

基于视觉密码的 Kerberos 改进协议

胡志刚, 曾巧平

(中南大学信息科学与工程学院, 长沙 410083)

摘要:介绍 Kerberos 协议认证系统,分析 Kerberos 协议存在的局限性。提出一种基于视觉密码的新的认证方案。该方案将视觉密码技术融入 Kerberos 协议中,对改进前后协议的安全性进行比较分析,结果表明,该方案能有效地解决口令猜测攻击和重放攻击。

关键词: Kerberos 协议; 视觉密码; 身份认证

Improved Kerberos Protocol Based on Visual Cryptography

HU Zhi-gang, ZENG Qiao-ping

(College of Information Science & Engineering, Central South University, Changsha 410083)

【Abstract】 This paper introduces the authentication system of Kerberos protocol, and has a detailed analysis of the Kerberos protocol security. On this condition, it imports the scheme of visual cryptography into Kerberos protocol and constructs a new authentication scheme based on visual cryptography. It analyses the safety of Kerberos protocol, and the result shows that the new scheme can resist password attack and replay attack.

【Key words】 Kerberos protocol; visual cryptography; authentication

作为 TCP/IP 网络可信第三方鉴别协议, Kerberos 协议提供了一种在开放式网络环境下进行身份认证的方法。Kerberos 协议由于其优美的设计风格和方便易行,目前已经被许多组织采用。美国麻省理工学院于 2005 年对 Kerberos v5 版本^[1]进行修改并推出新的 Kerberos 协议规范^[2],但口令猜测攻击、重放攻击、时钟同步问题等缺陷依然存在。本文分析这些缺陷,并将视觉密码技术融入到 Kerberos 协议当中,构建出一套新的认证方案。

1 Kerberos 协议原理及安全性分析

1.1 Kerberos 协议原理

Kerberos 认证系统的认证过程包括 3 个通信方:客户端,应用服务器, Kerberos 服务器。应用服务要想为客户提供服务或客户端要想得到使用服务的权限,都必须先进行 Kerberos 服务器注册。Kerberos 服务器把相应的信息存入数据库,为认证提供信息保证。Kerberos 认证系统模型见图 1。

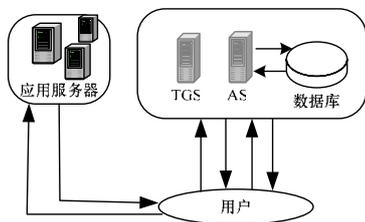


图 1 Kerberos 认证系统模型

Kerberos 认证系统的认证过程如下:

- (1) $C \rightarrow AS: \{C, TGS, IP, timestamp\}$
- (2) $AS \rightarrow C: \{K_{c, tgs}, TGT\} K_c$
- (3) $C \rightarrow TGS: \{S, TGT, A_{c, tgs}\}$
- (4) $TGS \rightarrow C: \{K_{c, s}, T_{c, s}\} K_{c, tgs}$
- (5) $C \rightarrow S: \{S, T_{c, s}, A_{c, s}\}$

$$(6) S \rightarrow C: \{timestamp + 1\} K_{c, s}$$

客户端 C 向认证服务器 AS 发送认证请求。 AS 返回票据授权票 TGT 和会话密钥 $K_{c, tgs}$ 。客户端收到 AS 返回的信息,客户端根据用户口令生成私钥 K_c 对收到的信息解密,并将得到的 TGT 连同验证码 $A_{c, tgs}$ 一起发送给 TGS 。 TGS 比较 TGT 和 $A_{c, tgs}$ 的信息是否一致来验证客户端的身份,如果身份被确认, TGS 返回访问服务器的票据 $T_{c, s}$ 和会话密钥 $K_{c, s}$ 给客户端。客户端将接受到消息解密得到会话密钥 $K_{c, s}$,并把 $T_{c, s}$ 和验证码 $A_{c, s}$ 一起发送给服务器。服务器比较 $T_{c, s}$ 和 $A_{c, s}$ 是否一致来验证客户端的身份,如果身份被确认,就将时戳加一返回给客户端。客户端比较时戳的有效性实现对应用服务器的认证。

整个认证过程完成后,客户端和服务器端就用会话密钥 $K_{c, s}$ 进行通信。

1.2 Kerberos 协议安全性分析

(1) 口令猜测攻击

在 Kerberos 协议认证过程中,用户向 AS 请求认证时, AS 会把相关信息用客户端的密钥 K_c 加密后发送给客户端。该密钥是根据客户输入的口令随机生成的。攻击者可以收集大量相关信息,通过计算和密钥分析来进行口令猜测。如果攻击者掌握了足够的信息,就有可能猜测出用户的口令。若用户选择的口令不够强,就不能有效地防止口令猜测攻击。

(2) 重放攻击

Kerberos 协议是通过在消息中加入时戳来防止重放攻击。整个认证过程需要各个服务器和客户端的时钟保持同步,这在分布式的环境中是非常困难的。由于变化的和不可预见的网络延迟的本性,不能期望分布式时钟保持精确的同步。

作者简介: 胡志刚(1963 -),男,教授、博士生导师,主研方向:网络并行计算,网络安全;曾巧平,硕士

收稿日期: 2009-01-06 **E-mail:** fengdeshizheqp@sina.com

一般来说,在认证过程中时间相差 5 min 就认为是新的消息。这样,时戳就带来了重放攻击的隐患,在规定的时间内,攻击者完全可以事先把伪造的消息准备好,一旦得到票据就马上发出。这在规定的时间内是很难被察觉的。

(3)时钟同步问题

整个 Kerberos 协议都严重依赖时钟,而在分布式环境中实现精确的时钟同步几乎是不可能的。此外,在认证过程中,认证码的有效性也是由时钟决定的。如果主机的事件发生错误,原来的认证码就是可以被替换的。攻击者也可以通过干扰时钟的方式使认证过程失败。

(4)可信第三方的安全问题

Kerberos 协议的整个认证过程是基于可信第三方的。如果第三方服务器(Kerberos 协议服务器)不安全,实现整个系统的安全也就不可能了。一旦攻击者利用执行 Kerberos 协议和记录用户口令的软件来代替用户的 Kerberos 软件,整个系统的客户端都将被其控制。一般来说,装在不安全服务器上的密码软件都存在这个问题。

(5)密钥管理与维护

Kerberos 协议的认证过程是以是否知道密钥作为认证的依据,一旦攻击者窃取密钥,就可以伪装成相关的服务器窃取用户信息。这就给密钥的管理和更新带来了很大困难,采取特别细致的安全管理措施也将付出很大的代价。

2 改进的 Kerberos 协议

2.1 视觉密码

一个集合 P 拥有 w 个参与者,他们将一幅密图 s 编码分成 w 个影子图像(shadow image),称为图份(share)。 P 中的每一个参与者都获得一个图份。这些参与者中的某些许可的子集能够可视地恢复密图,而任何其他子集得不到关于 s 的任何信息。这就构成了一个视觉密码方案^[3]。下文以最简单的二值图像视觉密码为例,简单介绍视觉密码的基本原理。

视觉密码对图像以像素为单位来操作。二值图像由黑、白两种像素所组成的。原始图像中的每一个像素,都被加密到 2 张共享份中,在共享份中该像素被加密成 2 个像素,黑白像素的加密规则^[4]如图 2 所示。

| Pixel | | Share1 | Share2 | Result | Pixel | | Share1 | Share2 | Result |
|-------|-----------|--------|--------|--------|-------|-----------|--------|--------|--------|
| □ | $P = 0.5$ | ■ □ | ■ □ | □ | □ | $P = 0.5$ | ■ □ | ■ □ | □ |
| | $P = 0.5$ | □ ■ | □ ■ | □ | | $P = 0.5$ | □ ■ | □ ■ | □ |
| ■ | $P = 0.5$ | ■ □ | □ ■ | ■ | ■ | $P = 0.5$ | ■ □ | □ ■ | ■ |
| | $P = 0.5$ | □ ■ | ■ □ | ■ | | $P = 0.5$ | □ ■ | ■ □ | ■ |

图 2 视觉密码规则

视觉密码技术不需要任何高深的数学理论支撑,运行效率非常高,其安全性主要依赖于伪随机数的伪随机特性。针对 Kerberos 协议存在的缺陷,本文采用视觉密码技术与随机数的机制来解决口令猜测攻击、重放攻击等问题。将视觉密码技术应用到认证系统中的方法如下:根据认证方随机产生的密钥生成一幅视觉图像 P ,再根据双方共享的影子图像 IC_u 生成一幅新的影子图像 IC_t 发送给被认证方,被认证方将 IC_t 放进可计算设备,与自己已有的 IC_u 叠加合成视觉图像 P ,被认证方通过视觉从视觉图像 P 中读取该密钥。由于攻击者无

法由其中一幅影子图像得到原始图像信息,从而能够确保共享密钥的安全。同时,根据随机数在线更新共享的影子图像 IC_u 能保证每次认证的影子图像都是随机的。

2.2 用户注册

用户向注册机构提供有效的身份证明,获得 ID(整个系统是唯一的),影子图像序列 $IC_{c,as}, IC_{c,tgs}, IC_{c,s}$ 。其中, $IC_{c,as}$ 是客户端和 AS 相互认证的影子图像序列; $IC_{c,tgs}$ 是客户端和 TGS 相互认证的影子图像序列; $IC_{c,s}$ 是客户端和服务端相互认证的影子图像序列。假设每个影子图像序列的长度为 n 。

2.3 认证过程

(1)客户端向认证服务器发送认证请求。发送的信息包括客户端的 ID, IP, TGS 的名称,以及随机数 $N_{c,as}$ 。整个信息以明文的形式发送。

$$C \rightarrow AS : \{ID, IP, TGS, N_{c,as}\}$$

(2)认证服务器收到认证请求,随机生成客户端的私钥 K_c ,并将其编辑成视觉图像,根据 $IC_{t,as}^i$ 生成另一幅影子图像 $IC_{t,as}^i$ 。AS 随机生成客户端和 TGS 的会话密钥 $K_{c,tgs}$,按同样的方式,根据 $IC_{c,tgs}^i$ 生成另一幅影子图像 $IC_{c,tgs}^i$ 。然后计算出 $MAC(K_c, N_{c,as}; IC_{t,as}^i)_{AS}$,将 $MAC(K_c, N_{c,as}; IC_{t,as}^i)_{AS}$, TGT(包含 TGS 的名称、客户端名称、客户端 IP、会话密钥 $K_{c,tgs}$; 用 K_{tgs} 加密)和 $IC_{c,tgs}^i$, 用 K_c 加密后,连同 $IC_{t,as}^i$ 发送给客户端。同时,根据随机数 $N_{c,as}$ 更新影子图像,即根据 $N_{c,as}$ 和 n 求余的结果,选取影子序列中的一幅作为下次认证的影子图像。

$$AS \rightarrow C : \left\{ \left\{ TGT, MAC(K_c \oplus N_{c,as}; IC_{t,as}^i)_{AS}, IC_{c,tgs}^i \right\} K_c, IC_{t,as}^i \right\}$$

(3)客户端向 TGS 发送票据请求。客户端接收到 AS 的应答信息,把 $IC_{t,as}^i$ 送进具有可计算机能力的 E_u 中,通过视觉读取客户端私钥 K_c 。利用 K_c 解密得到 AS 发送过来的 $MAC(K_c, N_{c,as}; IC_{t,as}^i)_{AS}$, $IC_{c,tgs}^i$ 和 TGT。客户端自身也计算出 $MAC(K_c, N_{c,as}; IC_{t,as}^i)_c$ 与 AS 发送过来的 MAC 进行比较,看是否一致,如果不一致,就退出登录。如果相符,客户端把 $IC_{c,tgs}^i$ 送进 E_u 中,通过视觉读取 $K_{c,tgs}$ 。然后把要访问的服务器名字,票据授权票 TGT 和鉴别码 $A_{c,tgs}$ (包含 TGS 名称,客户端名称,客户端 IP; 用 $K_{c,tgs}$ 加密)及随机数 $N_{c,tgs}$ 发送给票据授权服务器。同时也按式(2)更新客户端的影子图像。

$$C \rightarrow TGS : \{S, TGT, A_{c,tgs}, N_{c,tgs}\}$$

(4)TGS 收到客户端的请求,用 K_{tgs} 解密 TGT 得到 $K_{c,tgs}$,并用其对 $A_{c,tgs}$ 解密后比较 TGT 和 $A_{c,tgs}$ 是否相符合。如果不一致,就退出登录。如果客户端身份被确认,TGS 把随机生成的会话密钥 $K_{c,s}$ 编辑成视觉图像,根据 $IC_{t,s}^i$, 生成另一幅影子图像 $IC_{t,s}^i$, 然后计算出 $MAC(K_{c,s}, N_{c,tgs}; IC_{t,s}^i)_{TGS}$ 和访问服务器的票据 $T_{c,s}$ (包含客户端名称,客户端 IP,服务器名称,会话密钥 $K_{c,s}$; 用 K_s 加密)发送给客户端。同时,也按(2)的方式,根据 $N_{c,tgs}$ 更新影子图像。

$$TGS \rightarrow C : \left\{ \left\{ T_{c,s}, MAC(K_{c,s} \oplus N_{c,tgs}; IC_{t,s}^i)_{TGS} \right\} K_{c,tgs}, IC_{t,s}^i \right\}$$

(5)客户端接收到 TGS 的应答信息,把 $IC_{t,s}^i$ 送进具有可计算机能力的 E_u 中,通过视觉读取客户端与服务器的会话密钥 $K_{c,s}$ 并用会话密钥 $K_{c,tgs}$ 解密得到 $T_{c,s}$ 和 $MAC(K_{c,s}, N_{c,tgs}; IC_{t,s}^i)_{TGS}$ 。客户端自身也计算出 $MAC(K_{c,s}, N_{c,tgs}; IC_{t,s}^i)_c$ 与

(下转第 163 页)