WAPI 产业联盟

每周新闻综述

WAPI 产业联盟秘书处　　主 办

2009 年 9 月 11 日　　内部资料

【产业要闻】

- 发改委颁布《电子信息产业技术进步和技术改造投资方向》 WAPI 赫列其中
- 诺基亚 5800iXM 支持 WAPI
- 索尼爱立信 1200 万像素机 Satio 将支持 WAPI
- 200 元蹭网卡能破解数百米无线网络
- 安全专家：一分钟内便可干掉 Wi-Fi 的 WPA 加密系统
- 李进良：建议规范无线城市 采用 TD+WAPI 自主技术

【行业视点】

- 诡异的无线世界：Wi-Fi 背后的几宗罪
- 警惕“蹭网族”偷网速更偷隐私
- 法制日报：蹭网属民事侵权 严重者涉嫌盗窃罪
- 信调查显示：80%以上用户支持国产标准 WAPI

【产业要闻】

发改委颁布《电子信息产业技术进步和技术改造投资方向》WAPI 赫列其中

源自:《中国证券报》·中证网

2009 年 9 月 3 日在国家发改委高技术产业司网站上（gjss.ndrc.gov.cn）正式发布了《电子信息产业技术进步和技术改造投资方向》， 在《电子信息产业技术进步和技术改造投资方向》中第五大项的“计算机产业及下一代互联网”类别中的数字化 3C 产品条目，WAPI 赫列其中，体现了国家相关领导部门对于我国自主创新的 WAPI 产业的重视与坚定支持。

诺基亚 5800iXM 支持 WAPI

源自：IT168

作为诺基亚 5800XM 的升级版，诺基亚 5800iXM 增加了对 WCDMA/HSDPA 网络的支持，并提供了对国产标准 WAPI 的支持，使得该机成为了继诺基亚 5530XM 之后又一款在国内问世诺基亚 WAPI 手机。

索尼爱立信 1200 万像素机 Satio 将支持 WAPI

源自：网易手机

虽然目前索尼爱立信 Satio 的具体上市时间以及售价我们还不清楚，但是目前能够肯定的是，1200 万像素的 Satio 将会分两批上市。其中第一批的 Satio 并不支持无线局域网络，而第二批 Satio 将会支持 WAPI 标准，相信会很好地兼容 WLAN 上网。

200元蹭网卡能破解数百米Wi-Fi网络

源自：《劳动报》

“蹭网族”最近网上走红，他们利用专业蹭网工具破译密码，就能免费享受高速上网，而且被蹭网者很难察觉。蹭网工具也一下子热卖起来，在一些IT卖场，用户花200元左右买个“卡王”就能破解周围数百米无线网络。不少电脑高手在网上广发帖子传授破解之策，对付蹭网族。

安全专家：一分钟内便可干掉Wi-Fi的WPA加密系统

源自：网界网

日本的两位安全专家称，他们已研发出一种可以在一分钟内利用无线路由器攻破WPA加密系统的办法。

这种攻击为黑客提供了扫描电脑和使用WPA(Wi-Fi保护接入)加密系统的路由器之间加密流量的方法。这种攻击是由日本广岛大学的Toshihiro Ohigashi和神户大学的Masakatu Morii两位学者开发的，他们准备在9月25日在广岛召开的一次技术会议上对此攻击做更详尽的讨论。

企业级Wi-Fi网络一般都会有安全软件来探测日本学者所描述的中间人攻击，Errata安全公司的CEO Robert Graham说。但是日本学者这一次所开发的针对WPA的真正切实可行的攻击有可能会让企业有理由彻底抛弃TKIP算法的WPA系统。Graham说：“WPA虽然不像WEP那么糟糕，但也可算是半斤八两吧。”

李进良：建议规范无线城市 采用 TD+WAPI 自主技术

源自：C114

鉴于无线局域网终端产品涉及千家万户，并被集成到几乎所有的办公、家庭和个人手持信息设备中，Wi-Fi 客观存在引发个人、企业、社会和国家安全等严重隐患，其影响远超过短信诈骗造成的危害。

同时鉴于 WAPI 产业经过五年的卧薪尝胆，艰苦奋斗，已经形成包括标准、芯片、终端、网络设备、增值服务、运营商、检测机构在内的完整产业链，其产品已成功走进 2008 北京奥运会，以其安全、稳定、高速的特点成为“科技奥运”新亮点。近期，工信部制订了《移动用户终端无线局域网技术指标和测试方法》的行标，预示着具有 WAPI 功能的移动终端将获准入网。这一切进展表明 WAPI 现在是到了终止延期、强制实施的时候了。

鉴于“无线城市”是各地政府管理该市的应用网络，必须高度重视网络信息安全；建设“无线城市”又是各地的政府行为，必须贯彻政府优先采购国产设备的规定，借以扩大内需；建议工信部发布《无线城市指导性意见》，坚决摒弃 WiMAX+Wi-Fi 的不安全技术路线，不采用 2G/3G+WLAN 的模糊技术路线；明确采用 TD-SCDMA+WAPI 的自主创新技术路线。在全城无线城域网和广域网采用可与宽带 ADSL 相匹敌的 TD-HSDPA；在热点无线局域网采用既安全、又可运营可管理的 WAPI；并相应开发 TD+WAPI 的手机与数据卡，不允许 Wi-Fi 手机与数据卡入网，这符合国家自主创新的战略与强制性国家标准的规定。特别是 TD 与 WAPI 基于自主知识产权开发的芯片、终端和系统，国家的安全更有保证。对目前已经在网、但不符合 WAPI 标准的设备，应限期完成升级支持 WAPI。所有无线城市群的网络建设必须遵循国家采购法优先采购符合 TD 与 WAPI 国家标准的国产设备，这样就可以大大拉动内需，拉动消费，减缓全球金融海啸对我国所带来的负面影响。衷心希望全国各个城市都能自觉贯彻 TD+WAPI 的无线城市建设标准，让 3G 业务走进寻常百姓家。

【行业视点】

诡异的无线世界：Wi-Fi 背后的几宗罪

源自：51CTO

今天这篇文章的重点是帮助你更好的使用 WLAN，即使这意味着要减少使用 Wi-Fi。

我可以原谅你认为最新的 802.11n 标准已经是 Wi-Fi 的官方标准，但事实是他确实还不是，有许多无线设备厂商也已经厌倦了像 802.11n 这样工作小组，他们各自建立了自己的“标准草案”，并强迫不同的厂商上一起等待“标准的标准”。

其实现在的 Wi-Fi 标准都还是靠不住的。让我们从 Wi-Fi 标准历史来看：首先是 802.11，随后的 802.11a，然后 802.11g 的，和年后即将推出 802.11n 标准。而这一系列标准都只能证明无线委员会成员的愚昧和无知。（我们这里将不会提到属于 802.16 家族的 WiMAX 技术，因为我们在这里只讨论你的室内无线，不涉及长距离的 WLAN 技术。）

在这里我提出的第一个使用 WLAN 指导方针就是：那些小企业如果能够避免使用 Wi-Fi 技术则应当尽量避免使用。原因就是 Wi-Fi 的安全性存在严重漏洞。

我的第二个使用 WLAN 指导方针是，最好使用同一厂商的无线设备，以获得较好的 WLAN 功能。

第三，如果你的 Wi-Fi 信号在建筑外也可以侦测到，这就使黑客更加容易攻击。

最后，必须确定在您规划 Wi-Fi 网络时你就要考虑您要采取安全措施，而不是在完成规划后再回头考虑。这是因为 Wi-Fi 网络要求更严格的内部安全计划，即使你计划在路由器上安装一个注重保护的强大防火墙，这也并不能够阻止那些网络入侵者，他们通过那些穿过墙壁的信号而进入你的内部网络。而作为您的无线网络的主要部分，个人电脑的保护必须是有强制性要求的。

您的客户访问无线网络时进行身份验证方式也可能使您的网络安全遭到破坏。无线接入点广播 SSID(服务集标识符)使用户更容易找到你的网络的同时也邀请外界尝试连接到您的网络。这里建议您配置的无线客户端为自动连接到您的网络，最好不用广播您的 SSID。

目前，Wi-Fi 安全性已经被人所怀疑，特别是上周，日本的研究人员花了不到一分钟就入侵了一个加密 WPA(无线保护接入)，Wi-Fi 的安全性更是被人所诟病。

警惕 Wi-Fi“蹭网族”偷网速更偷隐私

源自：光明网

对于被“蹭网”的 Wi-Fi 网民来说，最大的感受就是自家网速突然变慢。如果遭到“蹭网者”电脑的 ARP 攻击，甚至连登录 QQ 或打开网页都会很困难。360 安全专家提醒说，近期 360 安全卫士监测到用户遭受的局域网 ARP 攻击的数量明显增多。而根据这些受攻击用户在论坛上的反馈，许多用户都在使用无线宽带网。

“无论是蹭别人的无线网络，还是被蹭的，很多人都没意识到，无线宽带网其实也是局域网的一种，无线网内的 ARP 攻击照样能轻松截取 MSN 聊天记录和电子邮件等隐私信息，而且会像甲型流感一样快速传播木马病毒。”360 安全专家介绍说，“因此，使用无线宽带网络的用户也必须开启 ARP 防火墙来保护自己的电脑。”

网友“非主流星”的遭遇便说明了蹭网的危害，他在一家专业安全论坛中抱怨说：“不知道是哪个不厚道的邻居接进了家里的无线网络，不停地 ARP 攻击我的电脑，害得我一打开网页就中了木马！” 对此，360 安全专家解释说，犇牛、机器狗、AV 终结者等恶性木马下载器大多具有 ARP 攻击的功能，可以把插入恶意代码的网络数据传输给无线网内其它电脑，让这些电脑访问任意网页都会下载由黑客指定的木马病毒。

“蹭网族”本来蹭的只是免费上网的小便宜，但如果发动 ARP 攻击来盗取邻居隐私，或传播木马来偷窃网游网银的账号，就成了网上犯罪；而如果被蹭者本

身是一名黑客，也完全有可能故意开放一个无线网络并设下陷阱，反咬“蹭网族”一口。如此看来，Wi-Fi 网络反而成为诱发网络犯罪的沃土。

蹭网属民事侵权 严重者涉嫌盗窃罪

源自:《法制日报》

河南振山律师事务所主任秦三宽律师认为，网络用户都与运营商签订了合同,享有专用权。“蹭网者”盗用正常用户已经付费购买的网络资源的数据流量，造成对方网速减慢或财产受损，属民事侵权。

秦三宽律师还认为，一些商家明知该产品具有违法性质，仍违规出售，应承担连带侵权赔偿责任。工商等市场监管部门应依法予以打击。

也有律师认为，如果“蹭网者”给用户造成的损失超过一定数额，还涉嫌盗窃罪。另外，“蹭网者”的行为扰乱了电信市场秩序，涉嫌侵犯了网络运营商的合法利益，公安机关可据此追究其相应的法律责任。

我国的电信条例规定，“盗接他人电信线路，复制他人电信码号，使用明知是盗接、复制的电信设施或者码号……属于扰乱电信市场秩序的行为，任何组织或者个人不得有这种行为。即便是“蹭网者”交流经验的网络平台——中国无线论坛，也已经发出一份“重要申明”：“我们不鼓励也不支持利用无线安全技术进行的‘蹭网’行为，更不支持利用无线技术入侵别人的电脑，以及各种破坏及违法行为。”

具有讽刺意味的是，在这份“郑重申明”下面，连篇累牍的“蹭网秘笈”、“简明蹭网指南”、“10 分钟破解无线路由器密码步骤”、“秀秀我的蹭网设备”等帖子早已浩如烟海。一些“资深”的“蹭网专业户”不断活跃在论坛当中，交流蹭网心得，传授蹭网方法。

民权律师事务所律师周彦峰认为，如今我国自主知识产权的无线网络协议 WAPI 已于今年 6 月获得国际认可，无线网络势必会作为一种新技术得以广泛应用。对于“蹭网”这种侵犯他人利益的举动，国家有必要在行业法律的层面加以明确。

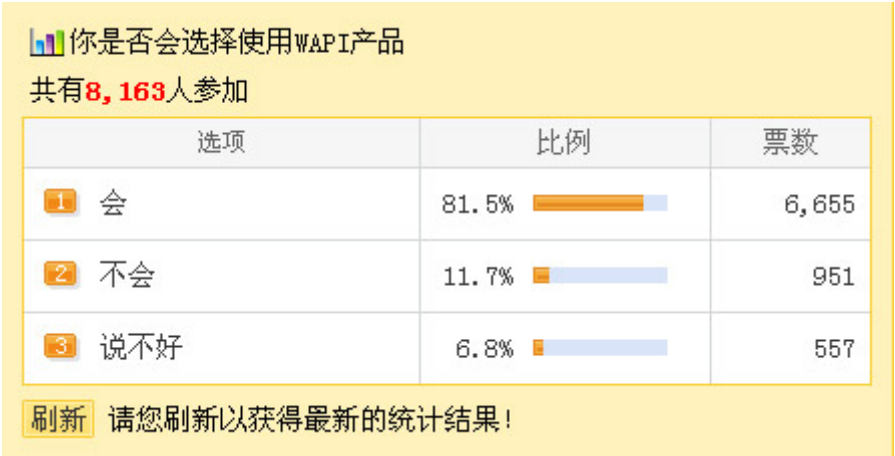
刘淑惠认为，公安机关无权处理民事侵权，但“蹭网者”给用户造成的损失数额如何认定，证据如何固定，是否构成盗窃罪，还有较大争议，目前还难以追究“蹭网者”的法律责任。

由于 Wi-Fi 安全所引发的问题日趋严重，不仅仅对于个人家庭用户造成了伤害，对各大企业的商业机密也构成了严重的威胁，甚至还为犯罪分子创造了便利途径。印度内政部已发布了禁令，禁止在敏感部门使用 Wi-Fi 技术上网，澳大利亚昆士兰州组成了世界上第一支警备力量，防范犯罪分子利用不安全的无线网络进行犯罪活动，美政府勒令互联网服务供应商保留 Wi-Fi 记录至少两年，以协助警方进行调查，英国卫生防护局主席、前政府首席科学顾问斯图尔特呼吁对 Wi-Fi 技术可能造成的负面影响进行“及时”调查，欧美国家往往法律森严，蹭网被拘捕的案例已经屡见不鲜，目前新加坡也明确界定“蹭网”属犯罪。

调查显示：80%以上用户支持国产标准 WAPI

源自：51cto

6 月 17 日，针对国产标准 WAPI 与西方标准 Wi-Fi 之间的博弈，在国内某知名网站所做的调查中，有超过 80%的被调查者支持使用 WAPI。



80%以上被调查用户支持国产标准 WAPI

截止 6 月 17 日凌晨 0 时，在该网站所做主题为“你是否会选择使用 WAPI 产品”的调查中，7168 名被调查者中，总共有 5845 人表示会使用，也就是说 81.5%

的被调查者支持使用 WAPI。11.7%的被调查者表示不会使用;6.8%的被调查者表示不好说。

采用 802.11i 技术 Wi-Fi 安全漏洞太大。自 2008 年下半年起，包括我国电信运营投资、“无线城市”等公共无线网络基础建设均已进入规模启动期，这些基础的公共无线网络设施未来将承载我国绝大多数的宽带无线互联网用户，如果这些大规模建设项目现在不重视无线网络安全问题，而是按照早期惯性采用“开放模式”，或是使用已被证明有严重安全缺陷的 802.11i 技术，将为用户和基础无线设施埋下巨大安全隐患。

业内专家指出，有关公共基础网络设施的无线安全问题，已很难简单的区分为个人安全、商务安全或是国家安全，即便有区分也是相对而不是绝对的，几者内在联系是非常紧密的；另一方面，无线局域网网络和终端产品涉及千家万户，并被集成到几乎所有的办公、家庭和手持信息设备中，所可能引发和带来的已不仅仅是信息安全问题，导致的将是不断产生个人、企业和电信运营网络安全问题，客观存在引发社会和国家安全等严重隐患，其影响也远超过短信假冒诈骗等对社会造成的危害。

业内笑称，网上可随处下载的“Wi-Fi 破解工具”使得很多普通人跃跃欲试。

WAPI 产业联盟

（中国计算机行业协会无线网络和网络安全接入技术专业委员会）

地址：北京海淀区知春路 27 号量子芯座 1702 室
邮编：100191
电话：010-82357754
传真：010-82357730 ext.807
邮箱：wapia@wapia.org
网站：http://www.wapia.org