也正是由于它不基于任何数学难解问题和密码体制，没有严格地理论推导与证明，而且 MD5 的压缩函数 G 存在一个碰撞，违背其基本设计准则之一即设计一个无碰撞的压缩函数；因而其安全性要想得到人们的信任只能随时间来考验和证明. 目前还没有有效的破译方案，只是对单轮的 MD5 有攻击结果.

2.1.2　SHA 算法

SHA 算法[12]也是根据 MD4 Hash 函数法改进而来的，对明文的处理过程和 MD5 相似，主要不同如下：1）SHA 输出的摘要长度为 160 比特，而非 128 比特. 2）SHA 的运算步骤数为 80，而非 64. 尽管 SHA 和 MD5 均为四回合运算，但在 SHA 中每回合包含有 20 个步骤的运算，每 512 比特明文块先分成 16 份 32 比特的子明文块，M_i $(i = 0, 1, \cdots, 15)$，再转换成 80 份，每份含有 32 比特的 W_i $(i = 0, 1, \cdots, 79)$，其中 $W_i = M_i$ $(i = 0, 1, \cdots, 15)$，$W_i = W_{i-3} \oplus W_{i-8} \oplus W_{i-14} \oplus W_{i-16}$ $(i = 16, 17, \cdots, 79)$. 3）SHA 的常数数目为 4 个，而非 64；逻辑函数定义也不一样. SHA 算法与 MD5 算法相比，它的杂凑值为160 bit，要寻找一个具有给定 Hash 值的计算困难性为 2^{160}，约为MD5 算法的 4.29×10^9 倍，对抗穷举攻击法和生日攻击法的能力就更强，安全性更高.

2.2　加密算法

密码体制一般分为分组（单钥）密码和公钥（双钥）密码两类，其中，分组密码体制以 DES（Data Encryption Standard）算法[13]为主要代表，而公钥密码体制则以 RSA（Rivest Shamir Adleman）、ECPKC（Elliptic Curve Cryptosystem）和 FAPKC（Finite Automata Pubic Key Cryptosystem）等算法为主要代表；这些算法安全分析如下.

2.2.1　DES 算法

DES 算法于 1977 年被美国确定为联邦数据加密标准算法，到 1998 年 12 月不再重新批准为联邦标准算法. 它的密钥长度为64 bit，其中8 bit为奇偶校验位，有效密钥长度为56 bit；利用这56 bit的密钥对每输入64 bit的明文进行置换、模 2 加和迭代等运算，产生 64bit 的密文. 这种算法的系统安全性全依赖于密钥的保密，它存在如下几方面的安全问题：1）DES 算法具有互补性，即：若文明组 x 和密钥 k 分别逐位取补得 bx 和 bk，且 $y = DES_k(x)$，则 $by = DES_{bk}(bx)$，其中 by 是 y 的逐位取补；这种互补性使得在选择性明文攻击时可以减少

其可能的密钥数一半，为 2^{55}个. 2) 存在弱密钥和半弱密钥；在 DES 算法中至少存在 4 个弱密钥和至少 12 个半弱密钥，如果使用弱密钥或半弱密钥，则在多重加密时第二次加密会还原第一次加密；3) 由于S 盒是 DES 算法实现非线性变换的关键，而它的设计准则至今还没有完全公开，所以有许多密码学家怀疑它存在“陷门”，一旦知道这些“陷门”，就可以破解 DES 算法；4) DES 算法的密钥长度太短，只有56 bit，密钥量约为 1.7×10^{17}个，对抗穷举攻击法、差分攻击法和线性攻击法等的能力较差，如：在 1998 年破译56 bitDES 只用 56 小时.

2.2.2 RSA 算法

RSA 算法[14]是由美国麻省理工学院三位教授 Rivest、Shamir 和 Adleman 于 1978 年首先提出的，它是一种基于分解因数的指数函数为单向暗门函数的公钥密码体制，它既可用作加密算法，又用作数字签名认证. 其算法如下：1) 公开密钥：n 和e，其中 $n=pq$ (p 和q 分别为两个大质数，都必须保密)，$\varphi(n)=(p-1)(q-1)$ ($\varphi(n)$ 必须保密)，任选一整数 e，$1 \leqslant e \leqslant \varphi(n)$ 且 e 和 $\varphi(n)$ 互质. 2) 私有密钥：d，d 为任选一整数 (d 必须保密)，且满足 $d=1 \pmod{\varphi(n)}$，即为 e 的逆元. 3) 对任意长度明文先进行数字化，并取长度 m 小于 $\log_2 n$ 比特的数字作为明文块，进行加密运算和解密运算. 4) 加密算法：$C=E(m)=m^e \pmod{n}$. 5) 解密算法：$D(c)=C^d \pmod{n}$.

从其算法可以看出，RSA 的安全性严重依赖于对 n 的因数分解，要使得 RSA 密码系统安全，必须注意如下三点：1) 必须十分注意其参数的选择；首先是 n，$n=pq$，p 和q 在选择时均必须是强质数，且相差较大，同时 $(p-1)$ 与$(q-1)$ 的最大公因数应较小；如若不然，p 和q 是常规素数表中的质数，或p 和q 相差不大，则易于用穷举攻击法分解出 n，得到p 和q 的值，而目前分解 2048 比特的大质数已超过了 64 位的计算机的运算能力，是足够安全的. 其次是 e 和d，e 不可以太小，太小虽然能缩短加密运算时间，但易遭低指数攻击法等密码分析方法的破译，因此 e 不可太小，应为16 bit以上的质数，且应为模 $\varphi(n)$ 的最大序；同样 d 不能太小，太小容易被猜出，降低了系统的安全性，因此 d 不能太小，1990 年 Wiener[15]又进一步证明了若 d 的长度小于 n 的四分之一时，则利用连分数演算法求出正确的 d；这样要求 d 的长度就比较长，从而增加了解密的运算时间和私钥保存的难度. 2) 针对RSA 密码系统除了因参数选择不当而易被破译外，还会因明文长度不够，小于 n，则采用 RSA 加密存在不动点，致使不动点处明文消息暴露. 因此要注意明文的长度，对不动点处的消息加以隐匿；3) 在 RSA 实际使用中还存在共模攻击问题，即每个人所采用的 n 相同，但 e 和 d 不相同，则密码分析者只要知道其中两个 e 和其相应的密文(由同一明文加密而成)，就可以采用扩展的欧几里德算法，恢复出其明文；因此在 RSA 体制中应尽量避免 n 相同.

2.2.3 椭圆曲线公钥密码算法

1985 年，Koblitz 和 Miller 分别将椭圆曲线用于公钥密码体制的设计. 利用椭圆曲线上的离散对数的计算比有限域上的离散对数的计算更困难，设计出密钥较短的公钥密码体制[16]；目前已成为国际上非常关注的一种密码算法. 其算法过程为：首先找到一条椭圆曲线 E (即由 Weierstrass 方程所确定的平面曲线)，将明文通过编码嵌入到 E 的点，然后在 E 上进行加密. 若嵌入变换以解决，则在椭圆曲线上加密，实际上它是将熟知的公钥加密运算移植到椭圆曲线上，主要有 Diffie-Hellman 密码系统、Masey-Omura 密码系统和 ELGamal 密码系统. 对这种椭圆曲线离散对数密码体制的安全性已进行了十多年的研究，尚未发现明显的弱点，但

对 ELGamal 密码系统应避免选用超奇异曲线，否则椭圆曲线群上的离散对数问题退化为有限域低次扩域上的离散对数问题，从而能在多项式时间上可解. 除超奇异曲线外，还有一类“反常曲线”，即椭圆曲线 E 在有限域 $GF(q)$ 上的点数正好等于 q，对于这类曲线，则易被由 Semave、Smart 等人所分析得出的攻击法所攻击[14]；因此，在所有椭圆曲线密码体制的标准中应禁止使用超奇异曲线和反常曲线.

2.2.4　有限自动机公开钥密码体制

我国学者陶仁骥、陈世华等人于 1985 年提出了一种有限自动机公开钥密码体制[17]，这种公开钥密码体制的保密性，建立在求非线性有限自动机的弱逆的困难性和矩阵多项式因式分解的困难性之上. 对这种时序密码体制的安全性，近几年来在国内有不少的研究，一方面已有学者对 FARKC-1、2 和 3 所用的特殊非线性有限自动机，其求逆是否困难和是否存在等效逆提出疑问，其中戴宗铎[18]利用半环研究一类可分非线性的有限自动机，确定并构造出全部具有输入线性存储可分弱逆的存储有限自动机及其弱逆，从而表明这类 FSPKC 体制不够安全，并提出了一种称之为“非线性核攻击”的攻击方法，由此得出要避免该攻击法私钥的非线性核必须符合三条准则，是否存在以及如何构造足够多的符合这三准则的私钥仍是一个有待研究的问题；另一方面针对这些所提出的问题，陶仁骥[19]则提出了自己的一些看法，并认为戴宗铎等所提出的 FARKC 体制不够安全的依据是没有经过严格的数理逻辑证明，双方存在着较大的争议. 随着对有限自动机公开钥密码体制研究的进一步深入，这种密码算法的安全性将会逐渐被揭示出来.

2.3　IPv6 密码算法特性的比较

上述几种主要密码算法特性的比较如表 1 所示，它们在密钥（或信息摘要）长度、加密速度上存在较大的差异，其中 SHA 作为认证算法，其抗破能力比 MD5 的要高，但加密速度要慢；在公钥加密算法中 ECC 在密钥长度为160 bit时，抗破能力就与密钥长度为1024 bit的 RSA 相当，FAPKC 的抗破能力也很强. MD5、SHA 和 FAPKC 的加密速度是在 33MHz 的 80486 计算机上所测得的，而 DES 和 RSA 的加密速度是采用专用硬件加密所测得的.

表 1　几种密码算法的特性比较

算法名称	密钥(摘要)的长度/bit	加密速度/Mbit·s^{-1}	破译方法	破译时间/年
MD5	128	1.4	生日攻击	585①
SHA	160	0.6	生日攻击	3.8×10^{7}①
DES	56	1×10^{3}	线性攻击	10/73②
RSA	1024	0.6	穷举攻击	1012③
ECC	160	40	穷举攻击	1012③
FAPKC	4152	2.08×10^{-2}	穷举攻击	4.4×10^{31}④

①$10^{9}$ 条指令/秒；②12 台 HP9000/735 工作站；③$10^{6}$ 条指令/秒；④$10^{9}$ 条指令/秒；密钥量为 2^{160} 个.

3　IPv6 的密钥管理

由于密码技术的核心内容是利用加密手段对大量数据的保护归结为对核心参量密钥的保护. 因此，密钥管理问题特别是有密钥的设置、产生、分配、存贮、进入、销毁和提取等是网络安全管理的核心问题. 在 IPv6 中将密钥管理与加密算法相隔离，具有独立的密钥管理

体制; 密钥管理协议是通过安全关联与其它安全体制相互作用. 良好的安全关联设计可使得 IPsec 体系具有如下功能: 1) 当有更好的密钥管理协议时, 可用新协议取代旧协议; 2) 在必要时可改变现有的密钥管理协议.

IPv6 的密钥管理协议一般分为两类: 一类是用于定义过程和分组格式的协议, 如 SKIP (Simple Key for Internet Protocol) 和 ISAKMP (Internet Security Association & Key Management Protocol) 协议; 另一类用于定义密钥交换功能的协议, 如 Oakley 协议.

3.1 SKIP 协议

SKIP 是一种非会话型密钥管理协议, 需与 AH、ESP 协议一起使用, 为通信的各方提供加密和认证服务. 它利用 Diffie-Hellman 密钥公共值算法, 对每个基于 IP 的信宿和信源均有一个认证过的 DH 值. 该值与另一个机密值相结合, 导出它共享的机密主密钥, 该主密钥只用来对其它密钥加密. 它是一个隐含的、成对的共享密钥, 不需分组发送, 也不需在带外进行协商. SKIP 利用该主密钥来对一个临时分组密钥进行加密, 该临时分组密钥是用于 IP 分组的加密和认证的. 当接受方收到了这个加密分组时, 它能计算出这个共享的机密主密钥, 再用该主密钥推导出这个临时分组密钥; 然后, 再用它对分组进行解密或加密.

3.2 ISAKMP 协议

ISAKMP 提供了 Internet 密钥管理的一个框架, 支持协商和安全关联管理. 安全关联协议含有执行各种网络安全服务所需的所有信息. 同时, ISAKMP 也定义了交换密钥产生方法和认证数据的部分, 防止窃听. 该协议的主要内容包括: 1) ISAKMP 认证、密钥交换和保护. ISAKMP 需要利用数字签名算法与来之可靠第三方的认证相结合, 完成认证工作; 但它没有规定一种特定的签名算法或认证中心. 基于用户的需求, ISAKMP 也允许实体间的初始通信时指明它使用哪种密钥交换机制. 在选好密钥交换方法后, 该协议提供了支持实际的密钥建立所需要的消息; 因此采用该协议的用户可根据自己的需求来选择密钥算法. 同时, 在该协议中采用一种防阻塞令牌的方法来保护计算机的资源免受攻击. 2) ISAKMP 端口分配和头部格式. IANA (Internet Assigned Number Authority) 分配给 ISAKMP 的用户数据报协议端口号是 500, 所有 ISAKMP 协议的执行必须在这个端口上, 包括信息的传送和接收; 它的头部格式如图 6 所示:

<table>
<tr><td colspan="5">发信者特征</td></tr>
<tr><td colspan="5">接受者特征</td></tr>
<tr><td>下一个负载</td><td>主要版本号</td><td>辅助版本号</td><td>交换类型</td><td>标记</td></tr>
<tr><td colspan="5">消息标记</td></tr>
<tr><td colspan="5">长度</td></tr>
</table>

图 **6** ISAKMP 的头部格式

在图 6 中, 发信者特征和接受者特征分别为初始化安全关联和响应安全关联的建立、通告和取消的实体的描述; 下一个负载是指信息中的第一个负载类型; 交换类型是指使用的交换类型值; 而标记为可选项, 一般分为 E 和 C 两种; 消息标记是用来标识协议状态的, 在协商的第一阶段为 0, 第二阶段为 1; 长度是指以字节为单位包括头部和信息负载在内的总消息长度.

3.3 Oakley 密钥确定协议

Oakley 密钥确定协议是一种密钥交换协议，它描述了一系列密钥交换的过程．每个过程称为一种模式；它还详细列出了每种模式所提供的服务，如完备的前向密钥机密保护、身份保护和认证．对它的主要内容分析如下：1) Oakley 协议的特点．与其它有关协议相比，Oakley 协议的特点主要表现为可从一个现有的密钥推出一个新密钥，并且对这个派出来的密钥进行加密和分发该密钥；此外，它还提供如下几个选项功能来确保这些密钥的安全：①提供别名记号，用来帮助避免拒绝服务型攻击；②提供一种选项，包括选择加密算法、密钥确定方法和认证方法；③加密密钥的确定是取决于双方为认证对方的身份所使用的密码算法和 DH 算法；④提供执行 DH 算法的机制；⑤具有基于对称加密或非对称加密算法的认证功能．Oakley 协议与 ISAKMP 协议是兼容的，所分配的端口号也为 500．2) 密钥交换信息和协议．安全的密钥交换处理过程产生了通信双方常用的密钥信息，包括：①一个密钥名；②机密密钥资料；③通信双方的身份；④认证中使用的三种算法，即加密算法、散列码算法和认证算法．通信双方在交换消息的过程中会规定各自的要求，直到双方对他们通信会话中常用的密钥信息达成一致为止；而密钥交换协议则是由三个或三个以上的消息所构成的，一般包括如下三个基本部分：①一个密钥别名记号；②一个 DH 算法的半密钥；③用于私有性的认证功能．消息的具体内容取决于通信双方所选择的功能．3) 认证．Oakley 协议可和若干个不同的认证标准相结合，为用户提供了多种认证选择，包括：预先共享的密钥、域名服务公共密钥、RSA 公共密钥和带认证的 DSS (Data Signature Standard) 密钥．使用下列因素的组合可使得认证的密钥起作用，它们是：认证算法、具有明确可信度等级的认证中心的身份、象 PGP (Pretty Good Privacy) 或 RSA 那样的认证类型和一个密钥 (通常为公钥)．

4　结论与建议

目前，基于 IPv6 的信息安全系统已初步建立起了 IP 层的安全机制框架，将密码算法和密钥管理与安全协议机制相隔离，便于采用多种密码算法和支持密码算法升级；而每种密码算法的安全性各不相同，采用不同的密码算法将有不同的 IPv6 信息安全强度；因而密码算法与 IPv6 的信息安全密不可分，具有较大的创新潜力．密钥管理也是 IPv6 互联网信息安全系统中非常重要的一个组成部分，目前已提出了几种密钥管理协议．

中国作为一个网络发展的大国，建立和发展自己的网络信息安全系统是很有必要，而且是非常迫切的．但由于我国目前没有成熟的解决方案，许多关键的技术和产品不得不严重地依赖于国外的．因此，研究和开发我国自主的、完整的 IPv6 信息安全系统，特别是 PKI (Public Key Infrastructure) 系统，以支持未来政府、企业和个人进行安全的信息交流已是刻不容缓的，所涉及的问题非常多；但从宏观上看：我国所建设的 IPv6 信息安全系统应当是既符合前面所述的国际公认的 IPsec 标准体系结构，使之具有良好的兼容性和通用性；又要具有自主知识产权和较强的安全性能，且易于升级．后者就与密码算法密切相关，因此，密码算法的创新将是一个很重要的突破口，它既可以是对现有密码算法的改进，也可以是一种新密码算法，如：量子密码、DNA 密码和混沌密码等；而评价一种密码算法的优劣则主要是看能否满足一定的实际安全性，同时兼顾算法实现的速度和密钥分配与贮存的难易等因素，如最近提出的混沌神经网络加密算法[20,21]就是一种新的高密码强度的加密算法，并已将其集成为一种专用芯片．

[参考文献]

[1] Silvano Gai. Internetworking IPv6 with Cisco Routers [M]. 萧湘工作室译. 北京: 机械工业出版社, 1999.

[2] Pete Loshin. IPv6 Clearly Explained [M]. 沙斐译. 北京: 机械工业出版社, 2000.

[3] Marcus Goncalves, Kitty Niles. IPv6 Networks [M]. 黄锡伟, 杨震译. 北京: 人民邮电出版社, 2000.

[4] 赵战生, 冯登国, 戴英侠. 信息安全技术浅谈 [M]. 北京: 科学出版社, 1999.

[5] 吕诚昭. 信息安全管理的有关问题研究 [J]. 电信科学, 2000, 16 (3): 22-26.

[6] S Kent, R Atkinson. Security Architecture for the Internet Protocol [EB/OL]. RFC 2401, 1998-11.

[7] S Kent, R Atkinson. IP Authentication Header [EB/OL]. RFC 2402, 1998-11.

[8] S Kent, R Atkinson. IP Encapsulating Security Payload (ESP) [EB/OL]. RFCA2403, 1998-11.

[9] Paul Fischer. Configuring Cisco Route for ISDN [M]. 李志, 张巧莉译. 北京: 机械工业出版社, 1999.

[10] K Krawczyk, M Bellare, R Canetti HMAC. Keyed Hashing for Message Authentication[EB/OL]. RFC2104, 1997-02.

[11] R Rivest. The MD5 Message Digest Algorithm [EB/OL]. RFC1321, 1992-04.

[12] Federal Information Processing Standards. FIPS PUB 180-1, Secure Hash Standard [EB/OL]. http://www.itl.nist.gov/. 1993-05-11.

[13] H Jr Katzan. The Standard data encryption Algorithm [M]. Petrocell: Books Inc, 1997.

[14] R Rivest, A Shamir, L Adlemn. A Method for Obtaining Digital Signatures and Pubic-Key Cryptosystems [J]. Communication of the ACM, 1978, 21 (2): 120-126.

[15] M J Wiener. Cryptanalysis of short RSA secret exponents [J]. IEEE Trans on Information Theory, 1990, 36 (3): 553-558.

[16] A J Menezes. Elliptic Curve Public Key Cryptosystem [M]. Boston: Kluwer Academic Publishs, 1993.

[17] 陶仁骥, 陈世华. 一种有限自动机公开钥密码体制和数字签名[J]. 计算机学报, 1985, 8(6): 401-409.

[18] 戴宗铎. 一类可分非线性有限自动机—兼 FAPKC3 加密与签名体制分析 [A]. 裴定一. 密码学进展—CHINACRPT' 96 [C]. 北京: 科学出版社, 1992, 87-93.

[19] Tao Renji. Remark on "Weak Invertibility of Finite Automata and Cryptamalysis on FAPKC" [A]. 王蕚芳, 杨伟成. 密码学进展—CHINACRPT' 2000. 北京: 科学出版社, 2000. 65-75.

[20] Donghui Guo, L L Cheng. A New Symmetric Probabilistic Encryption Schene Based on Chaotic Attractors of Neural Networks [J]. Applied Intelligence, 1999, 10 (1): 71-84.

[21] 郭东辉, 何小娟, 陈彩生. 基于神经网络混沌加密算法的专用芯片设计 [J]. 计算机学报, 2000, 23 (11): 1230-1232.

Studies on the Information Security of IPv6 Internet

LIU Niarr-sheng[1], GUO Dong-hui[2], LIU Rui-tang[2], WU Bo-xi[2]

(1. School of Biotechnology, Jimei University, Xiamen 361021, China;

2. Institute of Technical Physics, Xiamen University, Xiamen 361005, China)

Abstract: The security mechanism based on IPv6 Internet are briefly introduced at first in the paper. Secondly, the main encryption algorithms in the IPv6 are deeply analyzed. They include MD5, SHA, RSA, ECC, and FAPKC. Thirdly, the key management in the IPv6 Internet is deeply dissertated. Some proposals for the information security of IPv6 Internet in China are finally offered.

Key words: IPv6; information security; encryption algorithm