

一种新的网络接入控制方法及其认证会话性能分析

刘 伟¹⁾ 杨 林²⁾ 戴 浩^{1),2)} 侯 滨²⁾

¹⁾(解放军理工大学指挥自动化学院 南京 210007)

²⁾(中国电子系统设备工程公司 北京 100039)

摘 要 随着网络规模不断膨胀,网络安全问题日益突出,如何构建可信网络已成为当前的研究热点.可信网络的核心技术之一是用户、设备的接入认证及管理.该文分析了网络接入技术的现状,提出了一种新的可信网络接入控制方法,重点对方法中认证会话的失败概率进行了理论分析与模拟仿真,用以指导接入控制设备中软、硬生命周期参数的设置,该方法结合了现有的数字证书机制的优点,可以有效提高网络接入的可控可管性.

关键词 可信网络;认证;网络接入控制;软生命周期;硬生命周期

中图法分类号 TP393

A New Network Access Control Method and Performance Analysis of Authentication Session

LIU Wei¹⁾ YANG Lin²⁾ DAI Hao^{1),2)} HOU Bin²⁾

¹⁾(College of Command Automation, PLA University of Science and Technology, Nanjing 210007)

²⁾(Institute of China Electronic System Engineering, Beijing 100039)

Abstract With the constantly expansion of network scale, the problems of network security become more and more intractable. Currently, how to establish trusted network has been a research hotspot. One of the key technology of trusted network is access authentication and management to users and devices. This paper analyses the status quo of trusted network access control technology, puts forward a new method for network access control, the emphases is on the theoretic analyses and simulation on the probability of authentication session failure, so as to direct the parameters setting in the access control device. The new method combines the merits of digital certificate and can effectively promotes the control-ability and manageability of network.

Keywords trusted network; authentication; network access control; soft-life time; hard-life time

1 引 言

管,网络中的病毒、木马、恶意入侵行为层出不穷,严重影响了网络的正常运行.因此如何提高网络的管控性是近年来可信网络的研究热点之一^[1-2]①.

目前,由于缺乏有效的用户身份认证和行为监

典型的网络接入控制技术主要有思科的网络准

收稿日期:2007-05-07;修改稿收到日期:2007-07-23.本课题得到国家预研基金(513150604)资助.刘 伟,女,1979年生,博士研究生,主要研究方向为网络安全. E-mail: xflw1001@163.com. 杨 林,男,1970年生,博士,研究员,博士生导师,主要研究领域为信息安全. 戴 浩,男,1945年生,博士生导师,中国工程院院士,主要研究领域为网络工程与网络安全等. 侯 滨,女,1970年生,高级工程师,研究方向为网络安全.

① 蒋屹新.从可信计算到可信网络. http://media.ccidnet.com/art/2617/20060512/551589_1.html

入控制(Network Admission Control, NAC)技术^①、微软的网络接入保护(Network Access Protection, NAP)技术^②以及 TCG 组织的可信网络连接(Trusted Network Connection, TNC)技术^③。上述三种技术本质上都是采用两元三实体的结构。以 TCG-TNC 为例,其架构中有三类逻辑实体:网络访问请求者(Access Requestor, AR)、策略执行点(Policy Enforcement Point, PEP)、策略决策点(Policy Decision Point, PDP)。TCG-TNC 在实现时,网络接入层采用的传统方法是 IEEE 802.1x。802.1x 主要用于用户到网络的认证,是一种两元结构,接入控制设备(即对应的策略执行点)并不参与到网络与用户认证的过程中,仅起到传输、中转认证消息的功能,这种两元的认证方法很容易引入安全风险,已有文献^[3-4]指出 IEEE 802.1x 存在安全漏洞,例如存在针对 EAP-success 消息的中间人攻击,并被形容为是一条“马其诺防线”。此外,802.1x 不支持证书机制,从而丧失了证书机制的安全特点。

为了强化无线网络接入认证控制,Ana Sanz Merino 等人^[5]开发了一种结合链路层和 Web 认证的方法,使用加密的方式保护用户对公共无线局域网的访问。用户首先使用 IEEE 802.1x 中的账号来建立一个链路层会话密钥,然后将其摘要值嵌入到 Web 认证中。Gianluigi Me 等人^[6]提出了一种接入认证系统,它整合了挑战/响应过程和一次性口令,由认证服务器发出挑战,移动设备通过固定终端与系统中的其它设备通信,移动设备一旦被接受,就必须与 Web 站点或应用进行认证。Manabu Hirano 等人^[7]提出了一个简单的设备认证框架,目的在于提供面向设备的认证与授权机制,这些设备是指除计算机之外的、在网络中处于就绪状态的一些信息设备,例如,打印机。作者在智能卡上开发了一种新的软件,实现了对等的基于公钥基础设施(Public Key Infrastructure, PKI)的认证与授权。美国国防部也在积极开展基于 PKI 的认证机制一体化的工作^[8]。在有线网络的接入控制中,最流行的方法是使用有线通用接入卡(Wired Common Access Card, 简称 CAC)读卡器实现网络对终端用户的认证或计算机对用户的认证。但上述技术都是针对初始接入前的认证过程,没有涉及接入后的认证和保护机制,即无法确保终端用户的持久可信性。

本文利用 Web 认证技术并基于数字证书机制设计了一种新的接入控制方法,使得三个实体都参

与认证过程,访问请求者必须先经策略执行者认证后,才能进行下一步的认证过程。更重要的是,在本文所提出的接入控制方法中,强调通过接入控制设备定时验证接入认证设备与用户之间共享密钥的方式,实现对入网之后的用户进行持续可信性验证,以有效地解决用户的身份认证、授权访问,防止假冒用户等问题,进一步提高网络的安全性、可控可管性。

2 一种新的网络接入控制方法

新的网络接入控制方法如图 1 所示。

整个接入控制过程简述如下:用户通过插入证明自身身份的 USB-KEY(X. 509 数字证书)登录计算机,基于网络接入认证协议(Network Access Authentication Protocol, NAAP),终端用户将其数字证书与入网请求一同发送给接入控制设备,以验证请求上网的终端用户身份,身份认证通过后,接入控制设备通过授权管理协议(Authorization Management Protocol, AMP)与授权管理服务器交互,验证用户是否具有入网权限,并根据用户的身份设定相应的入网权限。只有通过了认证与授权的用户,方可接入受保护网络。用户接入网络之后,接入控制设备通过定时验证共享密钥的方式来确认联网用户身份的可信性,一旦发现假冒用户,便断开网络连接。当用户退网后,接入控制设备将用户的上网情况记入日志,上报授权管理服务器,以便对用户的上网行为进行审计与管理。在本方法中,接入控制设备实际上是集 PDP 与 PEP 的功能于一身,既有策略执行功能又有策略决策功能。

为提高网络的可控可管性,确保接入网用户身份的可信性,本文采用了定时验证共享密钥的方式,在接入控制设备与用户之间进行定期的认证会话。接入控制设备中设有软生命期和硬生命期两类计时器。其中,软生命期表示接入控制设备对网内的终端用户发送认证请求消息的时间间隔,即软生命期结束时,接入控制设备再次对入网的终端用户发出认证请求消息,同时,软生命期计时器清零,并等待终

① Cisco Company. Cisco network admission control. <http://www.cisco.com/en/US/netsol/ns617/>, 2006

② Microsoft Corporation. Network access protection platform architecture. <http://www.microsoft.com/technet/network/nap/>. 2006, 12

③ Trusted Computing Group. TCG specification trusted network connect TNC architecture for interoperability revision 1.1. <http://www.trustedcomputinggroup.org>. 2006, 5

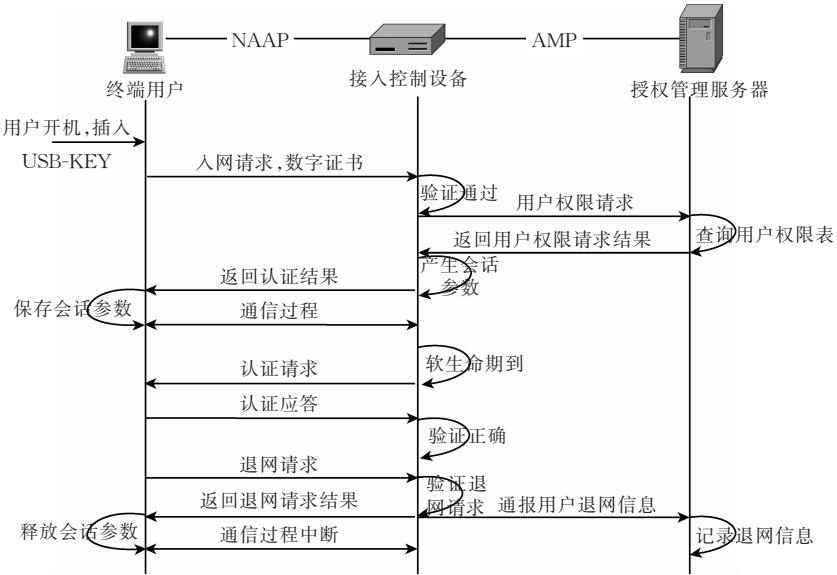


图 1 新的网络接入控制方法

端用户的应答;硬生命期表示接入控制设备等待终端用户应答消息的最大时间间隔,当硬生命期结束时,接入认证设备将断开网络与终端用户的连接.当用户端收到认证请求消息后,便会给接入控制设备返回一个认证应答的消息,当接入控制设备成功地接收到一个终端用户的应答消息后,其硬生命期计时器清零.如果在接入控制设备的硬生命期结束时,仍未收到终端用户的应答消息或终端不能做出正确响应,此次认证会话结束,接入控制设备断开用户与网络的连接,用户将不能够访问网络资源.

采取认证会话机制能否及时、有效地发现假冒用户身份的行为,关键在于接入控制设备中硬生命期、软生命期等参数的取值,如果选取的时间间隔过长,则不能有效地保证用户身份的可信性,因为在此时间间隔,假冒用户可能已经对网络造成了破坏,也就失去了认证会话的意义;而如果时间间隔过短,将会加重网络负载,影响终端用户的应用.因此,本文借鉴 BGP(Border Gateway Protocol)会话与 BGP 计时器、TCP 报文重传的分析方法^[9]给出认证会话失败概率与接入控制服务器中软、硬生命期等参数之间的关系,以此来指导实际中各参数的设置.

3 认证会话性能分析

由于认证会话对于下层的可靠性很敏感,传输层的故障会直接导致认证会话失败,本文将分别讨论两种不同的传输机制(即 TCP 和 UDP)对认证会话的影响.文中所用到的符号定义如表 1 所示.

表 1 主要符号含义

$\langle s,u \rangle$	接入控制设备 s 与终端用户 u 之间的认证会话
ΔT_s	接入控制设备的软生命期
ΔT_h	接入控制设备的硬生命期
T_e	链路出现故障的时刻
ΔT_r	链路故障修复时间的平均值
RTT	往返时间
i	第 i 次重传
i'	硬生命期结束之前的最后一次重传
$T_r(i)$	第 i 次重传的时刻
p_s	认证会话失败概率
$\Delta T'$	采用 UDP 传输机制时发送认证请求消息的时间间隔

3.1 采用 TCP 传输机制

设认证会话发生在接入控制设备 s 和终端 u 之间,记为 $\langle s,u \rangle$. 在 T_e 时刻, s 和 u 之间的链路出现故障,认证会话过程中断,经过 ΔT_r 时间后, s 和 u 之间的通信才能恢复, ΔT_r 为网络故障修复时间的平均值. 若因链路中断而导致的消息延迟时间超过接入控制设备 s 中的硬生命期,此次认证会话失败,记失败概率为 p_s .

考虑如下一个典型的认证会话传输过程. 接入控制设备 s 在 T_0 时刻成功地将认证请求消息 $auth_i$ 发送给终端 u , 经过一个往返时间 RTT 后, s 收到 u 的认证应答消息 ans_i . 在 T_e 时刻, s 与 u 之间的链路发生故障,导致在 $T_0 + \Delta T_s$ 时刻发出的 $auth_{i+1}$ 丢失, TCP 将重传 $auth_{i+1}$. 经过 ΔT_r , 即在 $T_e + \Delta T_r$ 时刻, s 与 u 之间的通信恢复, $auth_{i+1}$ 最终到达 u . 正常情况下, 当 u 接收到 $auth_i$ 后, 在忽略延迟的情况下, 等待 ΔT_s 时间后将会收到 $auth_{i+1}$, 而当网络出现故障时, u 接收 $auth_{i+1}$ 的时间将被延长. 设 s 与 u 之间的通信中断发生时刻 T_e 是在 $[T_0, T_0 + \Delta T_s]$ 区间中

的一个随机变量,并在该区间内服从均匀分布。

进一步将 $[T_0, T_0 + \Delta T_s]$ 划分为两个子区间: ΔT_m 和 ΔT_n . 其中, ΔT_m 是指接入认证设备从发出第 i 个认证请求消息到接收到第 i 个认证应答消息的时间间隔;而 ΔT_n 是指接入认证设备接收到第 i 个认证应答消息到发送第 $i+1$ 个认证请求消息的时间间隔,通常, $\Delta T_m \ll \Delta T_n$, 且 $\Delta T_m + \Delta T_n = \Delta T_s$, 如忽略传输时延,则可认为 $|\Delta T_m| = RTT$. 以下分两种情况进行讨论。

(1) $T_e \in [T_0 + \Delta T_m, T_0 + \Delta T_s]$

当 $T_e \in [T_0 + \Delta T_m, T_0 + \Delta T_s]$ 时, u 成功地收到了 $auth_i$ 并且 s 成功地收到 ans_i , 如图 2 所示。

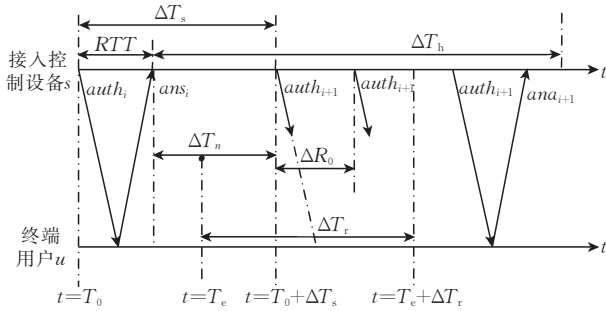


图 2 $T_e \in [T_0 + \Delta T_m, T_0 + \Delta T_s]$ 时的情况

在 $t = T_0$ 时刻,接入控制服务器 s 发出认证请求消息 $auth_i$,终端用户 u 收到后发出应答消息 ans_i . 在 $T_0 + \Delta T_s$ 时刻,进入下一轮认证会话, s 发出 $auth_{i+1}$,但由于网络出现故障在先, $auth_{i+1}$ 在传输中被丢失, s 将重传. 由于 TCP 提供一种面向连接的、可靠的数据包传输,因此,在收到 u 的 ans_{i+1} 之前,不会再发送其它认证会话。

在 TCP/IP 实现中^[10],重传时限(RTO)的值 ΔR_0 的计算方式为

$$\Delta R_0 = \max(sr_{tt} + 4 \times r_{ttvar}, min_{rto}),$$

其中, sr_{tt} 是已平滑的 RTT 估计器, r_{ttvar} 是已平滑的 RTT 平均偏差估计器, min_{rto} 是 ΔR_0 的最小值. 默认的 ΔR_0 的最小值为 $1s$ ^[9].

当使用指数退避算法计算 ΔR_0 时,设接入认证设备 s 首次传送认证请求消息 $auth_{i+1}$ 的时刻为 T_0 ,如网络出现故障,以后的重传时刻分别为 $T_0 + \Delta T_s + \Delta R_0$, $T_0 + \Delta T_s + 2\Delta R_0$, $T_0 + \Delta T_s + 4\Delta R_0$, ..., 可以得到第 i 次重传 $auth_{i+1}$ 的开始时刻为

$$T_r(i) = \sum_{k=1}^i \min(2^{k-1} \Delta R_0, \Delta R_m) + T_0 + \Delta T_s,$$

其中, ΔR_m 是最大的重传时限. 默认的 ΔR_m 的值为 $64s$ ^[13].

设 $\rho = 1 + \left\lfloor \log_2 \frac{\Delta R_m}{\Delta R_0} \right\rfloor$, 则上式可简化为

$$T_r(i) =$$

$$\begin{cases} (2^i - 1)\Delta R_0 + \Delta T_s + T_0, & i \leq \rho \\ (2^\rho - 1)\Delta R_0 + (i - \rho)\Delta R_m + \Delta T_s + T_0, & i > \rho \end{cases}.$$

为了避免 s 的硬生命期超时, s 必须在 $T_0 + \Delta T_h$ 时刻之前成功地发送 $auth_{i+1}$, 才能在 $T_0 + \Delta T_h + RTT$ 时刻收到 u 的应答 ans_{i+1} . 记 i' 为在硬生命期结束之前, $auth_{i+1}$ 的最后一次重传, 即 $i' = \max\{i; T_r(i) \leq T_0 + \Delta T_h\}$. 则

$$i' = \begin{cases} \left\lfloor \log_2 \left(\frac{\Delta T_h - \Delta T_s}{\Delta R_0} + 1 \right) \right\rfloor, & \Delta T_h \leq (2^\rho - 1)\Delta R_0 + \Delta T_s \\ \left\lfloor \frac{\Delta T_h - \Delta T_s - (2^\rho - 1)\Delta R_0}{\Delta R_m} \right\rfloor + \rho, & \text{其它情况} \end{cases}$$

因此,得出以下命题。

命题 1. 当采用 TCP 传输机制且 $T_e \in [T_0 + \Delta T_m, T_0 + \Delta T_s]$ 时,认证会话失败概率与软、硬生命期之间的关系为

$$p_{s2} = \begin{cases} 0, & \Delta T_r \leq T_r(i') - \Delta T_s \\ 1, & \Delta T_r \geq T_r(i') - RTT \\ \frac{\Delta T_s - [T_r(i') - \Delta T_r]}{\Delta T_s - RTT}, & \text{其它情况} \end{cases}.$$

证明. 在 s 的硬生命期到达之前,最后一次可容忍的重传时刻为 $T_r(i') < T_e + \Delta T_r$, 因此, $p_{s2} = P[T_e > T_r(i') - \Delta T_r]$, 由于 T_e 是 $[T_0 + \Delta T_m, T_0 + \Delta T_s]$ 上的均匀分布, 得出

$$\begin{aligned} p_{s2} &= 1 - P[T_e < T_r(i') - \Delta T_r] \\ &= 1 - \frac{[T_r(i') - \Delta T_r] - RTT}{\Delta T_s - RTT} \\ &= \frac{\Delta T_s - [T_r(i') - \Delta T_r]}{\Delta T_s - RTT}. \end{aligned}$$

证毕。

(2) $T_e \in [T_0, T_0 + \Delta T_m]$

当 $T_e \in [T_0, T_0 + \Delta T_m]$ 时, s 成功收到 ans_{i-1} , 由于网络出现故障, $auth_i$ 和/或 ans_i 丢失在网络中, 如图 3 所示。

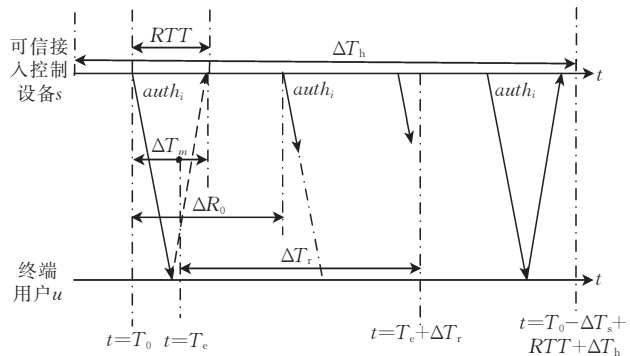


图 3 $T_e \in \Delta T_m$ 时的情况

在此情况下, s 会认为没有成功地发送 $auth_i$, 根据 TCP 的指数退避算法, s 在 $T_0 + \Delta R_0$ 开始重传 $auth_i$, 得到认证会话的重传序列为

$$T_r(i) = \begin{cases} (2^i - 1)\Delta R_0 + T_0, & i \leq \rho \\ (2^\rho - 1)\Delta R_0 + (i - \rho)\Delta R_m + T_0, & i > \rho \end{cases}$$

为了在 s 的硬生命期结束前, 收到 u 的应答消息, s 必须在 $T_0 - \Delta T_s + \Delta T_h$ 之前发送出 $auth_i$, 因此, 在硬生命期结束之前的最后一次重传为 $i' = \max\{i: T_r(i) \leq T_0 - \Delta T_s + \Delta T_h\}$, 则

$$i' = \begin{cases} \left\lceil \log_2 \left(\frac{\Delta T_h - \Delta T_s}{\Delta R_0} + 1 \right) \right\rceil, & \Delta T_h \leq (2^\rho - 1)\Delta R_0 + \Delta T_s \\ \left\lceil \frac{\Delta T_h - \Delta T_s - (2^\rho - 1)\Delta R_0}{\Delta R_m} \right\rceil + \rho, & \text{其它情况} \end{cases}$$

命题 2. 当采用 TCP 传输机制且 $T_e \in [T_0, T_0 + \Delta T_m]$ 时, 认证会话失败概率与软、硬生命期之间的关系为

$$p_{s1} = \begin{cases} 0, & \Delta T_r \leq T_r(i') - RTT \\ 1, & \Delta T_r \geq T_r(i') \\ \frac{RTT - [T_r(i') - \Delta T_r]}{RTT}, & \text{其它情况} \end{cases}$$

由于 T_e 在区间 $[T_0, T_0 + \Delta T_s]$ 内服从均匀分布, 因此可以将上述两种情况下的结果合并为

$$p_s = \frac{(\lceil \Delta T_m \rceil p_{s1} + \lceil \Delta T_n \rceil p_{s2})}{\Delta T_s}$$

3.2 采用 UDP 传输机制

由于 UDP 不提供可靠性的传输, 因此在设计过程中增加了重传机制, 具体描述如下: 当接入控制设备给终端用户发送认证请求之后, 如果等待 ΔT_s 时间后, 仍未收到终端用户的应答消息, 那么接入控制设备将每隔 $\Delta T'$ 重新给该终端用户发送认证请求消息, 若在硬生命期结束之前, 都未收到应答, 那么认证会话结束, 并断开该用户与网络的连接。

同样分为两种情况考虑. 当 $T_e \in [T_0 + \Delta T_m, T_0 + \Delta T_s]$ 时, 认证会话的重传序列为 $T_r(i) = T_0 + 2\Delta T_s + (i - 1)T'$, 并且在接入控制设备中的硬生命期结束之前的最后一次重传为 $i' = \left\lfloor \frac{\Delta T_h - 2\Delta T_s}{T'} \right\rfloor + 1$.

命题 3. 当采用 UDP 传输机制且 $T_e \in [T_0 + \Delta T_m, T_0 + \Delta T_s]$ 时, 认证会话失败概率与软、硬生命期之间的关系为

$$p_{s2} =$$

$$\begin{cases} 0, & \Delta T_r \leq T_r(i') - \Delta T_s \\ 1, & \Delta T_r \geq T_r(i') - RTT \\ \frac{\Delta T_s - [T_r(i') - \Delta T_r]}{\Delta T_s - RTT}, & \text{其它情况} \end{cases}$$

证明方法与上述情况类似, 故在此略去。

而当 $T_e \in [T_0, T_0 + \Delta T_m]$ 时, 认证会话的重传序列为 $T_r(i) = T_0 + \Delta T_s + (i - 1)T'$, 且最后一次重传为 $i' = \left\lfloor \frac{\Delta T_h - 2\Delta T_s}{T'} \right\rfloor + 1$.

命题 4. 当采用 UDP 传输机制且 $T_e \in [T_0, T_0 + \Delta T_m]$ 时, 认证会话失败概率与软、硬生命期之间的关系为

$$p_{s1} = \begin{cases} 0, & \Delta T_r \leq T_r(i') - RTT \\ 1, & \Delta T_r \geq T_r(i') \\ \frac{RTT - [T_r(i') - \Delta T_r]}{RTT}, & \text{其它情况} \end{cases}$$

证明. 略。

同理可得, 当采用 UDP 传输机制时, 总的认证会话失败概率为

$$p_s = \frac{(\lceil \Delta T_m \rceil p_{s1} + \lceil \Delta T_n \rceil p_{s2})}{\Delta T_s}$$

4 仿真实验

以 TCP 传输机制为例, 仿真时采取的参数为 $R_0 = 1s$, $R_m = 64s$, $RTT = 1.5s$. 图 4 给出了当软生命期 $\Delta T_s = 30s$ 时, 认证会话失败概率 p_s 与硬生命期 ΔT_h 、网络故障恢复时间 ΔT_r 之间的关系图. 如图 4 所示, 在保持 p_s 为 0 的情况下, 随着 ΔT_h 增大, 可容忍的 ΔT_r 的值也越大. 图 5 给出了当硬生命期 $\Delta T_h = 90s$ 时, 认证会话失败概率 p_s 与软生命期 ΔT_s 及网络故障恢复时间 ΔT_r 之间的关系图. 由于 ΔT_s 控制着认证会话中更新区间的大小, 因此, ΔT_s 越小, 认证会话能否成功的确定性越强, 如图 5 所示. 当 $\Delta T_s \leq 30s$ 时, 要保证认证会话成功, 网络故障的恢复时间集中于 $65 \sim 75s$ 之内, 而当 $\Delta T_s > 30s$ 时, 认证会话是否成功的随机性明显增大. 图 6 给出了当网络故障恢复时间 $\Delta T_r = 30s$ 时, 认证会话失败概率 p_s 与硬生命期 ΔT_h 、软生命期 ΔT_s 之间的关系图. 图中显示, 当 ΔT_h 越大, ΔT_s 越小时, 认证会话成功率保持得越久. 图 6 中, 仿真结果呈现出明显的阶梯状, 主要是因为, 认证会话的失败概率 p_s 直接

由认证会话的最后一次重传时刻 $T_r(i')$ 、网络故障恢复时间 ΔT_r 决定, 而 $T_r(i')$ 又由软生命期 ΔT_s 、硬生命期 ΔT_h 决定, 当 ΔT_s 及 ΔT_r 固定时, p_s 主要由 $T_r(i')$ 决定, 而在 TCP 传输机制中, 相邻两次的重传之间存在一定的时间间隔, 因此, 在此时间间隔之内, ΔT_h 的值的变化并不会引起 p_s 的改变. 如图 6 中所示, 当 $\Delta T_s = 40s$, $\Delta T_h \in [103s \sim 150s]$ 时, 都使得 $p_s = 0$.

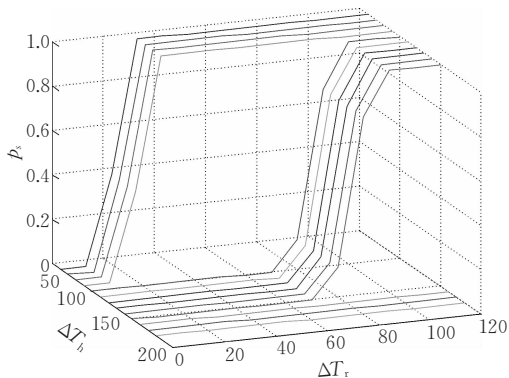


图 4 p_s 与 ΔT_h 、 ΔT_r 之间的关系图

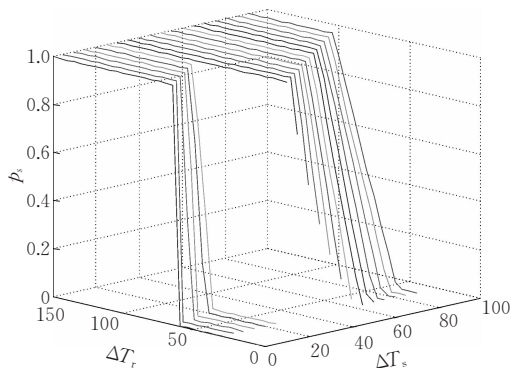


图 5 p_s 与 ΔT_s 、 ΔT_r 之间的关系图

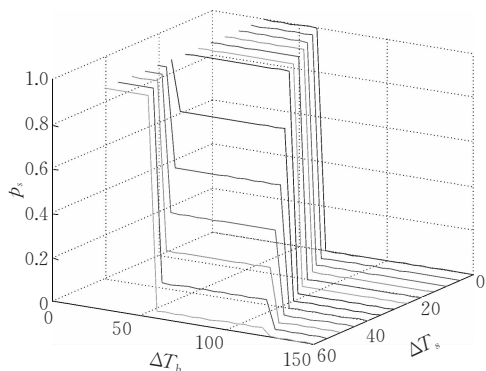


图 6 p_s 与 ΔT_h 、 ΔT_s 之间的关系图

源头开始做好网络接入控制. 本文设计了一种新的网络接入控制方法, 结合了现有的数字证书机制的优点, 更好地实现了网络的可控可管性. 目前已经实现了接入控制设备以及授权管理服务器的原型系统, 下一步的工作包括分析系统的安全性、对网络性能的影响以及受攻击时的可用性、生存性等问题.

参 考 文 献

- [1] Lin Chuang, Ren Feng-Yuan. Controllable, trustworthy and scalable new generation Internet. *Journal of Software*, 2004, 15(2): 1815-1821(in Chinese)
(林闯, 任丰原. 可控可信可扩展的新一代互联网. *软件学报*, 2004, 15(2): 1815-1821)
- [2] Lin Chuang, Peng Xue-Hai. Research on trustworthy networks. *Chinese Journal of Computers*, 2005, 28(5): 751-758(in Chinese)
(林闯, 彭雪海. 可信网络研究. *计算机学报*, 2005, 28(5): 751-758)
- [3] Lee Hyun-Woo, Kim Kwihoon, Ryu Won, Lee Byung-Sun. Performance of an efficient performing authentication to obtain access to public wireless LAN with a cache table//*Proceedings of the IEEE International Conference on Communications (ICC'06)*. Istanbul, 2006; 2376-2381
- [4] Arun Saha. Mart molle thinking outside the box; Extending 802.1x authentication to remote "Splitter" ports by combining physical and data link layer techniques//*Proceedings of the 28th Annual IEEE International Conference on Local Computer Networks (LCN'03)*. Germany, 2003; 324-333
- [5] Ana Sanz Merino, Yasuhiko Matsunaga, Manish Shah. Secure authentication system for public WLAN roaming//*Proceedings of the Mobile Networks and Applications*. Netherlands, Springer Science+Business Media, 2005; 355-370
- [6] Gianluigi Me, Daniele Pirro, Roberto Sarrecchia. A mobile based approach to a strong authentication on Web//*Proceedings of the International Multi-Conference on Computing in the Global Information Technology-(ICCGI'06)*. Bucharest, 2006; 67-71
- [7] Manabu Hirano, Takeshi Okuda, Suguru Yamaguchi. Application for a simple device authentication framework: Device authentication middleware using novel smart card software//*Proceedings of the 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07)*. Japan, 2007; 31-34
- [8] Brendan DeBow, Khalid Syed. 802.11 wireless network end-user authentication using common access cards//*Proceedings of the Military Communications Conference 2006(MILCOM 2006)*. Washington, DC, 2006; 1-5
- [9] Xiao L, Nahrstedt K. Reliability models and evaluation of internal BGP networks//*Proceedings of the IEEE INFOCOM, 2004. Twenty-Third Annual Joint Conference of the IEEE Computer and Communications Societies*. 2004; 1593-1604

5 结束语

为了更好地解决现有的网络安全问题, 必须从

[10] Wright G R, Stevens W R. TCP/IP Illustrated Volume 2 — The Implementation. Beijing: China Machine Press, 2002: 680-710(in Chinese)

(莱特,史蒂文斯. TCP/IP 详解. 卷 2:实现. 北京:机械工业出版社, 2002: 680-710)



LIU Wei, born in 1979, Ph.D. candidate. Her research interests focus on network security.

YANG Lin, born in 1970, Ph.D. , professor, Ph.D. su-

Background

This research is supported by the Pre-research Program of National Defence under grant No. 513150604.

As the quickly expansion of network scale, more and more end-points and users access to network, the extension and deepness of various application constantly increase, all of these result in the difficulty of network management and maintenance. It is imminence to solve these problems, such as protecting the network security, protecting the border of the network; implementing uniform management to network user, strengthening the supervision and control of user network

pervisor. His main research interests focus on information security.

DAI Hao, born in 1945, Ph.D. supervisor, member of the Chinese Academy of Engineering. His main research interests include network engineering and network security.

HOU Bin, born in 1970, senior engineer. Her research interests focus on network security.

behaviors; reinforcing the integrate management of network resources, providing high quality of service and security guarantee to user; impulsing the establishment of trusted network, forming colligated network security defense ability etc. The main objective of network access control scheme investigate by the authors is to provide uniform security authentication and authorization mechanism for communication system, by validating the identity of network user, definitude the privilege of network resource for users, then can protect the resource under control against abuse unlawfully.