第37卷 第24期
Vol.37 No.24

计 算 机 工 程
Computer Engineering

2011年12月
December 2011

·安全技术·

文章编号：1000—3428(2011)24—0109—03 文献标识码：A 中图分类号：TP309

改进的 Kerberos 单点登录协议

邵叶秦[a]，陈建平[b]，顾 翔[b]

(南通大学 a. 现代教育技术中心；b. 计算机科学与技术学院，江苏 南通 226019)

摘 要：现有 Kerberos 协议易受密码猜测字典攻击和报文重放攻击。为此，提出一个改进的 Kerberos 单点登录协议。在认证报文中添加随机数并使用动态密钥，防止密码猜测字典攻击，为每个报文添加一个唯一的序列号，防止报文重放攻击。实验结果证明了改进协议的有效性。

关键词：单点登录；Kerberos 协议；字典攻击；重放攻击

Improved Kerberos Single Sign-on Protocol

SHAO Ye-qin[a], CHEN Jian-ping[b], GU Xiang[b]

(a. Center of Modern Educational Technology; b. School of Computer Science and Technology, Nantong University, Nantong 226019, China)

【Abstract】This paper analyzes the problems of the password guessing dictionary attacks and message replay attacks in current Kerberos protocol. An improved single sign-on protocol is proposed. The prevention of password guessing dictionary attacks is achieved by adding a random number and employing a dynamic key in authentication messages. The resistance of replay attacks is realized by marking the message between a client and its corresponding server with a unique serial number. Experimental results show that the improved protocol is valid.

【Key words】single sign-on; Kerberos protocol; dictionary attack; replay attack

DOI: 10.3969/j.issn.1000-3428.2011.24.036

1 概述

整个社会信息化的不断推进和越来越多的独立应用系统导致了多个系统、多个账号、多次用户登录问题的产生。单点登录是用户使用一个账号，进行一次登录认证就可访问与其权限相匹配的所有应用和资源，有效地提高了账号使用的方便性和可管理性。

Kerberos 是一个基本的单点登录协议，目前被广泛地用于登录认证当中。文献[1]分析了 Kerberos 协议存在的问题。文献[2]减少了协议在无线网络中的认证时延。文献[3]解决了协议在 Web 环境下的安全隐患。文献[4]对协议的密码猜测攻击缺陷进行了改进。文献[5]把用户密码分成 2 个部分，通过 2 个服务器合作来认证用户以防止短密码的密码猜测字典攻击。最新版的 Kerveros5 协议[6]在加密系统、票据寿命、二次加密等方面进行了改进。尽管如此，Kerberos 协议仍存在密码猜测字典攻击、重放问题、时间同步等问题。为此，本文提出一个防字典攻击和重放攻击的 Kerberos 单点登录协议。

2 Kerberos 协议

2.1 协议介绍

Kerberos 协议是麻省理工学院为 Athena 项目设计的网络认证协议。它依靠可信任的第三方进行统一认证直接访问所有应用。Kerberos 协议以域为单位进行管理，每个域中包含若干客户端(Client)，若干应用服务器(Server)，一个认证服务器(Authentication Server, AS)及一个票据授权服务器(Ticket Granting Server, TGS)。协议的认证过程如图 1 所示。3 个阶段的描述如下：

(1)第 1 阶段：Client 用账号信息向 AS 发出认证请求，认证通过后，取得访问 TGS 的票据和会话密钥。

(2)第 2 阶段：Client 用访问 TGS 的票据和新产生的认证算子向 TGS 发出访问 Server 的票据请求，取得访问 Server 的票据和会话密钥。

(3)第 3 阶段：Client 用访问 Server 的票据和新产生的认证算子向 Server 发出访问请求，认证通过就可访问相应的服务。

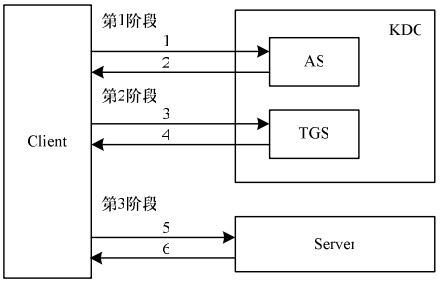

图 1 Kerberos 认证过程

2.2 协议缺陷

Kerberos 虽然是一个改进的安全认证协议，但仍存在以下缺陷：

(1)密码猜测字典攻击

在 Client 使用密码向 AS 发出认证请求时，攻击者可以截取相应报文，对密码实施在线或离线的基于字典的攻击。而用户为了使用方便，选择的密码一般比较简单或具有明显的规律，如 123456、abc123、电话号码等。这为密码猜测字

基金项目：江苏省高校自然科学基金资助项目(08KJB520009)；江苏省现代教育技术研究“十一五”规划立项课题基金资助项目(2010-R-16939, 2010-R-16884)

作者简介：邵叶秦(1978－)，男，实验师，主研方向：网络安全；陈建平，教授；顾 翔，副教授

收稿日期：2011-07-01 **E-mail：**hnsyk@163.com

典攻击带来了可能。

(2)报文重放问题

已经使用过的报文如果被攻击者存储或重用，就会发生报文重放攻击。理论上可以将使用过的报文保存起来，通过核对报文来确认是否被重放，但实现起来有难度。Kerberos 虽然在票据中加入时间戳以防止报文重放攻击，但票据存在有效期(一般为 5 min)，在此期间内攻击者仍可重放报文。

(3)时间同步

Kerberos 协议是在网络上的时钟都同步的前提下实施的，但实际上很难做到这一点。尽管网络时间协议可以实现时钟同步，但其本身存在安全性问题，因此，不能用来解决时钟同步问题。

针对以上问题，本文提出一个改进的防密码猜测字典攻击和报文重放攻击的 Kerberos 单点登录协议。

3 改进的单点登录协议

3.1 协议描述

改进协议使用动态密钥作为 Client 和 AS 之间的共享密钥。动态密钥每次认证时都不相同。考虑到安全性，动态密钥由一个本地的离线 *key*，上一次的加密密钥 *kd* 和一个由 Client 和 AS 在上一次认证过程中协商的随机数 *rnd* 通过单向函数运算得到。改进协议的过程如图 2 所示，用到的标识如表 1 所示。

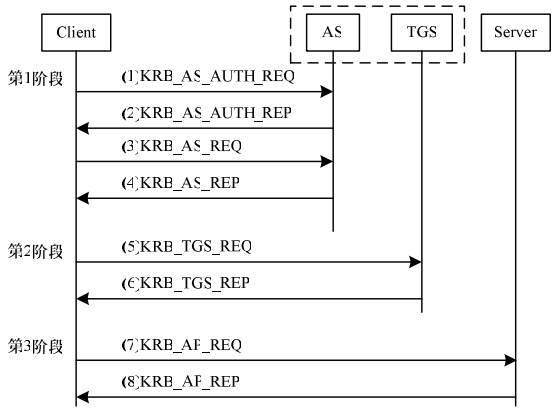

图 2 改进的单点登录协议过程

表 1 协议中标识的意义

标识	意义
c	客户端
v	应用服务器
ts_n	时间戳
id_x	x 的标识
$realm_x$	x 所在的域
add_c	客户端的地址
$nonce_n$	1 个随机数
$option_s$	选项信息
$ticket_x$	用 x 的密钥加密过的票据
$times$	票据相关的时间字段
$enc\text{-}part$	KDC 返回给客户端的加密信息
k_x	x 与 KDC 共享的密钥
$k_{x,y}$	x 与 y 共享的会话密钥
$E_{kxx}[yy]$	使用 k_{xx} 对 yy 加密
$subkey$	通信子密钥
$seq\text{-}number$	随机序列号

第 1 阶段：Client 和 AS 使用动态密钥进行加密通信，一方面完成用户的认证，返回访问 TGS 的票据和会话密钥，另一方面协商随机数，更新动态密钥。因此，协议在最开始增加 KRB_AS_ AUTH_REQ 和 KRB_AS_AUTH_REP 2 个步骤。协议的具体报文如下：

(1)KRB_AS_AUTH_REQ，Client 向 AS 发出的认证请求报文，内容为：

$\{E_{Kd}[pwd, nonce_1, rnd], id_c\}$

其中，*rnd* 是一个随机数，负责对保存在本地的一个 *key* 进行更新；*pwd* 是用户密码。

(2)KRB_AS_AUTH_REP，AS 向 Client 发出的认证响应报文，内容为：

$\{E_{Kd}[nonce_1+1, nonce_2]\}$

(3)KRB_AS_REQ，Client 向 AS 发出的票据请求报文，内容为：

$\{E_{Kd}[nonce_2+1, options, id_c, realm, id_{tgs}, times_1, nonce_3]\}$

(4)KRB_AS_REP，AS 向 Client 发出的票据请求响应报文。AS 为 Client 与 TGS 产生会话密钥，一份加密后返回给 Client，并复制一份封装在访问 TGS 的票据里。报文的内容为：

$\{realm_c, id_c, ticket_{tgs}, enc\text{-}part\}$

其中，

$ticket_{tgs}=realm_{tgs}, id_{tgs}, E_{Ktgs}[k_{c,tgs}, realm_c, id_c, times_1, add_c]$

$enc\text{-}part=E_{Kd}[k_{c,tgs}, nonce_3, times_1, realm_{tgs}, id_{tgs}, add_c]$

第 2 阶段：Client 利用访问 TGS 的票据换取访问 Server 的授权票据。具体报文如下：

(5)KRB_TGS_REQ，Client 向 TGS 发出票据授权请求报文，内容为：

$\{options, realm_v, id_v, times_2, nonce_4, authenticator_c, ticket_{tgs}\}$

其中，$authenticator_c=E_{Kc,tgs}[realm_c, id_c, ts_2]$

(6)KRB_TGS_REP，TGS 向 Client 发出的票据授权请求响应报文。TGS 收到请求后，为 Client 与 Server 产生会话密钥，一份加密后返回给 Client，并复制一份封装在访问 Server 的票据里。报文的内容为：

$\{realm_c, id_c, ticket_v, enc\text{-}part\}$

其中，

$ticket_v=realm_v, id_v, E_{Kv}[k_{c,v}, realm_c, id_c, times_2, add_c]$

$enc\text{-}part=E_{Kc,tgs}[k_{c,v}, nonce_4, times_2, realm_v, id_v, add_c]$

第 3 阶段：Client 利用访问 Server 的票据访问相应的服务。Client 向 Server 发出的每个请求报文都有一个相互区别的标识，Server 通过判断该标识是否符合重放条件，来确定报文是否被重放。具体报文如下：

(7)KRB_AP_REQ，Client 向 Server 发出的访问请求报文，内容为：

$\{options, ticket_v, authenticator_c\}$

其中，

$authenticator_c=E_{Kc,v}[realm_c, id_c, ts_2, subkey, seq\text{-}number]$

(8)KRB_AP_REP，Server 向 Client 发出的访问请求响应报文，内容为：

$\{E_{Kv}[ts_2, subkey, seq\text{-}number]\}$

3.2 防密码猜测字典攻击的实现

为了防止密码猜测字典攻击，一方面，本文在报文中添加随机数，增加密码猜测字典攻击的难度；另一方面，Client 和 AS 通信时用来加密的密钥，不再是预先存储的不变的用户密码，而是由双方在上一次通信时协商的随机数 *rnd*、本地的离线 *key* 和上一次的加密密钥 *kd* 通过运算得到。具体过程由协议的第 1 阶段来完成。

3.2.1 随机数的协商

随机数的协商采用类似 3 次握手的方式进行。Client 利用第 1 个报文以加密的方式向 AS 发送一个随机数，AS 接收

到后，利用第 2 个报文通知 Client 随机数协商成功。

3.2.2　密钥信息的更新

动态密钥的更新由第 2 个~第 4 个报文完成，方法如下：

(1)Client 成功收到第 2 个报文后，知道随机数已协商好。用户利用下面 2 个公式更新本地的离线 *key* 和上次的加密密钥 *kd*，并通过第 3 个报文通知 AS 动态密钥更新完成。

$key=f\{key, rnd\}$

$kd=f(kd, key)$

其中，*f* 是一个不可逆函数；*key* 的初始值是用户注册时产生的一个字串；*kd* 的初始值是用户的密码。

(2)AS 收到第 3 个报文，知道 Client 已经成功更新动态密钥，利用同样的公式更新本地的 *key* 和 *kd*，并通过第 4 个报文通知 Client 动态密钥更新完成。

整个更新操作对用户是透明的。在更新过程中，一旦动态密钥更新失败，双方动态密钥自动恢复到本次更新前的状态。

3.2.3　密钥信息的存储

改进的协议需要保存用户离线的 *key* 和动态密钥 *kd*。为了保证用户在不同的电脑上都能正常使用，不同的电脑需要记录每个用户各自不同的离线 *key* 和动态密钥 *kd*。而 AS 按照(用户名、IP、离线 *key* 和动态密钥 *kd*)的格式保存相应的密钥信息。这些操作对用户也是透明的。

3.3　防报文重放攻击的实现

经过分析，前 2 个阶段的双向通信都是加密的，因此，有效的报文重放攻击发生在 Client 向 Server 发出访问请求时(即第 7 个报文)。

为了防止 Client 和 Server 之间的这种报文重放攻击，Client 和 Server 需要协商一个随机数，作为防报文重放攻击序列的起点。Client 每次发出的请求，不管是正常的，还是重放的，该序列值都在原来的基础上加 1。Server 记录每次接收到的请求的最大序列号。当一个请求到来时，Server 将请求中的序列号与自己记录的最大序列号进行对比，如果新到请求中的序列号大于最大的序列号，Server 认为这是一个正常的请求，进行具体处理，并将记录的最大序列号更新为新到请求中的序列号，否则，Server 认为这是一个过时的重放请求，将其丢弃。如果冒充者重放某个报文，由于 Server 端记录的最大序列号大于或等于这个重放报文中的序列号，重放的报文被丢弃。

3.4　改进协议的优势分析

改进的协议相比于标准的 Kerberos 协议增加了 2 个步骤，具有以下优势：

(1)改进的协议在传送用户密码时添加了随机数 $nonce_1$，使得密码猜测字典攻击不仅要穷举用户密码，而且要穷举随机数。通过控制随机数的位数，用户密码的强度不再是系统安全的瓶颈，提高了协议报文抗密码猜测字典攻击的能力。

(2)每次通信的加密密钥不再是不变的用户密码，而是每次认证都用不相同的动态密钥。这使得 Client 和 AS 的通信报文更具随机性，增加了密码猜测字典攻击的难度，保证了通信数据的安全性。

(3)每次通信的加密密钥由上一次通信的密钥和保存在本地的离线 *key* 以及动态协商的随机数共同运算得到。只知道本地的离线 *key* 或通过网络窃听获得动态协商的随机数，都无法得到下次通信的密钥，保证了通信数据的安全性。

(4)通信密钥是动态变化的，这使得报文重放攻击只能在本轮通信过程中有效，而且只能在第 7 个报文进行重放，但由于每个报文都有唯一编号，因此这一步的报文重放攻击也不能实现。

4　实验结果与分析

本文的实验环境是一个包括 3 个 Client、2 个 Server 和 1 个 KDC 的局域网，如图 3 所示，其中，AS 和 TGS 位于一台机器上。

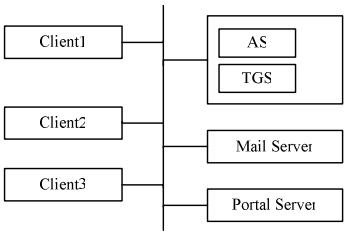

图 3　局域网结构

在实验中，各个 Client 和 KDC 的共享密钥、各个 Server 和 KDC 的共享密钥，TGS 和 AS 的共享密钥都存储在 KDC 的数据库中。协议使用 CBC 模式的 Triple-DES 进行对称加密。各个票据的有效期为 8 h，认证算子有效期为 5 min。抓包工具使用 Ethereal 软件。

为了测试协议的抗密码猜测字典攻击能力，实验对抓到的第 1 个报文实施密码猜测字典攻击。在兼顾效率和安全性的情况下，本文选择 128 位的随机数 *nonce*1，实验结果表明本文提出的方法能够抵抗字典攻击。为了测试协议的抗报文重放攻击能力，实验对抓到的第 7 个报文实施报文重放攻击，结果同样表明本文的方法是有效的。

5　结束语

本文通过分析 Kerberos 协议存在的问题，提出了一个改进的 Kerberos 单点登录协议。实验结果证明，本文的改进协议能有效地阻止密码猜测字典攻击和报文重放攻击。下一步将考虑在协议中使用除 Triple-DES 外的其他加密算法，从而进一步提高协议性能。

参考文献

[1] Bellovin S, Merritt M. Limitations of the Kerberos Authentication System[J]. Computer Communications Review, 1990, 20(5): 119-132.

[2] Marin-Lopez R, Pereniguez-Garcia F, Ohba Y, et al. A Kerberized Architecture for Fast Re-authentication in Heterogeneous Wireless Networks[J]. Moblile Networks & Applications, 2010, 15(3): 392-412.

[3] 张小红, 樊中奎. 基于认证协议的 Web 单点登录优化设计[J]. 计算机工程, 2010, 36(13): 146-148.

[4] Diffie W, Hellman M E. New Directions in Cryptography[J]. IEEE Trans. on Information Theory, 1976, 22(6): 644-654.

[5] Brainard J, Juels A, Kaliski B, et al. A New Two-server Approach for Authentication with Short Secrets[C]//Proc. of the 12th USENIX Security Symposium. Washington D. C., USA: [s. n.], 2003.

[6] Neuman C, Yu T, Hartman S, et al. The Kerberos Network Authentication Service(V5)[EB/OL]. (2005-07-01). http://www.ietf.org/rfc/rfc4120.

编辑　顾姣健