微信加密的通信原理分析研究

□郑坤　武警吉林总队网管中心

【摘要】　随着科技日益发展，各种新技术、新材料应运而生，被广泛应用到不同领域、行业中，发挥着不可替代的作用。在新时代下，微信是腾讯公司开发了一款即时通讯软件，能够实现跨通信运营商、跨操作系统平台的信息交互。因此，本文作者对微信加密通信原理这一主题予以了探讨。

【关键词】　微信加密　通信原理　探讨

随着微信平台逐渐完善，还新增加了很多功能，比如，朋友圈、消息推送。微信已成为一种关键性通信手段，其用户群涉及到不同的年龄段、社会层次，使用人数不断增多，其影响力遍及中国大陆、东南亚，甚至一些外国用户也在使用，深受社会大众的喜欢。当下，微信已成为我国网络社交软件中的主流，其通信是否安全、保密已成为社会大众关注的焦点。

一、微信产品特点

第一、微信使用设备大众化。在日常生活中，用户不需要受到时空的限制，借助手机、电脑等移动通信设备的力量，便能进行一系列的操作，比如，发送语音、图片等。在这个过程中，微信能够提供各种服务，比如，即时通信服务。而用户可以马上把各种信息分享到自己的微信朋友圈中，亲人、好友等都能第一时间看到。第二、注重在强关系链的信息分享。在应用的过程中，微信可以跨越多重壁垒，比如，运营商、社交网，使现实与虚拟相连接，成为知识经济时代中一种新的社交节点。和微博相比，微信远远优于它，能够实现点对点的精准沟通、交流，甚至可以实现多人群组聊天，在丰富社会大众日常生活的同时，也带去了更多的便利。第三、用户可以自由选择消息的私密性、公开性。更为重要的是，微信好友在进行私密话题传播的时候，用户可以对私密话题、传播的范围进行合理化的控制，具有一定的私密性。在一定程度上，不同用户群组可以根据自身的需求，把相关的行业问题、敏感问题迅速传播到不同领域、行业中，使对应的重要信息公开化，成为更多人关注的焦点。第四、微信具有较大的通信交流平台。实际上，在初始阶段，微信只是一款手机的通信工具，用户可以免费发送信息。在经过一系列演变之后，微信具有的功能日渐增多，比如，漂流瓶、朋友圈、二维码。简单来说，它已成为社会大众日常生活中不可或缺的移动通信、社交关系管理平台。

二、微信加密的通信原理

2.1 加密算法、通信协议

1.1RSA 加密算法。在新形势下，RSA 加密算法具有较大的影响力，已有 20 年的发展历史，可以抵挡当下所有已知密码的攻击，保护通信内容安全。RSA 加密算法属于公开秘钥密码机制，也属于一种不对称算法。RSA 加密算法的安全性和密钥长度有着密不可分的联系，属于正比例关系。如果密钥的长度不断增加，RSA 安全系数也会随之增高。就微信系统中应用的 1024 位密钥来说，如果当下的计算速度为基准，需要长达两年的时间才能破解，可见破难度之大。RSA 加密算法的加密流程主要体现在这些方面。首先，在加密过程中，加密端会产生一些文字串符号，得到相应的 CER 认证公钥。其次，对应的加密机制在 Encoding 作用下，以不同的代页码为载体，把一系列字符串符转化为不同形式的编码，以 byte[] 形式呈现出来。在此基础上，byte[] 字节会以流明文的形式被发送。最后，以 CER 证书公钥为纽带，对 byte[] 字节流明文进行加密操作，需要采用 byte[] 密文形式进行发送。

2、AES 随机密钥加密算法。简单来说，AES 加密算法可以保护对应的电子数据，可以应用 128、192、256 位密钥，甚至可以用 128 位分组加密、解密数据，能够重复置换、替换所输入的数据。在微信通信中，所使用的 128 位 AES 随机密钥、其加密强度远远大于 56 位 DES 加密强度，比它的 1021 倍还要多。从某个侧面来说，即时有一台可以在一秒内破解 DES 密码的机器，也需要花费大约 149 亿万年的时间破解 128 位的 AES 密码。就以当下的解密技术而言，只有 AES 知道对应的密钥才能破解。

3、ProtocolBuffer 通信协议。它是 Google 公司开发的，可以描述、传输、存储结构化的数据，建立在二进制基础上，但并不复杂。在应用过程中，开发人员只需要以相关的语法为纽带，来定义结构化的消息模式。并充分利用命令行工具中的一些简单命令语句，就可以生成对应的代码文件。在新形势下，ProtocolBuffer 能够支持不同形式的语言环境，比如，python 语言环境，能够应用到很多领域中，比如，数据的存储、文件的配置。

2.2 微信系统的登录验证程序、通信程序

1、验证流程。第一、在微信通信系统运行中，移动客户端会产生一个由多种元素组合而成的登录包，比如，用户的账号、密码，需要使用 RSA 的公钥加密登录包，并把它发送给对应的服务器。第二、服务器在接收到密文登录包治好，需要合理应用 RSA 私钥来解密，获取登录包中的相关信息，比如，用户的账号。在此基础上，服务器会全方位校验用户的账号、密码，对用户身份进行确认。随之，会产生一个验证包，需要借助 AES 密钥的力量，把它加密成验证包密文的形式，发送到客户端。第三、客户端在接收到验证包密文之后，也会应用 AES 密钥来解密，获取其中的验证信息，并对一系列通信信息进行加密。

2、交互流程。客户端在解密验证包之后，会得到一个从服务器中计算出的随机 AES 密钥，而所有的通信过程都需要对此进行加解密通信。简单来说，微信的各种通信传输都

光网络的智能化发展—SDON 开创新型网络架构

□常新征　梁燕　中国联通邯郸市分公司

【摘要】　自光网络作为传送网发展至今，在数据网络的推动下，从传统的点到点 WDM 光网络到 ASON 再到 SDON，智能化发展趋势越来越明显。在当前大型多域异构的网络环境下，SDON 以其配置灵活，扩展、调节、适应能力强的特点必将主宰未来光网络的智能化发展方向。

【关键词】　光网络　智能化　SDN

一、引言

光网络自兴起以来，从最初所承载的单一话音业务，直到现在的多业务、大数据、高容量传送平台的应用，从最初的点对点通信到现在的动态配置传输需求，其技术的发展在几十年的时间里历经多个标志性的里程碑。在网络带宽容量不断提升、多业务、大数据以及网络的灵活性、扩展性的需求驱动下，光网络的智能化发展已经势在必行。

二、光网络智能化发展历程

纵观光网络的发展历程，可将其分为两条主线：即传送技术的发展以及网络设计架构思想的演变。最初传统的波分复用技术（WDM）、90 年代中期的稀疏波分复用技术（CWDM）、密集波分复用技术 DWDM）网络发展到现在的频谱灵活光网络、分组增强型的光传送网（OTN），光传输由取代电成为信息主要承载介质这一基本功能发展为现在的能够满足传输损伤感知与质量评估、可调单元的参数选择以及 DSP 算法性能控制等功能，传输质量大幅提升。光网络发展到 21 世纪初，人们提出的自动交换光网络（ASON）的概念，从控制层面的角度真正开启了光网络智能化的开端，为光网络实现向高度智能化软件定义光网络（SDON）的平滑演进提供了技术支持。

三、智能光网络

3.1 ASON 的技术优势

ASON 是最初的“智能光网络”，因采用格形组网来避免大量故障影响业务的情况而具备极强的生存能力；网络提供的保护恢复方式遵从优先级原则，提供差异化的服务；为客户提供最优路由，资源利用率高达 50% 以上；升级扩容能力更强，扩大网络中的链路容量即可实现扩容；建设和维护成本有所降低，网络规模越大，经济性越强 [1]。ASON 通常采用 GMPLS 协议，若需完成对多种传送颗粒的有效控制，实现传送网智能化，必须对其扩展和延伸，同时还需进一步提高网络保护恢复的性能。ASON 可加载于 SDH 或 OTN 为其提供控制平面，实现光层和电层相结合的智能调度，将传输、交换和数据三个本身不存在联系的网络有效结合在一起，实现全网 ASON 智能化。

3.2 ASON 所暴露的问题

①网络高度异构性。长期共存的多种类型的传输 / 交换标准和技术如 SDH、WDM、OTN 以及不同设备的结构 / 接口类型往往增加了域间连接的复杂度；

②两大接口商用化程度低。ASON 体系架构中包含三种接口，即用户网络接口 UNI、外部网络节点接口 E–NNI、内部网络节点接口 I–NNI，网络信息在网络之间任一方向的任何边界 / 接口不是共用。但需要注意的是，UNI 和 E–NNI 两个接口都未被大范围的商用化，成为阻碍 GMPLS/ASON 智能化控制平面大范围推广的主要原因；

③保密性需求。一般来说域内网络网络拓扑结构以及资源信息的保密性是由运营商掌握的，来自于不同制造商的不同的技术规范和设备参数是不开放的，这就会导致域内信息不能被整个网络所共享，增加路由和连接控制的困难；

④控制平面复杂。应用 UNI 接口需要对 GMPLS 进行扩展，从而增加代码的复杂性；网络出现不可预期的爆争情况时，GMPLS 中所采用的分布式链路状态路由协议（OSPF 等）又会面临收敛性和稳定性的问题。

四、光网络的高度智能化

4.1 SDON 的技术优势

是建立在随机 AES 密钥基础上的。就其交互流程来说，微信通信的保密性和随机 AES 密钥息息相关，一旦获取了随机 AES 密钥，微信通信信息便不具有其保密性。

三、结语

总而言之，在新时代中，微信是重要的社交软件，发挥着不可替代的作用，对其加密原理予以分析具有一定的实践意义。但从长远来说，还需要对其登录过程、通信交互过程中的信息安全、通信加密问题进行更加深入的研究，不断优化微信系统，但其必将会走上长远的发展道路，更好地服务于社会大众。

参 考 文 献

[1] 赵明 . 一种通用加密通信系统方案 [J]. 电子技术 . 2010(05).
[2] 刘栩 , 石乃轩 , 王健 , 季晓勇 . 多重加密通信系统的设计与实现 [J]. 通信技术 . 2010(05).
[3] 张月华 , 张新贺 , 刘鸿雁 . AES 算法优化及其在 ARM 上的实现 [J]. 计算机应用 . 2011(06)
[4] 瞿白 . RSA 算法参数的选择 [J]. 科技资讯 . 2010(28)
[5] 朱贤军 , 李敬兆 . 无加密模式下对云数据的隐私保密 [J]. 计算机技术与发展 . 2013(06)