 近几个月来，假冒URL地址窃取用户密码的现象愈演愈烈。据反钓鱼组织统计，今年四月份全球共出现该类案件2683起，五月份2100起，而去年五月仅发生同类案件495起，与去年同期相比，攻击数量增长了近五倍。在国内各种通过网络开展的犯罪活动日益频繁，例如建立虚假网站诱骗消费者购物，假冒邮局骗取邮资等，不过最频繁出现的还是假冒网上银行。所有的现象都说明在网上可利用的信息价值越来越大的同时，网络犯罪也正逐步向我们逼近。整个电子商务面对着信任危机，一起起安全事件的爆发，正不断考验着消费者的信心。 如今，CIO们也在考虑如何让消费者得到安全可靠的网上交易环境。防范假冒网站是所有电子商务人都必须面对的一个问题，因此钓鱼网站不会局限于一个地区和国家。从安全技术发展和现实应用上分析，服务器证书技术的应用范围还是比较广泛的。从来自全球服务器证书的顶级提供商VeriSign的数据显示，在全球500强企业中有93%的企业以及全球电子商务50强中94%的企应用该服务，其全球累计颁发的服务器证书超过45万张。作为一种事前防范手段，每张服务器证书都具有一个与网站地址相对应的网站，证书所有者可以借此对外表明自己网站的真实可靠性，相当于出示一个“ 网络身份证 ”，同时该技术还可以对信息传输通路进行加密，确保重要信息安全。 服务器证书以信任链作为纽带，将全球可信站点联系在一起，构建安全的网络环境。整个信任链的建立是由安全服务厂商

和各浏览器厂商等合作商共同完成的。第三方安全技术厂商通过严格的安全措施和有效的鉴证方法保证发放资格证书真实准确，而浏览器厂商会对认证机构的信誉进行评价，只有符合要求的安全服务商才进入能他们的信任链。 以IE6.0版本为例，上网者可以通过几种方式进行查看。第一、网站地址是否为“ https:// ”；第二，网页右下角是否有金色安全小锁标志；第三，网站是否有VeriSign等国际知名机构的签章标志，只要三者有其一，网民就可以放心向其提交资料了。然而，由于钓鱼网站所引发的安全事件不断上升，最新版本IE7.0中服务器证书技术得到了进一步加强，地址栏会通过颜色变化将它们予以区分：地址栏呈现红色为钓鱼网站，绿色的是受信站点，黄色的是可疑网站。 就个人安全意识看，国外网民普遍对于个人信息保护具有很高的安全意识。通常他们会向配置了“ 网站身份证 ”的网站提交信息，而对于一些无法确认身份的网站，他们会比较谨慎。相对于国外网民，国内网民很少知道服务器证书对于个人信息安全的作用，在假冒网站面前仍感迷茫，众多国内网民仍停留在通过杀病毒软件等事后防范措施支撑着自己脆弱的安全防线。安全知识的匮乏，使得网民遭受钓鱼网站侵害事件不断出现。 在网站经营者方面，他们把更多的精力投入到探索如何打造一个全新服务模式，从而吸引和留住客户，而相对忽视了网站的信誉建设。目前，服务器证书应用领域主要集中在金融站点、大型网上交易网站等。网站运营者对于“ 网络身份证 ”这种信任服务了解度仍然不高，缺少安全技术手段保护网站的客户信息，很少通过宣传提供鉴别钓鱼网站的知识，网民的安全感不足，最终导致客户缺少对于网站的信任，整个网络信任环

境极为脆弱。一些商务网站将服务器证书技术与个人数字证书技术两方面特性进行结合，推出了更为灵活的服务：网站通过向高端会员颁发个人数字证书，从而实现网站与客户的双向识别，持有个人证书的客户可以享受到更为全面快捷的服务。而数字证书技术作为可靠的电子签名技术，也为未来高端电子商务的发展打下了基础。