即时通讯行业动态口令解决方案

北京坚石诚信科技股份有限公司

2008-5-12

目 录

1. 概述

即时通讯在国内自 1998 年面世以来发展迅速。预计到 2010 年，中国即时通讯市场规模将达到 1.14 亿美元。而随着电信运营商的加入,市场竞争将更加激烈，市场格局将进一步变化。

1.1 即时通讯软件

即时通讯(IM)是指能够即时发送和接收互联网消息等的业务。自 1998 年面世以来，特别是近几年的迅速发展，即时通讯的功能日益丰富，逐渐集成了电子邮件、博客、音乐、电视、游戏和搜索等多种功能。即时通讯不再是一个单纯的聊天工具，它已经发展成集交流、资讯、娱乐、搜索、电子商务、办公协作和组织客户服务等为一体的综合化信息平台。

随着移动互联网的发展，互联网即时通讯也在向移动化扩张。目前，微软、AOL、Yahoo、腾讯等重要即时通讯提供商都提供通过手机接入互联网即时通讯的业务,用户可以通过手机与其他已经安装了相应客户端软件的手机或电脑收发消息。

1.1.1 即时通讯行业现状和发展趋势

即时通讯最初是由 AOL、微软、雅虎、腾讯等独立于电信运营商的即时通讯服务商提供的。但随着其功能日益丰富、应用日益广泛，特别是即时通讯增强软件的某些功能如 IP 电话等，已经在分流和替代传统的电信业务，使得电信运营商不得不采取措施应对这种挑战。2006 年 6 月，中国移动已经推出了自己的即时通讯工具--Fetion，中国联通也将推出即时通讯工具“超信”，但由于进入市场较晚，其用户规模和品牌知名度还比不上原有的即时通讯服务提供商。

近年来，即时通讯市场用户规模增长迅速，市场规模前景广阔。随着互联网用户的快速增长，即时通讯用户也日益增长，iResearch 预测到 2010 年中国即时通讯用户数量将超 2 亿,而中国即时通讯市场规模到 2010 年将达到 1.14 亿美元。

移动即时通讯市场有着更加巨大的成长空间和诱惑力。据 iResearch2006 年 5 月发布的调查报告显示，2005 年我国移动即时通讯的用户已达到 500 万；未来几年移动即时通讯用户规模将呈现快速增长，预计到 2010 年中国移动即时通讯用户将达到 2000 万人。

目前即时通讯行业仍处于高速发展期，在未来的发展中呈现出整合多种业务、扩张移动平台、渗透组织用户、融入收费内容的发展趋势。对于移动运营商来说，既有机会存在，但同时也存在威胁。机会是移动运营商拥有顺应即时通讯

行业发展的多业务资源，在此阶段介入又可以利用原有即时通讯发展时积累的用户使用习惯和业务、运营经验，更快地取得成功。

随着宽带网的普及，即时通讯的内涵也开始变化。与过去的纯文本交流不同，新型的即时通讯业务融合了视频、音频交流等宽带应用元素。目前各种即时通讯除提供了基本的即时互动交流外，还能提供视频、语音通讯服务，在短信收发、文件共享、数据传输、游戏、娱乐、个性化设置等方面也都有大的开拓和创新。总之，多媒体化是即时通讯未来的发展方向，未来即时通讯将捆绑更多的互联网和电信增值业务功能。

移动通讯业务的迅速发展使得传统的互联网即时通讯服务商将移动用户作为下一步市场发展的重点，这在移动增值服务成为即时通讯服务商收入的主要来源之后体现尤为突出。即时通讯业务承载的设备也趋于多样化，用户通过 PC、手机、PDA 以及其他设备等都可以使用即时通讯。

1.1.2 即时通讯软件的用户群体

为了更好地理解即时通讯软件对特定用户的价值和意义，可以将庞大的即时通讯用户进行分类，各类用户在使用即时通讯软件的过程中，逐渐形成自己的使用习惯和定位。首先可以将即时通讯用户分为组织用户和个人用户。

组织用户主要可以分为两种类型:

（1）使用通用的、开放的即时通讯软件作为组织对内和对外的沟通交流平台。大多数中小组织普遍采用这种方式，主要的优势是即时通讯软件已经比较多，而且功能也比较丰富，基本上可以满足组织对内对外沟通和交流的目的，再加上即时通讯软件还可以免费使用；缺点是无法满足组织的特殊需求。

（2）自主研发或购买组织专用的即时通讯软件，实现组织对内和对外的沟通和交流。这种方式主要是大组织以及对即时通讯具有特殊需求(比如业务需求、安全需求等)的组织所采用。这种方式主要的优势在于可以满足组织特定的业务和安全需求；缺点是需要支付相当的开发或者购买费用。

个人用户从总体上也可以分为两类:

（1）免费用户在即时通讯软件的用户中占多数，使用即时通讯软件的主要目的是聊天、娱乐等非经济活动的用户通常都是免费用户，这类用户对安全性需求低一些，所以选择免费服务。

（2）付费用户，其中商务人员、业务人员、中小组织主和自由职业者是付费用户的主要来源，主要是因为这些用户使用即时通讯软件对其具有重要的经济价值，对安全性要求也更高，愿意通过支付一定的费用来保证即时通讯软件的正常使用或者享受一定的附加服务。

1.1.3 即时通讯软件的优势

在众多的网络应用中，即时通讯之所以受到广大用户的喜爱，主要是即时通讯软件相比于其他的网络应用具有明显的优势，主要体现在以下几个方面:

（1）即时通讯软件比 Email 具有更快的反馈速度

（2）便于快速解决问题
（3）多功能便利性
（4）看到对方是否在线/有空
（5）获得某人的注意
（6）可联系到没有在 EMAIL 或电话中回话的人
（7）节约长途话费
（8）高效搜集信息，包括各种联系信息、历史交流信息等

正是上述的各种优势，使其能够满足广大用户的各种各样的需求，从而吸引大量用户使用，用户量的增加促使开发商对软件的改进和完善，从而使得用户得到更好的服务，使得即时通讯的发展进入一个良性循环。

1.2 即时通讯软件的安全

即时通讯软件在取得快速发展并给人们带来诸多好处的同时，自身也存在一定的安全问题。在即时通讯软件中发生的各种各样的安全问题，其中最主要的就是盗号问题。本节将对此进行探讨。

1.2.1 盗号成为重要安全问题

即时通讯软件遭遇的安全问题主要体现在三个方面:

（1）木马、病毒等恶意代码利用特定的即时通讯工具提供的通讯平台进行传播，以达到传播自己进行更大范围破坏的目的。

（2）木马程序对即时通讯软件或系统进行监控，以达到窃取用户帐号和密码的目的。

（3）盗号者通过发送虚假信息（如中奖、注册新用户送礼等）制造陷阱，引诱用户上当，然后趁机盗取用户帐号。

在所有的即时通讯软件安全问题中，盗号问题是最为严重的一种。要解决即时通讯软件的安全问题，必须解决的问题就是防止用户帐号被盗。

1.2.2 盗号频发的主要原因

在即时通讯软件带给人们越来越多方便和快捷的同时，困扰人们的盗号问题也变得越来越突出，严重影响被盗号者的利益。从总体上来看，即时通讯软件盗号事件频发的主要原因包括以下几个方面:

（1）即时通讯软件的安全机制不足

目前即时通讯软件基本上都是采用用户帐号加静态密码（即每次认证使用固定内容作为密码）的方式进行用户身份认证。该方式在安全性方面存在先天不足的缺陷，因为一旦帐号和密码被盗，盗号者对该帐号就有完全控制权。从当前的计算机安全现状来看，盗取用户帐号和密码的方式多种多样，有令人防不胜防的感觉。

（2）盗号者唯利是图

在即时通讯软件发展的早期阶段，即时通讯软件用户量较小，而且功能相对简单，用户对其的依赖性也相对比较小，再加上用户基本上都是免费用户，此时盗号并没有实际利益，所以盗号事件发生较少。

随着即时通讯软件用户量的增加，功能的扩展，使得用户将其融入到自己的工作、学习和生活的各个层面后，用户对其的依赖性大大提高了。部分人慢慢愿意通过付费来使用即时通讯软件，特别是出现了某些特殊帐号进行明码标价的交易。此时的即时通讯软件帐号已不再是一个简单的标识符号了，而是已经具有经济价值的资源。盗号者为了追逐经济利益，采取各种各样的手段进行盗号。

（3）补救措施缺乏可操作性

为了解决帐号被盗的问题，开发商通常会提供一些补救措施，主要的方式包括通过回答自定义问题找回密码，发送密码到注册时指定的邮箱以及发送密码到注册时指定的手机等，这几种方式看起来好像可以解决问题，但是在实际操作时还是存在多种不足。

回答自定义问题找回密码存在的障碍主要有注册时可能没有设置问题答案、设置了问题答案但是没有在意、设置了问题答案因为时间忘记了等，其中最大的问题就是对于长时间不使用的问题答案很容易忘记。

发送密码到注册时指定的邮箱的最大问题就是过分依赖于注册邮箱的安全，特别经过比较长一段时间以后，很可能忘记使用的是哪个邮箱注册（特别是当一个人具有很多个邮箱的时候）、注册邮箱密码忘记、注册邮箱被注销以及注册邮箱被盗等，都会给找回密码带来问题，总之必须首先保证邮箱是安全的，如果邮箱被盗，此时将帐号和忘记的密码发送到邮箱，岂不更加危险。

发送密码到注册时指定的手机的最大问题就是对手机安全的依赖，如果手机发生丢失、SIM 损坏、因手机换号导致以前注册的号码被注销等情况，不但不利于找回密码，而且还可能导致把帐号和密码发送给别人。

如果安全考虑不充分的话，还可能被盗号者修改各种注册设置，当用户请求密码时，密码会更加当前设置发送给盗号者指定的位置，对于找回密码也就成为一句空话了。

（4）用户安全意识薄弱

使用即时通讯软件的用户应该说绝大多数都不是计算机相关专业人员，往往会出现只关注应用，而忽视安全的情况，再加上计算机和网络安全形势本来就不容乐观的现实环境，使得盗号者有机可乘。

需要特别指出的是在公共场所（如网吧、学校机房、图书馆等）使用即时通讯软件，必须提高安全意识，积极采取相关防御措施，才能避免安全风险。

（5）盗号方式多样化

盗号方法主要包括技术性盗号和非技术性盗号两种方式，技术性盗号包括针对特定即时通讯软件的盗号木马、键盘记录木马、截屏、系统功能调用拦截以及文件信息分析等。非技术性盗号包括窥视和针对特定即时通讯软件的网络钓鱼。

要做到有效防止盗号，必须针对上述各种盗号方式都有效的“防盗”技术，才能达到真正防止盗号者盗号的目的。

（6）相关法律法规不健全

目前，在国内对网络虚拟资产（包括即时通讯软件帐号、网络游戏帐号、电

子游戏帐号以及各种电子货币等）进行保护的相关法律法规还不健全，因此，给盗号者采取各种手段进行疯狂盗号提供了可乘之机。

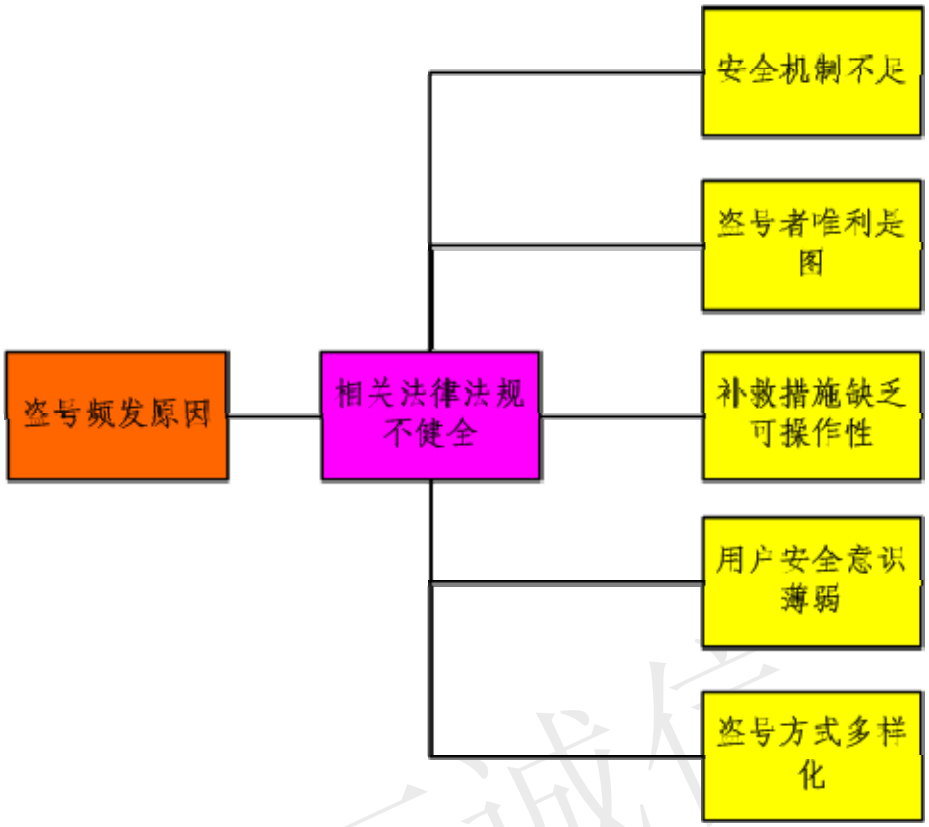

图1 盗号频发的主要原因

1.2.3 防止盗号的解决方案

防止盗号的最好方法就是加强用户的身份认证，使用增强型的双因素动态口令身份认证技术配合传统的用户帐号加静态密码身份认证技术，可以有效防止盗号的发生。在具体的使用策略上，有三种方式可供选择：第一种方式是在用户登录时添加动态口令身份认证；第二种方式是在取回密码的时候添加动态口令身份认证；第三种方式是在用户登录和取回密码时都使用动态口令身份认证技术。下面对这三种方式做一个简单的介绍。

第一种方式，每次登录时都使用动态口令双因素认证

每次启动时都使用动态口令双因素认证大大提高了每次登录的安全性，可以有效避免帐号被盗，主要原因是每次登录时使用的动态口令都不相同，即使别人能够通过各种方法和手段得到用户的登录帐号和密码，还是无法正常登录，因为动态口令的最大一个特点就是每次登录时所使用的密码都不相同，这些不同的密码由用户在需要的时候通过专门的硬件产生，再加上用户的静态密码构成新的认证密码，只有一次性密码和静态密码的认证都通过的时候才会用户才能完成登录，这大大提高了用户登录时的安全性。

采用这种认证方式也有一定的缺点，哪就是用户在每次登录的时候都必须同

时输入静态密码和动态密码，所以用户也必须随身携带动态口令令牌（专门用户生成动态口令的专门硬件设备），以便在登录以前能够得到动态口令。

第二种方式，只在取回密码时才使用动态口令双因素认证

采用这种方式是一个比较折中的方法，因为通常情况下，用户登录的次数远远大于取回密码的次数，所以对于正常的登录操作没有任何的影响，而只是在密码遗忘或者盗号发生以后，用户通过自己的动态口令令牌使用动态口令就可以找回自己的密码，然后更改密码就完成了重新找回帐户的过程，甚至根本不用服务商的服务。最大的好处是使用动态口令身份认证以后，

采用这种方式的基本思路是在盗号发生以后采取积极有效补救措施，当然在盗号发生以后和找回以前仍然存在一定的安全风险，主要体现在用户相关信息（比如联系信息、好友信息等）可能被偷看、篡改、删除等，从而给用户带来一定程度的损失，这是该方式的最大缺点。

第三种方式，在登录和取回密码时都使用动态口令双因素认证

采用这种方式的最大好处就是得到最大的安全性，缺点就是在登录时和静态密码遗忘并取回密码时都需要动态口令令牌生成动态口令，所以要求用户需要随时携带动态口令令牌。

1.3 动态口令认证技术

动态密码即一次性密码，使用一次以后就自动作废，下次进行身份验证的时候需要新的密码。动态密码和传统的静态密码配合使用，可以大大提高系统身份认证系统的安全。

1.3.1 基本原理

动态密码基本的思路是将共同密钥信息（作为计算动态密码的常量）和加密算法同时保存在认证服务器和动态密码令牌硬件内，再选择一个认证服务器和动态令牌都可以使用的变量（比如动态密码生成次数或者当前时间或者挑战码）用于计算的动态密码，需要认证的时候，由动态令牌首先计算出动态密码，然后传输给认证服务器，认证服务器采用对应的信息计算出动态密码，通过比较这两个密码是否相同来判断输入的动态密码是否正确。

采用时间作为变量来计算动态密码而进行认证的技术称为时间同步认证技术，采用动态密码生成次数作为变量来计算动态密码而进行认证的技术称为事件同步认证技术，使用由认证服务器返回的数值作为变量来计算动态密码而进行认证的技术称为挑战/应答认证技术。

（1）时间同步认证技术

基于时间同步认证技术是把时间作为变动因子，一般以 60 秒作为变化单位。所谓“同步”是指用户动态密码令牌和认证服务器所产生的口令在时间上必须同步，不然，令牌产生的动态口令和认证服务器产生的动态口令不相同，服务器无法完成认证。在实际使用中，保持动态令牌和认证服务器的时间完全相同有一定的困难，所以通常允许存在一定的时间差异，比如 20 分钟。

（2）事件同步认证技术

基于事件同步认证技术是把已经生成动态口令的次数（即事件序列）作为动态口令令牌和认证服务器计算动态口令的一个运算因子，与令牌和认证服务器上的共同密钥产生动态口令。这里的同步是指每次认证时，认证服务器与令牌保持相同的事件序列。如果用户使用时，因操作失误多产生了几组口令出现不同步，服务器会自动同步到目前使用的口令，一但一个口令被使用过后，在口令序列中所有这个口令之前的口令都会失效。其认证过程与时间同步认证相同。

（3）挑战/应答认证技术

挑战/应答方式的变动因子是由认证服务器产生的随机数字序列，作为令牌和认证服务器生成动态口令的变动因子。

1.3.2 工作过程

这里以事件同步认证技术的动态口令令牌配合登录即时通讯服务器的认证过程为例，说明用户使用动态口令完成身份认证的过程。

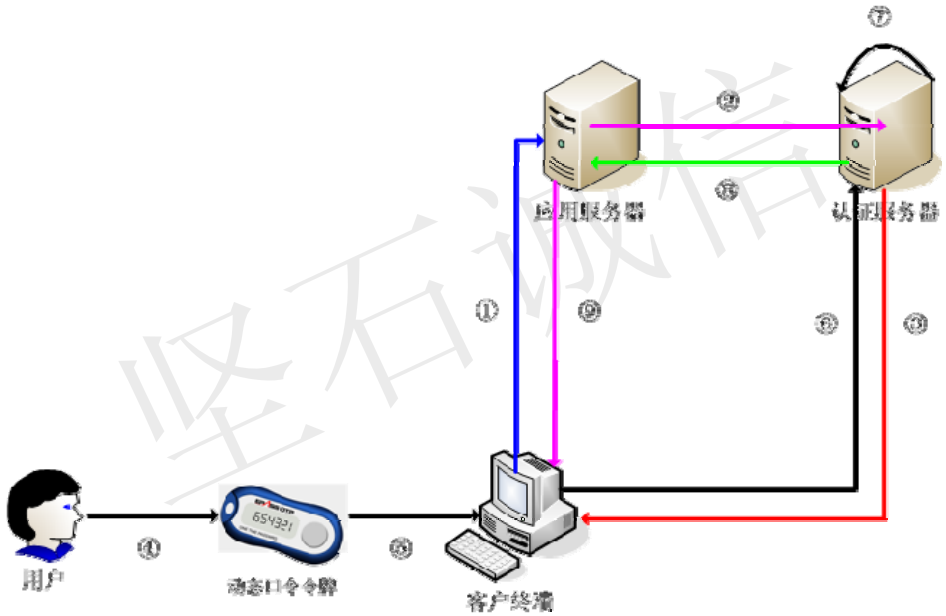

图2 动态口令身份认证系统工作过程

① 客户请求接入应用服务器;

② 应用服务器请求认证服务器对客户的身份的合法性和真实性进行认证;

③ 客户终端弹出身份认证对话框;

④ 客户激活令牌，生产动态口令;

⑤ 客户将帐号和口令键入终端的身份认证对话框;

⑥ 客户终端将帐号和口令通过网络传输给认证服务器;

⑦ 认证服务器调用客户信息，产生与客户信息和事件相关的随机序列，并与客户输入的口令进行比对，判别客户身份的合法性和真实性;

⑧ 认证服务器将认证结果报告给应用服务器;

⑨ 应用服务器根据客户身份的合法性和真实性反馈给客户终端，并决定可

以提供服务或拒绝服务。

1.3.3 动态口令特点

动态密码技术用于身份认证，主要具有以下特点:

（1）动态性：动态口令令牌产生的口令每分钟变化（针对时间同步技术的动态口令卡而言）一次，不同时刻使用不同口令登录，每个口令都只在其产生的时间范围内有效。

（2） 随机性：动态口令每次都是随机产生的，不可预测。

（3）一次性：每个动态口令使用过一次后，不能再连续重复使用。

（4）抗偷看窃听性：由于动态性和一次性的特点，即使某一个动态口令被人偷看或窃听了，也无法使用。

（5）不可复制性：动态口令与口令卡是紧密相关的，不同的口令卡产生不同的动态口令。而且口令卡是密封的，卡内密钥数据一旦断电就会丢失。因此也就保证只有拥有口令卡的用户才能使用动态口令，其他用户无法获得，也无法共享。

（6）方便性：口令卡随身携带，动态口令显示在卡上，无需再为记忆复杂的、定期更改的口令而烦恼。

（7）危险及时发现性：口令卡随身携带，一旦遗失或失窃，就会及时发现、及时挂失，把损失降到最小。

（8）抗穷举攻击性：由于动态性的特点，如果一分钟内穷举不到，那么下一分钟就需要重新穷举，因此新的动态口令可能就在已经穷举过的口令中。另外还可以通过系统设置，限制一分钟内用户登录尝试的次数，从而进一步降低穷举攻击的风险。

2. 坚石 OTP 解决方案

OTP 是坚石诚信科技有限公司推出的动态口令身份认证产品，通过使用动态口令身份认证技术来提高身份认证的准确性，防止帐号和密码泄露后被再次使用的风险。

2.1 方案概述

OTP 身份认证系统对各种应用环境具有广泛的灵活性和适应性，能够适应各种使用环境，只需要在服务器端安装和配置相应的身份认证模块，无需对客户端软件做任何的改动，也无需在客户端安装任何软件。

2.2 总体方案

OTP 身份认证解决方案采用基于模块化的分层体系结构、成熟的技术和开放体系结构，系统具有高可靠性、可用性和可维护性，同时向相关服务提供商和各用户提供良好的灵活性和性价比。

2.2.1 OTP 系统组成

OTP 身份认证服务器和认证备份服务器完全独立于即时通讯服务器的业务系统，只需要在原有认证服务器系统或业务系统中安装认证代理模块即可，不用更改原有网络结构设计。

基本结构如图 3 所示。

1. OTP 动态口令身份认证系统

OTP 动态口令身份认证系统是完成用户身份认证功能的核心，根据具体的需求情况，可以为即时通讯软件的登录、修改密码、找回密码、删除信息等关键操作提供用户身份认证功能。当某个操作需要增强的用户身份认证功能时，就可以启用对应的保护，当用户执行对应的操作时，就会要求用户输入动态口令进行认证，由即时通讯服务器传递认证信息给认证服务器，认证服务器根据其存储的信息验证用户的登录信息是否正确，如果正确，认证服务器返回认证成功，用户成功执行相关操作，否则，认证服务器返回认证失败，用户操作被禁止。

2. 认证备份服务器

后备认证服务器是对认证服务器的完全备份，它能够在认证服务器发生故障或检修时，及时接管认证服务器的认证工作。

3. 管理工作站

管理工作站提供动态身份认证系统的管理界面，它在网络管理员与认证服务器之间提供一个友好的操作界面，便于网络管理员对系统维护和用户管理。通过管理工作站，网络管理员可以进行网络配置、动态口令令牌管理（比如添加、删除、和用户绑定、锁定、解锁等）、用户管理（比如添加、删除、分配令牌等）以及认证日志管理等操作。

4. 动态口令令牌

动态口令令牌是一个单独的硬件设备，使用时无需连接任何外部设备，所以具有很大的灵活性，登录应用服务器时，只需要激活动态口令令牌，将生成的动态口令输入登录窗口中的对应位置即可。

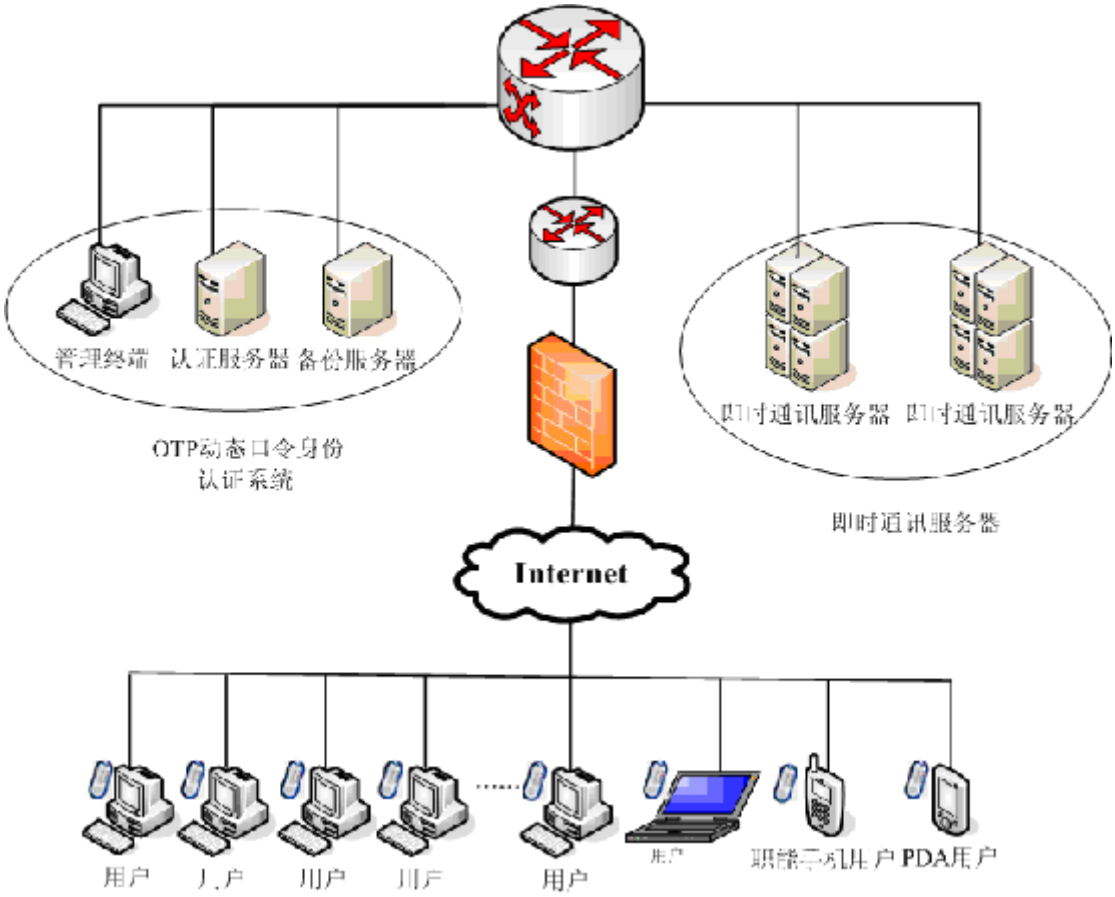

图3 OTP 认证解决方案系统组成图

2.2.1 OTP 系统工作流程

为了简洁地说明 OTP 系统进行动态口令身份认证的工作流程，这里以通过即时通讯软件登录服务器为例，说明整个认证过程，另外，这里不考虑复杂的网络结构以及其它的安全措施（比如防火墙）。

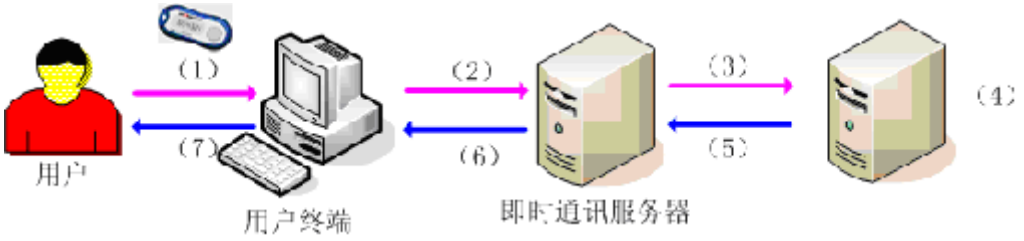

图 4 认证过程

（1）用户登录即时通讯软件时，输入帐号、静态密码和动态口令;

（2）帐号、静态密码和动态口令从用户终端通过互联网传递到即时通讯服务器;

（3）即时通讯服务器首先验证静态密码是否正确，如果不正确，直接向用户返回认证失败消息，如果静态密码认证成功，即时通讯服务器将用户帐号和动

态口令传递给 OTP 认证服务器，请求进行认证；

（4）OTP 认证服务器通过得到的帐号和动态口令，首先读取存储在服务器中的相关信息，并计算出动态口令，将收到的动态口令和计算得到的动态口令进行比较，判断收到的口令是否为有效口令；

（5）OTP 认证服务器将认证结果发送给即时通讯服务器；

（6）即时通讯服务器根据接收到的认证结果进行处理，如果认证成功，即时通讯服务器允许用户登录，并将成功登录信息返回给用户；如果认证失败，即时通讯服务器拒绝用户登录，并将失败信息通过互联网返回给用户；

（7）如果用户成功登录，标识用户身份认证成功，如果失败，则显示失败原因。

2.2.3 OTP 系统与应用服务器的集成

OTP 系统和即时通讯服务器进行集成时，考虑到和原系统的兼容性以及安全性，通常保留原有系统静态密码认证，此时就可以实现动态口令和静态口令相结合进行身份认证，其基本逻辑结构如图 5 所示。

由即时通讯服务器的认证模块进行静态密码认证，动态口令的认证由 OTP 认证代理传递给 OTP 认证服务器进行认证，认证完成后返回认证结果。两种认证只要有一种认证失败就可以认为认证失败，此时应用服务器就可以拒绝用户登录应用服务器。为了防止拒绝服务攻击，静态口令认证应该在动态口令认证以前执行，如果静态口令认证失败，就不再进行动态口令认证，而是直接返回认证失败，即只有在成功通过静态口令认证的前提下才进行动态口令认证。

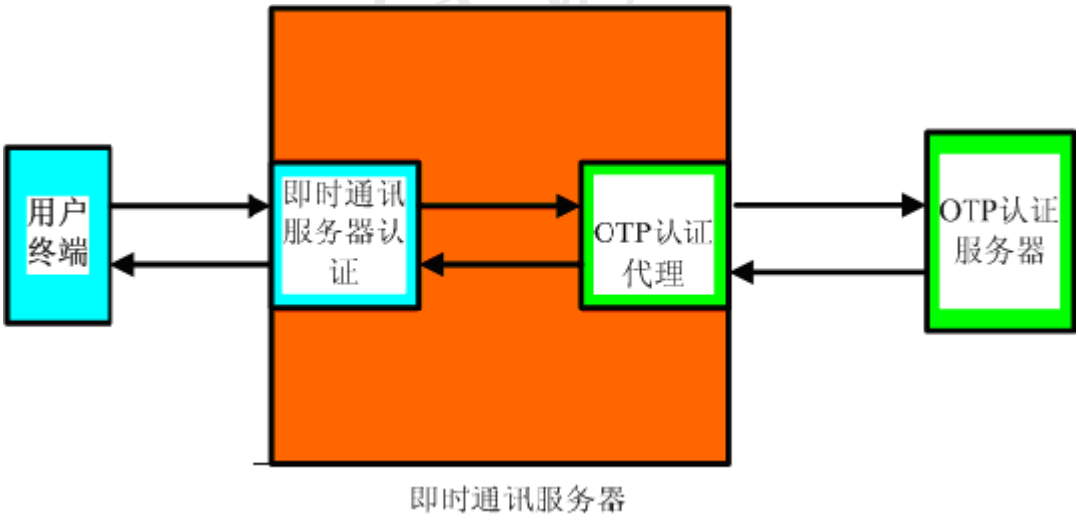

图 5 应用认证组件图

2.2.4 OTP 系统对即时通讯的保护模式

OTP 提供的动态口令身份认证具有很大的灵活性，服务提供商和用户可以根

据需要选择多种认证方式。

首先，作为服务提供商，可以为付费用户提供动态口令来保护用户登录和用户的关键操作（比如修改密码、密码找回、修改系统设置、修改或者删除相关信息等），当用户进行这些操作时，要求用户提供动态口令进行验证，即使用户为了登录方便没有设置保护，只要用户在关键操作上设置了保护，那么盗号者通过盗取的号码和密码进入后还是无法进行密码修改、删除或修改用户相关的信息等操作，还是可以保护用户帐号的安全。通过这些保护措施，可以有效防止盗号者采用各种手段进行盗号。

其次，作为付费用户，可以根据服务提供商提供的安全保护功能，根据自己的安全需求和喜好设置安全保护模式，比如可以保护登录、保护修改密码、保护密码找回、保护删除好友、保护修改系统设置等。只要用户认为对自己重要的操作，都可以设置保护，在进行操作时，都会要求用户输入动态口令。即使为了操作方便用户没有设置登录保护，使得盗号者盗号成功，那么盗号者登录以后对于用户设置保护的操作项均无法进行操作（因为操作需要动态口令），因为盗号者无法得知这些动态口令是什么。

通过上述的分析可知，OTP 提供的动态口令身份认证保护方式具有极大的灵活性，可以完全满足用户对方便性和安全性的需求。

2.3 方案对相关利益者的效益分析

采用 OTP 身份认证解决方案提供即时通讯行业的身份认证安全具有很大的灵活性和性价比。主要体现在服务提供商和用户两个方面，下面对其进行简单的分析和整理。

2.3.1 对服务提供商的利益

（1）服务提供商通过提供符合用户需求的安全服务，从而达到留住老用户、吸引新用户，并树立组织的良好服务形象，提升在同行中的竞争力。

（2）服务提供商可以通过收费服务来为用户提供安全服务，这样既可以满足用户需求，又能增加收入。

（3）通过采用用户自助服务，可以有效降低管理、维护和服务成本，还可以提高服务效率，可以说是一举两得。

（4）通过采取安全措施，减少用户帐号被盗事件的发生，可以大大降低客户服务的各种相关费用。

（5）通过提供安全措施，提升服务质量，满足用户的各种层次的安全需求（尤其是对安全性和方便性的需求），促进组织的发展。

2.3.2 对即时通讯个人用户的利益

（1）采用简单、方便，不需要改变用户使用习惯的方式向用户提供高安全

性的选择，满足用户对安全性的需求，为用户利益提供保障。

（2）通过采用用户自助服务的方式完成安全性提升或帐号找回，能够满足用户对服务实时性的要求，不会受是否在服务商工作时间的限制。

（3）用户帐号的安全就是用户隐私和相关经济利益的安全。

（4）用户可以根据自己的需要，在安全性和方便性之间作出合适的选择。

（5）通过采取安全措施，保护帐号的安全，从而减少因为帐号丢失而导致的各种损失（比如客户、供应商等的联系方式、交流记录等）。

2.3.3 对即时通讯组织用户的利益

（1）组织用户使用即时通讯软件对组织具有重要价值和意义，通常是其工作中经常需要使用的，所以保护其帐号安全具有重要意义。

（2）组织用户使用即时通讯软件的目的主要是为了方便、快捷地开展工作，从而提高工作效率，降低各种不必要的花费等，所以保护用户帐号安全是实现其初衷的必然选择。

（3）组织用户帐号被盗，导致组织用户无法正常工作，通常会造成较大的损失，包括效率损失、机会损失等，最终导致的是经济的损失，可以看出保护帐号安全，也是保护企业经济安全的一个方面。

2.4 OTP 的特点

北京坚石诚信科技有限公司作为一家专业从事软件保护及智能身份认证的高科技公司，推出的 OTP 动态身份认证系统具有如下特点:

（1）操作简单，使用方便。

（2）集成性，采用 OATH 国际标准算法，可以和第三方动态口令身份认证系统进行无缝集成。

（3）灵活性，提供完整的 SDK 二次开发平台，几乎可以和任何需要身份认证的应用系统进行集成，同时提供定制化开发。

（4）扩展性，基于组件的分层体系结构设计，方便系统扩展功能以及系统升级和维护。

（5）标准化，采用国际标准协议，包括 RADIUS，OATH，LDAP，ODBC，HOTP 等。

（6）开放性，系统提供和第三方动态口令身份认证系统进行集成的接口，用以向客户提供多系统解决方案。

（7）支持负载均衡，可以满足大型组织的海量用户认证需求，同时提供冗余备份。

（8）支持多种数据库，Oracle、SQL Server、My SQL、Access 等。

（9）支持多种平台，Windows、Unix、Linux。

（10）保护现有投资，可以和 AD/LDAP 进行绑定。

（11）无需安装任何驱动程序，也无需连接任何设备。

（12）外型小巧、方便携带、通过 RoHS 认证。

3. 结束语

即时通讯软件作为一种重要的网络应用，以其简单、方便、实用的特点赢得了大量的个人用户和组织用户，不管是免费用户还是付费用户，都希望自己在实用即时通讯软件时的利益能够得到保障，所以在当前即时通讯软件的安全机制和安全体系还不完善、即时通讯盗号事件频发的情况下，及时推出相关安全解决方案，以保护合法用户的利益，满足用户的需求，同时促进即时通讯软件的进一步发展。