文章编号:1001 - 9081(2006)02 - 0346 - 03

H.323 视讯网的安全解决方案及身份认证实现

郝洛玫[1],喻占武[2],李 锐[2],胡 滨[2]
(1. 武汉大学 电子信息学院,湖北 武汉 430072;
2. 武汉大学 测绘遥感信息工程国家重点实验室 多媒体通信工程中心,湖北 武汉 430072)
(yew80417@hotmail.com)

摘 要:在对 H.323 视讯网的安全性问题进行分析的基础之上,根据 H.235 建议提出 H.323 视讯网的安全解决方案,内容主要包括:完整性检查,保密性检查和身份认证。实现了保障网络安全的最重要环节——身份认证,详细阐述 H.323 GK(GateKeeper)和 RADIUS Server 的联合认证过程,其中包括基于 PAP 协议的 User-Password 认证和基于 CHAP 协议的 Chap-Password 认证。

关键词:H.323; H.235; GK; 身份认证; 远程拨号用户认证服务
中图分类号: TP309 **文献标识码**:A

Security solution of H.323 net and implementation of identity authentication

HAO Luo-mei[1], YU Zhan-wu[2], LI Rui[2], HU Bin[2]
(1. *Department of Electronic Information , Wuhan University, Wuhan Hubei* 430072, *China;*
2. *State Key Laboratory of Information Engineering in Surveying, Wuhan University, Wuhan Hubei* 430072, *China*)

Abstract: A security solution of H.323 net based on Recommendation H.235 and according to analysis of security problems of H.323 net was proposed. The solution provided integrity, confidentiality and authentication for H.323 net. Identity authentication which was the most important part of the security was implemented. The point was united authentication process of H.323 GK (Gatekeeper) and RADIUS server which includes User-Password authentication based on PAP protocol and Chap-Password Authentication based on CHAP protocol.

Key words: H.323; H.235; GK; identity authentication; RADIUS

随着社会的发展与进步,人们不再满足于简单的音频对话,对于多媒体通信的需求日益增加。由于分组网络低廉的成本优势和计算机的灵活控制能力,基于 IP 网络的多媒体通信业务成为了当今通信领域的发展热点之一。H.323 作为一种成熟并且已经市场化的多媒体通信协议,涵盖视频、音频和数据的传输、通信控制、网络接口等诸多方面。然而,要成为真正运营级的多媒体网络,必须严格保证通信过程的安全性,因此 H.323 视讯网的安全问题不容忽视。本文针对 IP 网络上常见的安全问题,在 H.235 的基础上,分析了如何保障 H.323网络的安全,并且实现了保障网络安全最重要的环节——身份认证,重点阐述了 H.323 GK 和 RADIUS server 联合认证过程。

1 H.323 视讯网的安全问题分析

传统的基于 ATM 的 PSTN 网络中,用户终端设备为"傻瓜"终端。每个接入网络用户均有对外公开的唯一 ID,因此在这种网络中较难发生恶意攻击,而且发生攻击时很容易追查攻击的来源。而在分组交换网中,所有的终端为智能终端,终端用户可以通过多种接入方式接入到网络,并且由于 H.323视讯网控制和承载的分离,使得用户更加难以控制。由此所带来的安全问题主要有:非法用户盗用通信网络资源;敏感信息窃取;拒绝服务攻击(攻击者通过阻塞信道来阻止合法用户接入网络);通话干扰(施放杂乱信息,或者伪装服务拒绝来发起攻击)等。而且由于大多数 H.323 信令使用动态端口,防火墙必须为 H.323 信息流开放部分端口,这也造成了安全隐患。

2 基于 H.235 建议的安全解决方案

要解决上述问题,最基本的方法就是认证和加密。因此 ITU 于 2000 年推出 H.235 建议,又于 2003 年 5 月推出 H.235v3,为基于分组网络的 H.323 系统引入安全机制。H.235 推荐了各种消息的流程、结构以及算法,用以保证 H.323 系统中信令通道、媒体控制通道和媒体流的安全。结合实际的应用,依据 H.235 建议的规定,本文实现了借助网守加强 H.323网络的安全性,从一定程度上解决了 H.323 视讯网的安全问题。

基于 H.235 协议,一般情况下,H.323 网络的安全性主要考虑以下三个方面:

1) 完整性(integrity)检查:用来保证数据在传播过程中不被更改,使用与身份认证相同的方法对整个字段进行加密,产生 cryptotoken 字段。但当 H.323 消息穿越 NAT 时,消息中的 IP 地址和端口将被改变,而 cryptotoken 是根据终端原始 IP 和端口产生的,因此这种情况下,根据 H.235v3 的规定,可以只做身份认证而不做完整性检查。

2) 保密性(confidentiality)检查:用于保护 H.323 信令及媒体流不被窃听,保证信息的私密性。使用 H.235 介绍的加

收稿日期:2005 - 09 - 03;**修订日期**:2005 - 10 - 28 **基金项目**:国家 973 规划项目(2004CB318206)

作者简介:郝洛玫(1980 -),女,甘肃庆阳人,硕士,主要研究方向: 多媒体通信; 喻占武(1969 -), 男,湖北武汉人, 教授, 博士生导师,主要研究方向:多媒体通信、视讯交换技术、分布式存储系统; 李锐(1974 -),女,湖北武汉人,助理研究员,博士,主要研究方向:多媒体通信;胡滨(1969 -),男,湖北武汉人,博士,主要研究方向:多媒体通信.

密解密技术,使得媒体流承载的真实信息无法被窃听者得到。而对于发生在呼叫开始的 H.225 信道信令,使用 TLS 或 IPSEC 协议保证信令不被窃听。交互 H.225 信令时可以实现媒体控制信道(H.245)安全参数的传递,再通过保密的 H.245 信道来传递或者使用已经确认的证书,该证书用于协商在 RTP 层媒体流的加密方式。

3) 身份认证(authentication):是用户向服务实体证明自己身份的过程,H.235 推荐的认证方式主要包括非署名认证和署名认证。非署名认证的通信实体之间在通信建立之前对对方信息一无所知,通信开始后,双方动态产生一个信息交流的私钥用以维持后续通信。署名认证包括基于数字证书的认证和基于静态密码的认证,这种方式要求通信实体双方在通信开始之前在协议之外完成部分信息交流。

3　身份认证实现过程

身份认证是 H.235 安全机制中最为重要的环节,本文着重介绍身份认证的机制及实现过程。

3.1　非署名认证

非署名认证过程中,在呼叫建立之前,GK 并不知道终端的信息,适用于 GK 允许未注册终端的呼叫,主要用于相对安全的局域网内,保护通信过程的保密性,实现对终端的控制和管理。

认证过程:

1) 终端向 GK 发送 GRQ(GatekeeperRequest)消息,该消息应当包含本地终端支持的加密算法集。

2) GK 收到 GRQ 之后检验终端加密算法集并选择可接受算法,同时,GK 产生一个与该终端共享的私钥 secret,及当前 GK 的唯一标识符 gatekeeperID,一个 16bit 的随机数 random,一并包含到 GCF(GatekeeperConfirm)消息中回送给当前认证发起终端;若 GK 收到的 GRQ 消息中未包含终端支持的加密算法集,则向当前终端发送拒绝消息 GRJ(GatekeeperReject)。

3) 终端收到 GK 发来的 GCF 之后,用与 GK 约定的加密算法进行加密(以 hash 为例,MD5(gatekeeper ID + secret)),将加密结果存入 cryptotoken 的 generalID 中;使用如下运算生成数字摘要:(random) xor (requestnum) xor (generalID),其中 requestnum 表示当前请求序列号,generalID 是上面产生的结果(需要注意的是,如果 generalID > 16bit,则只截取 generalID 的后面 8bit 与(random)xor(requestnum)的前面 8bit 相异或,产生数字摘要);generalID 与数字摘要承载在 RRQ(RegistrationRequest)消息中发送给 GK。

4) GK 收到终端发送的 RRQ 之后首先验证 gatekeeperID,采用与终端协商的密钥 secret 和加密算法进行运算,然后同 RRQ 消息中的 generalID 相比较,如果不一致则向终端发送拒绝消息 RRJ;如果上述比较结果一致则继续验证,使用 GK 保存的发送给终端的 random,提取终端当前请求序列号 requestnum,及终端发送的 generalID,采用与终端相同的方法生成摘要,将此结果与终端 RRQ 消息中的数字摘要相比较,如果一致则发送 RCF(RegistrationConfirm)消息,否则发送 RRJ(RegistrationReject)消息;RCF 的 cleartoken 域中要求包含 endpoint 和 random。

3.2　署名认证

对终端用户身份的认证,GK 可以连接后端数据库,实现 3 种方式的认证:对称密码加密认证、哈希密码加密认证及 PKI 数字签名认证。

然而,GK 作为 H.323 系统的中枢,要并发处理大量端点的呼叫控制和管理,及一些扩展服务,若要管理大量终端资料,其数据库将是非常庞大的,而认证过程中的加密、解密也给 GK 带来沉重负担,这些都使得 GK 性能下降,从而引起整个 H.323 系统性能的下降。

将终端的认证服务交由专门的认证服务器——RADIUS 服务器,GK 只需发送终端信息到认证服务器,然后根据认证结果来判定是否允许终端接入,减轻了 GK 的负担,提高了系统性能,而且 GK 可以发送一些通话信息给后端服务器,从而实现计费信息采集和记帐功能。本文采用 RADIUS 服务器及后端数据库实现用户的认证\计费,GK 不再承载用户认证(认证\计费过程如图 1 所示)。

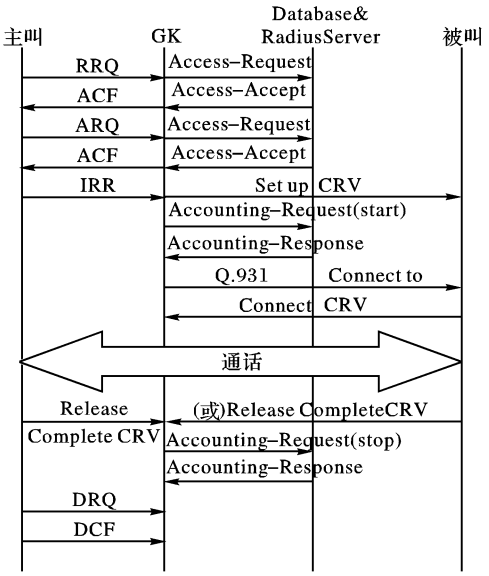

图 1　认证/计费过程

根据 RADIUS 协议的规定:针对 PAP 协议和 CHAP 协议实现两种不同模式的认证,分别对应与 RADIUS 属性域的 User-Password 和 Chap-Password 属性(RADIUS 包结构如图 2 所示)。

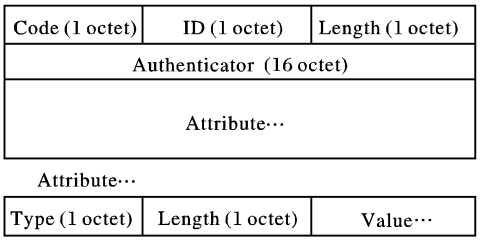

图 2　RADIUS 包结构

3.2.1　基于 PAP 协议的 User-Password 认证

认证前提包括:1)终端拥有一个唯一标识符 generalID,并且保存在 RADIUS 服务器后端数据库中,终端对该 generalID 已知,同时终端拥有多个别名 Alias;2)终端拥有与本终端唯一标识符 generalID 相对应的私钥 password,并且保存在 RADIUS 服务器后端数据库中,GK 对对应于该终端多个别名的固定私钥 password 已知;3)RADIUS 服务器及其客户端 NAS(GK 在这里充当 NAS)对用来实现数字签名的公钥 secret 已知。

认证过程:

1) 终端向 GK 发送 GRQ 消息。

2) GK 向终端发送 GCF 消息。

3) 终端向 GK 发送 RRQ 消息(包含终端 generalID、终端

别名和一些配置信息),GK 检验该终端 generalID 及终端别名,如果该终端在 GK 中配置了固定别名 fixusername,则 GK 使用该 fixusername 填充 RADIUSPDU 属性域的 Username 字段,若未配置固定别名,则使用 RRQ 中的 generalID 填充(通常 fixusername 和 generalID 一致)。GK 使用对应于当前终端的固定私钥 password 填充 RADIUSPDU 属性域的 UserPassword 字段,password 属于客户敏感信息,因此不应当以明文方式在网路上传送,因此以密文填充 UserPassword 字段。

加密算法如下(以哈希为例):

将用户私钥 password 后位补零,补至 16 字节,结果设为 p1,以[MD5(secret + RA)] xor p1 填充 UserPassword 字段;若 password 长度大于 16 字节,将其以 16 字节为单位划为若干块 p1,p2,…,最后一块若不足 16 字节则以 0 补齐,加密文本块称作 c1,c2,…,中间结果称作 b1,b2…,做如下运算(RA 表示 RADIUS 认证字 Authenticator):

b1 = MD5(secret + RA) c1 = p1 xor b1

b2 = MD5(secret + c1) c2 = p2 xor b2

…

依此类推,最终填入 UserPassword 字段的结果为:c1 + c2 + …;

GK 向 RADIUS 服务器 1812 端口发送 Access-request 消息,除了用以认证的 Username 字段和 UserPassword 字段外,还应包含多种配置信息。

4) RADIUS 服务器收到来自 GK 的 Access-request 消息后依据 Username 字段查询后端数据库,检查该用户是否存在,若不存在则发送 Access-reject 消息。

若该用户存在,则以上述加密算法以相反的方向使用共享密钥 secret 对收到的 Access-request 消息的 UserPassword 字段解密,得到该用户的原始密码 password,接着在数据库中查询该用户密码与解密得到的密码进行比较,若比较结果不一致则发送 Access-reject 消息,若一致则发送 Access-accept 消息(包含终端配置信息)。

5) GK 若收到 Access-reject 消息,则向终端发出拒绝消息 RRJ;若收到 Access-accept 消息,则向终端发送 RCF,允许该终端接入。

6) 终端收到 RCF 后,向 GK 发送包含主、被叫信息的通话请求消息 ARQ。

7) GK 再次向 RADIUS 服务器发送 Access-request 消息,请求进一步认证,认证过程和前一次类似,增加了部分主、被叫信息。RADIUS 服务器根据验证结果发送 Access-reject 或 Access-accept 消息。

8) GK 若收到 Access-reject 消息,则向终端发出拒绝消息 ARJ;若收到 Access-accept 消息,则向终端发送 ACF,允许该终端建立通话过程,认证结束。

3.2.2 基于 CHAP 协议的 Chap-Password 认证

认证前提包括:1)终端拥有一个唯一标识符 generalID,并且保存在 RADIUS 服务器后端数据库中,终端对该 generalID 已知;2)终端拥有与本终端唯一标识符 generalID 相对应的私钥 password,并且保存在 RADIUS 服务器后端数据库中,终端对该 password 已知;3)RADIUS 服务器及其客户端 NAS(GK 在这里充当 NAS)对用来实现数字签名的公钥 secret 已知。

认证过程:

1) 终端向 GK 发送 GRQ 消息,该消息应当包含本地终端支持的加密算法集,终端支持认证方式集。

2) GK 收到 GRQ 之后检验终端加密算法集并选择可接受算法(以 hash 为例),并为终端选择 RADIUS 认证方式,向终端发送 GCF。

3) 终端收到 GCF,产生注册请求消息 RRQ,RRQ 消息的 taken 域中应包含:generalID;用来产生 challenge 的唯一不重复 timestamp;产生此次 challenge 的随机序号 random(一个字节);用来保护密码的 challenge, challenge = MD5(random + password + timestamp)。

4) GK 收到 RRQ 消息后,检查 taken 域,提取其中的 generalID 填充 RADIUS 属性域的 User - name 字段;random + challenge 填充 RADIUS 属性域的 Chap - Password 字段;timestamp 填充 RADIUS 属性域的 Chap - Challenge 字段,若该 timestamp 为 16 字节,也可用其填充 RADIUS 认证字 Authenticator;GK 向 RADIUS 服务器 1812 端口发送 Access-request 消息,该消息包含终端支持的协议,IP 地址等多种配置信息。

5) RADIUS 收到来自 GK 的 Access-request 消息后,检索数据库查找该用户是否存在,若不存在则发送 Access-reject 消息;若存在则检索数据库获得对应于 generalID 的用户私钥 password,提取 Access-request 消息的 Chap - password 字段的 random(1 字节),提取 Chap - Challenge 值(即上述 timestamp),该字段不存在则提取 RADIUS 认证字 Authenticator,做如下计算 MD5(random + password + timestamp),将计算结果与 Chap - password 字段 value 域的后 16 个字节相比较,若相同则发送包含配置信息的 Access-accept 消息,否则发送 Access-reject 消息。

6) GK 若收到 Access-reject 消息,则向终端发出拒绝消息 RRJ;若收到 Access-accept 消息,则向终端发送 RCF,允许该终端接入。

7) 终端收到 RCF 后,向 GK 发送包含主、被叫信息的通话请求消息 ARQ。

8) GK 再次向 RADIUS 服务器发送 Access-accept 消息,请求进一步认证,认证过程和前一次类似,增加了部分主、被叫信息。RADIUS 服务器根据验证结果发送 Access-reject 或 Access-accept 消息。

9) GK 若收到 Access-reject 消息,则向终端发出拒绝消息 ARJ;若收到 Access-accept 消息,则向终端发送 ACF,允许该终端建立通话过程,认证完成。

3.2.3 结果分析

上述两种认证过程通过检验 RADIUS 认证字 Authenticator,保证 RADIUS 响应消息的安全性:GK 发送的 RADIUS 认证请求包,使用 16 字节随机数填充 RequestAuthenticator 域;RADIUS 收到认证请求包后,创建 RADIUS 认证响应包,Length 表示该包的长度,使用 MD5(Code + ID + Length + RequestAuthenticator + Attributes + Secret)填充 ResponseAuthenticator 域;GK 收到 RADIUS 响应包后首先检验认证字 Authenticator,将使用上述相同方法的计算结果与 ResponseAuthenticator 相比较,若不一致则丢弃该包,若一致,则检验包信息。

(下转第 351 页)

区和可变区组成。不变区包括固定的信息,如进程的名字、进程的路径、文件的长度、资源类型等,可变区是二进制化的系统资源使用情况的离散序列,长度可变。初期形成的抗体,根据阴性选择原理,经过自体耐受期后,被释放到模拟的考试过程中执行检测任务,在检测到非我抗原后,该抗体进行克隆选择,经过几次重复的阴性选择和克隆选择后,不断的进化,最终形成成熟的检测体集合。免疫考试系统中检测器的识别演化过程加入到动态安全模块中,就构成了动态安全模块如图 3 所示。

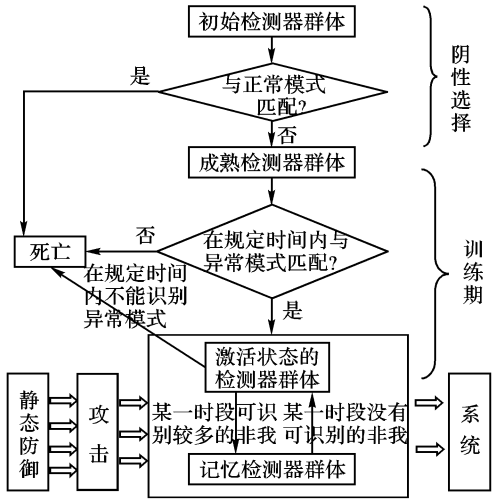

图 3　自适应的生物免疫动态防御子模块

在免疫网络安全考试系统中,关键是要准确及时地识别“自我”和“非我”,这个过程由检测器完成。考试系统中的“自我”和“非我”是动态变化的,因此检测器群体也在不断地发生变化,并相互协调保证了考试系统不断地应对外部环境的变化,更好地防御外来入侵。

在免疫网络安全考试系统中,检测器对已知的异常情况的识别是采用 R - 邻近匹配算法通过模式匹配来完成的。

这样,经过不断的进化,考试免疫系统可以自适应地最大程度地保证考试的安全。由于检测数据对于本系统的检测和分析极为重要,不仅需要检测其是否受到破坏,还要进行恢复,所以需要加密并采用分布式的数据存储方法以保证数据本身的安全。

由上所述,自适应的生物免疫动态子模块利用阴性选择和生命周期等机制,使各个检测器群体随着考试的外界环境的变化而不停地演化,从而自适应地保护了网络考试系统的安全。

3　结语

本文提出了将静态防御技术和融入免疫技术的动态防御技术相结合的方法用来保护考试系统的安全,使系统能自适应地防御外来的异常情况。当然如何更好地应对外来的异常情况还有很多问题有待解决,如怎样提高检测的准确性和及时性,在免疫机制中如何提高整个系统的自适应性,如何更好地实现安全系统的动态平衡,如何在复杂的变化的网络数据中识别各种异常模式等都是以后需要解决的问题。

本系统已应用于四川师范大学教育网格系统中,运行半年,效果良好。

参考文献:

[1] FORREST S, HOFMEYR S. Computer Immunology[J]. Communications of the ACM, 1997, 40(10): 88 - 96.

[2] HOFMEYR S, FORREST S. Immunity by design: An artificial immune system[Z]. GECCO'99, San Francisco, CA, 1999.

[3] HOFMEYR S, FORREST S. Architecture for an artificial immune system[J]. Evolutionary Computation, 2000, 8(4): 443 - 473.

[4] FORREST S , HOFMEYR S . Design Principles for Immune Systems&Other Distributed Autonomous systems[A]. Segal L A. and Cohen I R. eds. Oxford univ. press[C]. 2000.

[5] HOFMEYR S. An immunological model of distributed detection and its application to computer security [PH D dissertation][D]. University of New Mexico, Albuquerque, 1999.

[6] GONZALEZ D. An immunogenetic approach to intrusion detection [D]. The University of Memphis, Tech Rep: CS - 01 - 001, 2001.

[7] NINO D. A comparison of negative and positive selection algorithms in novel pattern detiction[A]. The IEEE Int'l Conf on Systems, Man and Cybernetics(SMC)[C]. Nashville, 2000.

[8] BENTLEY K. Investigating the roles of negative selection and clonal selection in an artificial immune system for network intusion detection[A]. The special Issune on Artificial Immune Systems in IEEE Transactions of Evolutionary Computation[C]. 2001.

[9] BENTLEY K. Towards an artificial immune system for network intrusion detection: An investigation of clonal selection with a negative selection operator[A]. The Congress on Evolutionary computation (CEC - 2001)[C]. Seoul, Korea, 2001.

(上接第 348 页)

基于 PAP 的 User-Password 认证使得用户能够以不同的别名在同一终端上登陆,但是为了防止用户私钥 password 以明文方式在网路上传输,需在 GK 上保存该终端的私钥,增加了 GK 的开销。基于 CHAP 的 Chap-Password 认证对用户私钥全程加密,安全性较高,并且 GK 不需知道用户密码,减轻了 GK 的负担,但是终端用户只能以唯一的合法用户名登陆。实际应用中可根据需要选取合适的认证方式进行用户身份的认证。

4　结语

本文针对 H.323 网络的特点,在采用 H.235 机制基础之上,分析了如何对各种 H.323 信令及媒体流进行安全保护,重点阐述了用户身份认证的各种实现过程,经测试,运行效果良好,对 H.323 视讯网实现运营的安全考虑有一定的参考价值。值得注意的是,信令及媒体流的加密解密造成的时延对实时性要求较强的多媒体通信来说有一定的影响,如何选择高效并且安全的加密算法应当是安全问题中值得研究的另一个方面。

参考文献:

[1] H.235 Version 3. Security and Encryption for H-series (H.323 and other H.245-based) Multimedia Terminals[s].

[2] H.323 Version 5. Packet-based Multimedia Communication systems [s]. 1997.

[3] RIGNEY C, WILLENS S. Remote Authentication Dial In User Service (RADIUS)[S]. RFC 2865, June 2000.

[4] RIGNEY C. RADIUS Accounting[S]. RFC 2866, June 2000.

[5] HUANG Y-F, DENG Z, LI X. Security Issues in VOIP Based on H.323[J]. 武汉大学学报(自然科学版), 2004, 9(4): 420 - 424.