无线 WIFI 安全问题及对策研究

杨丰瑞　刘孟娟

（重庆邮电大学，重庆 400065）

摘　要：随着 WIFI 技术在我国的的广泛应用和发展，用户隐私泄露、密码窃取和钓鱼 WIFI 等安全问题日益凸显。通过对家用 WIFI、企业 WIFI 和商用 WIFI 三种不同应用场景的研究，分析无线 WIFI 的安全现状并提出相应的防控措施，为政府制定无线 WIFI 网络安全监管策略提供参考。

关键词：无线 WIFI；安全问题；防控措施

中图分类号：TB　　文献标识码：A　　文章编号：1672-3198(2015)05-0174-03

1　无线 WIFI 安全现状及分析

2014 年 6 月，央视《消费主张》曝光人们日常使用的无线网络存在巨大的安全隐患，无线 WIFI 安全问题引起了极大关注。无线 WIFI 网络是一种使用 802.11 系列标准协议，将个人电脑、手持设备等终端设备以无线方式接入网的络技术。与传统固网相比，无线 WIFI

3　中职会计技能大赛对教学改革的几点建议

3.1　以竞赛内容为导向，促进教学方法、内容的改革，强化以赛促教理念

上面我们谈到的中职会计技能大赛的岗位性、实用性，应该是会计学科教学的导向，日常的教学中特别是实训教学中应该从中得到启发，例如，教师在日常课堂教学中，可以参照会计技能大赛的部分业务内容分解成项目或任务的形式进行课程设计，将企业岗位最仿真的、最实用的技能与知识点有机地融合到课程教学中。教学内容应尽可能与会计的日常岗位规范、标准和要求相对应。根据会计岗位工作要求选择教学内容，有利于学生把会计理论知识向会计技能进行转化，提升学生的学习兴趣，提高课题教学含金量。以竞赛内容为导向，促进教学方法、内容的改革，强化以赛促教的理念是中职学校教学改革的关键。

3.2　在学校经常举办形式多样的技能竞赛，形成良好的技能学习氛围

学科组可以参照国赛的形式，组织专业老师设计出多种多样的技能竞赛项目，首先在校内形成良好的技能氛围，让学生感受技能竞赛的紧张、快乐和技能学习的成就感，同时也更真实体验岗位工作的规范、标准，培养学生严谨的工作作风。竞赛组织方式内容可以多种多样，促进学生对专业学习的学习兴趣和良好的学习氛围，同时学校也可经常与兄弟学校或者是参加各级组织举办的技能大赛，通过多种竞赛不但使职业学校可以了解现代企业需要什么样的会计专业技术人才，使专业任课老师更进一步了解行业的规范、标准及中职会计人才的岗位要求，使中职会计人才培养目标定位更加清晰，培养更多符合企业需求合格的中职会计人才。

3.3　以竞赛为契机，提升教师的教科研能力

在当前职业学校技能大赛越来越受到社会各方面的关注，以赛促教、以赛促学的理念也是得到了广大职业学校的认可，特别是得到了企业单位、用人单位更加高度关注，显示了企业对中职技能实用型人才培养的期待。技能大赛作为一个很好的展示平台和信息平台，作为从事中职会计专业的教学老师应该关注会计行业对岗位的要求和行业发展信息，以竞赛为契机，例如，根据竞赛内容设计出符合中职会计学生的实训项目、实训任务，有条件的组织开发符合本校实际和会计岗位规范、标准的实用型校本教材。教师只有通过加强自身的学习，努力提高自己的教科研能力，不断地接收和改善知识结构，定期进行学习或到企业参与具体财务工作的实践，才能不断提高专业能力，积累实践经验，提升教师的教科研能力。

4　结语

中职会计技能大赛对于改变中职会计教学方法、内容以及加强教学与岗位需要贴近等方面的作用是巨大的，对于教师的教科研能力水平的提高和激发学生的学习兴趣是有很大的促进作用的，以赛促教、以赛促学正成为推动中职学校会计教学改革的强大动力，但我们也不能使技能竞赛仅仅成为某些尖子生的展现平台，不能忽视的个别中职学校只强调了出成绩，而忽略了技能大赛的本来意义，中职学校一定要将技能大赛对教学促进的意义融合到学校日常教学中，只有这样才能推动学校的会计专业教学改革朝着教学内容岗位化、规范化、职业化的方面发展，真正体现了职业技能大赛的举办意义。

参考文献

[1] 周艳艳. 论会计技能大赛对会计教学课改的作用[J]. 教书育人·高教论坛，2011，(11).

[2] 倪双琴. 利用会计技能大赛　推动会计课程改革[J]. 中国校外教育，2011，(16).

作者简介：杨丰瑞(1963－)，男，重庆人，博士，教授，硕士生导师，研究方向：通信运营管理；刘孟娟(1990－)，女，重庆邮电大学经济管理学院硕士研究生，研究方向：通信运营管理。

网络的无需布线、网络组建简单等优势极大地促进了其推广应用；而其介质特殊的穿透性和开放性，以及其安全机制本身固有的漏洞，使得无线 WIFI 网络面临着严重的安全威胁。

根据现有 WIFI 的应用范围，我们将其分为家庭、企业和商用三种不同的 WIFI 类型。而不同 WIFI 类型拥有与自身应用场景相对应的特点，所以其面对的安全威胁也不同。因此，我们将从家用 WIFI、企业 WIFI 和商用 WIFI 三个方面分析其安全现状。

1.1 家用 WIFI

伴随着具备 WIFI 功能的设备不断增多，再加上无线 WIFI 应用起来的方便性，WIFI 已悄然走入众多的家庭用户。美国市场调研公司 Strategy Analytics 早在 2006 年 5 月的调查报告《家庭网络采用 WIFI 的情况》预测，中国将成为全球 WIFI 家用市场的主要增长动力，并于 2016 年为 WIFI 贡献 1.1 亿个家庭网络用户。而无线路由器作为家用 WIFI 的一个无线 AP，其安全性影响着家用 WIFI 网络的安全。据我国 360 安全卫士发布的《2013 年第三季度家用无线路由器安全报告》显示，国内用户修改或重新设定路由器管理帐号和密码的比例还处在一个较低的水平，98.6％的家用无线路由器存在弱密码风险。

家用 WIFI 面临的安全威胁，主要来自家庭外部和家庭内部两个方面。家庭外部的安全威胁主要针对无线路由器，黑客通过 CSRF 漏洞攻击能够越过 WIFI 密码的验证，直接入侵用户路由器管理界面，对路由器 DNS、管理密码等设置进行篡改，从而实现劫持网站、插入广告、诱导用户进入钓鱼网站以及屏蔽安全软件的升级、云安全查询等目的。同时，黑客 CSRF 攻击手法已经升级，可直接修改用户路由器默认的管理端口。而来自家庭内部的安全，主要涉及 WIFI 密码和路由器管理密码问题。WIFI 密码结构单一、破解难度系数低以及密码更新周期长是导致 WIFI 密码存在安全问题的主要原因。

1.2 企业 WIFI

随着 WIFI 技术的广泛应用，越来越多的企业组建了基于 WIFI 接入的 Intranet 企业网，分享无线网络给企业生产、管理及营销带来的极大便利。目前国内使用 WIFI 的企业非常普遍，有的甚至已经取消传统有线网络，完全依靠 WIFI 进行办公。然而，大部分企业缺乏有效的 WIFI 管理措施，尤其是 2013 年曝光的“棱镜门计划”披露了美国 NSA 窃听企业高层的信息，无线 WIFI 安全问题更是引起了企业的广泛关注。

来自企业 WIFI 的安全问题主要分为以下四方面：一是 WIFI 网络信号容易被搜索发现，这为非法用户接入 WIFI 网络创造了基本条件，WIFI 接入点设备的广播信息中携带了许多可以用来推断 WEP 密钥的明文信息如 WIFI 网络的名称、SSID 号等，这些信息为非法用户入侵 WIFI 网络创造了必要条件；二是非法用户伪装成合法的 WIFI 网络用户或者网络地址，欺骗 WIFI 网络的认证机制入侵网络，从而达到非法访问网络资源的目的；三是拒绝服务攻击（DOS），该攻击通过产生大量的数据包，耗尽网络资源，使网络无法响应合法用户的请求，导致网络瘫痪；四是通过客户端接入非法 AP 来窃取客户端的信息。当攻击者得知企业网络的 SSID，则可使客户端错误关联到非法 AP 上，通过攻击客户端来窃取企业数据。

1.3 商用 WIFI

商用 WIFI 即商用宽带无线网络，常用于咖啡、餐厅等免费为用户提供宽带无线网络的公共场所。与家用和企业 WIFI 相比，商用 WIFI 起步相对较晚。但随着移动互联网产业的发展，商用 WIFI 得到了咖啡厅、餐厅等商业场所的喜爱。不过其人流量大、需求多种多样的特点也为其带来安全隐患，可能引发严重后果。

商用 WIFI 安全问题主要体现在以下三方面。一是商用 WIFI 缺乏相应的规范标准。当前的公共场所无线网络环境，我国除对经营性场所类的网吧实行实名制外，其余公共场所无线网络的管理措施还停留在备案制层面，所以亟待建立一个标准规范的服务保障体系。二是钓鱼 WIFI 盛行。公安部第一研究所专家苏智睿曾指出，无线 WIFI 将常规有线网络中的物理线路变成逻辑上的虚拟链路（无线电波）来传输数据，这种安全性上的“先天缺陷”，促生了钓鱼 WIFI。恶意用户通过开启与商业 WIFI 热点一致的 SSID，骗取无线用户接入，窃取用户个人信息、网银、支付宝密码等，给商业 WIFI 带来极大安全威胁。三是大功率无线网卡威胁商业 WIFI 安全。“大功率无线网卡”俗称“蹭网卡”，通过破解密码，强行共享他人无线网络，增加了商业 WIFI 网络负担，拖慢网速，造成稳定性差。更严重的是，通过截获无线数据，还可以分析出商业 WIFI 用户的网银、邮件等重要数据，给商用 WIFI 用户带来直接的财产损失。

2 无线 WIFI 安全对策建议

鉴于无线 WIFI 广泛运用，而其安全性可能引发的严重后果，因此，本文根据无线 WIFI 应用范围，针对家用、企业和商用三种 WIFI 不同特点给出了安全对策建议，从而在一定程度上保障无线 WIFI 的安全，保证无线 WIFI 消费者合法利益。

2.1 加强家用 WIFI 路由器密码设置，提高用户安全意识

第一，对于用户来说，加强路由器密码复杂程度，选择 WPA2 加密认证方式设置密码，且密码长度至少在 10 位以上，包含字母、数字和特殊符号。同时，将路由器管理的默认 IP 地址修改为自己设定的特殊 IP 地址，降低 CSRF 等自动攻击的成功率。最后，开启路由器 MAC 地址过滤功能，只允许已知的设备接入路由器。

第二，对路由器厂商来说，在路由器设计中增加密码修改提醒或强制修改管理密码。即对没有修改过管理帐号和密码的用户，在其每次登录路由器时，给予风险提示，甚至强制要求用户设定新的管理帐号和密码。

第三，加大 WIFI 安全宣传力度，提高用户安全意识。一方面，监管机构可对公共场所 WIFI 进行安全性

认证，并进行标识。同时，要求无线 WIFI 网络服务提供商提供该 WIFI 安全等级提示，从而用户可以选择性的连接，避免接入不安全 WIFI 网络。另一方面，对 WIFI 用户进行 WIFI 安全使用宣传。根据网络安全技术和组网经验，向无线 WIFI 用户普及无线 WIFI 网络安全知识。

2.2 规范企业 WIFI 网络建设，建立安全应急机制

第一，规划企业 WIFI 网络设计，建立安全应急机制。监管部门应要求企业规划 WIFI 网络设计，考虑网络的整体安全，对网络用途、密级进行认证。需将网络安全纳入网络的规划设计中，采取系统和整体策略来实现 WIFI 网络的安全。其次，鼓励企业建立安全应急机制，当非法用户接入企业内部网络时，启动安全机制，自动切断其连接。最后，企业对员工实施安全密码和身份验证管理。

第二，隐蔽 SSID 广播信息。SSID(Service Set Identifier)服务集标识用来标识不同无线网络的名称，是网络站点找到指定无线网络的重要信息。通过关闭服务访问点 AP 对外的 SSID 广播信息，使非法用户无法进行入网连接，合法用户则采用企业网管事先分配的网络 ID 安全接入本无线网络。

第三，过滤网络接入站点的 MAC 地址与 IP 地址。无线接入站点的 MAC 地址是入网认证的重要依据，在访问接入点 AP 上设置 MAC 地址过滤策略可以有效防止非法用户的入侵，这对企业中一般使用相对固定的网络站点是非常有用的一种安全措施。

第四，入侵检测与访问控制。在无线网络中使用无线网络入侵检测设备，一旦在网络中检测到任何未授权的设备，如流氓接入点，就发出报警。同时，通过 AAA 服务器对连接到无线网络用户的访问进行控制，通过这一主动防御措施，加强无线网络的安全性。

第五，启用 WPA/WPA2 加密功能。WPA/WPA2 数据加密技术是 IEEE 802.11n 协议中最基本的无线网络安全策略，是提高企业 WIFI 网络信息安全的基本方法。具体如下：(1)在网络传输的每帧数据中插入帧校验和来检验数据的完整性，防止非法用户在数据流中插入已知文本来试图破解 WPA/WPA2 加密的密钥；(2)确保每个无线站点和无线访问接入点 AP 上都同时启用 WPA/WPA2 功能；(3)不使用常见的 WPA/WPA2 密钥，特别是缺省设置；(4)WPA/WPA2 密钥由用户来设定并能够经常更改；(5)使用高的 WPA2 版本并不断升级更新。

2.3 规范商用 WIFI 建设，保障用户信息安全

第一，完善商用 WIFI 规范标准，建立服务保障体系。公共商用场所的无线宽带网络作为工业和信息化部提出的“宽带普及提速工程”的重要组成部分，其重要性不言而喻。鉴于商用 WIFI 在应用方面的特点以及现行市场的不完善，政府、业务单位和服务商应共同努力，促进商用 WIFI 服务体系的建立。政府方面，从宏观方面着手，加强对如何建设健康、安全的商用 WIFI 应用生态环境的研究，保证公共商业场所宽带无线上网服务的质量、稳定性和安全性，推动中国商用 WIFI 应用的创新和服务标准的规范。加强业务单位和服务商方两者合作，解决好商用宽带无线网络的安全性、稳定性、登陆速度等问题，破解公共无线网络用户体验和服务质量差等困局，建设健全商用宽带无线网络的服务规范和服务标准。

第二，提高辨别意识，抵制钓鱼 WIFI 陷阱。一方面，用户应加强终端设备设置，关闭自动连接 WIFI 功能；同时，应谨慎对待公共场合的 WIFI 无线网络，尽量避免使用来源不明的免费 WIFI。另一方面，用户应及时更新、升级浏览器。浏览器作为最容易泄露用户信息的软件，用户可通过从官方网站进行下载和安装浏览器、养成定时更新升级的良好习惯。

第三，从源头着手，有效遏制大功率无线网卡流通渠道。大功率无线网卡主要针对本身没有对无线路由器进行加密的上网资源以及使用 WEP 简单加密方式对无线路由器进行加密的商用 WIFI。虽然目前对此类行为没有作出明确的法律规定，但是这无疑对合法拥有商用 WIFI 的用户造成了安全威胁。所以，可以通过与相关无线网络监管部门合作，限制大功率无线网卡的生产制造，规范其正常用途。同时，从商用 WIFI 用户自身来避免大功率无线网卡的安全威胁也是一种有效途径。用户通过隐藏无线路由器 SSID5 使无线路由器对其他设备不可见，再辅以 WPA2 对无线路由器进行加密可以降低被搜索到的可能性。

3 结语

本文创造性的从家用 WIFI、企业 WIFI 和商用 WIFI 三个角度分析了其安全现状，从而很好的解决了现有文章对 WIFI 安全问题一概而论的问题，使原本界限模糊的 WIFI 安全问题变得清晰、明朗。同时，针对性地对不同应用场景的 WIFI 提出安全对策建议，对于家用 WIFI，从路由器密码设置和用户安全意识着手，有效保护路由器安全；对于安全性高要求更高的企业 WIFI，从专业技术和整体设计的角度出发，保障企业 WIFI 安全；而对于发展迅速的商业 WIFI，除提高用户辨别钓鱼 WIFI 之外，政府部门的有效监管才能从根本上保障无线 WIFI 消费者的合法利益。

参考文献

[1] 牛钢. WIFI 技术在实际建设运行中的应用和研究[D]. 北京：北京邮电大学，2012.

[2] 杨哲. 城市无线网络安全技术与威胁浅析[J]. 信息安全与技术，2011，(25)：22-24.

[3] 彭海深. 基于 WIFI 的企业网信息安全研究[J]. 科技通报，2012，28(8)：145-147.

[4] 孙无极. WIFI 接入对园区网络构成安全隐患极其对策[J]. 实践与经验，2010，(7)：116-118.

[5] 360 互联网安全中心. 2013 年第三季度家用无线路由器安全报告[R]. 北京：360 互联网安全中心，2013：2-5.