

网游行业动态口令安全解决方案

坚石诚信

北京坚石科技股份有限公司

2008-4-15

目 录

1. 概述	3
1.1 网游背景	3
1.1.1 网游的特点	3
1.1.2 网游发展迅速	3
1.1.3 玩家青睐网游的原因	4
1.2 网游盗号问题	5
1.2.1 网游与玩家的关系	5
1.2.2 网游盗号形势严峻	6
1.2.3 网游盗号原因	6
1.3 动态口令认证技术	7
1.3.1 基本原理	7
1.3.2 工作过程	8
1.3.3 动态密码特点	9
2. 坚石 OTP 解决方案	10
2.1 方案概述	10
2.2 总体方案	10
2.2.1 OTP 系统组成	10
2.2.2 OTP 系统工作流程	12
2.2.3 OTP 系统与网游服务器的集成	12
2.3 方案效益分析	13
2.3.1 对网游服务提供商的好处	13
2.3.2 对网游玩家的好处	13
2.4 OTP 的特点	14
3. 结束语	14

本文中提到的“口令”和“密码”具有相同的含义，根据习惯在具体的环境中进行选择使用其中一个来表达。

1. 概述

网络游戏（以下简称“网游”）作为一种全新的休闲娱乐方式，受到广大网游爱好者（以下简称“玩家”）的关注和喜爱，近年来，取得了快速的发展。与此同时，和其它网络应用一样，面临着一定的安全问题。

1.1 网游背景

网游作为一种重要的网络应用并取得快速发展，首先得益于计算机技术和网络技术的发展，尤其是宽带网络技术的发展；其次，网游因其自身特点而得到广大玩家的青睐，从而形成了大量的网游用户；最后，加上网游服务提供商为满足玩家的各种需求而进行的大量人力、物力和财力投入。

1.1.1 网游的特点

网游服务是由专门的网游服务提供商提供，而玩家可以在任何可以连接到网游服务器的计算机上操作，通常情况下，虽然玩家在自己的计算机上要安装客户端软件，但是游戏的主要数据都存储在网游服务器上，只有当玩家成功登录以后，才根据具体需要将相关的数据下载到玩家的计算机上，这就为网游提供了很大的灵活性，不管是在自己家里，还是网吧，或者公司，或者朋友家里，只要计算机能够连接网游服务器并安装合适的客户端软件，玩家通过自己的帐号就可以登录到网游服务器，开始自己喜欢的网游。

网游作为一种全新的休闲娱乐方式，和其它的休闲娱乐方式（比如读书、听音乐、看电影、看电视、参加体育运动等）相比，有其自身独特的优点，比如可以参与其中、很生动、很形象、有完整故事情节、有很强的挑战性、可以得到挑战成功后的满足感等，也正是这些特点吸引了大量的玩家。

1.1.2 网游发展迅速

经过十几年的发展，目前中国的网游市场已经具有长足的发展，不但如此，在今后相当一段时期内仍将继续快速发展。目前网游市场的发展呈现以下的特点：

（1）网游用户数增长迅速 其中付费用户过半

据统计，截至 2007 年 12 月，中国网络游戏用户数已达到 4017 万，其中付费网络游戏用户已达到 2236 万。预计 2012 年中国网络游戏用户数将达到 8456

万，其中付费网络游戏用户数将达到 5038 万。

(2) 网游市场规模庞大 自主研发产品占主导

2007 年，中国网络游戏市场实际销售收入为 105.7 亿元人民币，预计 2012 年中国网络游戏市场实际销售收入将达到 262.3 亿元人民币；新投入到中国网络游戏市场公测的网络游戏产品总计 76 款，其中中国自主研发的网络游戏达到 53 款。

(3) 角色扮演类网游占八成 休闲类网游潜力巨大

2007 年，中国大型角色扮演类网络游戏市场实际销售收入为 80.3 亿元人民币，预计 2012 年中国大型角色扮演类网络游戏市场实际销售收入将达到 163.3 亿元人民币；休闲类网络游戏市场的实际销售收入为 25.3 亿元人民币，预计 2012 年中国休闲类网络游戏的实际销售收入将达到 99 亿元人民币。

(4) 电信、IT、出版成为网游最大的受益行业

2007 年，电信业务受网络游戏带动产生的直接收入达 261.1 亿元人民币；IT 行业由此产生的直接收入达 97.6 亿元人民币，接近中国网络游戏市场实际销售收入，IT 产业收入的主要来源是 PC、网络游戏服务器、网络及存储产品、软件及服务；出版和媒体行业由此产生的直接收入在 2007 年达到 42.5 亿元人民币，这部分的收入主要来源是游戏类报纸、杂志、书籍、网络媒体的发行与销售收入；其中出版和媒体广告由此产生直接收入为 10 亿元人民币。

(5) 网游研发队伍不断壮大 广东、北京表现突出

截至 2007 年 11 月，中国网络游戏研发公司数量已达 126 家，研发从业人员达到 21034 人，自主研发的网络游戏达到 250 款。广东、北京成为网络游戏研发公司增长最快的区域，广东的网络游戏研发公司达到 19 家，北京的网络游戏研发公司达到 41 家。

(6) 手机网游成新的亮点

2007 年，中国手机网络游戏市场运营收入达到 1.2 亿元人民币，比 2006 年的 3200 万元人民币增长 275%。预计 2008 年中国手机网络游戏市场运营收入将达到 3.8 亿元人民币。

1.1.3 玩家青睐网游的原因

网游得到众多玩家青睐的原因主要是因为玩家在网游中可以得到自己感兴趣的東西。虽然每个玩家得到的东西可能不一样，但他们总是可以得到他们想要的某种东西。总体上来说，主要有以下原因：

(1) 打发时间，当暂时没有事情可做而感到无聊时，如果条件许可，可以借助网游来打发时间。

(2) 治疗感情创伤，当感情上受到伤害时，可以借助网游打发时间，随着时间的流逝，这种伤害会逐渐减轻，俗话说，时间是治疗感情伤害的良药。同时，也可以借助网游发泄自己心中的感情，这种发泄方式比其它的发泄方式更值得推荐。

(3) 释放工作压力，当感到工作压力很大的时候，不妨通过网游放松一下。实践证明，一个人如果工作压力不能得到适当的放松，长期下去，不但影响自己

的工作，而且不利于身体健康，有的情节严重的甚至出现极端现象（如精神失常等）或者极端行为（比如跳楼自杀等）。

（4）开启智力，网游经过游戏设计者精心设计，其中存在大量的逻辑推理和逻辑判断，更有锻炼玩家对周围环境变化的反应速度和准确度的设计，通过这些精心设计，玩家可以在不知不觉中提高自己的感知能力和反应能力。

（5）广交朋友，通过网游，可以找到和自己志趣相投的朋友，除了网游活动以外，也许可以找到自己工作或者事业上的合作伙伴。

（6）树立信心，当一个人受到生活的重大打击时，可能会失去生活的信心，此时如果能够借助于网游，使自己暂时忘记现实生活中的种种不幸，假以时日，受打击的人就可以逐渐从打击中恢复到现实生活。

（7）丰富精神生活，对于不善于或者不喜欢与人交流并且业余活动又很少的人，通常活动比较少，可以借助于网游丰富自己的精神生活。

除了上述提到的种种原因以外，对于具体的玩家可能还会有自己的特殊原因。在此不一一列举。

1.2 网游盗号问题

网游的安全问题目前最主要的就是玩家帐号和密码被盗用，造成玩家的虚拟财产损失以及玩家心理上的伤害，进而可能影响其正常的工作、学习和生活。如何保护玩家的帐号和密码的安全就成了网游安全的一个突出问题。

1.2.1 网游与玩家的关系

随着玩家在网游上各种投入的增加以及在网游中取得的成果的累积，网游在玩家心目中的地位在不断提高、影响在不断地加大，主要体现在以下方面：

（1）玩家为了取得好的成果，必须投入大量的时间。

（2）玩家为了尽快取得成果，必须投入大量的精力，而且常常是废寝忘食。

（3）玩家在长期的、连续奋斗的过程中，必须有相当的体力支持。

（4）通过大量投入以后取得的成果，玩家自然是很看重，毕竟是通过自己的辛苦劳作而得来的，所以会产生一定的感觉。

（5）为了能够投入到网游中并且取得好的成果，必要的花费是少不了的，比如为网游而专门购买的网络设备和计算机以及外设的花费，网游过程中购买网游装备的花费，以及玩网游时必须的电费、上网费等。

（6）通过玩网游所积累的虚拟财产，虚拟财产可以实现经济利益，不过大多数玩家应该不是为这个目的，更多的是希望通过积累大量的虚拟财产来满足自己精神上的满足。

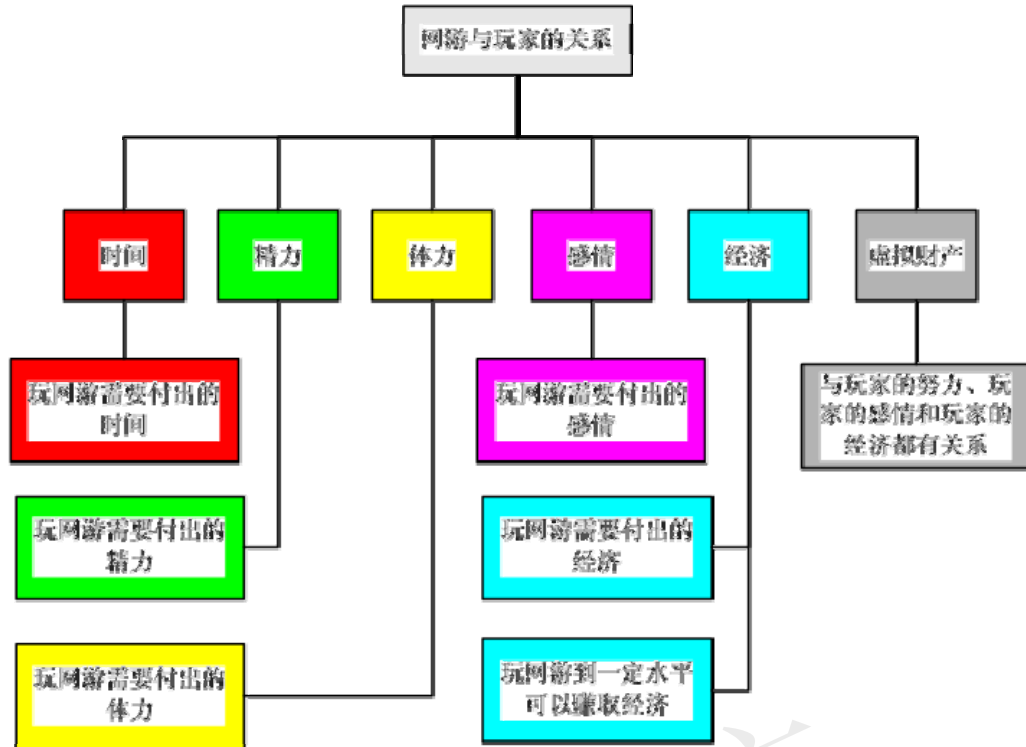


图 1 网游对玩家的影响

1.2.2 网游盗号形势严峻

根据金山 7 月份发布的《2007 年上半年中国互联网安全报告》显示，在上半年新增的木马病毒中，盗号木马是最严重的一类病毒，占到木马病毒总数的 76.04%，高达 58245 种。而蠕虫、下载木马、脚本漏洞病毒几乎都是为盗号木马来服务的，其目的就是通过自身传播能力、攻击能力，将自身做为载体将盗号木马安装到用户系统中。

据有关统计数据显示，有过被盗号亲身经历的网游玩家占 38.12%，遇到过但被自己识破了的占 21.42%，身边朋友有被盗号经历的占 17.08%，这些怵目惊心的数字，足以说明当前网络游戏盗号问题的严重性，从某种程序上来说，如何解决网游盗号问题，保障网游安全，已成为网游行业亟待解决的问题。

1.2.3 网游盗号原因

网游盗号现象日趋严峻的主要原因包括两个方面：（1）盗号者主观原因，主要是受到利益诱惑，再加上当前相关法律法规不完善；（2）网游帐号自身的安全保护机制不完善，给盗号者以可乘之机。

网游盗号者主要是受到利益诱惑而进行盗号，据相关资料显示，从事网游盗号、转卖等活动可以使盗号者赚取几十万、几百万甚至上千万的经济利益，再加上目前暂无明确的法律和法规限制，这使得盗号者毫无顾忌。

当前网游帐号普遍采用静态密码进行身份认证，静态密码本身具有弱安全性

的特点，其面临的安全风险较大，其缺点主要表现在以下几个方面：

(1) 输入泄密：在输入口令时可能被偷看，或用远程摄像机录像，还可能被键盘记录木马程序所记录。

(2) 传输泄密：在电话上输入的口令可能会在电话上被窃听；在网上交易时口令会在网络上传输时被截取分析。

(3) 特征性泄密：为了方便记忆，用户的静态口令往往会与日期、姓名、电话、证件、家庭、公司等熟悉的对象相关联，因此容易被猜测或用黑客字典分析。

(4) 共享性泄密：为了简单方便，用户会在电子邮箱、银行信用卡等多个系统中使用相同的静态口令，因此假如有一个系统被破解，那么用户在其它系统上的帐号也就危险了。

(5) 记录泄密：为避免复杂的、难于记忆的口令被忘记，用户往往会将其记录在纸上或电脑文件中，这记录下来的口令可能会失窃。

(6) 可被穷举攻击：由于静态口令在一段时间内保持不变，所以可以被黑客工具长时间地、多电脑地进行穷举分析。

(7) 泄密不可知性：当静态口令泄密后，系统和用户都无法及时地获知口令是否已经泄密。只有当造成危害之后、或者查看了日志之后才能确切知道。

(8) 不方便性：定期更换口令，设置复杂口令，可能会容易忘记，一旦口令忘记可能会导致一些不必要的损失和不便，具有很大隐患。

(9) 长期性：静态口令多使用一天就多一天泄密的危险，其危险性与日俱增。

静态密码的基本特点，也是其致命弱点就是每次登录时使用相同的密码进行验证，一旦玩家密码泄露，对于使用静态密码进行身份认证的网游，玩家就没有任何安全可言。所以为了保护网游玩家利益，防止网游帐号被盗，采用新的技术手段，弥补静态密码身份认证技术的弱点，就成了网游服务商和玩家必然的选择。

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,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,一旦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网游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。

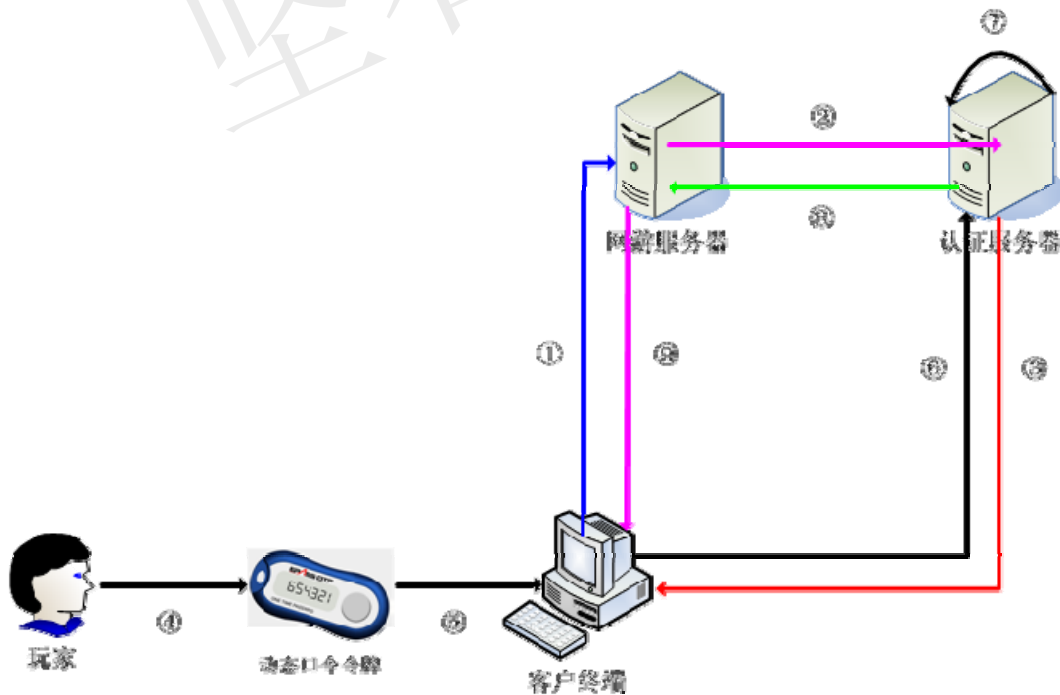


图2 动态口令身份认证系统工作过程

- ① 玩家请求接入网游服务器；
- ② 网游服务器请求认证服务器对客户身份的合法性和真实性进行认证；
- ③ 玩家终端（即客户端）弹出身份认证对话框；
- ④ 玩家激活令牌，生成动态口令；
- ⑤ 将帐号和口令键入终端的身份认证对话框；
- ⑥ 玩家终端将帐号和口令通过网络传输给认证服务器；
- ⑦ 认证服务器调用玩家信息，产生与玩家信息和事件序列相关的动态口令，并与玩家输入的口令进行比对，判别玩家身份的合法性和真实性；
- ⑧ 认证服务器将认证结果报告给网游服务器；
- ⑨ 网游服务器根据玩家身份的合法性和真实性反馈给玩家终端，并决定可以提供服务或拒绝服务。

1.3.3 动态密码特点

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

2.1 方案概述

为解决网游玩家帐号和密码容易被盗取的问题，坚石诚信科技有限公司推出了自主知识产权的动态口令（OTP）身份认证解决方案，可以大大提高玩家帐号和密码的安全，有效防止帐号被盗，从而避免不必要的各种损失。

保护玩家帐号和密码主要包括两个方面的内容：一是网游服务提供商通过采用安全的身份认证技术来提供安全认证解决方案；二是用户配合服务提供商的方案做好自己的帐号和密码的保护工作。

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，同时向网游服务提供商和网游玩家提供良好的灵活性和性价比。

2.2.1 OTP 系统组成

考虑到各个网游服务系统的差异以及玩家计算机环境的不同，OTP 身份认证系统提供了充分的灵活性来满足这种需求。认证服务器和认证备份服务器完全独立于网游服务器系统，只需要在原有认证服务器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。

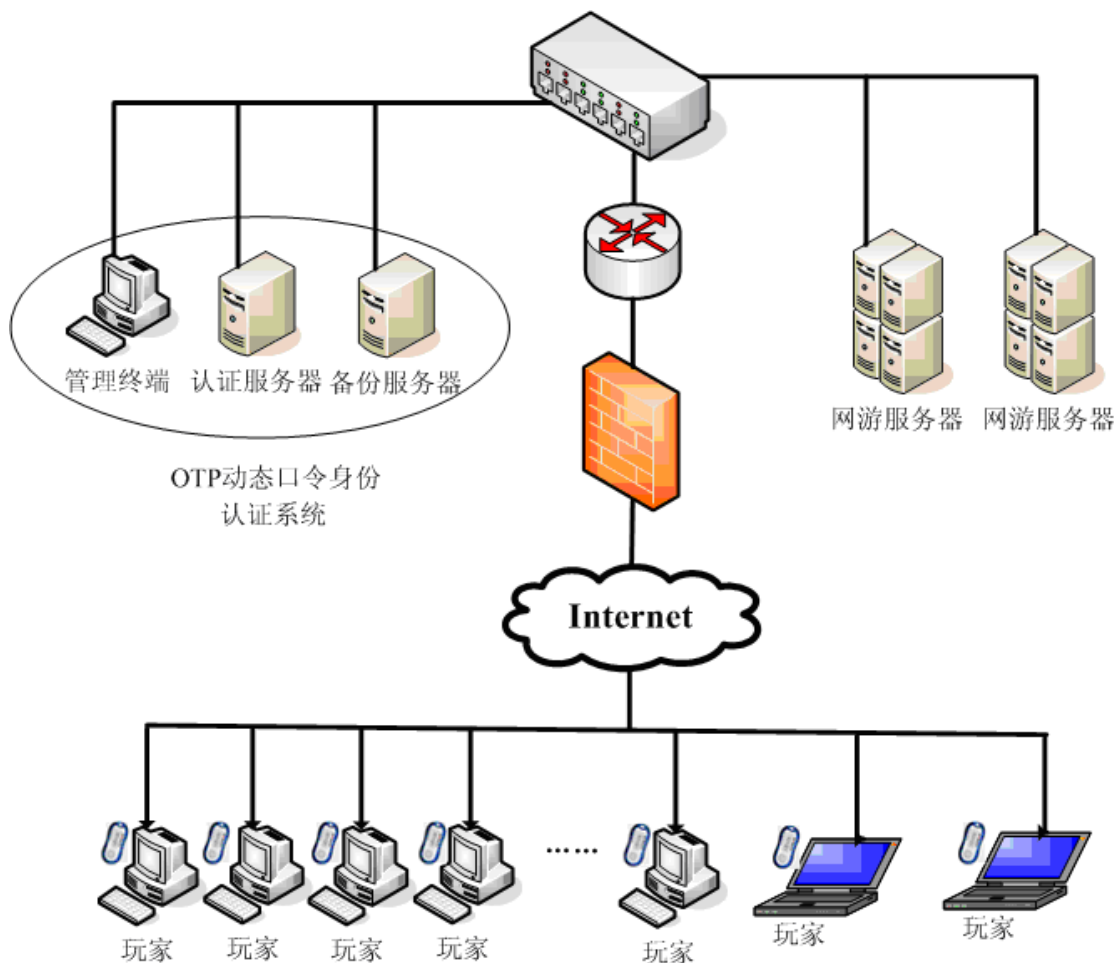


图3 OTP 认证解决方案系统组成图

1. 认证服务器

认证服务器是系统的核心部分，安装在网游服务提供商的内部网络，与网游服务器通过局域网连接，向网游服务器提供身份认证的功能。当网游服务器接收到玩家发送的登录信息时，由网游服务器传递登录信息给认证服务器，认证服务器根据其存储的信息验证玩家的登录信息是否正确，如果正确，认证服务器返回认证成功，玩家成功登录网游服务器并可以进行后续操作，否则，认证服务器返回认证失败，玩家登录网游服务器失败。

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，登录网游服务器时，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。

2.2.2 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）。

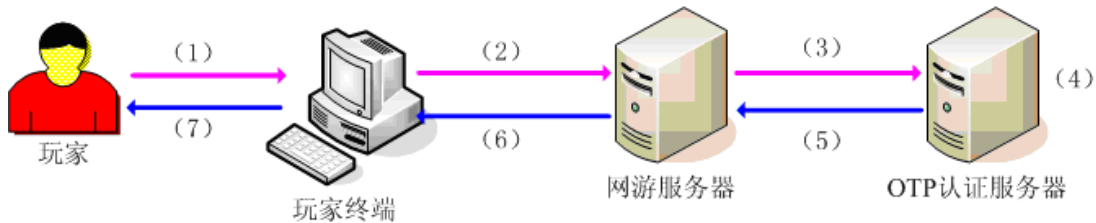


图 4 认证过程

- (1) 玩家启动网游客户端，并在登录窗口中输入帐号和动态口令；
- (2) 帐号和动态口令从玩家终端传送到网游服务器；
- (3) 帐号和动态口令从网游服务器传送到 OTP 认证服务器；
- (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网游服务器；
- (6) 网游服务器根据接收到的认证结果进行处理，如果认证成功，网游服务器允许玩家登录，如果认证失败，网游服务器拒绝玩家登录，并将失败信息返回给玩家。
- (7) 如果认证通过，玩家可以进入游戏，如果认证失败，玩家得到登录失败提示。

2.2.3 OTP 系统与网游服务器的集成

OTP 系统和网游服务器进行集成时，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。

由网游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，此时网游服务器就可以拒绝玩家登录网游服务器。静态口令认证和动态口令认证的顺序可以根据需要进行选定。

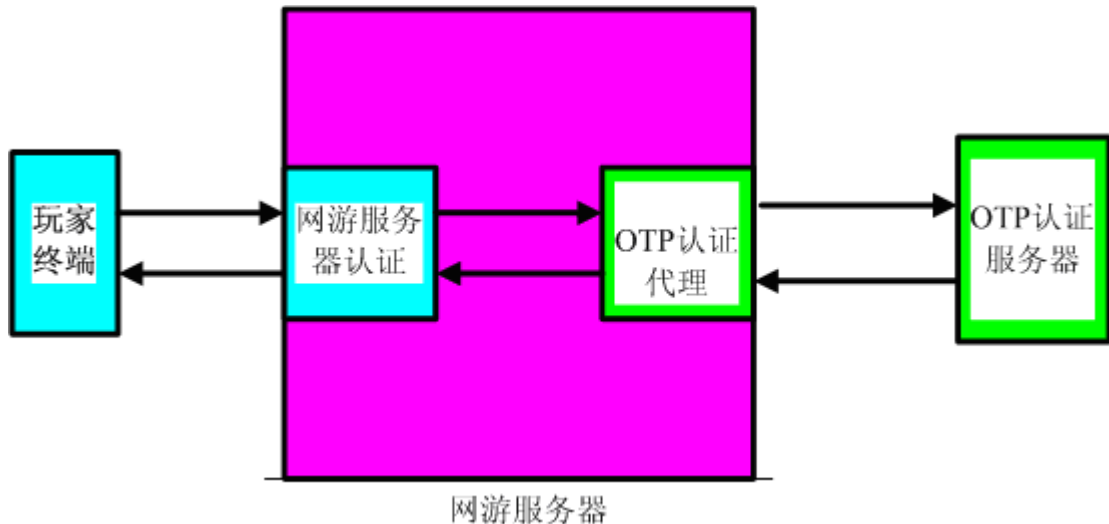


图 5 组件结构图

2.3 方案效益分析

采用 OTP 身份认证解决方案提高网游帐号安全性具有很大的灵活性和性价比。主要体现在网游服务提供商和玩家，下面对其进行简单的分析和整理。

2.3.1 对网游服务提供商的好处

- (1) 向玩家提供网游帐号保护功能，满足网游玩家对帐号安全性的需求。
- (2) 安装配置灵活方便，不用更改原有网络结构。
- (3) 完善和提供网游帐号安全服务，提高玩家满意度，建立忠诚度。
- (4) 减少因网游盗号引起的投诉，从而减少相关管理费用。
- (5) 减少因网游盗号引起的玩家不满意，从而减少玩家转移到其它网游的可能性。
- (6) 减少因网游盗号引起的名誉损失，有利于建立良好的公众形象。
- (7) 提供更好的网游帐号安全服务，吸引更多玩家。

2.3.2 对网游玩家的好处

- (1) 提高网游帐号的安全性。
- (2) 方便密码管理，通过动态口令令牌产生口令，避免密码遗忘或记错。
- (3) 使用方便，无需安装任何软件，也无需连接计算机。
- (4) 具有广泛的适应性和灵活性，对使用环境没有限制，可以在任何计算机上使用。
- (5) 无需改变玩家的操作习惯，无需玩家付出时间和精力来学习如何使用，完全实现即看即会。

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

OTP 身份认证解决方案是一个技术解决方案，在防止技术性的网游盗号方面上有其独特优势。同时，为了有效地解决网游盗号问题，还需要玩家提高其安全意识和安全保护技能，网游服务提供商和安全服务提供商积极提供相关安全解决方案，政府职能部门制定和完善相关法律法规。