HTTP、SSL/TLS和HTTPS协议的区别与联系

时间：2016-05-13 文章来源：马海祥博客 访问次数：14260 收藏到： 6

今天在请求数据的时候，服务器使用的是https请求，相对安全些，但是结果让我请求图片和资源的时候也使用https请求，我之前写的http请求根本用不了！我就感到非常的不爽！最后听公司的人说了下，最后他们决定重要信息使用https访问，但是对于资源什么的就使用http吧！

开始没什么认识，只感觉到使用https请求数据的时候，要经过安全验证，安全性很高！仔细查了一些资料，原来使用https是要分场合的，不是什么时候都可以用的，对此，我们不妨先来看一下HTTP、SSL/TLS和HTTPS协议之间的区别与联系。

1、“HTTP”是什么?

超文本传输协议（HTTP，HyperText Transfer Protocol)是互联网上应用最为广泛的一种网络协议，所有的WWW文件都必须遵守这个标准，设计HTTP最初的目的是为了提供一种发布和接收HTML页面的方法（具体可查看马海祥博客《深入解析互联网协议的原理》的相关介绍）。

1960年美国人Ted Nelson构思了一种通过计算机处理文本信息的方法，并称之为超文本（hypertext），这成为了HTTP超文本传输协议标准架构的发展根基。

简单来说，HTTP就是一个网络协议，是专门用来帮你传输Web内容的，关于这个协议，就算你不了解，至少也听说过吧？比如你访问我的博客的主页，浏览器地址栏会出现的网址：http://www.mahaixiang.cn，大部分网站都是通过HTTP协议来传输Web页面、以及Web页面上包含的各种东东（图片、CSS 样式、JS 脚本）。

2、“SSL/TLS”是什么?

分类目录

SEO新闻	SEO思维
移动端SEO	SEO问答
医疗SEO	淘宝SEO
企业SEO	站外SEO
网站设计	交互设计
网站策划	网页制作
营销策划	营销案例
竞价技巧	数据分析
写作技巧	微信微博
自媒体	新媒体
内容营销	网站运营
O2O模式	App运营
产品运营	网赚教程
创新思维	电子商务
名人访谈	创业故事

热点推荐


企业云计算中存储必备的9大要素



运营思维 更多>>


传统企业电商该如何制定网络销售渠道策略

立即访问


一个顶尖的产品经理要具备那些能力?

立即访问

SSL是“Secure Sockets Layer”的缩写，中文叫做“安全套接层”，它是在上世纪90年代中期，由网景公司设计的（顺便插一句，网景公司不光发明了 SSL，还发明了很多 Web 的基础设施——比如“CSS 样式表”和“JS 脚本”）。

为啥要发明SSL这个协议捏？因为原先互联网上使用的HTTP协议是明文的，存在很多缺点——比如传输内容会被偷窥（嗅探）和篡改，发明SSL协议，就是为了解决这些问题。

到了1999年，SSL因为应用广泛，已经成为互联网上的事实标准，IETF就在那年把SSL标准化，标准化之后的名称改为TLS（是“Transport Layer Security”的缩写），中文叫做“传输层安全协议”。

很多相关的文章都把这两者并列称呼（SSL/TLS），因为这两者可以视作同一个东西的不同阶段。

3、“HTTPS”是什么意思?

解释完 HTTP 和 SSL/TLS，现在就可以来解释 HTTPS 啦，咱们通常所说的 HTTPS 协议，说白了就是“HTTP 协议”和“SSL/TLS 协议”的组合，你可以把 HTTPS 大致理解为——“HTTP over SSL”或“HTTP over TLS”（反正 SSL 和 TLS 差不多）。

HTTPS（全称：Hyper Text Transfer Protocol over Secure Socket Layer），是以安全为目标的HTTP通道，简单讲是HTTP的安全版。即HTTP下加入SSL层，HTTPS的安全基础是SSL，因此加密的详细内容就需要SSL。

它是一个URI scheme（抽象标识符体系），句法类同http:体系，用于安全的HTTP数据传输。

https:URL表明它使用了HTTP，但HTTPS存在不同于HTTP的默认端口及一个加密/身份验证层（在HTTP与TCP之间），这个系统的最初研发由网景公司(Netscape)进行，并内置于其浏览器Netscape Navigator中，提供了身份验证与加密通讯方法，现在它被广泛用于万维网上安全敏感的通讯，例如交易支付方面。

4、谈谈“对称加密”和“非对称加密”的概念

如果我们想搞明白“对称加密”和“非对称加密”的概念，首先，我们就要先知道什么是“加密”和“解密”?

（1）、什么是“加密”和“解密”?

通俗而言，你可以把“加密”和“解密”理解为某种互逆的数学运算，就好比“加法和减法”互为逆运算、“乘法和除法”互为逆运算。

“加密”的过程，就是把“明文”变成“密文”的过程；反之，“解密”的过程，就是把“密文”变为“明文”，在这两个过程中，都需要一个关键的东东——叫做“密钥”——来参与数学运算。

（2）、什么是“对称加密”?

所谓的“对称加密技术”，意思就是说：“加密”和“解密”使用相同的密钥。这个比较好理解，就好比你用 7zip 或 WinRAR 创建一个带密码（口令）的加密压缩包，当你下次要把这个压缩文件解开的时候，你需要输入同样的密码，在这个例子中，密码/口令就如同刚才说的“密钥”。

对称加密是最快速、最简单的一种加密方式，加密（encryption）与解密（decryption）用的是同样的密钥（secret key），这种方法在密码学中叫做对称加密算

法，对称加密有很多种算法，由于它效率很高，所以被广泛使用在很多加密协议的核心当中。

（3）、什么是“非对称加密”?

所谓的“非对称加密技术”，意思就是说：“加密”和“解密”使用不同的密钥，这玩意儿比较难理解，也比较难想到，当年“非对称加密”的发明，还被誉为“密码学”历史上的一次革命。

非对称加密为数据的加密与解密提供了一个非常安全的方法，它使用了一对密钥，公钥（public key）和私钥（private key），私钥只能由一方安全保管，不能外泄，而公钥则可以发给任何请求它的人，非对称加密使用这对密钥中的一个进行加密，而解密则需要另一个密钥。

由于篇幅有限，对“非对称加密”这个话题，我就不展开了，有空的话，我会再单独写一篇文章在马海祥博客上发布。

（4）、各自有啥优缺点?

看完刚才的定义，很显然：（从功能角度而言）“非对称加密”能干的事情比“对称加密”要多，这是“非对称加密”的优点，但是“非对称加密”的实现，通常需要涉及到“复杂数学问题”，所以，“非对称加密”的性能通常要差很多（相对于“对称加密”而言）。

这两者的优缺点，也影响到了 SSL 协议的设计。

5、HTTP协议的特点

作为背景知识介绍，还需要再稍微谈一下 HTTP 协议本身的特点，HTTP本身有很多特点，考虑到篇幅有限，马海祥只谈那些和HTTPS相关的特点，想要了解更深入的HTTP知识，可查看马海祥博客《HTTP服务的七层架构技术解析及运用》的相关介绍。

（1）、HTTP的版本和历史

如今咱们用的 HTTP 协议，版本号是 1.1（也就是 HTTP 1.1），这个 1.1 版本是1995年底开始起草的（技术文档是RFC2068），并在1999年正式发布（技术文档是RFC2616）。

在 1.1 之前，还有曾经出现过两个版本“0.9 和 1.0”，其中的 HTTP 0.9 没有被广泛使用，而 HTTP 1.0 被广泛使用过。

（2）、HTTP 和 TCP 之间的关系

简单地说，TCP 协议是 HTTP 协议的基石——HTTP 协议需要依靠 TCP 协议来传输数据。

在网络分层模型中，TCP 被称为“传输层协议”，而 HTTP 被称为“应用层协议”。

有很多常见的应用层协议是以 TCP 为基础的，比如“FTP、SMTP、POP、IMAP”等。

TCP被称为“面向连接”的传输层协议，关于它的具体细节，俺就不展开了（否则篇幅又失控了），你只需知道：传输层主要有两个协议，分别是TCP和UDP，TCP比UDP更可靠，你可以把 TCP 协议想象成某个水管，发送端这头进水，接收端那头就出水，并且 TCP 协议能够确保，先发送的数据先到达（与之相反，UDP不保证这点）。

（3）、HTTP协议如何使用 TCP 连接?

HTTP对 TCP 连接的使用，分为两种方式：俗称“短连接”和“长连接”（“长连接”又称“持久连接”，叫做“Keep-Alive”或“Persistent Connection”）

假设有一个网页，里面包含好多图片，还包含好多外部的CSS文件和JS文件，在“短连接”的模式下，浏览器会先发起一个 TCP 连接，拿到该网页的 HTML 源代码（拿到 HTML 之后，这个 TCP 连接就关闭了）。然后，浏览器开始分析这个网页的源码，知道这个页面包含很多外部资源（图片、CSS、JS）。然后针对每一个外部资源，再分别发起一个个 TCP 连接，把这些文件获取到本地（同样的，每抓取一个外部资源后，相应的 TCP 就断开）。

相反，如果是“长连接”的方式，浏览器也会先发起一个 TCP 连接去抓取页面，但是抓取页面之后，该 TCP 连接并不会立即关闭，而是暂时先保持着（所谓的“Keep-Alive”），然后浏览器分析 HTML 源码之后，发现有很多外部资源，就用刚才那个 TCP 连接去抓取此页面的外部资源。

在 HTTP 1.0 版本，默认使用的是“短连接”（那时候是 Web 诞生初期，网页相对简单，“短连接”的问题不大）。

到了1995年底开始制定 HTTP 1.1 草案的时候，网页已经开始变得复杂（网页内的图片、脚本越来越多了），这时候再用短连接的方式，效率太低下了（因为建立 TCP 连接是有“时间成本”和“CPU成本”），所以，在 HTTP 1.1 中，默认采用的是“Keep-Alive”的方式。

6、SSL/TLS协议的基本运行过程

SSL/TLS协议的基本思路是采用公钥加密法，也就是说，客户端先向服务器端索要公钥，然后用公钥加密信息，服务器收到密文后，用自己的私钥解密，但是这里有两个问题：

（1）、如何保证公钥不被篡改?

解决方法：将公钥放在数字证书中，只要证书是可信的，公钥就是可信的。

（2）、公钥加密计算量太大，如何减少耗用的时间?

解决方法：每一次对话（session），客户端和服务器端都生成一个"对话密钥"（session key），用它来加密信息。由于"对话密钥"是对称加密，所以运算速度非常快，而服务器公钥只用于加密"对话密钥"本身，这样就减少了加密运算的消耗时间。

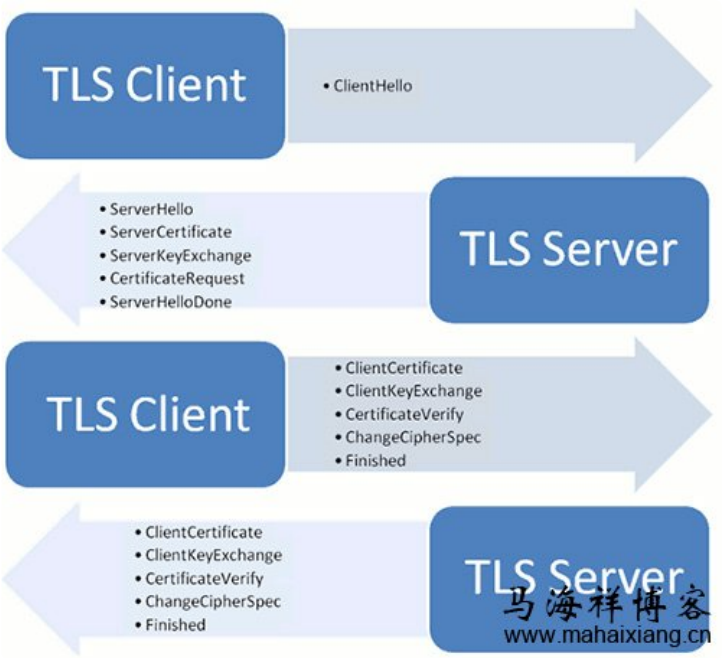
因此，SSL/TLS协议的基本过程是这样的：

（1）、客户端向服务器端索要并验证公钥。

（2）、双方协商生成“对话密钥”。

（3）、双方采用“对话密钥”进行加密通信。

上面过程的前两步，又称为“握手阶段”（handshake）。



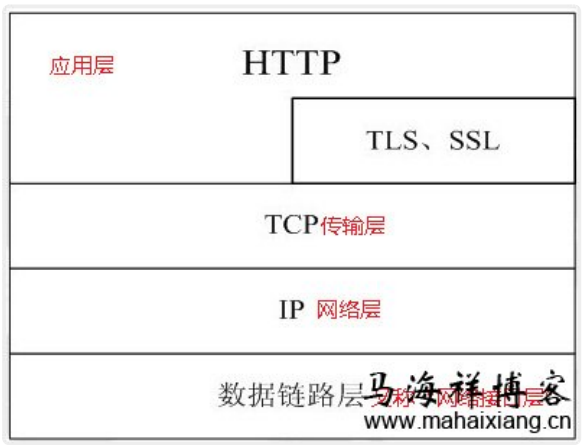
以上图片就是“握手阶段”涉及四次通信，需要注意的是，“握手阶段”的所有通信都是明文的。

7、SSL、HTTP和HTTPS协议的联系

SSL是Netscape公司所提出的安全保密协议，在浏览器(如Internet Explorer、Netscape Navigator)和Web服务器(如Netscape的Netscape Enterprise Server、ColdFusion Server等等)之间构造安全通道来进行数据传输，SSL运行在TCP/IP层之上、应用层之下，为应用程序提供加密数据通道，它采用了RC4、MD5 以及RSA等加密算法，使用40位的密钥，适用于商业信息的加密。

同时，Netscape公司相应开发了HTTPS协议并内置于其浏览器中，HTTPS实际上就是SSL over HTTP，它使用默认端口443，而不是像HTTP那样使用端口80来和TCP/IP进行通信。HTTPS协议使用SSL在发送方把原始数据进行加密，然后在接受方进行解密，加密和解密需要发送方和接受方通过交换共知的密钥来实现，因此，所传送的数据不容易被网络黑客截获和解密。

然而，加密和解密过程需要耗费系统大量的开销，严重降低机器的性能，相关测试数据表明使用HTTPS协议传输数据的工作效率只有使用HTTP协议传输的十分之一。



假如为了安全保密，将一个网站所有的Web应用都启用SSL技术来加密，并使用HTTPS协议进行传输，那么该网站的性能和效率将会大大降低，而且没有这个必要，因为一般来说并不是所有数据都要求那么高的安全保密级别，所以，我们只需对那些涉及机

密数据的交互处理使用HTTPS协议，这样就做到鱼与熊掌兼得（具体可查看马海祥博客《从SEO的角度来分析网站是否该采用HTTPS协议》的相关介绍）。

总之不需要用https的地方，就尽量不要用。

8、HTTPS协议的需求是什么?

花了好多口水，终于把背景知识说完了，下面正式进入正题，先来说说当初设计HTTPS是为了满足哪些需求?

很多介绍 HTTPS 的文章一上来就给你讲实现细节，对此，马海祥觉得这是不好的做法，一上来就给你讲协议细节，你充其量只能知道如何做，无法理解为什么，我在前一个章节讲了“背景知识”，在这个章节讲了“需求”，这就有助于你理解了。

为什么要设计成这样？——这就是 WHY 型的问题。

（1）、兼容性

因为是先有 HTTP 再有 HTTPS，所以，HTTPS 的设计者肯定要考虑到对原有 HTTP 的兼容性。

这里所说的兼容性包括很多方面，比如已有的 Web 应用要尽可能无缝地迁移到 HTTPS；比如对浏览器厂商而言，改动要尽可能小。

基于“兼容性”方面的考虑，很容易得出如下几个结论：

①、HTTPS还是要基于 TCP 来传输

如果改为 UDP 作传输层，无论是 Web 服务端还是浏览器客户端，都要大改，动静太大了。

②、单独使用一个新的协议，把 HTTP 协议包裹起来

所谓的“HTTP over SSL”，实际上是在原有的 HTTP 数据外面加了一层 SSL 的封装，HTTP 协议原有的 GET、POST 之类的机制，基本上原封不动。

打个比方：如果原来的 HTTP 是塑料水管，容易被戳破；那么如今新设计的 HTTPS 就像是在原有的塑料水管之外，再包一层金属水管，一来，原有的塑料水管照样运行；二来，用金属加固了之后，不容易被戳破。

（2）、可扩展性

前面说了，HTTPS 相当于是“HTTP over SSL”。

如果 SSL 这个协议在“可扩展性”方面的设计足够牛逼，那么它除了能跟 HTTP 搭配，还能够跟其它的应用层协议搭配，岂不美哉?

现在看来，当初设计 SSL 的人确实比较牛，如今的 SSL/TLS 可以跟很多常用的应用层协议（比如：FTP、SMTP、POP、Telnet）搭配，来强化这些应用层协议的安全性。

接着刚才打的比方：如果把 SSL/TLS 视作一根用来加固的金属管，它不仅可以用来加固输水的管道，还可以用来加固输煤气的管道。

（3）、保密性（防泄密）

HTTPS需要做到足够好的保密性。

说到保密性，首先要能够对抗嗅探（行话叫 Sniffer），所谓的“嗅探”，通俗而言就是监视你的网络传输流量，如果你使用明文的 HTTP 上网，那么监视者通过嗅探，就知道你在访问哪些网站的哪些页面。

嗅探是最低级的攻击手法，除了嗅探，HTTPS 还需要能对抗其它一些稍微高级的攻击手法——比如“重放攻击”（后面讲协议原理的时候，会再聊）。

（4）、完整性（防篡改）

除了“保密性”，还有一个同样重要的目标是“确保完整性”。

在发明 HTTPS 之前，由于 HTTP 是明文的，不但容易被嗅探，还容易被篡改。

举个例子：比如咱们的网络运营商（ISP）都比较流氓，经常有网友抱怨说访问某网站（本来是没有广告的），竟然会跳出很多中国电信的广告，为啥会这样呢？因为你的网络流量需要经过 ISP 的线路才能到达公网，如果你使用的是明文的 HTTP，ISP 很容易就可以在你访问的页面中植入广告。

所以，当初设计 HTTPS 的时候，还有一个需求是“确保 HTTP 协议的内容不被篡改”。

（5）、真实性（防假冒）

在谈到 HTTPS 的需求时，“真实性”经常被忽略，其实“真实性”的重要程度不亚于前面的“保密性”和“完整性”。

举个例子：你因为使用网银，需要访问该网银的 Web 站点，那么，你如何确保你访问的网站确实是你想访问的网站?

有些天真的同学会说：通过看网址里面的域名，来确保，为啥说这样的同学是“天真的”？因为 DNS 系统本身是不可靠的（尤其是在设计 SSL 的那个年代，连 DNSSEC 都还没发明），由于 DNS 的不可靠（存在“域名欺骗”和“域名劫持”），你看到的网址里面的域名未必是真实滴！

所以，HTTPS 协议必须有某种机制来确保“真实性”的需求（至于如何确保，后面会细聊）。

9、HTTPS和HTTP的区别

超文本传输协议HTTP协议被用于在Web浏览器和网站服务器之间传递信息，HTTP协议以明文方式发送内容，不提供任何方式的数据加密，如果攻击者截取了Web浏览器和网站服务器之间的传输报文，就可以直接读懂其中的信息，因此HTTP协议不适合传输一些敏感信息，比如信用卡号、密码等。

为了解决HTTP协议的这一缺陷，需要使用另一种协议：安全套接字层超文本传输协议HTTPS。

为了数据传输的安全，HTTPS在HTTP的基础上加入了SSL协议，SSL依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。

一般来说，HTTPS和HTTP的区别主要为以下四点：

（1）、https协议需要到ca申请证书，一般免费证书很少，需要交费。

（2）、http是超文本传输协议，信息是明文传输，https则是具有安全性的ssl加密传输协议。

（3）、http和https使用的是完全不同的连接方式，用的端口也不一样，前者是80，后者是443。

（4）、http的连接很简单，是无状态的；HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，比http协议安全（具体可查看马海祥博客《HTTP与HTTPS的区别》的相关介绍）。

10、HTTPS和HTTP的性能比较

再来说最后一个需求——性能。

本来简单的http协议，一个get一个response，由于https要还密钥和确认加密算法的需要，单握手就需要6、7个往返，任何应用中，过多的round trip肯定影响性能，接下来才是具体的http协议，每一次响应或者请求，都要求客户端和服务端对会话的内容做加密/解密。

尽管对称加密/解密效率比较高，可是仍然要消耗过多的CPU，为此有专门的SSL芯片，如果CPU信能比较低的话，肯定会降低性能，从而不能serve更多的请求，加密后数据量的影响，所以，才会出现那么多的安全认证提示（具体可查看马海祥博客《HTTPS对网站性能优化的影响》的相关介绍）。

一般来说，引入HTTPS之后，不能导致性能变得太差，否则的话，谁还愿意用?

为了确保性能，SSL 的设计者至少要考虑如下几点：

（1）、如何选择加密算法（“对称”or“非对称”）？

（2）、如何兼顾 HTTP 采用的“短连接”TCP 方式?

SSL 是在1995年之前开始设计的，那时候的 HTTP 版本还是 1.0，默认使用的是“短连接”的 TCP 方式——默认不启用 Keep-Alive。

HTTPS的关键性能影响是CPU和往返，如果CPU很强的话，性能可能就是有人讲的80%；如果cpu是瓶颈的话，有人讲原来可以server330-500个请求每秒，现在只有30-50%，因此在使用https请求数据的时候要注意看看你的项目里面是否真的需要。

马海祥博客点评：

HTTPS是为了安全性而设置的，要验证很多的信息，相对应http请求的速度肯定有点慢，如果使用HTTPS的话很麻烦的，无意给服务器和客户端增加了很大的压力，所以，平时最好不要使用HTTPS，如果牵扯到个人隐私或者是其他的什么重要信息就一定要这么做了。

很多的时候你感觉有点问题，但是如果不去细细发觉的话，暂时没有什么问题，但是在你后面的维护，或者出问题的时候会弄的头痛不已，为了以后的方便，还是此刻就好好的把每一件事做好，分析好！

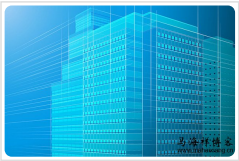
打赏

相关标签搜索： https https协议 http ssl

上一篇：今日头条的个性化推荐算法
下一篇：关于大型网站架构的负载均衡技术详解

相关文章推荐：

您可能还会对以下这些文章感兴趣！



关于大型网站架构的负载均衡技术详解

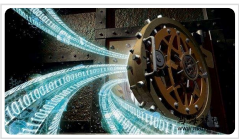
负载均衡是将负载（工作任务，访问请求）进行平衡、分摊到多个操作单元（服务器，组件）上进行执行，是解决高性能，单点故障（高可用），扩展性（水平伸缩）的终极解决方案。面对大量用户访问、高并发请求，海量数据，可以使用高性能的服务器、大型数据库，存储设备，高性能W……【查看全文】

阅读：809 关键词： 大型网站 网站架构 负载均衡 日期：2016-08-05

HTTP、SSL/TLS和HTTPS协议的区别与联系

HTTPS是为了安全性而设置的，要验证很多的信息，相对应http请求的速度肯定有点慢，如果使用HTTPS的话很麻烦的，无意给服务器和客户端增加了很大的压力，所以平时最好不要使用HTTPS，如果牵扯到个人隐私或者是其他的什么重要信息就一定要这么做了，很多的时候你感觉有点问题，……【查看全文】

阅读：14035 关键词： http ssl https https协议 日期：2016-05-13



详解内存数据库中的索引技术

传统的数据库管理系统把所有数据都放在磁盘上进行管理，所以称作磁盘数据库（DRDB:Disk-Resident Database），磁盘数据库需要频繁地访问磁盘来进行数据的操作，磁盘的读写速度远远小于CPU处理数据的速度，所以磁盘数据库的瓶颈出现在磁盘读写上，基于此，内存数据库的概……【查看全文】

阅读：3257 关键词： 内存数据库 索引技术 数据库 日期：2015-01-09

HTTPS建设使用的方案教程解析

百度已对部分地区开放HTTPS加密搜索服务，随后，百度实行全站化HTTPS安全加密服务，百度HTTPS安全加密已覆盖主流浏览器，旨在用户打造了一个更隐私化的互联网空间、加速了国内互联网的HTTPS化。同时也希望更多网站加入到HTTPS的队伍中来，为网络安……【查看全文】

阅读：42 关键词： seo https 日期：2018-02-01

HTTP服务的七层架构技术解析及运用

一般来说，计算机领域的体系结构普遍采用了分层的方式，从最底层的硬件往高层依次有：操作系统->驱动程序->运行库->系统程序->应用程序等等。从网络分层模型OSI来讲，由上至下为：应用层->表示层->会话层->传输层->网络层->数据链路层->物理层。当然实际应用的TCP/IP协……【查看全文】

阅读：4386 关键词： 七层架构解析 七层架构运用 七层架构技术 http服务 日期：2014-09-

计算机的开机启动原理

计算机从打开电源到开始操作，整个启动可以说是一个非常复杂的过程。总体来说，计算机的整个启动过程分成四个阶段：第一阶段：BIOS；第二阶段：主引导记录；第三阶段：硬盘启动；第四阶段：操作系统；直至执行/bin/login程序，跳出登录界面，等待用户输入用户名和密码。……【查看全文】

阅读：3039 关键词： 计算机 计算机启动 计算机原理 开机启动原理 日期：2014-01-16

基于贝叶斯推断应用原理的过滤垃圾邮件研究

随着电子邮件的应用与普及，垃圾邮件的泛滥也越来越多地受到人们的关注。而目前正确识别垃圾邮件的技术难度非常大。传统的垃圾邮件过滤方法，主要有关键词法和校验码法等。前者的过滤依据是特定的词语；后者则是计算邮件文本的校验码，再与已知的垃圾邮件进行对比。它们……【查看全文】

阅读：855 关键词： 贝叶斯推断 贝叶斯应用 贝叶斯原理 过滤垃圾邮件 垃圾邮件 日期：

今日头条的个性化推荐算法

互联网给用户带来了大量的信息，满足了用户在信息时代对信息的需求，但也使得用户在面对大量信息时无法从中获得对自己真正有用的那部分信息，对信息的使用效率反而降低了，而通常解决这个问题最常规的办法是推荐系统。推荐系统能有效帮助用户快速发现感兴趣和高质量的信……【查看全文】

阅读：12908 关键词： 今日头条 日期：2016-01-20

如何开启苹果系统的两步验证机制，避免iCloud帐号遭到攻击

首先，你需要登录至苹果的网页版Apple ID管理系统，你需要点击“管理你的Apple ID”，随后输入帐号密码信息。在登录之后，你需要从左侧导航栏中选择“密码和安全”选项，在这里，你将需要验证安全问题，随后下拉至“两步验证”区域，点击蓝色的“开始”链接并阅读其中的……【查看全文】

阅读：1407 关键词： 苹果系统 验证机制 icloud攻击 icloud帐号 icloud 日期：2014-09-

详解大型网站系统的特点和架构演化发展历程

大型网站的挑战主要来自庞大的用户，高并发的访问和海量数据，任何简单的业务一旦需要处理数以P计的数据和面对数以亿计的用户，问题就会变得棘手，大型网站架构主要就是解决这类问题。大型网站不是从无到有一步就搭建好一个大型网站，而是能够伴随小型网站业务的渐进发……【查看全文】

阅读：853 关键词： 大型网站 网站架构 网站系统 日期：2017-03-02

↓ 点击查看更多 ↓