TeamViewer 安全信息

目标群体

本文档的目标群体是专业网络管理员。本文档提供的信息属于技术信息且非常详尽。根据这些信息，IT 专业人员将全面详细地了解 TeamViewer 的安全标准，并在部署软件之前解决所有问题。您可以随时将此文档分发给客户，以减少任何可能发生的安全问题。

如果您认为自己不属于本文档的目标群体，“公司/软件”部分提供的信息仍然可以帮助您清楚地了解我们如何认真对待安全问题。

公司/软件

关于我们

TeamViewer GmbH 成立于 2005 年，总部位于德国南部的哥廷根（在斯图加特附近），在澳大利亚和美国设有子公司。我们专门开发和销售用于网上协作的安全系统。我们的免费增值许可模式使我们在短时间内得到迅速发展，目前有 2 亿多用户在 14 亿台设备上使用 TeamViewer 软件，遍及全球 200 多个国家。该软件有 30 多个语言版本。

我们对安全的理解

在任何一天的任何时候，都有 3000 多万用户正在使用 TeamViewer。这些用户正在互联网上提供自发的支持、访问无人值守的计算机（即服务器的远程支持）以及举行在线会议。根据配置，TeamViewer 可用于远程控制另一台计算机，就像您直接坐在计算机前面一样。如果登录到远程计算机的用户是 Windows、Mac 或 Linux 管理员，他们也将拥有远程计算机的管理员权限。

很明显，在可能不安全的互联网上授予这样强大的功能，必须通过严格的审查进行保护，以免受攻击。实际上，安全问题在我们的所有发展目标中占有重要地位，我们所做的一切都非常注重安全问题。我们希望确保您能安全地访问我们的计算机并保护自己的利益：数以百万计的全球用户只信任安全的解决方案，只有安全的解决方案才能确保我们的企业取得长期的成功。

质量管理

根据我们的理解，如果没有既定的质量管理体系，不可能实现安全管理。TeamViewer GmbH 是市场上为数不多的实施 ISO 9001 认证质量管理体系的供应商之一。我们的质量管理遵循国际公认的标准。我们每年都通过外部审计来审查质量管理体系。

外部专家评估

我们的软件 TeamViewer 已经被联邦信息技术专家和评审员协会（Bundesverband der IT-Sachverständigen und Gutachter e.V.，简称 BISG e.V.）授予五星质量标志（最高级别）。BISG e.V. 的独立评审员检查合格生产商的产品质量、安全和服务特点。

参考资料

目前，有超过 2 亿用户使用 TeamViewer。来自各行各业的国际顶级企业（包括银行、金融、医疗和政府等高度敏感的行业）都在成功地使用 TeamViewer。

我们邀请您查看在互联网上随处可见的关于我们的参考资料，初步了解客户如何接受我们的解决方案。您会发现，大概大部分其他公司都有相似的安全性和可用性要求，他们经过深入考察，最终决定使用 TeamViewer。为了让您进一步了解我们的软件，请查看本文档其余部分提供的技术细节。

TeamViewer 会议

创建会话和连接类型

在建立会话时，TeamViewer 会确定最佳连接类型。通过主服务器握手后，在所有情况下，70% 会通过 UDP 或 TCP 建立直接连接（甚至在标准网关、NAT 和防火墙之后）。其余连接通过 TCP 或 https 通道的高冗余路由器网络进行路由。您不必为了使用 TeamViewer 而打开任何端口

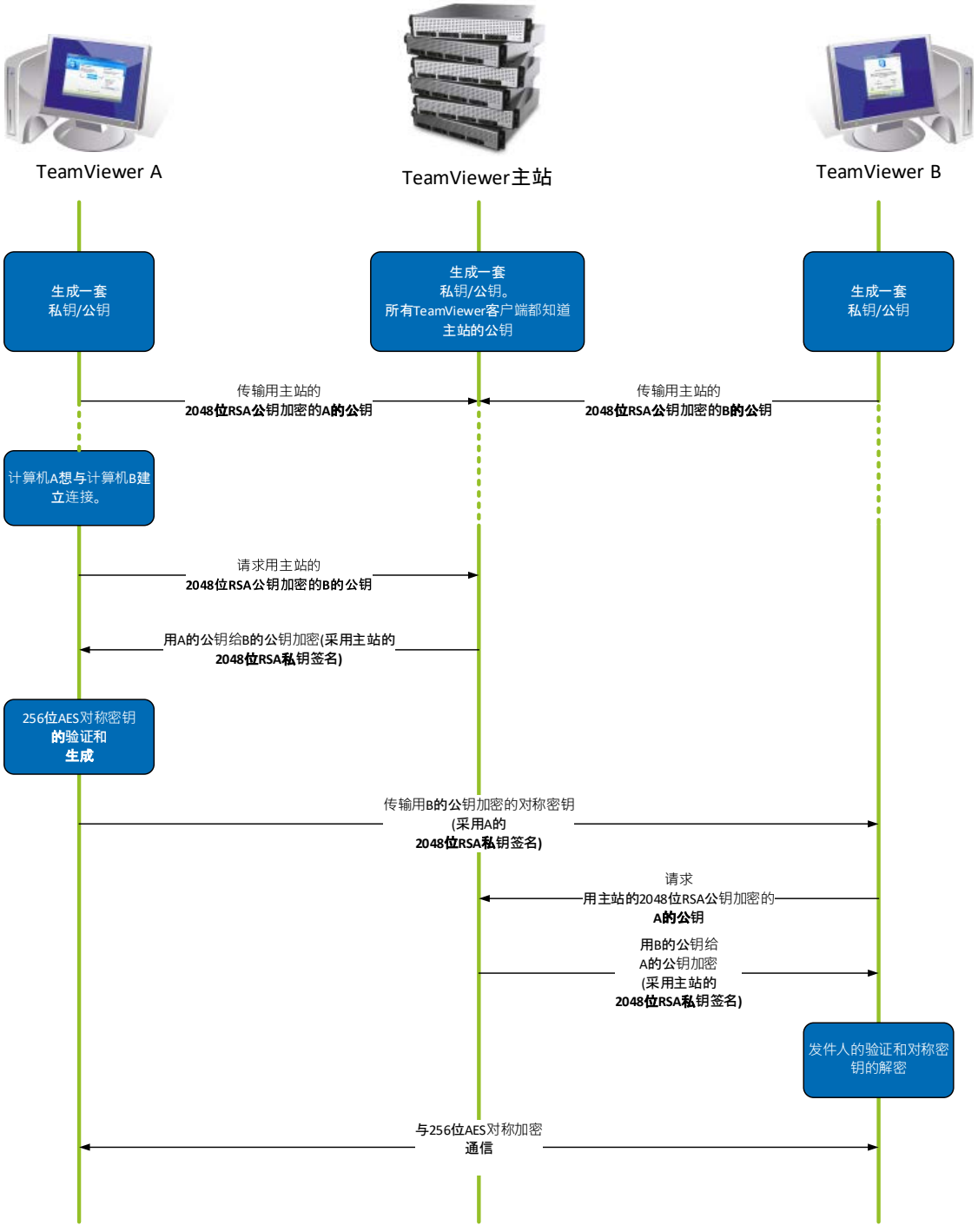
后面将在加密和验证一段说明，即使我们作为路由服务器运营商，也不能读取加密的数据通信。

加密和验证

TeamViewer 通信使用 RSA 公钥/私钥交换和 AES（256 位）会话加密来保护。该技术以 http/SSL 的可比较形式使用，现行标准认为该技术完全安全。由于私钥永远不会离开客户端计算机，因此，该程序可确保互连的计算机（包括 TeamViewer 路由服务器）无法解密数据流。

每个 TeamViewer 客户端已经实施了主集群的公钥，因此可以将消息加密到主集群，并检查由其签名的消息。PKI（公钥基础设施）可有效防止中间人攻击。尽管使用加密，但密码永远不会直接发送，只能通过质询-响应过程发送，并且只保存在本地计算机上。

在验证过程中，由于使用安全远程密码 (SRP) 协议，密码永远不会直接传输。本地计算机上只存储密码验证器。



TeamViewer 加密和验证

TeamViewer ID 的验证

TeamViewer ID 基于各种硬件和软件特性，由 TeamViewer 自动生成。在每次连接之前，TeamViewer 服务器会检查这些 ID 的有效性。

蛮力保护

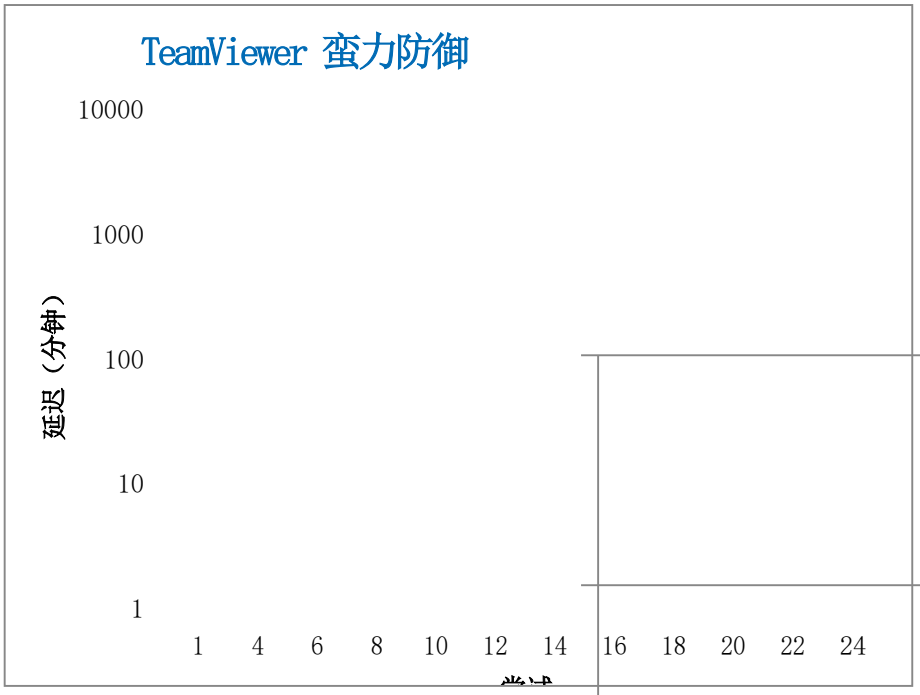
询问 TeamViewer

安全性的潜在客户经常询问有关加密的信息。我们可以理解，客户最担心第三方可以监视连接或 TeamViewer 访问数据被窃听。然而，实际情况是非常原始的攻击往往是最危险的。

在计算机安全领域，蛮力攻击是使用试错方法猜测用于保护资源的密码。随着标准计算机的计算能力不断增强，猜测长密码所需的时间不断减少。

为了防止蛮力攻击，TeamViewer 连接尝试之间的延迟时间呈指数级增加。因此，24 次尝试需要多达 17 个小时。只有成功输入正确的密码，延迟时间才会重置。

TeamViewer 不仅采用有效的机制来保护客户免受一台特定计算机的攻击，还可以防御尝试访问一个特定 TeamViewer ID 的多台计算机（称为僵尸网络攻击）。



表：蛮力攻击时 n 次连接尝试后等待的时间

代码签名

作为一项额外的安全功能，我们的所有软件都通过 VeriSign 代码签名进行签名。这样，软件的发行者总是易于识别。如果后来软件被更改，数字签名将自动变为无效。

数据中心和主干网

为了使 TeamViewer 服务拥有最佳安全性和可用性，所有 TeamViewer 服务器均位于符合 ISO 27001 标准的数据中心，并使用多冗余运营商连接和冗余电源。此外，我们只使用最先进的品牌硬件。另外，所有存储敏感数据的服务器均位于德国或奥地利。

通过 ISO 27001 认证意味着个人访问控制、摄像机监控、运动检测器、24x7 监控和现场安全人员可确保数据中心的访问权只会授予经授权的人员，并保证硬件和数据的最佳安全性。数据中心的单个入口点还有详细的识别检查。

TeamViewer 帐户

TeamViewer 帐户托管在专用的 TeamViewer 服务器上。有关访问控制的信息，请参阅上面的数据中心和主干网。针对授权和密码加密，使用安全远程密码协议（SRP，增强的密码-验证密钥协议 (PAKE)）。渗透者或中间人无法获得蛮力猜测密码所需的足够信息。这意味着即使客户使用强度较弱的密码也可以获得很强的安全性。TeamViewer 帐户中的敏感数据（例如云存储登录信息）使用 AES/RSA 2048 位加密存储。

管理控制台

TeamViewer 管理控制台是基于网络的平台，用于用户管理、连接报告以及管理计算机和联系人。它托管在经 ISO-27001 认证、符合 HIPAA 标准的数据中心。所有数据传输都通过使用 TSL（传输安全层）加密（互联网安全连接标准）的安全通道。敏感数据进一步使用 AES/RSA 2048 位加密存储。针对授权和密码加密，使用安全远程密码协议 (SRP) 。SRP 采用 2048 位模数，是一种成熟、 稳健、安全且基于密码的验证和密钥交换法。

基于策略的设置

在 TeamViewer 管理控制台中，用户可以为专属于他们的设备上安装的 TeamViewer 软件，定义、分配和执行设置策略。设置策略由生成策略的帐户进行数字签名。这可以确保能够将策略分配给设备的唯一帐户是设备所属的帐户。

TeamViewer 中的应用程序安全性

黑名单和白名单

特别是如果 TeamViewer 用于维护无人值守的计算机（即 TeamViewer 作为 Windows 服务安装），那么将这些计算机的访问权限制为多个特定客户端的额外安全选项可能很有用。

使用白名单功能，您可以明确指出允许哪些 TeamViewer ID 和/或 TeamViewer 帐户访问计算机。使用黑名单功能，您可以阻止某些 TeamViewer ID 和 TeamViewer 帐户。中央白名单是上述“管理控制台”中“基于策略的设置”的一部分。

聊天和视频加密

聊天记录与您的 TeamViewer 帐户相关联，因此使用与“TeamViewer 帐户”标题下所述的相同的 AES/RSA 2048 位加密安全方法进行加密和存储。所有聊天消息和视频通信都使用 AES（256 位）会话加密进行端对端加密。

没有隐身模式

没有能够让 TeamViewer 完全在后台运行的功能。即使应用程序作为 Windows 服务在后台运行，始终可以通过系统托盘中的图标看到 TeamViewer。

建立连接后，系统托盘上始终能看到一个小控制面板。因此，TeamViewer 被有意设计为不适合隐蔽地监控计算机或员工。

密码保护

对于自发的客户支持，TeamViewer (TeamViewer QuickSupport) 生成会话密码（一次性密码）。如果您的客户告诉您他们的密码，您可以通过输入他们的 ID 和密码连接到他们的计算机。在客户一端重新启动 TeamViewer 后，将生成新的会话密码，因此，您只有获得邀请，才能连接到客户的计算机。

如果部署 TeamViewer 用于无人值守的远程支持（例如服务器的远程支持），您可以设置单独的固定密码，以保护对计算机的访问。

传入和传出访问控制

您可以单独配置 TeamViewer 的连接模式。例如，您可以配置您的远程支持或会议计算机，使其不能建立传入连接。

将可用功能限制为实际需要的功能，总是意味着可以限制可能被攻击的潜在弱点。

双因素验证

TeamViewer 协助公司实施 HIPAA 和 PCI 合规要求。双因素验证增加一个额外安全层，以保护 TeamViewer 帐户不接受未经授权的访问。

除了用户名和密码之外，用户必须输入代码才能进行验证。该代码通过基于时间的一次性密码 (TOTP) 算法生成。因此，代码仅在短时间内有效。

通过双因素验证以及使用白名单限制访问权，TeamViewer 有助于满足 HIPAA 和 PCI 认证的所有必要条件。

安全测试

TeamViewer 基础架构和 TeamViewer 软件均经常进行渗透测试。测试由专门从事安全测试的独立公司执行。

其他问题？

如果您有其他疑问或想了解更多信息，请随时拨打400 120 3541（普通话）和 +86 (0) 10 8405 3649（普通话)联系我们，或发送电子邮件至support@teamviewer.com。

联系方式

TeamViewer GmbH
Jahnstr.30
D-73037 Göppingen
Germany
service@teamviewer.com