

一种新型网络通信协议的设计与研究

郭 锐,冯志杰,高宗宁

(中国科学院 信息工程研究所,北京 100093)

摘 要:互联网发展至今,尤其是移动互联网的快速发展极大地改善了人们的生活方式,但与之相伴的网络安全问题也愈发严重。这就迫使人们思考现有互联网体系架构设计的弊端,进而去寻求一种解决现有问题的途径。新型网络通信协议充分分析了现有 TCP/IP 网络的优缺点,针对其 IP 编址中存在的二义性问题展开思考,并结合通信市场上出现的各类终端的特点,提出了基于不同网络类型的两种数据包格式,在此基础上引入了 IPsec 的相关技术,为数据包通信添加安全保障。分析了现有网络存在的安全隐患,提出了加强安全通信的必要性。接着对新型网络通信协议进行了相关的探讨和研究,重点阐述了新型网络的特点及其与现有网络的区别。随后研究提出新型网络的整体框架,详细给出了各组成模块的功能原理。通过搭建测试环境对新型网络进行测试,验证了新型网络通信协议标准的可行性。

关键词:网络安全;IP 地址二义性;新型网络通信协议;安全通信

中图分类号:TP393.0

文献标识码:A

文章编号:1673-629X(2017)01-0075-05

doi:10.3969/j.issn.1673-629X.2017.01.017

Design and Research of a New Network Communication Protocol

GUO Rui, FENG Zhi-jie, GAO Zong-ning

(Institute of Information Engineering, CAS, Beijing 100093, China)

Abstract: With the rapid development of the Internet and the mobile Internet, the people's life has been greatly improved, but network security issues have become increasingly serious. To improve the network status, people are forced to think about the disadvantages of the traditional network architecture design. The new network communication protocol analyzes the advantages and disadvantages of the existing TCP/IP network. Based on the double meanings of IP address and all kinds of mobile terminals, the two packet formats are put forward. By drawing on the relevant technology of IPsec, the corresponding security module is added to guarantee the network security communication. The potential safety hazards is analyzed in the traditional network and the significance of strengthening safety communication is proposed. In the introduction of the new network communication protocol, it concentrates on discussing the new characteristics of the new network and its difference to the traditional network. And then, the structure of the new network is researched, and the function principle of each module is presented. By building the testing environment, the feasibility of the new network communication protocol is verified.

Key words: network security; double meanings of IP address; new network communication protocol; secure communication

0 引言

自二十世纪七十年代至今,计算机网络得到了快速普及,尤其是近年来移动互联网的迅速发展,给人们的生活带来了极大便利,但现有互联网体系暴露出的问题也越来越多。例如网络安全性差、移动支持性差、可控可管性差等,其中尤为突出的是网络的安全性问题^[1]。近几年发生的网络安全事件尤为频繁:2014 年 2 月,全球最大的比特币交易平台 Mt. Gox 自身账号中约 10 万个比特币被窃,损失估计达到 4.67 亿美元,被

迫宣布破产;2014 年 4 月发生的 Heartbleed 漏洞事件,影响范围波及各大银行、门户网站等;2015 年 5 月 29 日,某网络安全公司发布报告披露了一起针对中国的国家级黑客攻击细节,自 2012 年 4 月起境外名为“海莲花”的黑客组织利用木马病毒攻陷和控制政府人员、外包商、行业专家等目标人群的电脑,意图获取受害者电脑中的机密资料。种种事件表明,现有网络存在很大的安全隐患^[2]。

上述安全问题的根源在于现有网络体系架构固有

收稿日期:2015-12-16

修回日期:2016-03-25

网络出版时间:2017-01-04

基金项目:国家“863”高技术发展计划项目(2013AA01A214)

作者简介:郭 锐(1982-),男,工程师,从事新型网络通信和无线通信相关的安全问题研究。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20170104.1023.034.html>

的设计缺陷,现有互联网的体系架构是基于 TCP/IP 协议族^[3]的,而 TCP/IP 在设计之初是用于固定节点之间的通信,其 IP 地址具有双重属性^[4]:IP 地址既代表终端的身份又代表通信终端所处的位置。IP 层的上层协议(如 TCP、UDP、HTTP、FTP 等协议)都使用 IP 地址来标识通信终端,整个通信过程都和 IP 地址进行绑定,这意味着 IP 地址是一种身份标识。而 TCP/IP 协议族又使用 IP 地址来路由,可以通过某个 IP 地址找到其代表的网络接口,这意味着 IP 地址同时又代表网络端口的的位置信息。随着互联网的不断发展及其网络规模的不断扩大,基于 IP 地址的最初的互联网设计弊端逐渐凸显,移动性、安全性、路由聚合等问题也越来越突出。因此,解决 IP 地址二义性问题,研究新型互联网体系架构,特别是研究和制定具有自主知识产权的新型互联网体系标准已迫在眉睫。

1 新型网络通信组网模型

新型网络通信协议采用的组网模型如图 1 所示。

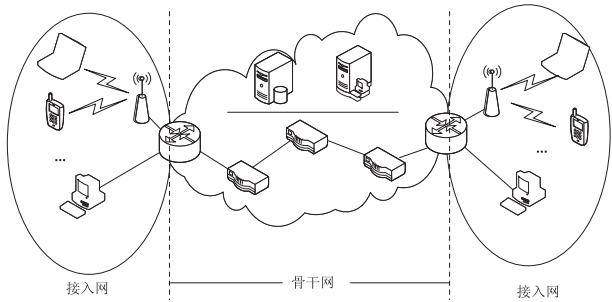


图 1 新型网络通信组网模型

新型网络通信将整个网络划分为两个部分:接入网和骨干网。接入网实现各类终端设备和各类子网的接入;骨干网负责数据包的路由和对终端设备的接入认证等工作。

为避免现有网络中 IP 地址存在的二义性缺陷,在新型网络中使用两类地址:终端地址和路由地址。在接入网中,为每个合法的终端分配一个终端地址,该终端地址会根据终端类型的不同而分为不同的长度,有 8 位、16 位、32 位、64 位和 128 位之分,在接入网内部终端间通信使用终端地址即可;在骨干网中,数据包从接入网经过边界路由器(连接接入网和骨干网的路由器定义为边界路由器)到达骨干网时,边界路由器要在数据包的外部封装一个新的报头,新报头的地址为能在骨干网中进行路由的路由地址,这样设计的目的是为了解决现有互联网中 IP 地址身份与位置绑定的缺陷。

1.1 新型网络通信中数据包报头格式设计

在借鉴现有网络中数据包报头格式设计^[5]的优缺点的基础上,删除一些不必要的字段,添加一些新型网

络中特有的字段,研究设计了两种分别在接入网和骨干网中使用的数据包报头格式,如图 2 所示。

版本号	载荷长度	F	跳数限制	下一首部
源地址长度	目的地址长度	保留		
源地址				
目的地址				
载荷数据				

(a)接入网数据包格式

版本号	载荷长度	F	跳数限制	下一首部
源地址				
目的地址				
载荷数据				

(b)骨干网数据包格式

图 2 数据包格式

(1)接入网中数据包格式。

接入网数据包格式如图 2(a)所示,其中:

- 版本号:3 位,表示新型网络通信协议的版本,值为 1。
- 载荷长度:13 位,表示数据包载荷的总长度,以字节为单位,数据载荷的最大长度为 8 KB。
- F:地址类型标志位,用来标志数据包中地址是终端标识还是路由地址,值为 0 表示终端地址,值为 1 表示路由地址。
- 跳数限制:7 位,表示数据包在网络中最长生存时间,每经过一台路由器该字段值减 1,当该字段减为零时,丢弃该数据包。
- 下一个首部:8 位,表示紧接在数据包报头后的载荷数据所代表的协议类型或扩展首部的类型。
- 源地址长度:8 位,表示源终端地址的长度。
- 目的地址长度:8 位,表示目的终端地址的长度。
- 源地址:长度不固定,源地址会因通信终端类型的不同而分为不同的长度,长度有 8 位、16 位、32 位、64 位和 128 位之分。
- 目的地址:长度不固定,目的地址会因通信终端类型的不同而分为不同的长度,长度有 8 位、16 位、32 位、64 位和 128 位之分。

(2)骨干网中数据包格式。

骨干网中数据包格式如图 2(b)所示,其中字段版本号、载荷长度、F、跳数限制和下一首部见接入网中数据包格式定义。源地址和目的地址长度为固定的 128 位。

之所以用两种报头格式是根据接入网和骨干网各自的网络特征来决定的,随着移动通信网络技术的发

展,各种各样的终端都可以接入到网络中,终端类型不同,为其分配的终端地址的长度会有所差异,因此在接入网中加入了源地址长度和目的地址长度字段来标识终端地址的长度。而在骨干网中采用固定的地址长度

是为了减少路由条目,方便路由聚合。

1.2 新型网络通信中数据包基本通信流程

新型网络中数据包的一次完整通信流程如图3所示。

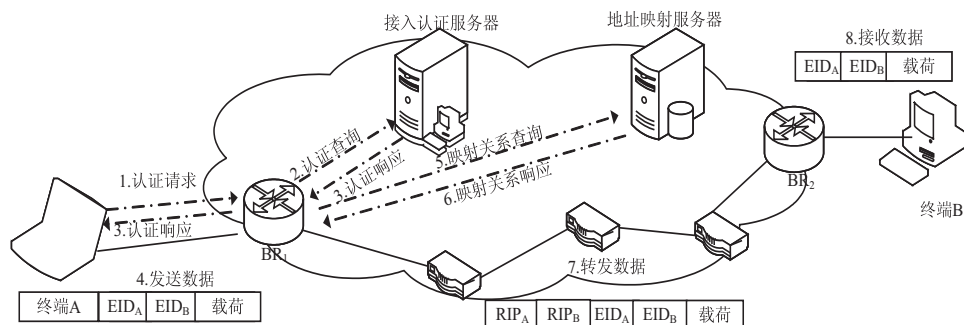


图3 新型网络中数据包的基本通信流程图

其中,接入认证服务器^[6]负责各类终端入网时的授权和认证,地址映射服务器存储各类终端的终端地址到其对应的边界路由器的路由地址之间的映射关系对,边界路由器内维护着两张映射表:本地映射表和对端映射表^[7]。本地映射表存储的是该边界路由器管辖范围内的各类终端与路由地址的映射关系对,而对端映射表存储的则是不在本地管辖范围内的终端与路由地址的映射关系对。当接入网中的数据包经边界路由器到达骨干网时,边界路由器查询地址映射服务器获得与终端地址对应的路由地址后,在接入网中的数据包头部外再封装一个骨干网中的数据包报头,外层报头中的地址为两台边界路由器的路由地址,具体流程如下所示:

步骤1:通信终端A向边界路由器BR₁发送接入认证请求数据包。

步骤2:边界路由器BR₁向接入认证服务器发送认证查询消息,查看网络是否允许终端A接入。

步骤3:接入认证服务器将认证结果通过边界路由器BR₁转发给终端A。

步骤4:如果认证通过,则终端A可以在该网络中发送数据包。当终端A向终端B发送数据包时,发送的数据包的格式应符合接入网中数据包的格式,数据包中的源和目的地址为通信双方的终端地址,地址标志位F的值为0。

步骤5:边界路由器BR₁收到该数据包,首先判断该数据包的目的地址是否为本地接入网的其他终端,若是,则直接将该数据包转发到目的终端;否则,边界路由器BR₁搜索对端映射表来查询终端B的终端地址所对应的路由地址。若查询到终端B的终端地址对应的路由地址,则边界路由器BR₁在收到的数据包的外层封装一个骨干网的数据包报头,报头中地址标志位F值为1,代表外层报头的源和目的地址为通信双

方所在的两台边界路由器的路由地址。若没找到终端B的映射关系对,边界路由器BR₁则向地址映射服务器发起映射关系查询消息。

步骤6:地址映射服务器将映射关系响应消息传给边界路由器BR₁。

步骤7:边界路由器BR₁将封装好的数据包传给骨干网中的路由器进行路由,骨干网中的路由器根据路由地址进行寻址路由。

步骤8:边界路由器BR₂收到数据包后,将数据包外层的骨干网报头进行剥离,然后根据内层报头的终端地址将数据包转发给终端B。

以上是新型网络中数据包的一次基本通信流程,新型网络与现有传统网络相比,其优点在于:

(1)将网络分成接入网和骨干网,从而为不同网络中各种技术的独立演进提供条件。

(2)网络管理者可以对不同的网络分别进行不同的管理,加强了网络的可控可管性能。

(3)根据各自网络的特点创造性地提出了接入网报头格式和骨干网报头格式,接入网报头格式的设计又充分兼顾了各种入网终端的特点。

(4)边界路由器的引入解决了现有网络中IP地址的二义性缺陷。

(5)通过引入现有网络的安全机制IPSec^[8-10]的相关技术,在新型网络通信协议栈中设计相应的安全模块,可以进一步增强新型网络通信过程中的安全保障。

2 新型网络通信协议的模块化实现

为了实现上述提到的新型网络通信协议的设计思想,提出了模块化的实现方法。为了加强新型网络通信中的安全性,借鉴了现有网络中IPSec的相关概念,在Linux系统内核^[11-12]中固化了相应的安全模块^[13]。

如图 4 所示,主要包括:地址封装映射模块、密钥配置模块、密钥接口层、身份验证与加密模块、算法模块。

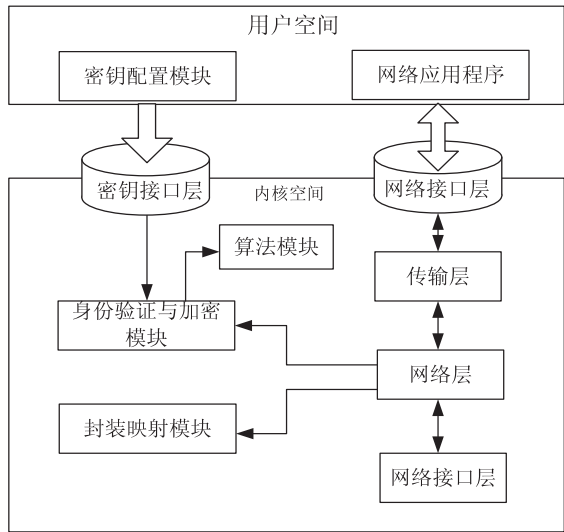


图 4 新型网络通信中各模块之间的关系示意图

- 密钥配置模块:该功能实体实现了用户对数据包加密或认证时的安全参数的配置,包括密钥的选择、安全通信方式的选择、安全参数索引的配置等。
 - 密钥接口层:负责用户空间与 Linux 内核之间的安全连接,通过密钥管理套接字把用户配置的安全参数传递给内核。
 - 身份验证与加密模块:该模块负责对需要进行安全处理的数据包进行认证或加密处理,包括查询安全关联数据库、生成消息摘要等操作。
 - 算法模块:该模块为安全通信提供各种算法支持,如 DES,3DES,MD5,SHA1 等。
 - 封装映射模块:该模块负责对通信数据包进行封装和解封装操作,并维护地址映射表。
- 上层用户可以根据自己的需要通过密钥配置模块给安全通信配置相应的安全参数,系统内核通过 PF_

KEY 套接字^[14]将安全通信参数存储在安全关联数据库中以便后续查找。当有安全通信需求时,通过网络层的相关调用函数触发身份验证与加密模块,身份验证与加密模块查询安全关联数据库,根据查询到的结果调用相应算法模块对数据包进行安全处理。在安全通信的发送端,内核协议栈中的网络层将上层传下来的数据进行加密或认证并添加相应的报头后交给下层处理。在安全通信的接收端,将从网络接口层上传上来的数据进行解密或认证后交由上层进行后续处理。其中的封装映射模块是在边界路由器上加载的,以此来完成对数据包的封装与解封装。

3 新型网络通信协议测试与验证

对新型网络通信协议的测试主要分为两部分:协议的一致性测试和协议的功能性测试。一致性测试的目的是验证新型通信协议栈与新型通信协议标准的符合程度,验证新型网络通信协议栈是否实现了新型网络通信协议标准所规定的功能。协议的功能性测试的目的是验证新型网络通信协议栈是否实现了地址封装映射的功能。由于对实验数据的分析是基于 Wireshark 抓包软件所抓到的数据的,但现有的 Wireshark 软件还不能识别该新型网络通信协议的数据包,为此扩展了 Wireshark 的功能使之能解析新型网络通信协议定义的数据包格式。

通过搭建相应的测试环境,在接入网中 Wireshark 抓包结果如图 5 所示。

在骨干网中 Wireshark 抓包结果如图 6 所示。由 Wireshark 抓包分析可知,在接入网和骨干网中抓到的数据包符合新型网络通信协议中规定的报头格式,在骨干网中数据包的外层报头的下一个首部字段值为 0 表示载荷数据是接入网的数据包,数据包经过

No.	Time	Source	Destination	Protocol	Length	Info
2	2014-06-05 14:40:33.372278	Micro-St_3d:6b:89	SuperMic_62:06:3f	IPNX	82	IPNX data
3	2014-06-05 14:40:33.372593	SuperMic_62:06:3f	Micro-St_3d:6b:89	IPNX	142	IPNX data
4	2014-06-05 14:40:33.385274	Micro-St_3d:6b:89	SuperMic_62:06:3f	IPNX	142	IPNX data

Frame 2: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)

Ethernet II, Src: Micro-St_3d:6b:89 (00:24:21:3d:6b:89), Dst: SuperMic_62:06:3f (00:25:90:62:06:3f)

IPNX Protocol

Message Header:
Version: 1
Payloadlen: 28
Flag: Endpoint ID
Hoplimit: 127
Nextthdr: 58
EIDs_len: 128
EIDD_len: 128
Reserved: 0
EIDs: 3415:0000:0001:0002:0000:0000:0000:0001
EIDD: 3415:0000:0001:0002:0000:0000:0000:0002
Data:

0000 00 25 90 62 06 3f 00 24 21 3d 6b 89 ee 20 1c .%.b.?. \$!=k...
0010 7f 3a 80 80 00 00 34 15 00 00 00 01 00 02 00 004.
0020 00 00 00 00 00 01 34 15 00 00 00 01 00 02 00 004.
0030 00 00 00 00 00 02 88 00 6c 67 e0 00 00 00 00 01lg.....
0040 00 02 00 00 00 00 00 00 00 01 02 01 00 24 21 3d\$!=
0050 6b 89 k.

No.	Time	Source	Destination	Protocol	Length	Info
2	2014-06-05 14:40:33.372278	Micro-St_3d:6b:89	SuperMic_62:06:3f	IPNX		82 IPNX data
3	2014-06-05 14:40:33.372593	SuperMic_62:06:3f	Micro-St_3d:6b:89	IPNX		142 IPNX data
4	2014-06-05 14:40:33.385274	Micro-St_3d:6b:89	SuperMic_62:06:3f	IPNX		142 IPNX data

Frame 2: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)

Ethernet II, Src: Micro-St_3d:6b:89 (00:24:21:3d:6b:89), Dst: SuperMic_62:06:3f (00:25:90:62:06:3f)

IPNX Protocol

Message Header:

Version: 1

Payloadlen: 28

Flag: Endpoint ID

Hoplimit: 127

Nexthdr: 58

EIDLen: 128

EIDLen: 128

Reserved: 0

EIDs: 3415:0000:0001:0002:0000:0000:0000:0001

EIDd: 3415:0000:0001:0002:0000:0000:0000:0002

Data:

000000259062063f0024213d6b89ee201c.%b.?.\$!=k...
00107f3a800000341500000100020000.:...4.
00200000000001341500000100020000.....4.
0030000000000288006c67e000000001.....1g.....
004000020000000000000102010024213d.....\$!=
00506b89k.

图 6 在边界路由器上的抓包结果

边界路由器的处理,在数据包的外层封装了一个骨干网的报头,外层报头中的地址为两台边界路由器的路由地址。新型网络通信协议栈已经基本完成了新型网络通信协议标准的要求,实现了地址封装映射的过程,达到了测试目的,从而验证了新型网络通信协议标准的可行性。

4 结束语

分析了现有互联网中存在的种种弊端,结合互联网现状和未来网络发展趋势,对设计一种具有自主知识产权的新型网络通信协议进行了大胆尝试。从目前的研究成果看,新型网络的设计还缺乏对移动性、更强的安全性等的支持,目前还处于前期研究阶段,后续的探索还将进一步深入。

参考文献:

[1] CNCERT/CC. 2014 年中国互联网网络安全报告[R/OL]. 2015. <http://www.cert.org.cn/publish/main/upload/File/2014%20Annual%20Report.pdf>.
[2] CNCERT/CC. 2015 年 5 月 CNCERT 互联网安全威胁报告[R/OL]. 2015. <http://www.cert.org.cn/publish/main/upload/File/2015monthly05.pdf>.

[3] Socolofsky T, Kale C. A TCP/IP tutorial[S]. [s.l.]:IETF, 1991.
[4] Postel J. Internet protocol[S]. [s.l.]:IETF,1981.
[5] Deering S, Hinden R. Internet Protocol, Version 6 (IPv6) specification[S]. [s.l.]:IETF,1998.
[6] 苏伟,刘琪,张宏科. 一体化标识网络体系及关键技术[J]. 中兴通讯技术,2011,17(2):1-4.
[7] 王上. 一体化网络接入交换路由分离映射的设计与实现[D]. 北京:北京交通大学,2008.
[8] Kent S, Atkinson R. Security architecture for the internet protocol[S]. [s.l.]:IETF,1998.
[9] Kent S, Atkinson R. IP authentication header[S]. [s.l.]: IETF,1998.
[10] Kent S, Atkinson R. IP Encapsulating Security Payload (ESP) [S]. [s.l.]:IETF,1998.
[11] 肖宇峰,李昕,时岩. Linux 网络内核分析与开发[M]. 北京:电子工业出版社,2010.
[12] 樊东东,莫澜. Linux 内核源码剖析(上册)[M]. 北京:机械工业出版社,2011.
[13] 许涛. 地址分离映射网 IPSec-VPN 的研究[D]. 北京:北京交通大学,2009.
[14] Stevens W R, Fenner B, Rudoff A M. UNIX network programming volume 1:the sockets networking API[M]. 3rd ed. Beijing:Posts and Telecom Press,2014.