

基于智能手机的 SSL VPN 虚拟通道技术在传染病疫情网络直报工作中的应用

党李成 许璐 朱国辉

(河南省疾病预防控制中心疫情信息管理中心 郑州 450000)

〔摘要〕 介绍智能手机的定义、运行的移动通信网络及安全隐患、SSL VPN 定义和优点, 结合 SSL VPN 技术和远程连接技术, 阐述 SSL VPN 技术在传染病疫情信息网络直报工作中的应用, 分析工作原理及具体操作流程, 实现智能手机端安全登录中国疾病预防控制中心信息系统, 完成正常的业务数据处理。

〔关键词〕 智能手机; SSL VPN; 传染病网络直报

〔中图分类号〕 R-056 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673-6036.2017.05.006

Application of the Smart Phone Based SSL VPN Virtual Channel Technology in the Direct Network Report of Epidemic Situation of Infectious Diseases DANG Li-cheng, XU Lu, ZHU Guo-hui, Epidemic Information Management Center of Henan Center for Disease Control and Prevention, Zhengzhou 450000, China

〔Abstract〕 The paper introduces the definition of smart phone, operating mobile communication network and hidden danger about safety, and definition and advantages of SSL VPN, states the application of SSL VPN technology in the direct network report of epidemic situation information of infectious diseases combining with SSL VPN technology and remote connection, analyzes the work principle and specific operation process, achieves safety login to the China Information System for Disease Prevention and Control with smart phones, and completes normal business data processing.

〔Keywords〕 Smart phone; SSL VPN; Infectious diseases network report

1 引言

随着移动通信技术的不断发展, 智能手机的应用范围越来越广泛, 不但扮演着移动支付、购物消费等生活角色, 而且也开始作为办公工具来使用。在疾病预防控制领域, 尤其是当遇到突发疫情、发生自然灾害等突发应急情况时, 智能手机由于其携带方便、通信快捷, 疾控工作人员不仅可以现场处

置疫情, 而且还可以借助智能手机完成传染病疫情信息网络直报等工作, 使得疫情信息以最快的速度传达到国家各级管理层面, 这一点在疾控工作中具有重要的意义。但是由于有些传染病所涉及的疫情信息事关社会公共利益和个人隐私, 需要保持高度的安全性, 在这种情况下, 如何保障智能手机成为安全可靠的传染病疫情网络直报工具就成为了一个需要思考的问题。

本文以传染病疫情网络直报工作为例, 尝试将 SSL (Security Socket Layer) VPN (Virtual Private Network) 技术应用于智能手机上, 既保证对传染病疫情信息数据及时处理, 又保障信息数据安全性。

〔收稿日期〕 2016-05-05

〔作者简介〕 党李成, 硕士, 助理工程师。

2 智能手机概述

2.1 定义

智能手机是指像个人电脑一样,具有独立的操作系统,独立的运行空间,可以由用户自行安装软件、游戏、导航等第 3 方服务商提供的程序,通过移动通信网络来实现无线网络接入手机类型的总称。

2.2 移动通信网络

本文所涉及的移动通信网络是近年来比较流行的一种无线网络接入方式,也是智能手机进入公共网络主要的接入方式,借助移动智能设备上的通信接口发送和接收移动通信基站和通信卫星传递过来的信号,从而接入公共 Internet 网络。当前应用范围比较广的移动通信网络主要有 GSM (Global System for Mobile Communication)、3G (3rd - Generation) 和 4G (the 4th Generation Mobile Communication) 等制式^[1]。

2.3 安全隐患

2.3.1 智能手机自身的安全隐患 (1) 手机木马病毒软件危害。目前我国手机软件应用平台主要以安卓系统为主,占据国内全部移动应用的 86.4%。一些不法厂商往往借助其开源性和开放性等特点,通过伪装篡改热门游戏/软件嵌入木马病毒,执行窃取用户信息、电子文档等违法勾当^[1-3]。(2) 智能手机操作系统漏洞。虽然智能手机操作系统的安全性不断提高,但是由于其自身固有的设计弊端和底层代码缺陷还是导致不可避免地存在各种系统漏洞,一旦这些漏洞为不法分子掌握,那么智能手机的安全将受到很大威胁^[1-3]。

2.3.2 移动通信网络的安全隐患 如图 1 所示,智能手机与移动通信基站发送和接收数据都采用无线信号的方式,这种方式容易被具备安装相应设备的可疑基站利用,对数据信息的安全带来很大隐患。这种安全隐患主要体现在 3 方面:(1) 信息的泄露。可疑基站可以监听智能终端与移动通信基站之间的数据,获取双方通过无线信号传递的数据信

息。(2) 伪造数据。可疑基站通过发送虚假数据给智能手机和移动通信基站,导致智能手机和移动通信基站之间传递的数据出现错误。(3) 干扰正常的数据传递。可疑基站可以通过向智能手机和移动通信基站发送错误信息,扰乱二者之间的正常通信,导致数据无法进行正常传递。

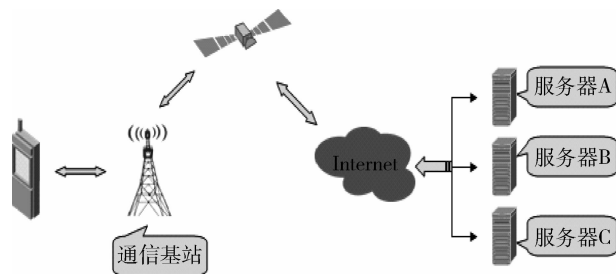


图 1 正常情况下移动通信网络数据链路

3 SSL VPN 简介

3.1 定义

SSL VPN 是一种基于 TCP/IP 协议族中的安全套接层协议的 VPN 技术,其通过强加密算法和认证机制来实现远程安全访问和异地结点安全互联^[4]。

3.2 优点

3.2.1 管理精细程度高 SSL VPN 是基于开放式系统互联 (Open System Interconnect, OSI) 7 层网络协议层中应用层的 VPN 技术,直接面向各种 Web 应用程序,对应用级别可实现精细化控制,对不同用户和不同应用程序之间可灵活地配置权限,适应于各种复杂的实际工作要求^[5]。

3.2.2 系统适用能力强 SSL 的系统适应能力体现在两方面:操作系统支持和应用环境支持。在操作系统方面,SSL VPN 采用国际标准的 TCP/IP 族协议,通用性非常好,只要是采用该协议的操作系统,不管是 Windows、Unix 的 Linux 等桌面 PC 操作系统还是 Android OS、IOS 等移动智能平台的操作系统,都能很好地兼容和支持^[6-8]。这就意味着 SSL VPN 不但可以在 PC 机上使用,而且还可以在各种智能手机上使用。在应用环境方面,SSL VPN 无须安装客户端 (在 PC 机上),就可以通过 Web 浏览器直接访问由 SSL VPN 服务器管理控制的设备

和应用程序，无须用户进行复杂设置即可上手操作，大大降低了操作难度。

3.2.2.3 安全保障能力好

SSL VPN 是一种可以虚拟访问通道的 VPN 技术, 用户通过 SSL 客户端进行的各种操作都是在虚拟的经过安全配置的环境中, 并且 SSLVPN 采用加密隧道和双因子身份认证两种技术相结合的方法, 实现了通信双方的数据安全和用户操作的不可抵赖性^[9]。另外, 由于 SSL VPN 可以针对不同应用程序进行细致的安全控制管理, 每个用户访问都只能访问经过安全配置的应用程序, 不能访问也无法影响到其他应用程序。

4 SSL VPN 技术在传染病疫情网络直报工作中的应用

4.1 应用原理

4.1.1 工作环境背景 在疫情信息网络直报工作中,基层网络直报用户和各级管理人员都需要登录中国疾病预防控制中心信息系统来完成相关工作。本文所考虑解决的问题有一个技术背景——中国疾病预防控制中心信息系统目前只支持 PC 浏览器访问和数据处理,对于手机端执行访问和处理数据有诸多不便,部分关键操作不能实现^[10]。

4.1.2 实现原理 要在智能手机端实现与 PC 端一样的效果, 本文采取远程连接技术和 SSL VPN 虚拟通道技术相结合的方式来实现^[11-12]。其实质就是在智能手机端通过 SSL VPN 手机客户端登录到 SSL VPN 防火墙, 借助 SSL VPN 防火墙连接远程连接服务器, 再通过操作远程连接服务器的网络浏览器来实现对中国疾病预防控制中心信息系统的操作, 见图 2。因为期间所有操作都是通过 SSL VPN 虚拟通道进行的, 所以可以很好地保障所有操作的安全。

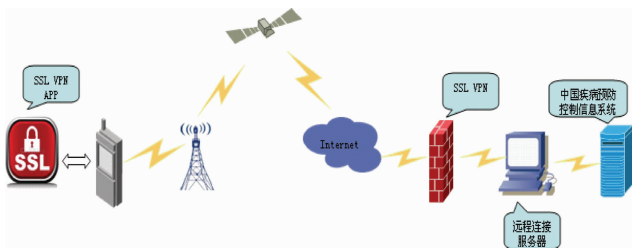


图2 SSL VPN 技术保障下的智能手机网络链接线路

注：图示中黄色闪电标识均为 SSL VPN 虚拟专用通道。

4.2 操作过程

第1步：在PC端搭建远程连接服务器，配置远程连接服务器。在远程连接服务器上安装TS终端服务，见图3。配置远程连接服务器相关设置，见图4。第2步：配置SSL VPN防火墙，见图5。第3步：在智能手机上安装VPN防火墙的APP，使用APP登录VPN防火墙，实现远程登录PC（远程连接服务器），最终实现正常访问中国疾病预防控制中心信息系统。



图3 远程连接服务器安装示意

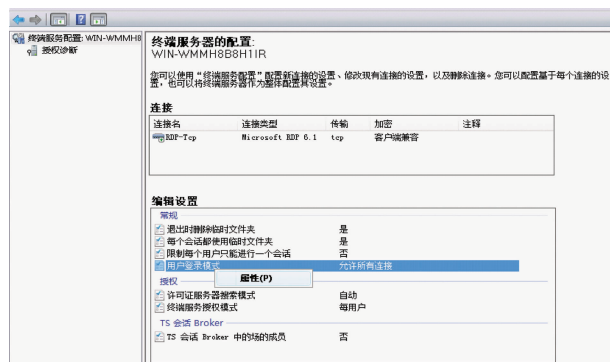


图4 远程连接服务器配置示意

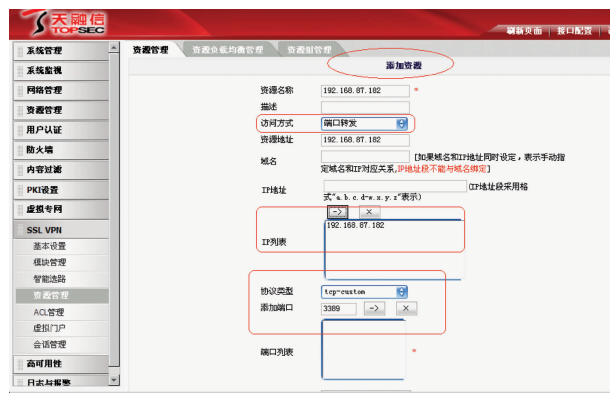


图5 SSL VPN 防火墙配置示意

4.3 智能手机端实际部署及相关操作

首先在智能手机上选择安装 SSL VPN 手机客户端 TopConnect。打开 SSL VPN 手机 APP TopConnect, 输入要登录的 SSL VPN 防火墙的用户名和密码以及验证码。登录 SSL VPN 防火墙服务器, 从 SSL VPN 服务器为该账户设置的资源列表中选择相应的应用程序, 点击相应链接进入该应用程序。

5 结语

本研究借助远程服务器和移动 SSL VPN 技术, 实现了在智能手机上对中国疾病预防控制信息系统的安全登录和安全操作, 达到了疫情网络直报工作实地核实、实时数据处理的目标。而且这种技术思路也适用于其他应用系统, 可实现使用智能手机等移动智能终端访问重要应用系统并安全操作的目的, 尤其是在突发传染病疫情应急情况下, 既保障公共卫生数据得到及时有效安全可靠的处理, 又保证公共卫生工作效率高效果好, 切实提高突发公共卫生应急响应能力。

参考文献

- 1 庞思铭, 张万涛. 移动终端安全问题探讨 [J]. 信息安全与通信保密, 2012, (11): 111-114.

- 2 党李成. 基于 Google Android 智能手机平台的研究与应用 [D]. 合肥: 安徽大学, 2010.
- 3 宋杰, 党李成, 郭振朝, 等. Android OS 手机平台的安全机制分析和应用研究 [J]. 计算机技术与发展, 2010, 20 (6): 152-155.
- 4 韩卫, 薛健, 白灵. 一种基于安全隧道技术的 SSL VPN 及其性能分析 [J]. 科学技术与工程, 2005, 5 (12): 791-796.
- 5 徐家臻, 陈莘萌. 基于 IPSec 与基于 SSL 的 VPN 的比较与分析 [J]. 计算机工程与设计, 2004, 25 (4): 586-588.
- 6 彭振宇. 基于 SSL 的虚拟专用网技术分析 [J]. 网络通讯与安全, 2007, 4 (23): 1235-1237.
- 7 龙锦远, 陆松年, 杨树堂. SSLVPN 技术研究及系统构建 [J]. 微计算机信息, 2009, (36): 103-105.
- 8 杨文凯. SSL+VPN 安全关键技术研究 [D]. 重庆: 西南交通大学, 2010.
- 9 熊蜀峰, 周本东. 基于角色的访问控制在 SSL VPN 中的应用 [J]. 计算机与数字工程, 2011, 39 (8): 105-108.
- 10 王俊玲, 姜韬, 张烨. 中国疾病预防控制信息系统安全性分析 [J]. 中国计划免疫, 2005, 11 (4): 320-321.
- 11 周亦敏, 邱立强. 嵌入式网络 SSL VPN 安全技术的研究 [J]. 微计算机信息, 2008, 24 (3-2): 47-49.
- 12 曾巧红, 徐文贤, 林绮屏. 基于 SSL VPN 的图书馆远程访问系统的构建 [J]. 情报科学, 2007, 25 (10): 1520-1524.
- 13 许波. 基于 SSL VPN 的远程访问控制平台研究 [D]. 天津: 天津理工大学, 2011.

2017 年《医学信息学杂志》征订启事

《医学信息学杂志》是国内医学信息领域创刊最早的医学信息学方面的国家级期刊。主管: 国家卫生和计划生育委员会; 主办: 中国医学科学院; 承办: 中国医学科学院医学信息研究所。中国科技核心期刊 (中国科技论文统计源期刊), RCCSE 中国核心学术期刊 (武汉大学中国科学评价研究中心, Research Center for Chinese Science Evaluation), 美国《化学文摘》、《乌利希期刊指南》及 WHO 西太区医学索引 (WPRIM) 收录, 并收录于国内 3 大数据库。主要栏目: 专论, 医学信息技术, 医学信息研究, 医学信息组织与利用, 医学信息教育, 动态等。读者对象: 医学信息领域专家学者、管理者、实践者, 高等院校相关专业的师生及广大医教研人员。

2017 年《医学信息学杂志》国内外公开发行, 每册定价: 15 元 (月刊), 全年 180 元。邮发代号: 2-664, 全国各地邮局均可订阅。也可到编辑部订购: 北京市朝阳区雅宝路 3 号 (100020) 医科院信息所《医学信息学杂志》编辑部; 电话: 010-52328673, 52328674, 52328671。

《医学信息学杂志》编辑部