站点要不要使用 HTTPS 协议

2010 年 5 月份谷歌已经提供 HTTPS 加密搜索服务，直到前段时间，为解决“第三方”对用户隐私的嗅探和劫持，百度也推出了全站 HTTPS 加密搜索服务。搜索引擎对 HTTPS 页面抓取问题的态度不尽相同，谷歌在算法更新中表示，“同等条件下，使用 HTTPS 加密技术的站点在搜索排名上更具优势”，而百度则在其 2014 年 9 月份的一份公告中表示“百度不会主动抓取 HTTPS 网页”。综合各方因素，对于普通站长而言，究竟是否要使用 HTTPS 协议呢？

HTTP 和 HTTPS 的基本概念

HTTP：是互联网上应用最为广泛的一种网络协议，是一个客户端和服务器端请求和应答的标准（TCP），用于从 WWW 服务器传输超文本到本地浏览器的传输协议。它可以使浏览器更加高效，使网络传输减少。

HTTPS：是以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版，HTTPS 的安全基础是 SSL，因此加密的详细内容就需要 SSL。HTTPS 协议的主要作用可以分为两种：一种是建立一个信息安全通道，来保证数据传输的安全；另一种就是确认网站的真实性。

HTTPS 和 HTTP 的区别主要如下

一、https 协议需要到 ca 申请证书，一般免费证书较少，因而需要一定费用。

二、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。

三、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。

四、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。

HTTPS 利与弊

优点：

SEO 方面

谷歌曾在 2014 年 8 月份调整搜索引擎算法，并称“比起同等 HTTP 网站，采用 HTTPS 加密的网站在搜索结果中的排名将会更高”。

安全性

尽管 HTTPS 并非绝对安全，掌握根证书的机构、掌握加密算法的组织同样可以进行中间人形式的攻击。但 HTTPS 仍是现行架构下最安全的解决方案，主要有以下几个好处：

1）使用 HTTPS 协议可认证用户和服务器，确保数据发送到正确的客户机和服务器；

2）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，要比 http 协议安全，可防止数据在传输过程中不被窃取、改变，确保数据的完整性；

3）HTTPS 是现行架构下最安全的解决方案，虽然不是绝对安全，但它大幅增加了中间人攻击的成本。

缺点：

SEO 方面

据 ACM CoNEXT 数据显示，使用 HTTPS 协议会使页面的加载时间延长近 50%，增加 10%到 20%的耗电。此外，HTTPS 协议还会影响缓存，增加数据开销和功耗，甚至已有安全措施也会受到影响也会因此而受到影响。

搜索引擎对 HTTPS 的态度

谷歌的态度

谷歌在 HTTPS 站点的收录问题上与对 HTTP 站点态度并无什么不同之处，甚至把“是否使用安全加密”（HTTPS）作为搜索排名算法中的一个参考因素，采用 HTTPS 加密技术的网站能得到更多的展示机会，排名相对同类网站的 HTTP 站点也更有优势。而且谷歌曾明确表示“希望所有的站长都能将使用 HTTPS 协议，而非 HTTP”更是表明了其对达到“HTTPS everywhere”这一目标的决心。

百度的态度

虽然百度曾表示“不会主动抓取 https 网页”，但对于“很多 https 网页无法被收录”也是“耿耿于怀”。去年 9 月份，百度曾就“https 站点如何建设才能对百度友好”问题发布了一篇文章，给出了“提高 https 站点的百度友好度”的四项建议及具体操作。

此外，近日的“百度全站 HTTPS 加密搜索”事件也再次彰显了百度对 HTTPS 加密的重视。可见，百度并不“反感”HTTPS 站点，所以“不主动抓取”应该也只是暂时的。

因此建议有条件的站点，从安全的角度考虑，应当在涉及安全的场景页面使用 HTTPS 协议。