一类基于KTC的主动节点密钥建立协议

唐 寅*[1] 杨 睿[2] 宫亚峰[2]

(1.电子科技大学电子工程学院 成都 610054；2.北京984信箱 北京 100091)

【摘要】主动网络是一种功能强大、配置灵活的新型网络体系。该文介绍了主动网络技术以及密钥建立协议在主动网中的应用功能，论述了网络安全中的密钥管理以及伪随机密钥与初始向量的产生过程，给出了一个基于密钥传递中心的主动节点密钥建立协议。

关 键 词 主动网；密钥；初始向量；密钥传递中心；密钥建立协议

中图分类号 TN915.08；TP309.7

A KTC-Based Key Establishment Protocol for Active Networks Nodes

Tang Yin[1] Yang Rui[2] Gong Yafeng[2]

(1. College of Electronic Engineering,UEST of China Chengdu 610054; 2. P.O.984, Beijing Beijing 100091)

Abstract Active networking is a powerful and flexible new networking Architecture.While this new technology presents opportunities for innovative networking services,it also presents significant security challenges. This paper introduces the technology of active networks and the functions of the key establishment protocol(KEP)firstly. Then describes the management of keys and how to produce a key & initialization vector. Finaly, a KTC-based key establishment protocol for active networks nodes is proposed.

Key words active networks; key; initialization vector; key translation center; key estabisment protocol

主动网络是一种新型的网络体系，它允许授权用户或第三方软件开发商对网络进行客户化编程。利用开放的可编程接口(如网络 APIs)和一系列服务组件方法及工具，主动网络的体系结构能够被定制。迅速创造、开发和管理新的服务是导致主动网络研究的关键因素。这种新型的网络体系把更多的计算处理任务放到廉价的网络节点中，可实现网络性能优化，加速新技术、新协议标准的开发和应用，具有广阔的前景[1]。美国华盛顿大学已成功开发出了主动网络交换机，如图1所示。该机具有可扩展交换核，可配置达20 Gb/s、160 Gb/s 性能；每个交换端口带有嵌入式处理器；端口内置的主动处理部件(APE，Active Processing Element)用于处理可扩展的主动报文。

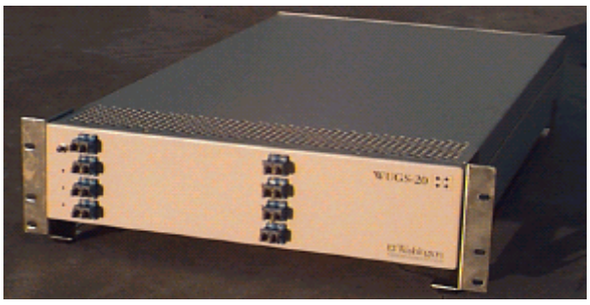

图1 主动网交换机

2002年6月28日收稿

* 男 32岁 博士生

在主动网中，以往授权用户只具有系统管理员才具有的部分网管权利，授权用户能管理配置主动节点的资源，因此对网络的安全性又提出了新的挑战[2]。主动数据包中携带了对网络节点资源进行访问的程序，在很大程度上可以对资源进行分配、修改等操作。所有这些都可能使网络受到恶意程序和有缺陷代码的攻击或影响。因此，构造一个安全的主动网络环境，例如，认证信息的源端、保护信息不被修改、保证主动节点不被侵犯等，所有这些安全问题的研究是主动网技术中的一个重要内容[3]。

通过密钥建立协议 KEP(Key Establishment Protocol)可以使主动网络的节点或主体间建立共享密钥和交换证书，也可以使主动节点启动失败时进行远程恢复和认证[4]，主动网络中 KEP 的作用主要表现在以下三个方面[5]：

1) 主动节点的安全启动和恢复；

2) 确认相邻主动节点；

3) 建立会话密钥以及节点或主体的认证和授权。

本文介绍了密钥管理分配体系，并描述了伪随机密钥(key)与初始向量(*IV*)的产生过程，并对基于 KTC 的主动节点 KEP 进行了分析讨论，最后给出了一个安全协议的实现。文中约定下列符号: K 为 *DEA* 密钥; V 为64位密钥种子 D_T 为时间矢量，每次密钥产生时被更新；I 为计算中间值; R 为64位矢量; T_A 为通信 A 方的标识; T_B 为通信 B 方的标识；R_A 为 A 方产生的随机数；R_B 为 B 方产生的随机数；N_A 为公证密钥; + 为异或; e 为加密; d 为解密; $ede(Y, X)$ 为 Y 在密钥 X 下的多重 EDA 加密; CT( ) 为计算密钥偏移的计数器。

1　密钥管理分配体系

根据近代密码学的观点，系统的安全应只取决于密钥的安全，而不取决于对算法的保密。在计算机网络环境中，由于用户和节点很多，需要使用大量的密钥。密钥的数量如此之大，而且又要经常更换，其产生、存贮、分配是极大的问题。如无一套妥善的管理方法，即带来很大的困难性和危险性。

在现代密钥管理体系中，通常可将密钥分为两类：密钥加密密钥和数据/会话密钥。前者用来加密或解密后者，后者用来加密或解密会话数据。动态密钥管理体系通常可分为二层或三层结构，如图2所示。

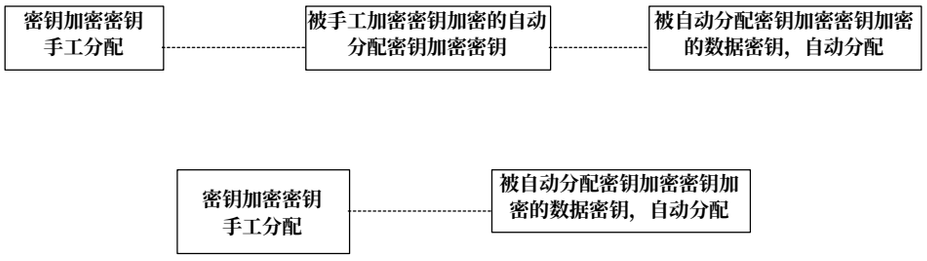

图2　密钥管理体系结构

由图2知，二层密钥管理体系只比三层密钥管理体系省去了中间层结构，即在数据密钥与手工加密密钥之间产生一层自动分配加密密钥。在二层密钥管理体系中，数据加密密钥经由手工分配的密钥加密密钥加密后进行分配；在三层密钥管理体系中，手工分配的密钥加密密钥用来加密自动分配密钥加密密钥，然后再由自动分配密钥加密密钥加密数据加密密钥后分配给用户。二层密钥管理体系是实现密钥分配管理的最基本体系，无论二层和密钥管理体系或三层密钥管理体系的最高层密

钥都只能以手工方式产生和分配[6]。

2 伪随机密钥与初始向量的产生

ANSI X9.17对伪随机密钥(key)与初始向量(*IV*)的产生要求如下：

1) keys 与 *IVs* 为随机量或伪随机量；

2) 在 keys 与 *IVs* 空间中选取 key 与 *IV* 的概率相等；

3) 前后选取的 key 与 *IV* 之间不存在关联；

4) 产生密钥的强度不超过密钥产生过程的强度；

5) 无法根据加密算法来攻击 key 与 *IV* 的产生过程。

按照以上要求得到 keys 与 *IVs* 的产生算法如下：

$$I=ede(D_T, K)$$

$$R=ede(I+V, K)$$

$$V=ede(R+I, K) \quad \text{（新）}$$

然后，将 *R* 的每个字节的第8位用校验位替换即得到所需的 DEA keys，而每次所得 *R* 即为所求的 *IVs*。

3 KEP 的建立

目前，密钥的管理分配模式可分为三类：1) 点对点模式，即通信双方直接管理共享通信密钥；2) KDC(Key Distribution Center)模式，通信双方的会话密钥由KDC管理生成；3) KTC(Key Translation Center)模式，通信双方的会话密钥由发起方产生/获取，并由 KTC 管理传递。

密钥传递中心 KTC 的功能是为需要通信而又尚未建立共享密钥的双方建立一个用于双方安全通信的共享密钥。KTC 作为可信赖的第三方与需要进行通信的双方分别具有共享密钥加密密钥。与 KDC 密钥建立环境不同的是，KTC 环境中的通信发起方具有产生或获取(数据)密钥的能力。当 KTC 收到来自通信发起方密钥建立请求后，KTC 分别依次处理密钥加密密钥和数据密钥，然后分别用公证密钥和接收方的密钥加密密钥加密发起方产生/获取的数据密钥，再返回给发起方，最后由发起方将经过公证的数据密钥传递给通信接收方，通信双方依据此数据密钥进行安全会话。

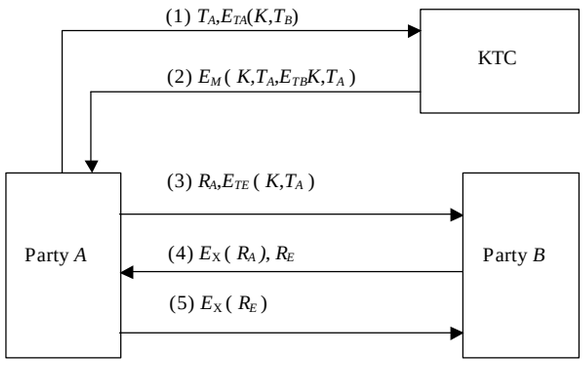

图3 ANN 密匙建立

根据上述原理可以在主动网络节点之间建立如图3所示的 KEP。

1) 节点 *A* 方产生/获取一个会话密钥 *K*，连同主动节点 *B* 方的标识 T_B 一起用 *A* 与 KTC 共享的密钥加密密钥 K_{TA} 加密，再与 *A* 的标识 T_A 一起发往 KTC；

2) KTC 用它与 *A* 的密钥加密密钥解密收到的请求，然后对收到的 *K* 及 T_A、T_B 进行认证，再分别用认证密钥 K_{NA} 加密 *K* 和 T_B，用 KTC 与 *B* 的密钥加密 *K* 和 T_A，最后将加密结果返回给 *A*；

3) *A* 产生一个随机数 R_A, 与 E_{TB}(*K*，T_A)一起发往 *B*；

4) *B* 用它与 KTC 共享的密钥加密密钥解密 *A* 发来的信息，得到 *K*，然后用 *K* 加密 R_A，再连同 *B* 产生的随机数 R_B 一起发给 *A*；

5) *A* 用 *K* 加密 R_B，再返还给 *B*。

ANSI X9.17定义密钥公证为：用通信双方的标识来确认密钥，会话密钥在传输前必须先经过公

证，公证的实现采用密钥加密密钥与公证章相异或。会话密钥被公证后只能通过公证时使用的密钥加密密钥和和通信双方的标识才能解开。公证密钥 K_{NA} 的产生过程如下：

$KKR=K_{TA}+T_{B1}$

$KKL=K_{TA}+T_{A1}$

$NSl=eKKR(T_{A2})$

$NSr=eKKL(T_{B2})$

$BV=NSl$ 最左边32位//NSr 最右边32位

$NS=BV+CT(\ )$

$K_{NA}=KK+NS$

主动节点 A 与 B 之间实现了秘密密钥 K 的共享，共享密钥可用于主动节点或主体(Principals)之间的认证授权，协议本身还可用于实现主动节点或主体之间交换证书等其他安全机制。

4 结 束 语

主动网络的出现使得网络功能由原来的存储-转发转变为存储-计算-转发，增强了网络系统的智能性、可扩展性。这种新型的网络体系把更多的计算处理任务放到廉价的网络节点中，可实现网络性能优化，加速新技术、新协议标准的开发和应用，具有广阔的前景。主动网的安全性研究涉及两方面内容：保护网络中主动节点的资源不被恶意的主动代码攻击和盗用；保证主动代码不受恶意网络节点的攻击，保证代码在传输过程中的完整性、可靠性以及数据的机密性。前者常见的安全技术包括认证证书、代码验证、存取控制和时间限制[7]。后者可以采用主动节点和主动代码的双向认证来保障主动代码的安全，涉及的安全机制包括严格规范定义执行环境与节点操作系统之间的接口、数字水印方法、容错技术等。

本文给出的 KEP 可以扩充新的安全机制，如数字签名、时间戳等来加强主动网络的安全性，防止抵赖、重放攻击等安全隐患的发生。

参 考 文 献

1　David，L，Tennenhouse. A survey of active network research. IEEE Commum.Mag, 1997, 35(1): 80-86

2　Alexander D S, Willian A A, Aagelsos D, *et al*. A secure active network enviroment architecture:Realization in switchware. IEEE Network, 1998(6): 37-45

3　Alexander D S, Arbangh, W A. Safty and security of progammable network Infrastructures. IEEE comm. Mag, 1998, (10): 84-92

4　Bob L.Active network protocol specification for hop-by-hop message aythentication and Integrity. http://www.isi.edu/abone/documents/ossec.txt

5　Psounis K. Active networks:application,security,safety,and architectures. IEEE Comm Surveys, 1999, 2(1): 45-457

6　王育民，刘建伟. 通信网的安全—理论与技术. 西安：西安电子科技大学出版社, 2000

7　李鸿培，王新梅. 主动网络节点的安全机制研究. 计算机科学，2001, 28(3): 46-49