Software Engineering and Applications 软件工程与应用, 2015, 4(6), 148-153
Published Online December 2015 in Hans. http://www.hanspub.org/journal/sea
http://dx.doi.org/10.12677/sea.2015.46019

Hans汉斯

Research on Security Authentication Protocol for Network Connection Control System

Lijia Yang, Qiuxi Zhong, Xiangyu Yan

College of Computer Science, National University of Defense Technology, Changsha Hunan
Email: 124589553@qq.com

Received: Dec. 9th, 2015; accepted: Dec. 23rd, 2015; published: Dec. 29th, 2015

Abstract

Based on the analysis of network security transmission technology, this paper designed a network security transmission system framework which was used in application circumstance, and proposed a set of corresponding security authentication protocol, then analyzed the security of the authentication protocol which might be attacked in the net.

Keywords

Network Security, Authentication, Network Connection Control System

面向网络互联安全控制系统的安全认证协议研究

杨力嘉，钟求喜，燕翔宇

国防科学技术大学计算机学院，湖南 长沙
Email: 124589553@qq.com

收稿日期：2015年12月9日；录用日期：2015年12月23日；发布日期：2015年12月29日

文章引用: 杨力嘉, 钟求喜, 燕翔宇. 面向网络互联安全控制系统的安全认证协议研究[J]. 软件工程与应用, 2015, 4(6): 148-153. http://dx.doi.org/10.12677/sea.2015.46019

摘　要

在分析网络安全传输技术基础上，针对网络互联安全控制系统应用场景设计了一个网络安全传输系统框架，提出了一套相应的安全认证协议，并对安全认证协议进行了网络攻击的安全性分析。

关键词

网络安全，认证，网络互联安全控制系统

1. 引言

随着互联网技术的迅猛发展，网络规模的不断扩大，网络给人们带来不少便利，网络信息安全问题也日益突显。如何抵御来自网络的各种攻击，让信息在互联网中安全传输成为网络应用的关注点，网络信息安全技术也一直成为研究热点。自 2013 年美国“棱镜”计划曝光以来，网络安全问题更上升到国家战略安全层面。

目前各大企业部门为保证网络信息安全，大多采用防火墙隔离方法。通过这种方法，虽然可以建立一个较为安全的内部局域子网络，网内信息交互安全也可以得到较好的保证，但是对于跨越子网络的信息传输安全此方法则显得无能为力。信息安全传输技术就是为解决这类问题而出现的网络安全技术，其主要负责保护信息在网络传输过程中的安全，防止信息被非法用户获取或窜改。利用该技术所实现的信息安全传输系统(以下简称安全传输系统)目前已被广泛应用到各个领域。

网络互联安全控制系统(以下简称安全控制系统)作为安全传输系统的核心硬件设备，是一台处于外网与子网(安全网络)之间，起着网关兼防火墙作用的安全控制设备。它依据逻辑隔离条件下的数据共享传输需求，面向局域网络的受控接入和互联控制，监控进出子网的报文并进行报文进出控制，达到信息安全控制与传输安全的目的。

安全传输系统为保证信息的安全传输，在进行报文传输之前，必须对整个系统的硬件设备进行安全认证，以确保信息发送者和接收者的身份真实性。安全认证的核心为安全认证协议，安全认证协议以密码学为支撑，是一套在特定的网络拓扑结构下，依赖相关的网络安全设备，检验网络设备之间的身份真实性的网络协议规范。它的最终目标是保证设备之间交换信息的真实性和不可否认性。为了达到以上目标，安全认证协议会涉及到设备之间的信息交换，可信第三方或者会话服务器的参与，根据认证的流程和方式不同，安全认证协议可分为具有可信第三方的对称密钥协议、无可信第三方的对称密钥协议、具有第三方的公开密钥协议、无可信第三方的公开密钥协议、应用密码校验函数的认证协议和对称密钥重复认证协议六类。目前比较主流的认证协议有 RADIUS、TACACS、Kerberos 等认证协议。

本文以跨网络信息安全传输为应用背景，设计一套信息安全传输系统，提出一套安全认证协议并进行协议的安全评估，以保障信息安全传输。

2. 基于网络互联安全控制系统的信息安全传输系统框架设计

信息安全传输系统是为解决网络信息传输安全问题而设计的一套完整的安全系统，其结构如图 1 所示。

硬件层为整个系统提供硬件支撑，主要包括网络架构和硬件设备两部分。网络架构即整个系统的网络拓扑结构，是由实际应用需求所决定；硬件设备主要由信息终端、路由设备和网络互联安全控制系统组成，其中网络互联安全控制系统为硬件层的核心部件。

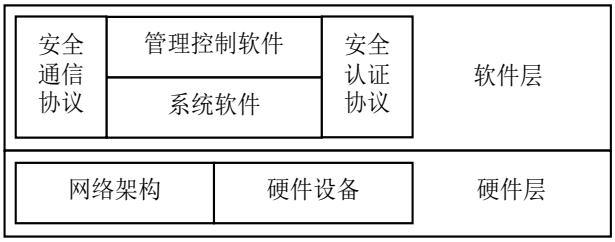

Figure 1. Architecture of secure transmission system
图 1. 安全传输系统体系结构

软件层负责整个系统的运行与管理，并为用户提供友好的交互界面。其内部又可分为系统软件、管理控制软件和安全协议，系统软件直接与硬件交互，为管理控制软件提供运行平台；管理控制软件负责与用户进行交互，并根据用户的指令对整个系统进行管理和控制；安全协议为系统各个设备之间信息交互提供通信规范，它的最终目的是实现网络信息传输的保密性、完整性和真实性，安全协议由安全认证协议和安全通信协议组成，安全认证协议负责验证信息交互的设备真实性并完成对通信密钥的交换，安全通信协议负责信息传输过程中的安全性。

本文针对跨网络信息传输的实际安全需求，基于网络互联安全控制系统为核心，结合互联网相关技术，设计一个安全传输系统框架，其总体结构如图 2 所示。

安全控制系统 B 安装在内部安全网 1 与外部网络之间，负责内部网 1 的边界安全；安全控制系统 C 安装在内部安全网 2 与外部网络之间，负责内部网 2 的边界安全。如果终端 A 与终端 D 需要通信，由于两个终端不在一个内部网络中，所以必须通过外部网络传输实现，A 首先与安全控制系统 B 建立会话并将信息发送至 B，然后 B 与 C 利用安全隧道技术[②]建立安全会话通道，通过安全会话通道将信息发送至 C，最后信息通过 C 发送至目标终端 D，整个传输流程完成。B 与 C 通信期间虽然跨越了外部网络，但是由于使用了安全会话通道，因此传输信息的安全性得到保证，通过整个传输过程，信息可以安全的在 A 与 D 之间交互，就好像两个终端处于同个安全子网中传输一样。

安全传输系统在正常运行前，必须对系统中所有设备的身份真实性进行认证。对通过身份认证的设备，系统对其提供正常服务，如果发现身份无法通过的设备，该系统会拒绝该设备接入，并发出报警，因此安全认证对安全传输系统至关重要。

3. 安全认证协议设计与安全性分析

针对安全传输系统框架的应用需求，本文设计一套安全认证协议，用以检测系统设备身份的真实性。认证协议利用高效率传输的 UDP 协议进行通信，并采用签名应答机制防止报文错误和丢包现象出现，如果认证过程中的任何流程环节出现报文错误或丢包现象，认证设备之间将会重启一个新的认证流程并对失败认证进行计数，失败次数超出阈值即判定认证失败。因为内部网络和外部网络安全风险及应用需求的不同，两种网络分别采用两种认证方式：内部网络中，终端和安全控制系统之间的认证采用以用户为认证主体的基于用户口令的双向认证方式；外部网络中，安全控制系统与安全控制系统之间采用以设备为认证主体的基于数字证书的双向认证方式。

3.1. 基于用户口令的双向认证协议

基于用户口令的双向认证，采用无可信第三方的对称密钥认证方法。协议要求参与主体双方都事先共享只有他们两人知道的秘密信息，并且知道秘密信息与协议主体的对应关系。

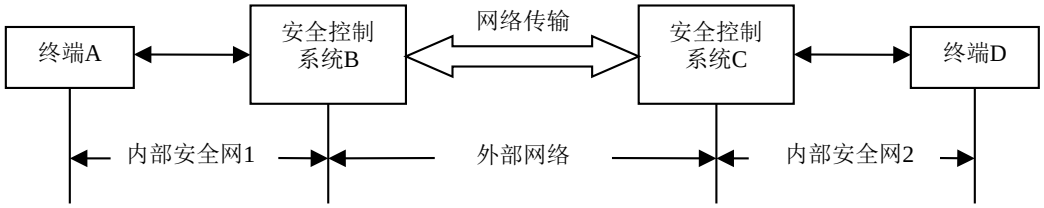

Figure 2. Framework of network security transmission system
图 2. 网络互联安全传输系统框架结构

3.1.1. 协议流程

(1) ClientHelloA→B: A, B, ($N_A \oplus K_{AB}$), H(A, N_A, K_{AB})

(2) ServerHelloB→A: B, A, ($N_B \oplus K_{AB}$), H(B, N_B, K_{AB}, N_A)

(3) ClientFinishA→B: A, B, H(N_A, N_B, K_{AB})

3.1.2. 符号说明

A, B: 协议主体 ID，代表认证双方的身份标识。

N_A, N_B: A, B 产生的随机数。

H(…): 基于密钥的哈希函数，对括号内的数据求哈希值。

K_{AB}: A、B 预先共享的秘密信息，为用户 A 的口令哈希值，即 K_{AB} = H(A_password)。

(a⊕b): 操作数 a 和操作数 b 的异或值，所得结果与操作数 a 字节位数相同。

3.1.3. 协议分析

(1) 通过 ClientHello，B 可利用共享的 K_{AB} 获得 N_A，计算 H(A, N_A, K_{AB})，并与其收到的哈希值比较，如果匹配，那么 B 确信 NA 是有效的。

(2) 通过 ServerHello，A 可利用共享的 K_{AB} 获得 N_B，计算 H(B, N_B, K_{AB}, N_A)，并与其收到的哈希值比较，如果匹配，那么 A 确信 B 生成和发送了这个包含可信任信息新鲜标识符 N_A 的哈希值，因为只有 B 和 A 拥有共享秘密 K_{AB}。因此 B 的主体活现性得到了认证，消息的新鲜性得到了保证。

(3) 通过 ClientFinish，B 确认了 A 的主体活现性，消息的新鲜性得到了保证。

综上所述，协议运行结束后，确认了 A, B 主体活现性、消息的新鲜性，达到了双向认证的安全目标。

3.2. 基于数字证书的双向认证协议

3.2.1. 协议流程

(1) ClientHello A→B: $Cert_A$, A, N_A, [A, N_A] K_A^{-1}

(2) ServerHello B→A: $Cert_B$, {B, N_B, N_A, [B, N_B, N_A] K_B^{-1} }K_A

(3) ClientFinish A→B: {A, N_{A1}, N_B, [A, N_{A1}, N_B] K_A^{-1} }K_B

(4) ServerFinish B→A: {N_{A1}, [N_{A1}] K_B^{-1} }K_A

3.2.2. 符号说明(未提及符号参照基于口令的认证协议)

$Cert_A$, $Cert_B$: A，B 的数字证书。

K_A，K_A^{-1}: A 的公钥和私钥。

K_B，K_B^{-1}: B 的公钥和私钥。

N_{A1}: A 产生的不同于 N_A 的随机数。

{…}K: 使用密钥 K 对{}中的消息进行加密。

[…]K: 使用密钥 K 对[]中的消息进行签名。

3.2.3. 协议分析

(1) 通过 ClientHello，B 只能确定消息是用证书 $Cert_A$ 的私钥签名的，但不能进一步确定其他信息。

(2) 通过 ServerHello，A 确信收到的消息是新鲜的，确认了 B 的活现性，B 的身份验证通过。

(3) 通过 ClientFinish，B 确认收到的消息是新鲜的，确认是与真实的 A 进行通信，保障了 A 的活现性。

(4) 通过 ServerFinish，A 再次确认收到的消息是新鲜的，是与真实的 B 进行通信，B 是活现的。

综上所述，在协议双方确认 A 的证书为 $Cert_A$，B 的证书为 $Cert_B$ 的前提下，协议运行结束后，确认了 A、B 主体活现性、消息的新鲜性，同时协议生成的 N_{A1}，N_B 具有保密性、新鲜性③、主体关联性，具有双向认证安全、双向密钥协商安全、双向密钥传输安全。另外，通过共享的 N_{A1}，N_B 作为密码材料，可生成用于安全控制设备之间建立安全通道的密钥，用于保护安全通道的参数协商。

3.3. 协议安全性分析

当今互联网络环境变幻莫测，网络攻击处处存在，安全认证协议设计的最终目的也是为了应对来自网络的各种威胁，目前针对认证协议的攻击主要有重放攻击和中间人攻击两种。

3.3.1. 重放攻击

重放攻击[1]又称重播攻击、回访攻击或新鲜性攻击，是指攻击者发送一个目标主机已接收过的数据报文，来达到欺骗系统的目的。攻击者还可利用重放方式大规模地发送数据报文，侵占目标主机的正常带宽和系统资源，导致正常的服务响应延迟或者中断，最终达到拒绝服务的目的。

针对重放攻击行为，本文中的两种认证协议均采用随机数验证的方式进行防御，即两种协议中的 N_A, N_B, N_{A1} 三个随机数既有作为密码材料的功能，又起着抵御重放攻击的作用。目标主机可以针对收到的随机数建立一个随机数缓存表，在一定时间内，收到相同随机数的同类报文，目标主机可直接予以丢弃，不予理睬，已达到防御重放攻击的目的。

3.3.2. 中间人攻击

中间人攻击[2]是一种“间接”的入侵攻击，这种攻击模型是通过各种技术手段将攻击计算机虚拟地放置在两台通信计算机之间，通过伪造数据报文的方式与两台通信计算机通信，使得两台通信计算机误认为通信正常，而攻击者从中获取有用信息。

抵御中间人攻击的最有效方式是让攻击者无法伪造通信双方的数据报文，在基于口令的认证协议中，由于中间人不知道用户口令，即无法获取 K_{AB} 值，因此，$(N_A \oplus K_{AB})$，$H(A, N_A, K_{AB})$, $(N_B \oplus K_{AB})$, $H(B, N_B, K_{AB}, N_A)$, $H(N_A, N_B, K_{AB})$字段也无法伪造，从而达到防御的目的；在基于数字证书的认证协议中，由于 K_A^{-1}，K_B^{-1} 只有 A 和 B 两个设备知道，那么攻击者也无法伪造$[A, N_A] K_A^{-1}$, $[B, N_B, N_A] K_B^{-1}$, $[A, N_{A1}, N_B] K_A^{-1}$, $[N_{A1}] K_B^{-1}$ 字段，至使中间人攻击失败，最终保证信息的真实性。

4. 结语

近些年互联网的高速发展，网民人数越来越多，特别是移动终端的普及，对网络的安全性提出了更高更特殊的要求，在这种背景下，改进和设计新的认证协议以适应新的网络环境成为网络技术中研究的重要问题，目前许多安全认证协议都具有各自的特点，能够在特殊的环境中起着良好的保护效果，但是一些比较通用的认证协议在某些特殊领域安全防护性相对较差。由此可见，未来安全认证协议的发展必然会根据不同领域的实际需求量身定做，设计出适用于该领域的真正有效的安全认证协议。

基金项目

国家自然科学基金(编号：61202482)。

参考文献 (References)

[1] 陈建熊, 孙乐昌. 认证测试对分析重放攻击的缺陷[J]. 计算机应用研究, 2009, 26(2): 739-741.

[2] 唐祚波, 缪祥华. 一种三方认证密钥协商协议的分析与改进[J]. 计算机工程, 2013, 39(1): 140-143.

注释

①AAA：即认证(Authentication)、授权(Authorization)和计费(Accounting)的简称，是一种对访问进行控制的安全管理机制，提供认证、授权和计费三种安全服务。

②安全隧道技术：是以加密技术为基础，利用一种网络协议传输另一种网络协议或私密数据的技术。发送者对待传输的原始信息进行加密和协议封装处理后，再作为数据嵌套装入另一种协议中而后发给接收者，接收者收到信息后通过协议解析、信息解密等手段获得原始信息。信息在网络中传输时始终处于加密状态，因此经过这样处理后的信息只有发送者和接收者能够解释和处理，对其他用户来说毫无意义，而从达到保护信息安全性的目的。

③新鲜性：即信息是通信双方通信即时产生的。