Google

透明度报告

常见问题解答

问题

Google 的实施情况

- 什么是加密？
- 什么是 HTTPS？
- 为什么要使用 HTTPS？
- Google 的 HTTPS 目标是什么？
- 为什么加密非常重要？
- 有哪些类型的加密？
- 这些图表中包含哪些协议？
- 哪些协议被视为经过了加密？
- 在哪里可以找到关于其他协议的数据？
- 为什么 Google 搜索未包含在产品图中？
- 你们有 2013 年 12 月以前的准确数据吗？

各大热门网站的实施情况

- “使用 HTTPS 的网站”是指什么？
- “新型 TLS 配置”是指什么？
- “默认 HTTPS”是指什么？
- 热门网站列表会不会发生变化？你们会更新此列表吗？
- 你们的数据来源有哪些？
- 此列表是按热门程度排序的吗？
- 我是一名网站站长，我的网站位于此列表中。如果我想迁移到 HTTPS，Google 会提供协助吗？

Certificate Transparency

- 什么是证书授权中心？
- 什么是证书？
- 为什么 Certificate Transparency 非常重要？
- 什么是 Certificate Transparency 日志？
- 此处显示的证书来自哪里？
- 为什么我的证书没有显示在此处？
- 为什么有些网站有多个证书签发方？
- 为什么有些证书列有多个 DNS 名称？

HTTPS 使用率

- Google 如何衡量 HTTPS 使用情况数据？
- 为何选择这 10 个国家/地区用于统计 HTTPS 使用率？

Google 的实施情况

什么是加密？

加密是一种新型的电子信息保护方式，就像过去使用保险箱和密码锁保护纸上信息一样。加密是密码学的一种技术实现方式：信息被转换为难以理解的形式（即编码），以便只有使用密钥才能将其转译为可理解的形式（即解码）。以设备加密为例，需要按照程序或设备提供的明确说明，利用可解译信息的 PIN 码或利用复杂的算法来破解密码。加密实际上是依靠数学对信息进行编码和解码。

什么是 HTTPS？

HTTP（超文本传输协议）是浏览器连接到网站时采用的技术手段。HTTPS 是经过加密的 HTTP 连接，更为安全可靠。如果您在网址部分看到的是 HTTPS 而非 HTTP，则表明与网站的连接是安全的。对于安全的连接，大多数浏览器还会显示安全连接图标，例如 Chrome 会显示一个绿色的挂锁图标。

为什么要使用 HTTPS？

即使您的网站并不处理敏感讯息，您也应使用 HTTPS 来保护您的网站。HTTPS 有助于保障网站的完整性，并捍卫用户的隐私和安全。此外，只有提供 HTTPS 的网站才能使用最新推出的一些非常强大的网络平台功能。

Google 的 HTTPS 目标是什么？

我们坚信，可靠的加密是确保所有网络用户安全无虞的基础。因此，我们正致力于在所有 Google 产品和服务中支持加密。您可以在“Google 的 HTTPS 实施情况”页面中看到我们这一目标的当前进展。

为什么加密非常重要？

我们的讯息要穿过复杂的网络系统才能从 A 点到达 B 点。在这个过程中，讯息很容易被知道如何操纵网络的非既定接收方拦截。此外，便携式设备（不仅仅只是手机）已成为我们生活中必不可少的一部分，其中不仅有我们的照片、讯息记录、电子邮件，还有存储在应用中的私人数据（为了方便起见，我们一般设为始终登入这些应用）。一旦设备丢失或被盗，捡到者或盗窃者就很容易获取我们最私密的信息，从而使我们面临身份被盗用、金钱诈骗甚至人身伤害等风险。

在这些情况下，加密机制可以为我们提供保护。经过加密的讯息在网络传输过程中即使被拦截，拦截方也无法理解其中的内容。此类讯息称为“密文”，而未经加密的讯息则是以“明文”形式传输的。对于设备加密，如果没有为加密的设备进行解密所需的 PIN 码或密码，不轨之徒就无法获取手机上的内容，而只能彻底清空设备。丢失数据固然令人痛心，但至少好过身份被盗用。

有哪些类型的加密？

在传输期间加密可保护从最终用户到第三方服务器的信息流。例如，当您在购物网站上输入信用卡凭据时，安全的连接有助于保护您的信息不会被第三方中途拦截。只有您和连接到的服务器可以解密这些信息。

端到端加密指的是只有发送方和接收方持有用于加密和解密讯息的密钥。即使是负责控制用户讯息传输系统的服务提供商，也无法获取讯息的实际内容。

静态时加密有助于保护未处于传输状态的信息。例如，计算机中的硬盘可以使用静态时加密机制，以确保在计算机被盗后盗窃者无法获取其中的文件。

这些图表中包含哪些协议？

这些图表显示的是通过 HTTP、HTTP/2、HTTPS、SPDY 和 QUIC 发出的请求。

哪些协议被视为经过了加密？

通过 HTTPS、SPDY 和 QUIC 发出的请求被视为已加密，因为它们均默认采用 TLS。此外还有 HTTP/2，因为 Google 不支持未加密的 HTTP/2 连接。

在哪里可以找到关于其他协议的数据？

我们目前发布 Gmail 邮件协议中的 TLS 使用情况数据。上方未列出的其他协议目前不在此报告的范围之内。

为什么 Google 搜索未包含在产品图中？

Google 搜索与 Google 的一些其他产品共用服务基础架构。因此，如果我们将 Google 搜索单独列为一个类别，可能无法保证其数据的准确性。

你们有 2013 年 12 月以前的准确数据吗？

抱歉，没有。2013 年 12 月之前的数据来源不够准确，无法用于衡量 HTTPS 使用情况。

各大热门网站的实施情况

“使用 HTTPS 的网站”是指什么？

如果 Googlebot 能够顺利抵达 https://*domain*，并且没有通过 HTTP 位置进行重定向，那么相应网站即被视为使用 HTTPS。

“新型 TLS 配置”是指什么？

自 2016 年 2 月起，如果网站提供 TLS v1.2 以及采用 AEAD 操作模式的密码套件，我们则会认定相应网站提供新型 HTTPS：

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

“默认 HTTPS”是指什么？

默认 HTTPS 指的是网站会将 HTTP 请求重定向到 HTTPS 网址。请注意，即便如此，网站仍可能会拒绝针对相应网域的 HTTPS 请求（例如，http://*domain* 重定向到 https://*subdomain.domain*，但 https://*domain* 拒绝该连接）。

另外请务必注意，即使某个网站被标记为具有默认 HTTPS，也不保证该网站每个网页上的所有流量都会通过 HTTPS 传输。Chrome 会在您访问的每个网页上显示 HTTPS 状态。如果您使用其他浏览器，请确保自己熟悉所用浏览器显示各种 HTTPS 状态的方式。

热门网站列表会不会发生变化？你们会更新此列表吗？

各个网站的热门程度会有所变化，但这些网站中的大多数通常会保持在前 100 名之内。在 2016 年底前，我们不会更新此列表中的网站，但我们会跟踪这些网站在全年的 HTTPS 状态。

你们的数据来源有哪些？

我们结合使用了公开数据（例如 Alexa 热门网站）和 Google 数据。这些数据是我们在 2016 年的头几个月收集的，此列表正是根据这些数据整理出来的。

此列表是按热门程度排序的吗？

不是。此列表包含前 100 名非 Google 网站，这些网站按字母顺序排列，并根据 HTTPS 使用情况分为三个类别。

我是一名网站站长，我的网站位于此列表中。如果我想迁移到 HTTPS，Google 会提供协助吗？

我们会提供一定程度的支持，协助此列表中的网站迁移到 HTTPS。请前往您的 security@*domain* 电子邮件地址了解更多信息，或通过 google.com 上的安全部分与我们联系。

Certificate Transparency

什么是证书授权中心？

证书授权中心 (CA) 是指向网站运营商签发数字证书的组织。操作系统（例如 Mac OS X 和 Windows）和网络浏览器（例如 Chrome、Firefox、Safari）会预加载一系列可信的根授权中心。新型操作系统通常会随附超过 200 个可信 CA，其中部分 CA 由政府管理。网络浏览器对每个 CA 的信任程度是相同的。此外，许多 CA 还会委托中间 CA 来签发证书。

什么是证书？

当您通过安全连接 (HTTPS) 访问某个网站时，该网站会向浏览器提供数字证书。此证书用于识别该网站的主机名，由已验证网站所有者的证书授权中心 (CA) 签发。只要用户信任相应的 CA，便可信任证书中提供的身份证明。

为什么 Certificate Transparency 非常重要？

当前模式要求所有用户都必须相信，数百个 CA 组织在为任何网站签发证书时不会出现任何错误。但在有些情况下，人为错误或假冒行为可能会导致误发证书。Certificate Transparency (CT) 改变了签发流程，新流程规定：证书必须记录到可公开验证、不可篡改且只能附加内容的日志中，用户的网络浏览器才会将其视为有效。通过要求将证书记录到这些公开的 CT 日志中，任何感兴趣的相关方都可以查看由授权中心签发的所有证书。这能够促使授权中心在签发证书时更加负责，从而有助于形成一个更可靠的系统。最终，如果使用 HTTPS 的某个网站的证书未记录到 CT 日志中，那么当用户访问该网站时，浏览器可能不会显示安全连接挂锁图标。

请注意，只有负责指定网域的组织才知道签发的哪些证书已获授权。如果证书未获授权，网域用户应与签发证书的 CA 联系，以确定应采取的适当措施。

什么是 Certificate Transparency 日志？

Certificate Transparency 日志是采用 RFC 6962 的服务器，允许任何相关方提交由广受信任的 CA 签发的证书。一旦有日志接受了某个证书，该日志的加密属性即可保证相应条目永远不会被移除或修改。

此处显示的证书来自哪里？

透明度报告中的证书是从一系列有效 Certificate Transparency 日志中获取的。这些日志中的许多证书是由 CA 在签发流程期间提交的。此外，我们还添加了 Google 在将网页编入索引时遇到的证书。网站所有者可以在此网站中搜索自己所控制的域名，以确保没有针对其网域误发证书的情况。

为什么我的证书没有显示在此处？

证书记录到至少一个 CT 日志后，就会显示在此处。您可以将自己的证书提交到某个日志，如果不行的话，您可能需要与 CA 联系。技术用户可以使用相关工具（例如 https://certificate-transparency.org 上提供的开放源代码工具）自行将证书提交到日志。

为什么有些网站有多个证书签发方？

许多大型组织会使用多个 CA 来满足各种各样的需求，其中可能包括合同义务、实施考虑事项和费用。

为什么有些证书列有多个 DNS 名称？

许多组织会选择签发可在多个网站使用的单一证书。例如，大型网站经常会为其资源使用多个子网域（如 www.google.com、mail.google.com、accounts.google.com），但会以单一证书指定所有这些子网域。

HTTPS 使用率

Google 如何衡量 HTTPS 使用情况数据？

数据由选择分享使用情况统计信息的 Chrome 用户提供。所属国家/地区以与用户浏览器相关联的 IP 地址为依据。

为何选择这 10 个国家/地区用于统计 HTTPS 使用率？

为了比较世界各地的 HTTPS 使用率，我们从不同的地理区域选择了 10 个拥有一定规模 Chrome 用户群的国家/地区。

Google 的实施情况

各大热门网站的实施情况

Certificate Transparency

HTTPS 使用率

变化