**网络安全设计报告**



**文档编写人：肖启超**

**所属单位：重庆易联数码科技股份有限公司**

**日 期：2020年8月**

**目 录**

[**1、安全设计背景** 1](#_Toc50480308)

[**2、网络安全设计要求** 1](#_Toc50480309)

[**3、常见的攻击手段和工具以及预防方式** 1](#_Toc50480310)

[**3.1 电子邮件炸弹** 1](#_Toc50480311)

[**3.1.1 工作原理** 1](#_Toc50480312)

[**3.1.1 预防方式** 1](#_Toc50480313)

[**3.2特洛伊木马** 2](#_Toc50480314)

[**3.2.1工作原理** 2](#_Toc50480315)

[**3.2.2 预防方式** 2](#_Toc50480316)

[**3.2.2.1端口扫描** 2](#_Toc50480317)

[**3.2.2.2.查看连接** 2](#_Toc50480318)

[**3.2.2.3.检查注册表** 2](#_Toc50480319)

[**3.2.2.4.查找文件** 2](#_Toc50480320)

[**3.3拒绝服务攻击（dos）** 3](#_Toc50480321)

[**3.3.1原理** 3](#_Toc50480322)

[**3.3.1预防方式** 4](#_Toc50480323)

[**3.4 IP欺骗攻击** 5](#_Toc50480324)

[**3.5病毒** 5](#_Toc50480325)

[**3.6嗅探攻击** 6](#_Toc50480326)

[**3.6.1原理** 6](#_Toc50480327)

[**3.6.1防御** 6](#_Toc50480328)

[**3.7 SQL注入** 7](#_Toc50480329)

[**3.7.1原理** 7](#_Toc50480330)

[**3.7.2防御** 7](#_Toc50480331)

[**3.8 XSS攻击** 8](#_Toc50480332)

[**3.9 口令攻击** 8](#_Toc50480333)

[**3.10 CC攻击（Challenge Collapsar）** 10](#_Toc50480334)

[3.11 CSRF攻击 11](#_Toc50480335)

[**3.11.1原理** 11](#_Toc50480336)

[**3.11.2预防方式** 11](#_Toc50480337)

[**3.12 zip炸弹攻击** 12](#_Toc50480338)

[**4、安全技术栈** 12](#_Toc50480339)

[**4．1安全研发** 12](#_Toc50480340)

[**4．2二进制安全** 13](#_Toc50480341)

[**5、举例说明** 17](#_Toc50480342)

**1、安全设计背景**

目前，随着电子信息化进程不断拓展，网络信息安全日益受到重视，现在网络攻击属于日常化，随机化，而网络攻击的手段也越来越专业化。基本上门槛很低，一个普通人使用网络工具都可以对目标网站进行攻击。或者专业人士进行专业攻击。而政府政务平台，网络金融等行业也极其容易遭受不同层度的攻击，业界也有不少网站被攻击的案例，轻则客户资料被盗取，重则损失巨大财富，故而网络安全刻不容缓，警钟长鸣

**2、网络安全设计要求**

对待网络安全永无止境，这个世界上不存在绝对安全的系统，如果有只是暂时没有被发现漏洞。比如：路由器转发从任何地方来的包，攻击者可以在任何一台联网的计算机进行攻击，攻击手法不断更新。所以针对网络安全的设计者来说，一方面要预防市面上已知的漏洞，通过设计和操作去预防，另一方面要时刻保持警惕，做到防御大于治疗。在设计阶段就规避这些安全问题。要制定合理的安全策略，必须覆盖数据的储存、传输和处理，覆盖计算机系统、局域网、和其他互联设备，必须考虑性能价格的权衡

**3、常见的攻击手段和工具以及预防方式**

**3.1 电子邮件炸弹**

**3.1.1 工作原理**

就是通过大量发送电子邮件，占满邮箱的空间，使得邮箱无法接受新的邮件。黑客就是利用这点，设计一些软件，在短时间内向指定邮箱发送大量地址不详，容量巨大，充满乱码或者其他恶意语言的邮件。因为每一个人的邮件信箱都是有限的，但庞大的邮件垃圾到达信箱的时候，就会把正常的邮件给冲掉。同时，由于它占用大量的网络资源，常常导致网络塞车，使大量的用户不能正常工作，最终造成邮箱瘫痪。

**3.1.1 预防方式**

用邮件程序的email-notify功能来过滤信件，它不会把信件直接从主机上下载只会把所有信件的头部信息(headers)送过来，它包含了信件的发送者、信件的主题等信息，用view功能检查头部信息，看到有来历可疑信件，可直接下指令它从主机server端直接删除。万一误用一般的邮件程序抓到mail bomb，看到在没完没了的下载的时候，强迫关闭程序, 重新运行程序,连回Server, 用 email notify 把它删除掉。

**3.2特洛伊木马**

**3.2.1工作原理**

特洛伊木马是一个程序，它驻留在目标计算机里，可以随计算机自动启动并在某一端口进行侦听，在对接收的数据识别后，对目标计算机执行特定的操作。木马，其实质只是一个通过端口进行通信的网络客户/服务程序。

网络客户/服务模式的原理是一台主机提供服务(服务器)，另一台主机接受服务(客户机)。作为服务器的主机一般会打开一个默认的端口并进行监听(Listen), 如果有客户机向服务器的这一端口提出连接请求(Connect Request), 服务器上的相应程序就会自动运行，来应答客户机的请求，这个程序称为守护进程(UNIX的术语,不过已经被移植到了MS系统上)。对于特洛伊木马，被控制端就成为一台服务器，控制端则是一台客户机，G\_server.exe是守护进程, G\_client是客户端应用程序。

**3.2.2 预防方式**

**3.2.2.1端口扫描**

端口扫描是检查远程机器有无木马的最好办法, 端口扫描的原理非常简单, 扫描程序尝试连接某个端口, 如果成功, 则说明端口开放,如果失败或超过某个特定的时间(超时), 则说明端口关闭。但对于驱动程序/动态链接木马, 扫描端口是不起作用的。

**3.2.2.2.查看连接**

　 查看连接和端口扫描的原理基本相同，不过是在本地机上通过netstat -a（或某个第三方程序）查看所有的TCP/UDP连接，查看连接要比端口扫描快，但同样是无法查出驱动程序/动态链接木马,而且仅仅能在本地使用。

**3.2.2.3.检查注册表**

上面在讨论木马的启动方式时已经提到，木马可以通过注册表启动（好像现在大部分的木马都是通过注册表启动的，至少也把注册表作为一个自我保护的方式），那么，我们同样可以通过检查注册表来发现冰河在注册表里留下的痕迹。

**3.2.2.4.查找文件**

查找木马特定的文件也是一个常用的方法，木马的一个特征文件是kernl32.exe,另一个是sysexlpr.exe，只要删除了这两个文件,木马就已经不起作用了。如果你只是删除了sysexlpr.exe而没有做扫尾工作的话,可能会遇到一些麻烦-就是你的文本文件打不开了, sysexplr.exe是和文本文件关联的,你还必须把文本文件跟notepad关联上。

另外，对于驱动程序/动态链接库木马，有一种方法可以试试，使用Windows的"系统文件检查器"，通过"开始菜单"-"程序"-"附件"-"系统工具"-"系统信息"-"工具"可以运行"系统文件检查器", 用“系统文件检查器”可检测操作系统文件的完整性，如果这些文件损坏，检查器可以将其还原，检查器还可以从安装盘中解压缩已压缩的文件（如驱动程序）。如果你的驱动程序或动态链接库在你没有升级它们的情况下被改动了,就有可能是木马(或者损坏了),提取改动过的文件可以保证你的系统安全和稳定。

**3.3拒绝服务攻击（dos）**

**3.3.1原理**

Dos攻击分为如下几种方式：

Synflood: 该攻击以多个随机的源主机地址向目的主机发送SYN包，而在收到目的主机的SYN ACK后并不回应，这样，目的主机就为这些源主机建立了大量的连接队列，而且由于没有收到ACK一直维护着这些队列，造成了资源的大量消耗而不能向正常请求提供服务。  
Smurf：该攻击向一个子网的广播地址发一个带有特定请求（如ICMP回应请求）的包，并且将源地址伪装成想要攻击的主机地址。子网上所有主机都回应广播包请求而向被攻击主机发包，使该主机受到攻击。  
Land-based：攻击者将一个包的源地址和目的地址都设置为目标主机的地址，然后将该包通过IP欺骗的方式发送给被攻击主机，这种包可以造成被攻击主机因试图与自己建立连接而陷入死循环，从而很大程度地降低了系统性能。  
Ping of Death：根据TCP/IP的规范，一个包的长度最大为65536字节。尽管一个包的长度不能超过65536字节，但是一个包分成的多个片段的叠加却能做到。当一个主机收到了长度大于65536字节的包时，就是受到了Ping of Death攻击，该攻击会造成主机的宕机。  
Teardrop：IP数据包在网络传递时，数据包可以分成更小的片段。攻击者可以通过发送两段（或者更多）数据包来实现TearDrop攻击。第一个包的偏移量为0，长度为N，第二个包的偏移量小于N。为了合并这些数据段，TCP/IP堆栈会分配超乎寻常的巨大资源，从而造成系统资源的缺乏甚至机器的重新启动。  
PingSweep：使用ICMP Echo轮询多个主机。  
Pingflood: 该攻击在短时间内向目的主机发送大量ping包，造成网络堵塞或主机资源耗尽。

**3.3.1预防方式**

确保所有服务器采用最新系统，并打上安全补丁。计算机紧急响应协调中心发现，几乎每个受到DDoS攻击的系统都没有及时打上补丁。

确保管理员对所有主机进行检查，而不仅针对关键主机。这是为了确保管理员知道每个主机系统在 运行什么？谁在使用主机？哪些人可以访问主机？不然，即使黑客侵犯了系统，也很难查明。

确保从服务器相应的目录或文件数据库中删除未使用的服务如FTP或NFS。Wu-Ftpd等守护程序存在一些已知的漏洞，黑客通过根攻击就能获得访问特权系统的权限，并能访问其他系统——甚至是受防火墙保护的系统。

确保运行在Unix上的所有服务都有TCP封装程序，限制对主机的访问权限。

禁止内部网通过Modem连接至PSTN系统。否则，黑客能通过电话线发现未受保护的主机，即刻就能访问极为机密的数据。禁止使用网络访问程序如Telnet、Ftp、Rsh、Rlogin和Rcp，以基于PKI的访问程序如SSH取代。SSH不会在网上以明文格式传送口令，而Telnet和Rlogin则正好相反，黑客能搜寻到这些口令，从而立即访问网络上的重要服务器。此外，在Unix上应该将.rhost和hosts.equiv文件删除，因为不用猜口令，这些文件就会提供登录访问！限制在防火墙外与网络文件共享。这会使黑客有机会截获系统文件，并以特洛伊木马替换它，文件传输功能无异将陷入瘫痪。

确保手头有一张最新的网络拓扑图。这张图应该详细标明TCP/IP地址、主机、路由器及其他网络设备，还应该包括网络边界、非军事区（DMZ）及网络的内部保密部分。在防火墙上运行端口映射程序或端口扫描程序。大多数事件是由于防火墙配置不当造成的，使DoS/DDoS攻击成功率很高，所以定要认真检查特权端口和非特权端口。检查所有网络设备和主机/服务器系统的日志。只要日志出现漏洞或时间出现变更，几乎可以肯定：相关的主机安全受到了危胁。

利用DDoS设备提供商的设备。

**3.4 IP欺骗攻击**

**3.4.1原理**

IP欺骗是在服务器不存在任何漏洞的情况下，通过利用TCP/IP协议本身存在的一些缺陷进行攻击的方法，IP欺骗之所以可以成功是因为信任服务的基础仅仅是建立在网络地址的验证上。IP 地址是容易被伪造的。攻击过程最难的部分是进行序列号估计,估计精度的高低是成功与否的关键所在。

**3.4.2预防措施**

抛弃基于地址的信任策略  
　　阻止这类攻击的一种非常容易的办法就是放弃以地址为基础的验证。不允许r\*类远程调用命令的使用;删除.rhosts 文件;清空/etc/hosts.equiv 文件。这将迫使所有用户使用其它远程通信手段,如telnet、ssh、skey等等。  
　　进行包过滤  
　　如果您的网络是通过路由器接入Internet 的,那么可以利用您的路由器来进行包过滤。确信只有您的内部LAN可以使用信任关系,而内部LAN上的主机对于LAN以外的主机要慎重处理。您的路由器可以帮助您过滤掉所有来自于外部而希望与内部建立连接的请求。  
　　使用[加密](http://hack.77169.com/List/List_46.html)方法  
　　阻止IP欺骗的另一种明显的方法是在通信时要求[加密](http://hack.77169.com/List/List_46.html)传输和验证。当有多种手段并存时,可能[加密](http://hack.77169.com/List/List_46.html)方法最为适用。  
　　使用随机化的初始序列号  
　　黑客攻击得以成功实现的一个很重要的因素就是,序列号不是随机选择的或者随机增加的。Bellovin  
　　描述了一种弥补TCP不足的方法,就是分割序列号[空间](http://idc.77169.com/)。每一个连接将有自己独立的序列号[空间](http://idc.77169.com/)。序列号将仍然按照以前的方式增加,但是在这些序列号[空间](http://idc.77169.com/)中没有明显的关系。

**3.5病毒**

下面列举几种常见的病毒攻击原理和预防方式

冲击波病毒（蠕虫类病毒）：通过ping命令探测主机——检查是否为win2k/xp系统——利用rpc漏洞获取权限——通过tftp上载必要文件——修改注册表，添加服务——感染其他机器；

这类病毒的预防手段：

禁止ping的icmp回应封包发出；打patch将漏洞补上；在管理工具 ——服务 中 ，将“允许远程编辑注册表”功能禁用；

　　网络天空病毒（邮件类病毒）：广发病毒邮件——用户收到邮件后打开运行——利用漏洞/欺骗执行邮件中的带毒程序 ——修改系统注册表设置——复制自身到系统目录——搜索本地htm，eml等文件中的邮件地址——利用自带smtp将病毒以多种标题连带欺骗文字向各个地 址发出——某些病毒会ddos攻击某些站点；

　　这类病毒的预防手段：

不阅读来历不明和没理由收到的信件；使用web方式在线阅读、管理信件；打上最新的浏览器、outlook补丁；禁止信件以html格式显示信件；平时不用administrator身份登陆，而以普通用户登录，让病毒修改注册表和系统文件的权限受到抑止；使用带邮件即时监控的杀毒程序；

　　新欢乐时光病毒（脚本类病毒）：outlook传播——浏览染毒邮件时利用outlook漏洞运行vb代码——各个目录下生成大量 folder.htt和desktop.ini文件，由于资源浏览器的脚本检查漏洞，浏览该目录即感染——搜索网络内其他机器共享——对有可写权限的（新 变种能自动枚举尝试123，111，用户名123这样的简单密码）其他机器共享目录上载folder.htt和desktip.ini文件——其他机器使 用资源浏览器浏览该文件夹时被感染

　　此类病毒的预防手段：

最好不使用网络邻居，必要使用的时候请只开放读取权限；打上outlook补丁和浏览器补丁；禁止采用html格式查看信件；采用带即时文件监控的杀毒程序：采用第三方资源浏览器浏览网络邻居资源，如total command等等；

**3.6嗅探攻击**

**3.6.1原理**

首先黑客终端加入嗅探目标终端的信息传输路径，以太网是一个广播型的网络，黑客终端再利用嗅探器，将自己的以太网卡设置成杂收模式，然后黑客终端就可以捕获以太网上所有的报文和帧。这种攻击不会影响网络中信息的正常传输过程，并且对网络和主机都是透明的。

**3.6.1防御**

对于通过集线器实施的嗅探攻击，需要有防止黑客终端接入集线器的措施，对于通过交换机实施的攻击，一是需要有防止黑客终端接入交换机的措施，而是交换机需要具有防御MAC表溢出攻击的机制。1.划分VLAN技术，将连接到交换上的所有主机逻辑分开，将他们之间的通信变为点到点的通信方式，2.在网络中布置入侵检测系统（IDS），以及防火墙等安全设备，针对对路由器和交换机的攻击进行识别。  
对于无线通信过程，只能通过传输信息进行加密来防御。

**3.7 SQL注入**

**3.7.1原理**

SQL 注入攻击技术就其本质而言，它利用的工具是SQL的语法，针对的是应用程序开发者编程中的漏洞，当攻击者能操作数据，向应用程序中插入一些SQL语句时，SQL注入攻击就发生了。攻击者直接将代码插入与 SQL 命令串联并执行的用户输入变量中，间接的将恶意代码注入要在表中存储或作为元数据存储的字符串，在存储的字符串随后串连到一个动态 SQL 命令中时，执行该恶意代码。SQL注入攻击是存在于常见的多连接的应用程序中的一种漏洞，攻击者通过在应用程序预先定义好的查询语句结尾加上额外的SQL语句元素，欺骗数据库服务器执行非授权的任意查询。这类应用程序一般是Web应用程序，它允许用户输入查询条件，并将查询条件嵌入SQL 语句中，提交到数据库中执行。通过构造畸形SQL语句攻击者能够获取额外的信息数据。

**3.7.2防御**

1：将输入中的单引号变成双引号。这种方法经常用于解决数据库输入问题，同时也是一种对于数据库安全问题的补救措施

2：使用存储过程

3：认真对表单输入进行校验，从查询变量中滤去尽可能多的可疑字符。

4：在程序中，组织SQL语句时，应该尽量将用户输入的字符串以参数的形式来进行包装，而不是直接嵌入SQL语言。

5：严格区分数据库访问权限。

6：多层架构下的防治策略。在多层环境下，用户输入数据的校验与数据库的查询被分离成多个层次。此时，应该采用以下方式来进行验证：用户输入的所有数据，都需要进行验证，通过验证才能进入下一层；此过程与数据库分离的；没有通过验证的数据，应该被数据库拒绝，并向上一层报告错误信息。

7：对于数据库敏感的、重要的数据，不要以明文显示，要进行加密。关于加密的方法，读者可以参考后面的章节。

8：对数据库查询中的出错信息进行屏蔽，尽量减少攻击者根据数据库的查询出错信息来猜测数据库特征的可能。

9：由于SQL注入有时伴随着猜测，因此，如果发现一个IP不断进行登录或者短时间内不断进行查询，可以自动拒绝他的登陆；也可以建立攻击者IP地址备案机制，对曾经的攻击者IP进行备案，发现此IP，直接拒绝。

10：可以使用专业的漏洞扫描工具来寻找可能被攻击的漏洞。

**3.8 XSS攻击**

**3.8.1原理**

XSS全名是：Cross-site scripting，为了和CSS层叠样式表区分所以取名XSS。是一种网站应用程序的安全漏洞攻击，是代码注入的一种。它允许恶意用户将代码注入到网页上，其他用户在观看网页时就会受到影响。这类攻击通常包含了HTML以及用户端脚本语言。

XSS攻击的主要目的则是，想办法获取目标攻击网站的cookie，因为有了cookie相当于有了seesion，有了这些信息就可以在任意能接进互联网的pc登陆该网站，并以其他人的生份登陆，做一些破坏。预防措施，防止下发界面显示html标签，把</>等符号转义

**3.8.1防御方法**

当恶意代码值被作为某一标签的内容显示：在不需要html输入的地方对html 标签及一些特殊字符( ” < > & 等等 )做过滤，将其转化为不被浏览器解释执行的字符。

当恶意代码被作为某一标签的属性显示，通过用 “将属性截断来开辟新的属性或恶意方法：属性本身存在的 单引号和双引号都需要进行转码；对用户输入的html 标签及标签属性做白名单过滤，也可以对一些存在漏洞的标签和属性进行专门过滤。

**3.9 口令攻击**

**3.9.1口令攻击的主要方法**  
　　1、社会工程学(social Engineering)，通过人际交往这一非技术手段以欺骗、套取的方式来获得口令。避免此类攻击的对策是加强用户意识。  
　　2、猜测攻击。首先使用口令猜测程序进行攻击。口令猜测程序往往根据用户定义口令的习惯猜测用户口令，像名字缩写、生日、宠物名、部门名等。在详细了解用户的社会背景之后，黑客可以列举出几百种可能的口令，并在很短的时间内就可以完成猜测攻击。  
　　3、字典攻击。如果猜测攻击不成功，入侵者会继续扩大攻击范围，对所有英文单词进行尝试，程序将按序取出一个又一个的单词，进行一次又一次尝试，直到成功。据有的传媒报导，对于一个有8万个英文单词的集合来说，入侵者不到一分半钟就可试完。所以，如果用户的口令不太长或是单词、短语，那么很快就会被破译出来。  
　　4、穷举攻击。如果字典攻击仍然不能够成功，入侵者会采取穷举攻击。一般从长度为1的口令开始，按长度递增进行尝试攻击。由于人们往往偏爱简单易记的口令，穷举攻击的成功率很高。如果每千分之一秒检查一个口令，那么86%的口令可以在一周内破译出来。  
　　5、混合攻击，结合了字典攻击和穷举攻击，先字典攻击，再暴力攻击。  
　　避免以上四类攻击的对策是加强口令策略。  
　　6、直接破解系统口令文件。所有的攻击都不能够奏效，入侵者会寻找目标主机的安全漏洞和薄弱环节，饲机偷走存放系统口令的文件，然后破译加密的口令，以便冒充合法用户访问这台主机。  
　　7:网络嗅探(sniffer)，通过嗅探器在局域网内嗅探明文传输的口令字符串。避免此类攻击的对策是网络传输采用加密传输的方式进行。  
　　8:键盘记录，在目标系统中安装键盘记录后门，记录操作员输入的口令字符串，如很多间谍软件，木马等都可能会盗取你的口述。  
　　避免以上几类攻击的对策是加强用户安全意识，采用安全的密码系统，注意系统安全，避免感染间谍软件、木马等恶意程序。  
　**3.9.2口令攻击的防护手段**  
　　1、好口令是防范口令攻击的最基本、最有效的方法。最好采用字母、数字、还有标点符号、特殊字符的组合，同时有大小写字母，长度最好达到8个以上，最好容易记忆，不必把口令写下来，绝对不要用自己或亲友的生日、手机号码等易于被他人获知的信息作密码。  
　　2、注意保护口令安全。不要将口令记在纸上或存储于计算机文件中；最好不要告诉别人你的口令;不要在不同的系统中使用相同的口令；在输入口令时应确保无人在身边窥视；在公共上网场所如网吧等处最好先确认系统是否安全；定期更改口令，至少六个月更改一次，这会使自己遭受口令攻击的风险降到最低，要永远不要对自己的口令过于自信。

**3.10 CC攻击（Challenge Collapsar）**

**3.10.1原理**

CC攻击的原理就是攻击者控制某些主机不停地发大量数据包给对方服务器造成服务器资源耗尽，一直到宕机崩溃。CC主要是用来攻击页面的，每个人都有这样的体验：当一个网页访问的人数特别多的时候，打开网页就慢了，CC就是模拟多个用户(多少线程就是多少用户)不停地进行访问那些需要大量数据操作(就是需要大量CPU时间)的页面，造成服务器资源的浪费，CPU长时间处于100%，永远都有处理不完的连接直至就网络拥塞，正常的访问被中止。

**3.10.2预防**

(1).取消域名绑定   
　　一般cc攻击都是针对网站的域名进行攻击，比如我们的网站域名是“www.abc.com”，那么攻击者就在攻击工具中设定攻击对象为该域名然后实施攻击。 对于这样的攻击我们的措施是在IIS上取消这个域名的绑定，让CC攻击失去目标。具体操作步骤是：打开“IIS管理器”定位到具体站点右键“属性”打开该站点的属性面板，点击IP地址右侧的“高级”按钮，选择该域名项进行编辑，将“主机头值”删除或者改为其它的值(域名)。   
经过模拟测试，取消域名绑定后Web服务器的CPU马上恢复正常状态，通过IP进行访问连接一切正常。但是不足之处也很明显，取消或者更改域名对于别人的访问带来了不变，另外，对于针对IP的CC攻击它是无效的，就算更换域名攻击者发现之后，他也会对新域名实施攻击。

(2).域名欺骗解析   
　　如果发现针对域名的CC攻击，我们可以把被攻击的域名解析到127.0.0.1这个地址上。我们知道127.0.0.1是本地回环IP是用来进行网络测试的，如果把被攻击的域名解析到这个IP上，就可以实现攻击者自己攻击自己的目的，这样他再多的肉鸡或者代理也会宕机，让其自作自受。 另外，当我们的Web服务器遭受CC攻击时把被攻击的域名解析到国家有权威的政府网站或者是网警的网站，让其网警来收拾他们。 现在一般的Web站点都是利用类似“新网”这样的服务商提供的动态域名解析服务，大家可以登录进去之后进行设置。

(3).更改Web端口   
　　一般情况下Web服务器通过80端口对外提供服务，因此攻击者实施攻击就以默认的80端口进行攻击，所以，我们可以修改Web端口达到防CC攻击的目的。运行IIS管理器，定位到相应站点，打开站点“属性”面板，在“网站标识”下有个TCP端口默认为80，我们修改为其他的端口就可以了。

(4).IIS屏蔽IP   
　　我们通过命令或在查看日志发现了CC攻击的源IP，就可以在IIS中设置屏蔽该IP对Web站点的访问，从而达到防范IIS攻击的目的。在相应站点的“属性”面板中，点击“目录安全性”选项卡，点击“IP地址和域名现在”下的“编辑”按钮打开设置对话框。在此窗口中我们可以设置“授权访问”也就是“白名单”，也可以设置“拒绝访问”即“黑名单”。比如我们可以将攻击者的IP添加到“拒绝访问”列表中，就屏蔽了该IP对于Web的访问。

## 3.11 CSRF攻击

**3.11.1原理**

你访问了信任网站A,然后A会用保存你的个人信息并返回给你的浏览器一个cookie，然后呢，在cookie的过期时间之内，你去访问了恶意网站B，它给你返回一些恶意请求代码，要求你去访问网站A，而你的浏览器在收到这个恶意请求之后，在你不知情的情况下，会带上保存在本地浏览器的cookie信息去访问网站A，然后网站A误以为是用户本身的操作，导致来自恶意网站C的攻击代码会被执：发邮件，发消息，修改你的密码，购物，转账，偷窥你的个人信息，导致私人信息泄漏和账户财产安全收到威胁。

**3.11.2预防方式**

添加csrftoken值后，web框架会在响应中自动帮我们生成cookie信息，返回给浏览器，同时在前端代码会生成一个csrf\_token值，然后当你post提交信息时，web框架会自动比对cookie里和前端form表单或ajax提交上来的csrf\_token值，两者一致，说明是当前浏览器发起的正常请求并处理业务逻辑返回响应，那么第三方网站拿到你的cookie值为什么不能验证通过呢，因为他没你前端的那个随机生成的token值啊，他总不能跑到你电脑面前查看你的浏览器前端页面自动随机生成的token值吧。

**3.12 zip炸弹攻击**

**3.12.1原理**

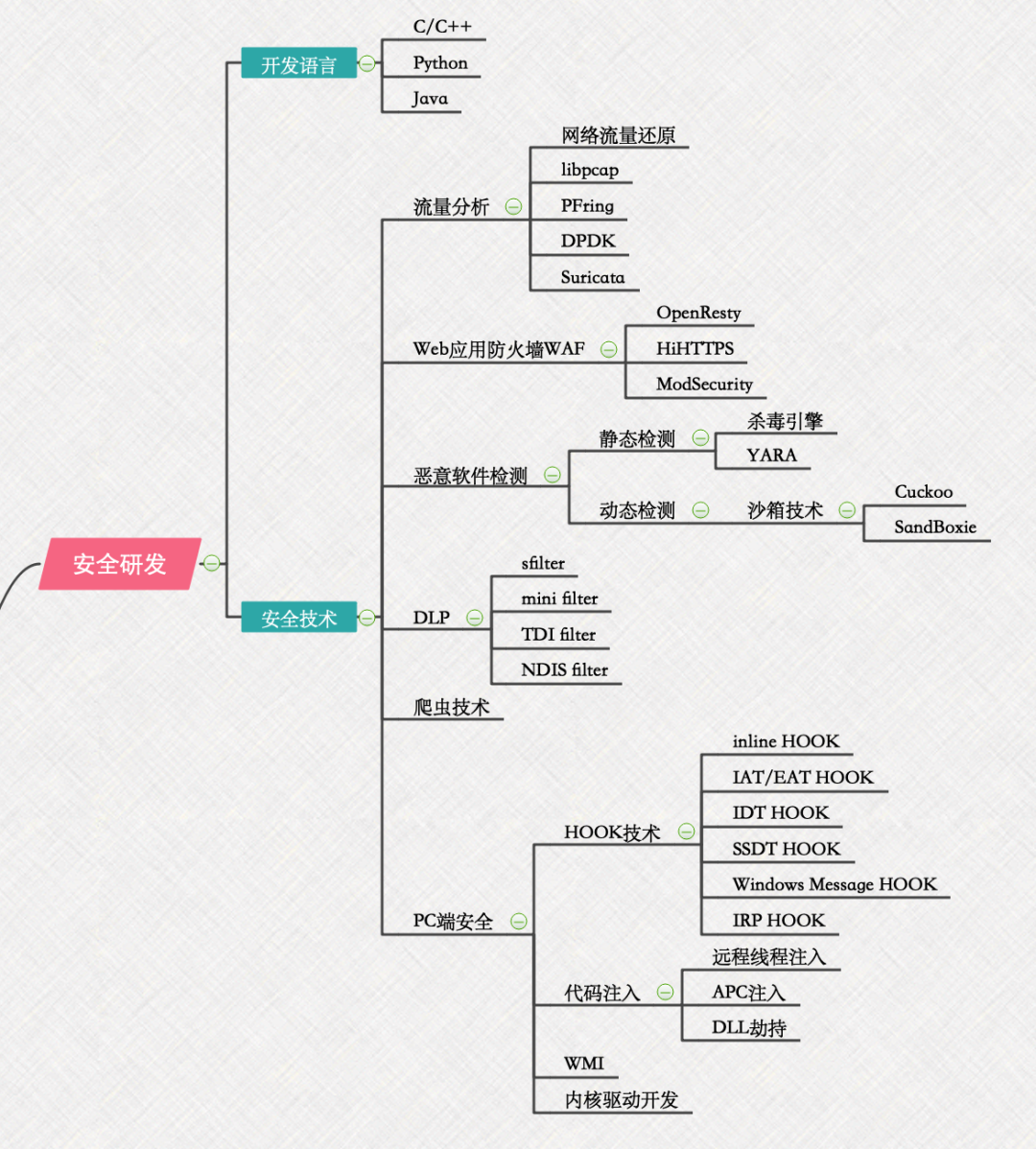
Zip压缩包具有高隐藏性，当压缩的文件或者文件目录过多时，就会导致解压出来很多文件，导致磁盘空间不足

**3.12.1预防**

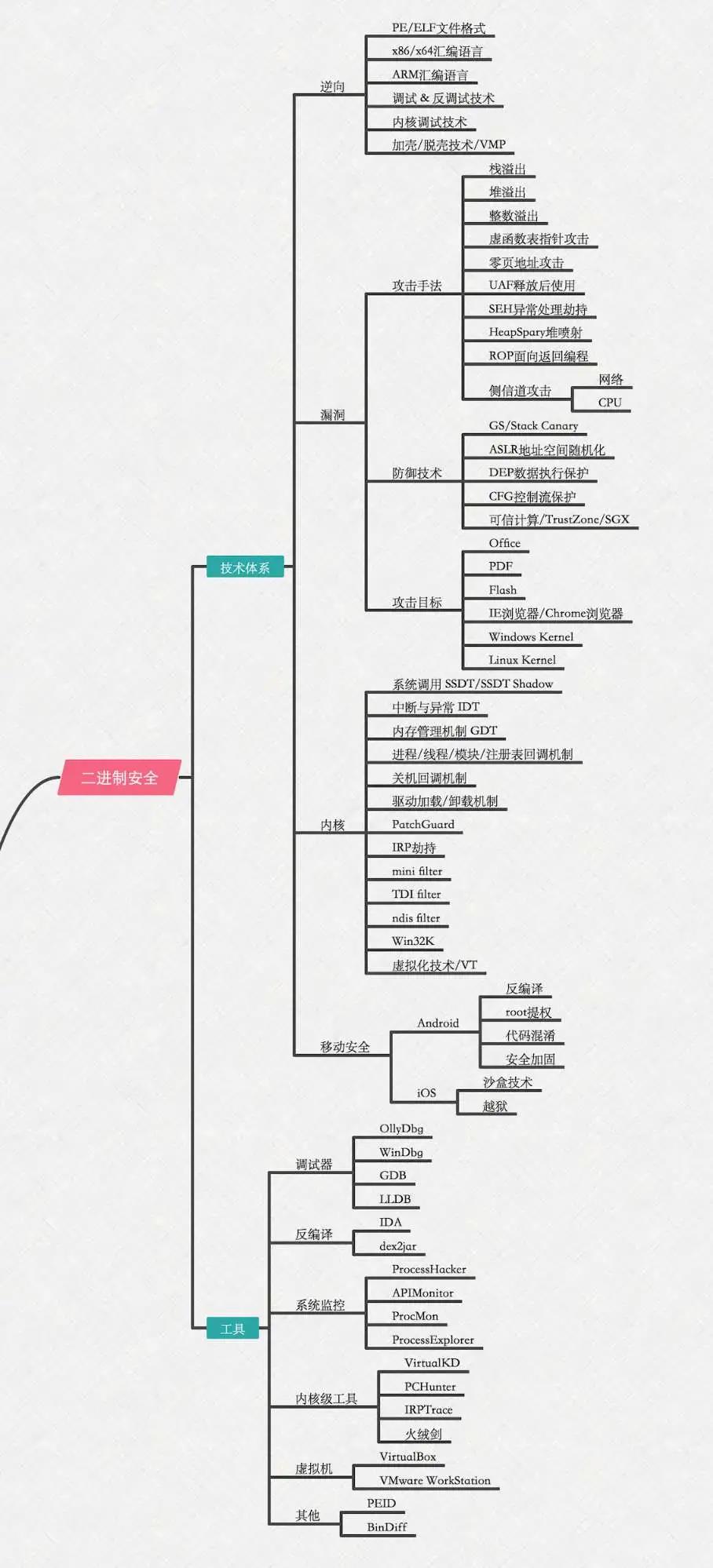
解压之前先判断大小，在判断解压之后的文件目录个数和深度，对于异常的文件不要解压

**4、安全技术栈**

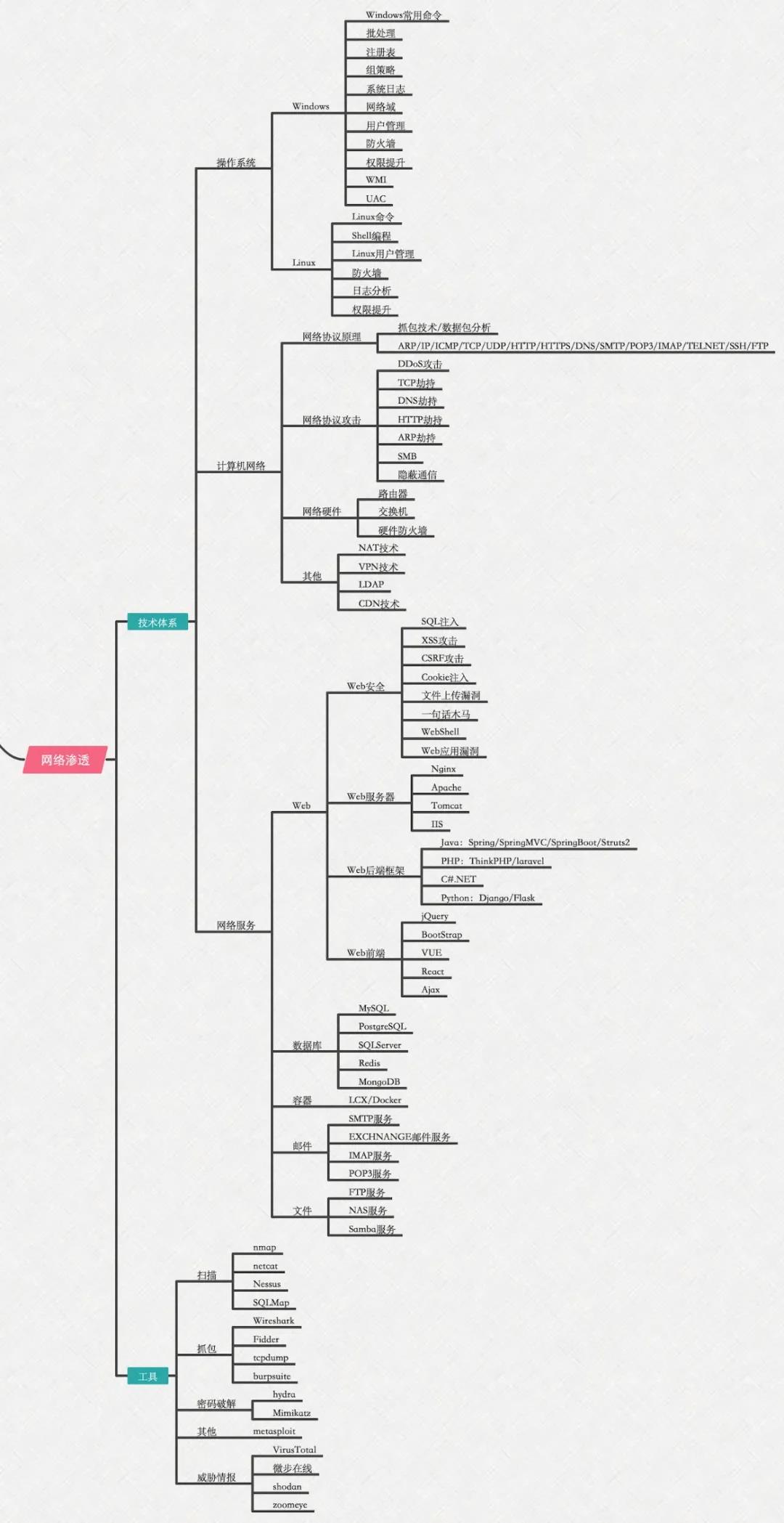
**4．1安全研发**



**4．2二进制安全**

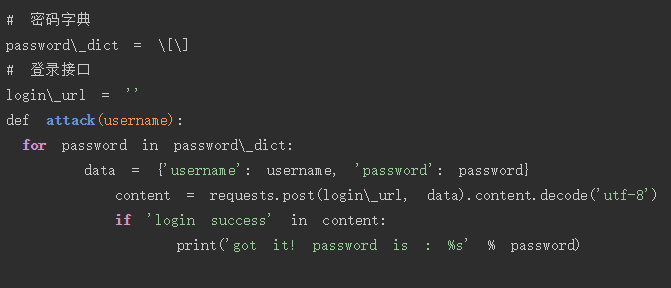


**4．3网络渗透**

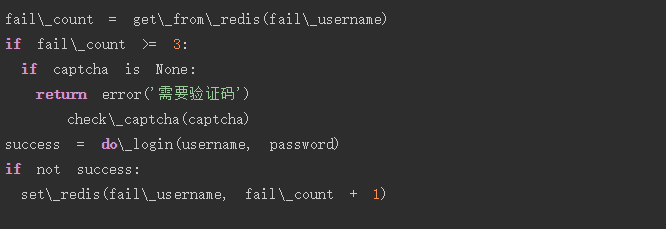


**5、举例说明**

就拿登陆接口举例：一个登陆接口只要暴露在公网上，那么很大概率上会被人盯上，尝试爆破这种简单且有效的方式：  
通过各种方式获得了网站的用户名之后，通过编写程序来遍历所有可能的密码，直至找到正确的密码为止。伪代码如下：



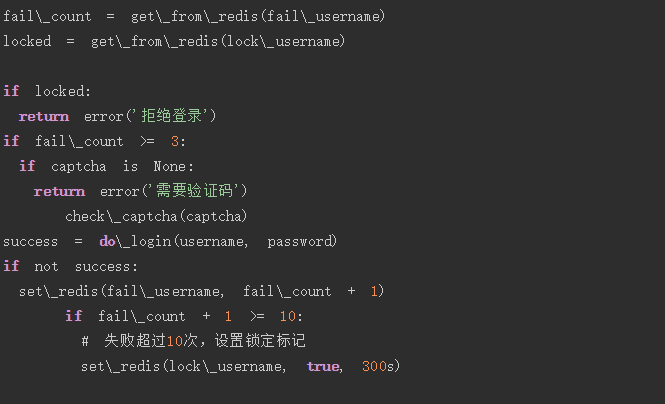
如此我们需要增加比较复杂的图片验证码。伪代码如下：



伪代码未考虑并发，实际开发可以考虑加锁。

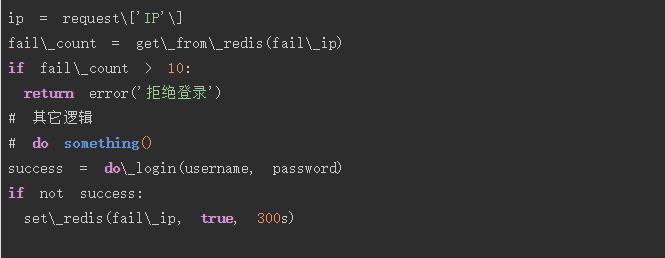
这样确实可以过滤掉一些非法的攻击，但是以目前的 OCR 技术来说的话，普通的图片验证码真的很难做到有效的防止机器人，当然，我们也可以花钱购买类似于三方公司提供的滑动验证等验证方案，但是也并不是 100% 的安全，一样可以被破解

如此进一步设计：直接限制非正常用户的登录操作，当它密码错误达到一定次数时，直接拒绝用户的登录，隔一段时间再恢复。比如我们设置某个账号在登录时错误次数达到 10 次时，则 5 分钟内拒绝该账号的所有登录操作。伪代码如下：



这样确实可以解决用户密码被爆破的问题。但是，这样会带来另一个风险：攻击者虽然不能获取到网站的用户信息，但是它可以让我们网站所有的用户都无法登录！  
攻击者只需要无限循环遍历所有的用户名（即使没有，随机也行）进行登录，那么这些用户会永远处于锁定状态，导致正常的用户无法登录网站！

如此我们可以针对 IP 来处理，直接把攻击者的 IP 封了不就万事大吉了嘛。我们可以设定某个 IP 下调用登录接口错误次数达到一定时，则禁止该 IP 进行登录操作。伪代码如下：



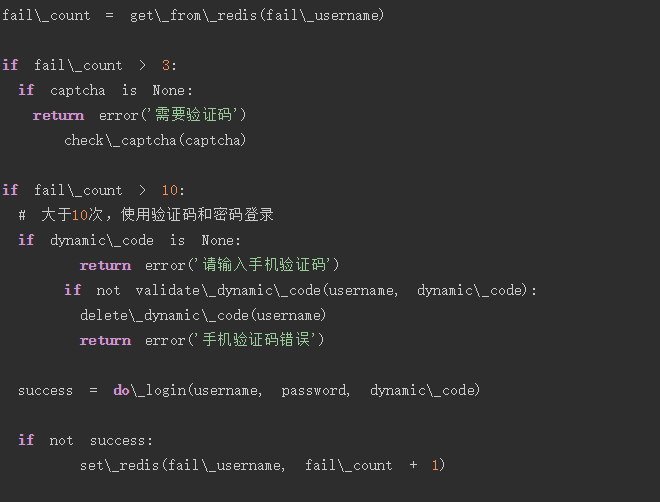
这样也可以一定程度上解决问题，事实上有很多的限流操作都是针对 IP 进行的，比如 niginx 的限流模块就可以限制一个 IP 在单位时间内的访问次数。  
但是这里还是存在问题：比如现在很多学校、公司都是使用同一个出口 IP，如果直接按 IP 限制，可能会误杀其它正常的用户，现在这么多 VPN，攻击者完全可以在 IP 被封后切换 VPN 来攻击

我们可以看到近些年来，几乎所有的应用都会让用户绑定手机，一个是国家的实名制政策要求，第二个是手机基本上和身份证一样，基本上可以代表一个人的身份标识了。所以很多安全操作都是基于手机验证来进行的，登录也可以。

当用户输入密码次数大于 3 次时，要求用户输入验证码（最好使用滑动验证）

当用户输入密码次数大于 10 次时，弹出手机验证，需要用户使用手机验证码和密码双重认证进行登录

伪代码如下：



我们结合了上面说的几种方式的同时，加上了手机验证码的验证模式，基本上可以阻止相当多的一部分恶意攻击者。但是没有系统是绝对安全的，我们只能够尽可能的增加攻击者的攻击成本。

把服务端的HTTP访问更换 HTTPS，把网站中所有的 HTTP 请求修改为强制使用 HTTPS。  
HTTPS 实际上就是在 HTTP 和 TCP 协议中间加入了 SSL/TLS 协议，用于保障数据的安全传输。相比于 HTTP，HTTPS 主要有以下几个特点：

内容加密

数据完整性

身份验证

除了 HTTPS 之外，我们还可以手动对敏感数据进行加密传输：

用户名可以在客户端使用非对称加密，在服务端解密

密码可以在客户端进行 MD5 之后传输，防止暴露密码明文

除了上面我们聊的这些以外，其实还有很多其它的工作可以考虑，比如：

**操作日志**，用户的每次登录和敏感操作都需要记录日志（包括 IP、设备等）

**异常操作或登录提醒**，有了上面的操作日志，那我们就可以基于日志做风险提醒，比如用户在进行非常登录地登录、修改密码、登录异常时，可以短信提醒用户

**拒绝弱密码** 注册或修改密码时，不允许用户设置弱密码

**防止用户名被遍历** 有些网站在注册时，在输入完用户名之后，会提示用户名是否存在。这样会存在网站的所有用户名被泄露的风险（遍历该接口即可），需要在交互或逻辑上做限制