

TAS(地御)网站第三方身份认证系统 技术白皮书

Bug.Center.Team 出品

网站安全成为了信息安全当中最关紧要的一部分

随着信息事业的发展,网站已经成为了必不可少的组成部分,越来越多人通过 Internet 进行商务活动、互动交流等等.因此网络衍生出很多利用这样子模式的网站程序.

例如:

网络社区程序:Dvbbs、Discuz、PHPWind 等等一系列的社区程序

电子商务程序:EcShop、ShopEX 等等一系列的电子商务程序

但是大家使用这些软件的时候,都会忽略到一些重要的问题.

(1) 使用这些程序的时候,程序的安全是谁负责的了?

(2) 个人的信息保障是谁负责的了?

现在网络上所提供的网站程序,代码的安全维护以及检测都是由官方自行负责的,通常他们都不会进行一系列的代码安全检测工作,往往都是外界发现安全漏洞之后,官方作为一个负责的程序商才会提供相关的安全补丁给予用户修补.当然外界发现的漏洞会存在着一个比较长的潜伏期,漏洞当被发现直到官方得到消息后,可能在时间上来说已经是很长的时间了,在这段时间里面,又有谁去负责这方面漏洞所造成的安全损失了?上面所提到的另外一个问题就是个人信息的保障,就算用户买了程序有关方面的服务,但是程序商根本不会对于程序自身漏洞导致的个人信息泄漏以及经济损失负责.故此 Bug.Center.Team(以下简称:BCT)为了保障用户的个人信息不因程序的漏洞致使泄漏、防护网站核心地带不被入侵,使得用户在安心使用网站程序的时候,给予用户一个安全防护.

所以 BCT 推出“**TAS(地御)网站第三方身份认证服务**”.

本白皮书将会介绍有关“TAS(地御)网站第三方身份认证系统”的详细资料,从详细的介绍当中,让你们明白该系统的特点、原理、功能、使用方法(如何利用系统消除账号密码的安全隐患、防止恶意攻击者的入侵、保护核心地带的安全)以及本系统的可扩展性,使得你可以更加的清楚明白系统的作用.从本书当中可以令你明白密码的重要性

网站核心地带的守护者-----“TAS(地御)第三方身份认证系统”

TAS(地御)第三方身份认证系统(以下简称:TAS)是由我们 BCT 根据现有的网站安全形势,结合用户以及程序商所需求而研发出来的一套第三方身份认证系统,该系统采用现有广泛使用的“双因素”认证技术.何谓“双因素认证技术”呢?

一、双因素认证技术

现有的网站以及程序来说,使用者通常使用的网络登录办法为:用户名+密码,这样子的组合,从安全的角度来说并不是安全的,单一静态的密码,需要进行长期性的密码维护,严格规定相当的长度以及复杂性才可以保证密码的安全以及强度.但是往往这些投入的时间以及人力物力都是很大的.

然而现有最安全的身份认证方式就是目前认为最安全的双因素认证机制,采用双因素认证机制会使得原有简单而又不安全的单一静态密码变得更加安全.在双因素认证机制下,单一的密码模式只会变成双因素认证机制的第一个要素.而第二个要素就是使用所拥有的特殊认证加强机制.

第一要素:需要使用者记忆的身份认证内容,例如密码和身份证号码等等.

第二要素:使用者拥有的特殊认证加强机制,例如动态密码卡,IC 卡,磁卡等等.

第三要素:使用者本身拥有的唯一特征,例如指纹,瞳孔,声音等等.

这样子的模式下,用户的信息就会得到一个很好的保护,从而不用担心相关的敏感信息被盗取了.

二、双因素认证技术的特点

双因素认证技术广泛应用在银行、电信、金融、制造、政府等等方面,双因素认证技术有访问控制特性、防窃听特性、防盗号特性.

(1) 访问控制

当用户使用双因素认证技术服务之后,用户登陆系统的情况下,系统会根据所设置的自动分配用户所拥有的权限.当恶意用户使用系统漏洞进行溢出情况下,恶意用户就算拿到系统的控制权限,但是因为双因素认证服务的监控下,服务会按照认证服务器的配置拒绝用户跨权执行.

(2) 防窃听

从系统入侵的角度来说,当恶意用户利用嗅探工具进行局域网内的嗅探的时候,因为网络协议的缺陷会导致正常用户在正常的情况下,无意中泄漏了有关的 ID+PASS,会直接威胁到有关的服务以及敏感信息的泄漏.当我们使用了双因素认证技术之后,就算恶意用户进行局域网内的嗅探攻击时候,恶意用户所嗅探到的 ID+PASS 也不能够进行登陆,因为双因素认证的关系,恶意用户所嗅探得到的 Password 并非是单一静态模式的,所以根本就没有办法进行使用.

(3) 防盗号

当用户访问的网站收到病毒的感染或者恶意用户利用有关的系统漏洞进行木马软件、间谍软件、键盘记录进行账号密码窃取的情况下,正常用户就会因此泄漏其 ID 以及 Password.但是使用双因素认证服务的时候,不管恶意用户如何利用有关的恶意软件进行入侵,也无法窃取密码.

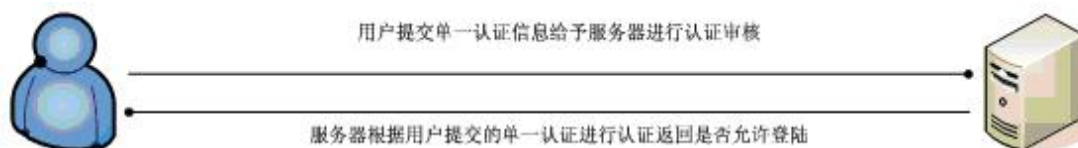
因为双因素认证技术采用了三种因素作为条件的限制,用户所盗窃得到的 Password 是基于双因素认证技术所产生的随机字符串,按照认证技术的特点,致使恶意用户无法利用,也无法盗取真实的 Password.

三、双因素认证技术原理

双因素认证技术原理采用的是第三方服务器提供服务,当安装了双因素认证技术服务程序之后,目标服务器的终端登陆等等的程序以及服务都会接入双因素认证技术接口程序,当用户登陆终端的时候,首先输入有关的身份名称,然后需要用户利用自身所设置的 PIN 码(个人身份识别码)在本地主机算出有关的身份认证安全码,方可利用有关的身份名称+身份认证安全码进行登陆.而第三方服务器就是作为一个身份认证安全码的对比.认证服务器采用 TCP 协议,以确保服务器与服务器之间的可靠通信.数据流经过加密,密钥会按照一定时间段更新一次.而密钥采用的就是与 UCT 时间同步,当用户输入 PIN 码(个人身份识别码)的时候,密钥就会按照时间以及固定的算法算出一个身份认证安全码,这个就是最为重要的部分了,就是因为这样子的算法加密以及时间生存期,导致恶意用户不管用短时间的嗅探或者长时间的盗取密码形式,都没有办法真正的盗取用户的实际 Password.

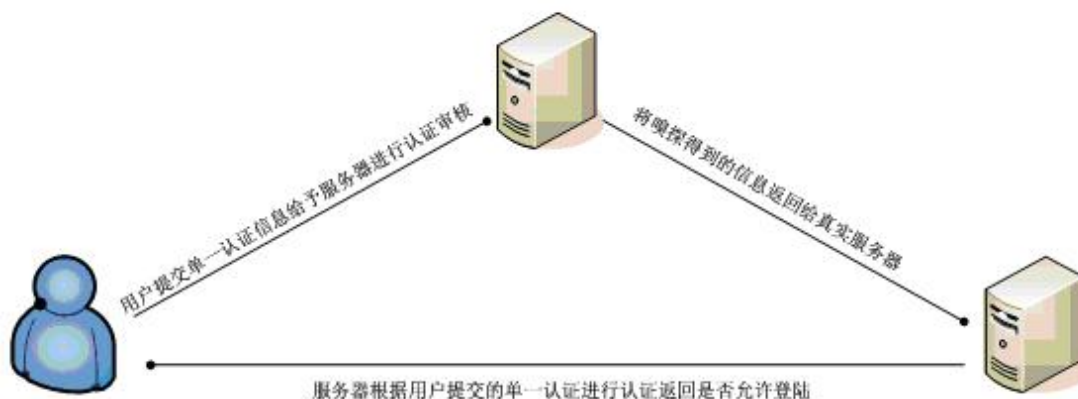
四、双因素认证技术使用方法

双因素认证技术可以使用电子商务,企业内部,会员服务器等等,而 TAS 主要针对的是网络程序,例如网络社会/论坛、网站 CMS、博客系统、交友系统、电子商务系统(网络商店、客户服务)、会员系统.当 TAS 没有接入以上的程序的时候,用户登陆网站或者后台都是会采用单一认证模式进行身份审核的.



非双因素认证技术
单一认证登陆模式

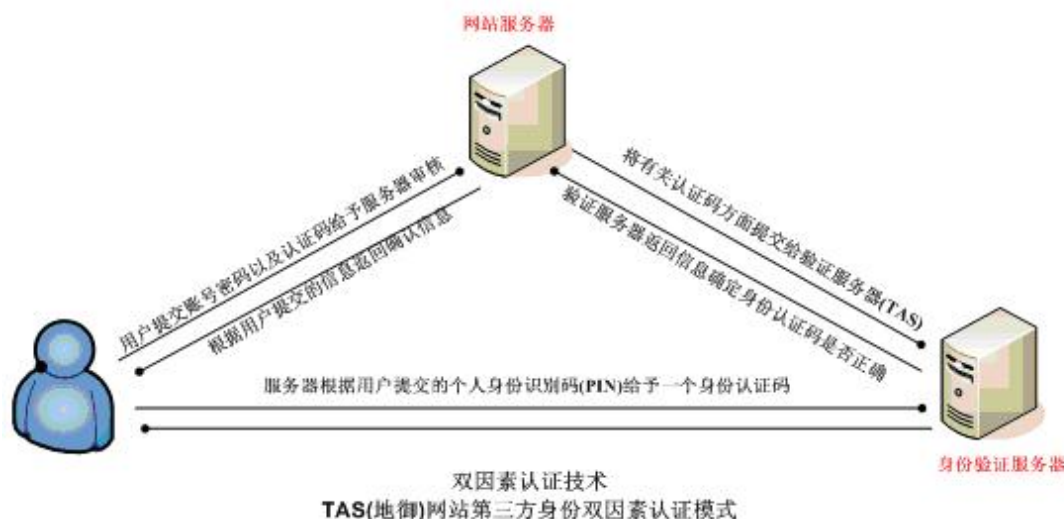
当网站采用单一认证模式进行网站以及后台登陆的时候,恶意用户就可以采取非法的手段进行账号密码的盗窃,例如在同一网段下进行嗅探攻击,或者是利用木马软件盗取账号密码.



非双因素认证技术
单一认证登陆下的嗅探攻击模式

如何利用 TAS 系统消除账号密码的安全隐患

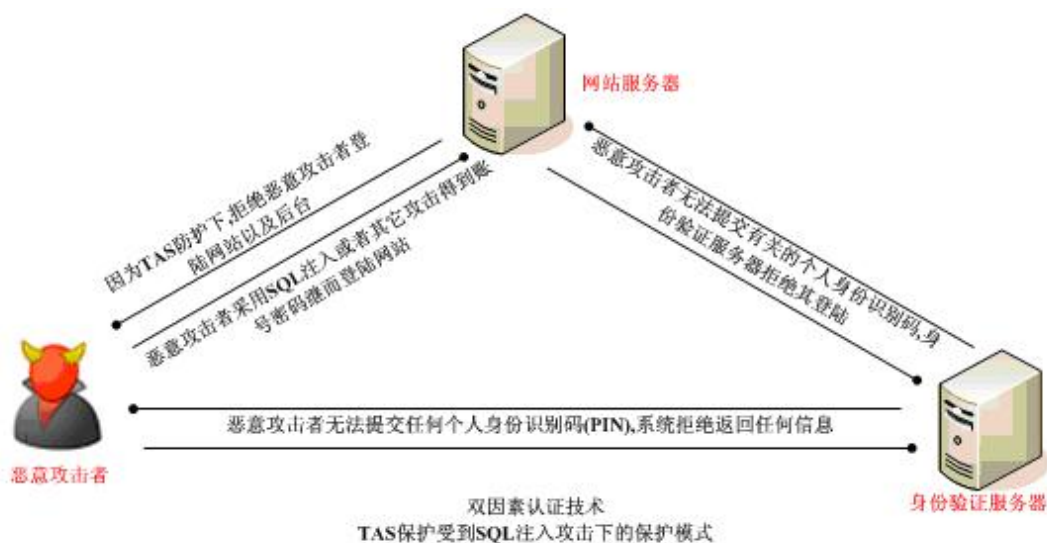
而采用了 TAS 服务之后,当用户登陆网站或者后台的时候,程序自身因为接入了 TAS 接口,就会在登陆处显示有关的提示,需要用户需要相关的认证码方可登陆.



采用了 TAS 身份验证系统之后,就算同一域网内进行嗅探攻击的话,就算拿到了网站程序自身的账号和密码,恶意用户利用嗅探得来的账号和密码以及个人身份认证码也无法进行登陆.因为 TAS 系统采用认证码生存期技术,当用户得到个人身份认证码开始计算,身份认证码会按照一个高密度的加密算法,以及一分钟的生存期限作为限制.就算嗅探到个人身份认证码被直到使用,但已经超过了生存期限所给予的范围,所以恶意攻击者也无法利用,从而给予用户一个安全的保障.

防止恶意攻击者的入侵

本文开始的时候,曾经说过因为现有的网络程序对于代码检测方面的重视度并不高,很难去控制外界所发现的漏洞数量以及严重程度,至此当恶意攻击者利用没公开的程序漏洞进行攻击的时候,网站就会很快的成为了攻击者摧残的目标,如果恶意攻击者可以拿到账号和密码当登陆系统时,TAS 会根据恶意攻击者所提交的请求,提示其提交相关的个人身份验证证明,因为无法提交的情况下,系统会自动拒绝其登陆请求



TAS 系统移植性

然而也有人会问,那样子 TAS 是否是将程序完全的修改达到这样子的效果了.TAS 系统采用的是结合多方面程序程序核心,程序不需要大量的修改现有的网站程序或者需要重新假设网站等等的操作,我们会按照现有流行网站程序进行接口编写,从而提供用户一个简单、又快捷的接入方式,我们也会提供一个接口开发包,使得程序商以及专业用户,可以根据自身的需求去进行接口的编写以及接入.

TAS 系统灵活性

TAS 系统不单是可以作为网站的登陆验证,也可以在网站的后台以及会员登陆区进行使用.特别是电子商务,网站对于商业用户来说是一个最好的选择.

TAS 系统扩展性

TAS 采用 Web 形式提供服务,强大的数据处理.为了减低用户在 TAS 上的资金投入,TAS 将会采用三种模式提供个人身份验证码.

第一种是网站提交个人识别码(PIN),网站及时返回个人身份验证码

第二种是网站提交个人识别码(PIN),网站及时以邮件的形式发送到有关邮箱当中

第三种是 TAS 系统采用短信接口模式,用户只需要在手机输入个人识别码(PIN),系统将会马上返回个人身份验证码给用户手机.

紧急状况处理

当用户丢失有关的个人识别码(PIN)时,用户可以马上登陆 TAS 用户平台,提交有关的身
份证明以及初始化注册的账号密码,系统将会再次发放一个全新的初始化个人识别码(PIN),
也就是 TAS 系统为了防止用户丢失个人识别码(PIN)或因为 TAS 系统的特殊性而 TAS 系统
受到攻击时,TAS 也可以不会泄漏个人识别码.初始化的注册账号和密码就是当个人识别码
(PIN)丢失或被盗用时,作为紧急使用的紧急账号.

结论

TAS(地御)网站第三方身份认证系统是为了保障网站管理员以及网站用户的双因素认证
技术产品,在这么多网络程序产品当中,你可以看到程序的漏洞,程序的缺陷以及也尝试过这
样子所带来的损失,作为一个网络第三方系统以及服务,TAS(地御)网站第三方身份认证系统
将会是你最佳的选择

关于 Bug.Center.Team

Bug.Center.Team-漏洞预警中心小组(简称 BCT)是一个专业研究脚本程序安全以及安
全服务的网络安全组织,凭借对于脚本程序多年来的研究经验,组织在成立至今聚集了一批
对于脚本程序有着专业知识的人才,在国内脚本程序安全领域当中有着一定的地位.

BCT 目前主要以脚本程序代码安全审核为主,并且对于网站、以及服务器的安全评估、
安全服务等等都有一定的成果.

我们相信以我们对于技术的执着,对于用户以及合作方的诚信、协作的态度,一定会
在网络安全领域创出自己独有的一片天.