基于混合机制的 Kerberos 安全性增强方案①

庄小妹[1], 唐西林[2]

[1](广东培正学院 计算机科学与工程系, 广州 510830)
[2](华南理工大学 理学院, 广州 510640)

摘 要: 针对 Kerberos 协议的弱点和安全性问题, 提出了一个基于混合加密机制的 Kerberos 改进方案, 目的是防范口令攻击和内部攻击. 给应用服务器和 AS 服务器分配公钥和私钥, 用户与服务器之间的会话密钥由 DH 密钥交换生成. 给出了改进后的 Kerberos 协议的六个步骤, 并对安全性进行分析. 分析结果表明, 新方案能够增强 Kerberos 协议的安全性, 而且比公钥加密机制高效.

关键词: 身份认证; Kerberos 协议; 口令攻击; 内部攻击; Diffie-Hellman 密钥交换协议

Enhanced Security Scheme of Kerberos Protocol Based on Hybrid Cryptosystem

ZHUANG Xiao-Mei[1], TANG Xi-Lin[2]

[1](Computer Science and Engineering, Guangdong Peizheng College, Guangzhou 510830, China)
[2](School of Science, South China University of Technology, Guangzhou 510640, China)

Abstract: Aiming at the vulnerability and security problem of Kerberos protocol, an enhanced scheme of Kerberos protocol based on hybrid cryptosystem is put forward. The aims of the improved scheme are able to defend the password attacks and the insider threads. Public keys and private keys are assigned to the application servers and the AS server, the session key between user and application server is generated by DH key exchanged algorithm. The improved Kerberos protocol is given by six steps and the security is analyzed. Analysis shows that the new scheme can enhance the security of Kerberos and is more efficient than Public key encryption mechanism.

Key words: user authentication; Kerberos protocol; password attack; insider thread; Diffie-Hellman key exchanged algorithm

根据信息安全组织 OWASP2013 年的 TOP 10 安全报告, WEB 十大安全威胁排行榜中, 失效的身份认证位居第二[1]! 可见在互联网, 由身份认证引起的攻击已经相当普遍和严重. 身份认证是信息安全的第一道关卡, 只有通过了身份认证, 用户才能获得相应的资源和访问权限. 如果身份认证失效, 用户就可能被假冒, 机密信息就有被泄露的威胁.

1 Kerberos工作原理

Kerberos 协议(简称 Kerberos)是 1994 年提出的[2], 是目前应用广泛, 也相对较为成熟的一种身份认认证机制. Kerberos 是一种基于可信赖第三方的 TCP/IP 网络安全认证协议, 它提供了一种开放网络中进行身份认证的方法, 可以有效解决分布式网络环境下用户访问系统资源的安全性问题. Kerberos 基于对称密钥体制, 通常采用 DES 加密算法, 但也可用其它算法替代. Kerberos 的 AS 服务器与网络上的每个不同实体分别共享一个不同的密钥, 是否知道共享密钥便是实体的身份证明[3].

1.1 Kerberos 的工作原理

为了方便描述, 我们所使用的形式化符如下:

C:用户
AS:认证服务器
TGS:票据服务器
V:应用服务器
IDc:用户 C 的 ID
IDtgs:票据服务器的 ID
IDv:应用服务器的 ID

① 收稿时间:2014-08-27;收到修改稿时间:2014-10-08

TS:时间戳

LIFETIME:生命期

Ticket-tgs:票据许可票据

Ticket-v:服务许可票据

Kc:用户 C 与 AS 之间共享的密钥

Ktgs:AS 与 TGS 共享的密钥

Kv:TGS 与 V 共享的密钥

Kc,tgs:C 与 TGS 的会话密钥

EKc:用 Kc 加密消息 m

Kerberos 的工作过程有三个阶段, 六个步骤. 最终用户 C 与应用服务器 V 相互认证, 并且获得它们之间的会话密钥.

第一阶段, 申请票据许可票据, 它的形式化表示如下:

1) C—>AS:IDc||IDtgs||TS1

2) AS—>C:

EKc[Kc,tgs||IDtgs||TS2||LIFETIME2||Ticket-tgs]

其中

Ticket-tgs=EKtgs[Kc,tgs||IDc||ADc||IDtgs||TS2||LIFETIME2]

第一个步骤是用户 C 发送明文消息, 申请票据许可票据. 认证服务器收到报文后, 检查用户 C 是否为合法用户, 如果是, 则生成密钥 Kc,tgs 和票据 Ticket-tgs 并通过第二个步骤发送给用户 C.

第二阶段, 申请服务许可票据, 它的形式化表示如下:

3) C—>TGS:IDv||Ticket-tgs||AUc

4) TGS—>C: Kc,tgs[Kc,v||IDv||TS4||Ticket-v]

其中

AUc=Kc,tgs[IDc||ADc||TS3]Ticket-v=EKv[Kc,v||IDc||ADc||IDv||TS4||LIFETIME4]

用户 C 收到第二个步骤的报文后, 用 Kc 解密, 获得 Kc,tgs, Ticket-tgs, 但 Ticket-tgs 是加密的, 用户 C 不能查看和修改其中的内容. 用户 C 生成认证码 AUc, 通过第三个步骤向 TGS 申请服务许可票据.

TGS 服务器收到申请后, 用 Ktgs 解密 Ticket-tgs, 并且获得包含在 Ticket 中的 kc,tgs. TGS 使用 Kc,tgs 解密认证码, 从而认证用户 C.

TGS 生成 Ticket-v, 以及 Kc,v, 然后用 Kc,tgs 加密, 通过第四个步骤发送给用户 C.

第三阶段, 客户端/服务器鉴别交换, 获得服务, 它的形式化表示如下:

5) C—>V:Ticket-v||AUc

6) V—>C:EKc,v[TS5+1]

其中

AUc=Kc,v[IDc||ADc||TS5]

用户 C 收到第四个步骤的报文后, 用 Kc,tgs 解密信息, 获得 Kc,v, 利用它生成认证码, 然后通过第五个步骤向服务器 V 申请服务.

服务器收到申请后, 用 Kv 解密 Titcket-v, 获得 Kc,v, 利用 Kc,v 解密认证码, 从而认证用户 C. 用户收到第六个步骤报文后, 通过 Kc,v 解密报文从而验证服务器的身份.

1.2 Kerberos 的不足

Kerberos 并非完善的身份认证协议, 它主要有以下两个不足之处:

1)口令攻击. Kerberos 的 v4, v5 版本均容易受到口令攻击. 从 AS 发往客户端的消息是用基于用户的口令加密的, 攻击者可能捕获消息, 并通过尝试各种口令解密. 如果某一次解密成功, 则攻击者可得到用户口令, 进而使用该口令从 Kerberos 获取认证[4].

2)内部攻击. Kerberos 服务器不能避免内部人员监听用户和应用服务器之间的通信过程, 获得机密信息. 文献[5]详细描述了第 4 版本的局限性.

针对以上的不足, 许多文献, 例如文献[6]~[12]提出不同的改进方案.

在文献[10]中提出了用 DH 密钥替换用户口令 Kc 加密第二个步骤的报文, 目的是解决 Kc 容易受到攻击的缺陷. 但是, 第一个报文是明文的, 第二个报文是用 Kc 加密的, 既然 Kc 不安全, 攻击者完全可以通过截获第一报文和第二个报文, 解密第二个报文, 然后发起中间人攻击.

文献[11], [12]提出的公钥机制能大大地增强 Kerberos 协议的安全性, 但几乎每一个步骤都涉及公钥机制的加密和解密, 协议的工作效率势必受到较大的影响, 并且每个用户都有自己的公钥和私钥, 无疑增加了密钥管理的难度.

2 基于混合加密机制的Kerberos协议方案和安全性分析

根据以上的分析, 对 Kerberos 的改进主要有两点, 一是给 AS 服务器和应用服务器分配公钥和私钥, 二

是使用 DH 密钥交换协议建立会话密钥, 目的是防范 Kerberos 口令攻击和内部攻击.

2.1 防范内部攻击的必要性

在 Kerberos 协议中, 用户与应用服务器之间的会话密钥是由 Kerberos 服务器生成的, 因此, Kerberos 服务器完全可以监听用户与应用服务器之间的全部会话, 这就为来自 Kerberos 服务器的内部攻击提供了可能. 在 Kerberos 的第 5 版本中, 第五个步骤的 AUc 增加了 subkey 域, 用户在发送报文的同时可以指定下一阶段的会话密钥 Subkey. 但是 AUc 是用 Kc,v 加密的, 内部人员仍然可以获得 Subkey, 因此使用 Subkey 不能避免内部人员的监听.

2.2 Diffie-Hellman 密钥交换协议

DH 密钥协商过程如下:首先随机选择大素数 p, 取 g 是 p 的本原根, g 和 p 可公开. Alice 选择一个保密的随机整数 a(0<a<p-1), 计算 $A=g^a \bmod p$ 发送给 Bob. 而 Bob 选择一个保密的随机整数 b(0<b<p-1) , 计算 $B=g^b \bmod p$ 发送 Alice. 然后 Alice 计算 $Ka=B^a \bmod p$, Bob 计算 $Kb = A^b \bmod p$, 因为

$Ka = B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p$,

$Kb = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p$.

所以 Ka=Kb=K, 因此通信双方拥有相同的密钥 K. 因为 a 和 b 是保密的, 攻击者只能得到 p、g、A 、B, 要想确定 K , 则必须求离散对数. 对于大素数, 求离散对数被认为是不可行的. 因此攻击者计算出 K 是不可行的.

DH 密钥交换的一个缺点, 就是存在中间人攻击.

2.3 Kerberos 协议的改进

改进后 Kerberos 的六个步骤如下:

1) C—>AS:EPUas(IDc||IDtgs ||AUc)

其中, AUc=Kc [IDc||TS1||Kt]

用户选择随机密钥 Kt, 生成验证码 AUc, 使用 AS 服务器的公钥 PUas 加密报文, 发送给 AS 服务器. AS 服务器用私钥解密, 根据 IDc 找到相应的 Kc, 再根据 Kc 解密 AUc, 从而验证用户的身份. 同时获得用户指定密钥 Kt.

2) AS—>C:

EKt[Kc,tgs||IDtgs||TS2||LIFETIME2||Ticket-tgs]

AS 使用用户的随机密钥 Kt 加密信息, 发送给用户 C. 用户 C 解密, 获得 Kc,tgs 以及 Ticket.

第三, 四个步骤不变.

5) C—>V:EPUv[Auc||A||g||p ||Ticket-v]

其中 AUc=Kc,v[IDc||ADc||TS5||Kp] , $A= g^a \bmod p$ 用户选择随机密钥 Kp, 生成 AUc, 使用应用服务器的公钥 PUv 加密 AUc 以及 A, g, p, 然后发送给服务器. 服务器收到报文后, 用私钥解密, 再用 Kv 解密 Ticke-v, 用 Kc,v 解密 AUc, 验证用户身份, 同时获得用户的指定密钥 Kp.

6) V—>C:Kp[(TS5+1) ||B]

其中 $B= g^b \bmod p$

即服务器使用用户指定的 Kp 加密信息以及 B, 发送给用户. 用户收到响应消息后, 解密信息, 从而验证服务器身份. 用户 C 和应用服务器分别得到密钥 $K=g^{ab} \bmod p$, 然后用 K 作为双方会话的密钥.

2.4 效率分析

改进后的 Kerberos 协议虽然使用了公钥机制, 但并不需要给任何一个用户分配公钥, 只需要给 AS 服务器和应用服务器分配公钥和私钥, 因此并没有增加密钥管理难度. 并且只有第一和第五步用公钥加密, 相比其他混合加密机制, 安全性得到保证的同时, 效率也得到了提高, Kerberos 协议的整体性能不会因此而受到影响. 第五、六步使用了 DH 密钥交换算法, 根据文献[10]的实验数据, 虽然 DH 比 Kerberos 原有的对称加密算法要慢一些, 但比常见的非对称加密机制下的身份认证要快得多.

2.5 安全性分析

1) 防范口令攻击. 第一个报文的 AUc 用 Kc 加密, 而整个报文使用了 AS 的公钥加密, 只有 AS 才能解密, 从而大大地增强了 Kc 的安全性, 防范口令攻击. 攻击者利用 Kc 假冒用户 C 的可能性大大减少. 第二个报文不再使用 Kc 加密而是使用 Kt, Kt 并非固定, 而是用户随机选择的, 即使被攻击者获得, 攻击者也不能利用 Kt 假冒用户 C, 减少了用户被假冒的可能性.

2) 防范内部攻击. 应用服务器和用户之间下一阶段的会话密钥 K 是用 DH 密钥交换得到的, 即使是 Kerberos 服务器也不能获得这个 K, 不能监听用 K 加密的信息, 很好地防范了内部攻击.

3) 防范中间人攻击. DH 密钥交换是通过第五步骤和第六步骤来完成的. 第五个步骤的 AUc 是用 Kc,v 加密, 服务器以此可认证用户的身份. 而收到第六步的报文后, 用户通过密钥 Kp 解密报文来验证服务器的身份. 从而在获得强密钥的同时也能防范 DH 的中

间人攻击.

4) 增强 AS 服务器对用户身份的认证. 第一个报文的AUc用Kc加密, 从而能够使AS验证用户的身份.

增强的Kerberos方案与Kerberos协议的比较如表1所示.

表 1 增强的 Kerberos 方案与 Kerberos 协议的比较

	防范口令攻击	防范内部攻击	防范中间人攻击	使用公钥机制	是否六个步骤完成认证
增强方案	是	是	是	是	是
Kerberos 协议	否	否	是	否	是

3 小结

Kerberos 协议是目前广泛使用的身份认证协议, 通过 Kerberos 服务器, 用户和应用服务器获得相互认证并获得会话密钥, 但这个会话密钥可被进行内部攻击. 而用户与认证服务器之间的口令也存在被攻击的威胁. 改进后的 Kerberos 协议在应用服务器和 AS 服务器使用公钥机制, 利用公钥加密随机密钥以及 DH 密钥交换信息, 能够防范 Kerberos 的口令攻击和内部攻击.

参考文献

1 http://www.owasp.org/index.php/Category.

2 Neuman B, Ts'o T. Kerberos:an Authentication service for computer networks. IEEE Communications, 1994, 32(9): 33–38.

3 陈志德,许力.网络安全原理与应用.北京:电子工业出版社,2012.

4 Stallings W.密码编码学与网络安全—原理与实践.王张宜,杨敏,杜瑞颖,译.北京:电子工业出版社,2012.

5 Bellovin SM, Merritt M. Limitations of the Kerberos authentication systems. ACM SIGCOMM Computer Communication Review, 1990, 20(5): 119–132.

6 邵叶秦,陈建平,顾翔.改进的 Kerberos 单点登录协议.计算机工程,2011,37(24):109–111.

7 张利华,杨秀青.Kerberos 协议的安全性增强方案.计算机工程与设计,2009,30(9):2124–2126.

8 Dua G, Gautam N, Sharma D, Arora A. Replay attack prevention in Kerberos authentication protocol using triple password. International Journal of Computer Networks & Communications, 2013, 5(2): 59–69.

9 胡志刚,曾巧平.基于视觉密码的Kerberos改进协议.计算机工程,2009,35(18):159–160.

10 陈锋,徐正全,徐彦彦.一种利用Diffie-Hellman密钥协商改进的Kerberos协议.计算机应用,2007,27(Z2):116–117.

11 刘克龙,卿斯汉,蒙杨.一种利用公钥体制改进 Kerberos 协议的方法.软件学报,2001,12(6):872–877.

12 胡宇,王世伦.基于混合体制的 Kerberos 身份认证协议的研究.计算机应用,2009,29(6):1659–1661.