 引言：企业做身份认证，除了用户名和密码之外，现在有了很多新的方法。 不久前，在强认证产品市场上进行选择还是像在“ 可口可乐 ”和“ 百事可乐 ”之间进行选择，各个产品都没有本质区别。只有不太多的几个选择，比如，非常流行的RSA的安全令牌SecurID、Axalto和Gemplus等公司生产的支持芯片的智能卡。 智能卡和令牌仍旧是很多公司竞争的项目，预计2007年将是智能卡行业的一个丰收年。而在这些表象的背后，用户认证技术这一曾经沉寂的市场上，却正在发生着许多变化。 为什么呢？首先，有目的的网络钓鱼攻击技术使得欺骗者能够非常容易地得到他们所需的用户信息，来渗透像在线银行和电子商务网站这样的敏感系统，更不用说企业的应用程序了。第二，Wi-Fi使得在防火墙后侵入企业网络成为可能，并发展成隐藏技术，使得发现恶意代码非常困难。第三，PKI解决方案非常贵！在任何情况下，企业网和企业信息方面完全免费的东西刺激了这个行业的快速发展，新起了一批公司，解决身份认证这个老问题。以下是几个需要关注的趋势： 一、生物测定（Biometrics） 十几年来，生物测定方法一直是“ 下一件大事 ”，最近，很多因素促使企业开始采用这种方法。像联想这样的大的PC制造商，在自己的设备中都有集成的生物测定扫描器，其中支持USB的扫描器更便宜一些。新一代的行为生物测定也开始做了。金融风险管理厂商Fair Isaac最近发布了一款新品，Falcon One，可以在线使用监测用户的行为

，比如击键、鼠标模式等。不久后就将成为存储巨擘EMC的一部分的RSA公司，在4月份收购了声音识别技术厂商PassMark Security。另一家行为生物测定厂商，BioPassword，声称其击键分析技术可以识别出骗子，甚至在他们已经偷了你的用户名和密码之后都可以。 二、多形态因子（More form factors） 强认证解决方案的一个最大的挑战就是购买和部署附加因子的费用。密钥被盗、智能卡丢失会损毁。对于怎样管理不同公司众多的令牌，厂商从来都没有好的解决方法。最近几年，Diversinet、RSA、Saflink和VeriSign都开发了可以通过无线方式把令牌发送到手机或PDS的技术。 三、基于风险的认证（Risk-based authentication） 每个人都想加强访问控制，但并不是每位用户或每个处理过程都足够强，可以达到双因子认证。结果是：企业采取一种更细的方法认证，把强的安全措施应用于高风险、高价值的处理过程，把轻度的安全防护应用于低风险行为。除了RSA和VeriSign，像Entrust和TriCipher这样的小一些的公司提供这样的解决方案，把对强的双因子认证的支持和像挑战/响应这样的软认证方法结合起来，从软件和硬件两方面，分析欺骗信息。 四、名誉服务（Reputation services） 随着隐藏技术（rootkits）、下载驱动及其它盗窃技术的快速繁殖，拥有正确的登录证书就和以前的要求不一样了。公司也想监测在线行为，来开发个人文档，分析该用户是谁，他将要做什么，从而预防出现关键的安全失误，即便在用户认证已经通过后也要万分小心。像cydelity、Cyverllance、Iden Trust、RSA和VeriSign这些公司，都在把反欺骗及反网络钓鱼和行为分析集成起来，来跟踪被攻击的机器和冒名顶替的员工。 100Test 下载频道开通，