

信息安全四大新技术探秘 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/287/2021_2022__E4_BF_A1_E6_81_AF_E5_AE_89_E5_c98_287053.htm 综述：展望安全新技术 让我们先来展望一下未来的安全手段。这些技术主要包括由门锁、监控探头和具有逻辑分析能力的IT系统整合而成的安全系统，还有可以穿透皮肤表层进行身份识别的生物识别技术，以及能够事先推断出被窃数据重要性以防范犯罪行为发生的网络系统等。幸运的是，大量诸如此类的工作目前正如火如荼地开展起来。这些刚刚萌生的技术体现出一种共同的趋势，即主动出击的防御特征。随着安全威胁的升级，系统与应用程序必须对面临的攻击做出准确判断，取得授权并及时自动回应，与此同时，还应该告知重要的IT和安全负责人员。自从2001年“911”恐怖袭击发生以来，安全领域取得的最大进步或许是物理技术与IT安全技术的结合。这种趋势在视频监控技术领域表现得十分显著。2007年年初，国际商业机器公司(IBM)将把智能监视(Smart Surveillance)中间件作为数字视频监控服务(DVS)的一部分置于其中。智能监视产品由IBM华生研究中心(T.J. Watson Research Center)开发，通过设备与逻辑能力的整合，使摄像机、雷达、化学感应器和音频监视系统等设备具备了分析能力，这样一来，它们就能对可疑活动进行检测，必要的时候还能发出红色警报。有了智能监视服务，停放在机场错误区域的卡车、试图闯入出口廊道的航空旅客，或者拿走货架物品正欲通过收银台的顾客，都会触发系统进行记录、产生文本信息或发出其他安全警报。IBM的中间件还有一个可供搜寻的索引，能够对相关项目(

譬如汽车牌照、车身颜色和驾驶员的脸部影像等)进行关联。从使用磁带保存模拟信号到使用硬盘存储数字视频信号的转变，完全改变了视频监视的摄录与管理市场，3VR安全公司(3VR Security，下称3VR)首席执行官(CEO)斯蒂芬拉塞尔(Stephen Russell)表示。3VR是一家视频管理系统制造商，公司的产品在2005年占据了38亿美元的全球市场份额。比如，数字视频包含一个时间戳，以此为基础可对其进行搜索，而这样的功能模拟视频是无法实现的。3VR采纳了这种做法并更进一步有所创新，它采取给数字视频添加可分析信息(例如生物数据或影像)，使数字视频数据具备可搜索条件。实现手段其实就是给视频影像贴标签，这种做法和谷歌公司(Google)给网页标注的办法大同小异。3VR的智能视频管理系统(IVMS)的最新版本包含一个软件开发者工具包，凭借这个工具，企业可以把可搜寻的监视系统同其他系统(包括接入设备和网络的权限控制系统，比如指纹扫描仪或者脸部识别系统)整合起来。拉塞尔表示，3VR的技术已被整合到多种系统中，比如用于银行环境中的金融交易系统、楼宇出入管理系统、以及数据源访问权限控制系统等。影像比对技术3年内有望研发成功。利用这项技术，公司的监视器可将捕捉到的视频影像，同已加载到系统中的雇员和既定访客数字影像进行比对。但思科系统公司(Cisco，下称思科)安全解决方案营销部副总裁杰夫普拉登(Jeff Platon)表示，这项技术广泛采用的前提是，脸部识别软件仍需大大改进，因为目前不到30%的精确度与实际要求仍然相去甚远。监视系统同IT网络进行整合意义重大。从历史发展的角度来看，安全技术分为两大阵营：信息安全是一方，而物理隔离墙、锁链和佩枪

的卫兵则是另外一方。由于物理与逻辑这两个截然不同的世界无法有效联结，两大阵营的融合进程屡屡受阻，直到数字视频信号实现了网络化，两者才能真正合而为一。思科正着手集合网络安全和物理安全先是兼并视频监视软硬件制造商SyPixx网络公司(SyPixx Network，下称SyPixx)，而后又在2006年4月发布了智能聚合环境(ICE)系统。2006年9月，思科又宣称正与锁具销售商亚萨合莱公司(Assa Abloy，下称亚萨合莱)合作，将思科生产的基于IP访问控制系统、身份管理系统同亚萨合莱的“智能”标记阅读器、门锁组件整合为一。这种整合可以对未使用标记的入门人员进行防范，例如阻止其登录公司本地网络。访问管理系统销售商Imprivata公司也在开发物理安全与网络安全整合技术。它的一卡式物理/逻辑用具(OneSign Physical/Logical用具)能够同安全标记系统并肩作战，预先对用户所处位置进行判断，然后再决定是否授予远程或本地网络登录权限。正是有了这些整合，现在在许多公司里，物理安全和IT安全的负责人才开始向首席安全官(CSO)进行汇报，BroadWare科技公司(下称BroadWare)CEO比尔斯汤兹(Bill Stuntz)这样认为。BroadWare是基于IP数字视频监视系统与服务供应商。“从模拟视频到数字视频的巨大转变，意味着物理安全正逐渐被纳入IT管理人员的管辖范围，他们终将掌控这部分的预算。”斯汤兹表示。

安全新技术(一)：穿透皮肤的指纹识别 设想一下，假如生物指纹扫描仪验证身份的手段不局限于指纹，同时还能检查手指的组织结构以及血色素指标，这将是怎样一种景象?这就是NanoIdent科技公司(NanoIdent Technologies，下称NanoIdent)想要看到的。这家奥地利公司致力于印制在玻

璃、薄塑料片或纸张上的新型半导体的研发，而不像过去那样，将它写入芯片之中。Nanoident将类似光子感应器和微流体感应器等特色安全设备植入其搭载系统芯片的半导体之中，这意味着它们能够被嵌入到手机或者信用卡大小的设备上，既不占用大量空间，也不会消耗很多电量。典型的“触击型”指纹传感器尺寸只有15毫米长、2毫米宽。它通过手指在敏感金属盘上按压捕捉影像，然后再和指纹数据库进行比对进行验证。由于它大小适中，得到了PC制造商们的青睐仅惠普公司(HP)一家，每个月装运的嵌有指纹阅读器的PC数量就高达25万台之多。Nanoident CEO克劳斯施罗特(Klaus Schroeter)表示，在移动电话这个受尺寸、价格和特色功能驱动的市场，这种传感器颇有潜力。Nanoident的指纹扫描器小到可以安装在移动电话机上，而它本身的面积又大到足以采集整枚指纹。施罗特认为，指纹认证技术若要得到广泛应用，首先需要提高它的精确度。指纹生物特征识别精确率已达到98%，但如果要部署这项技术并从容实现商用，就必须提高到99.9%。“现在指纹造假太容易了。”他解释道，只要接触玻璃留下指纹，就可以进行拍照，然后做成印章，精确率高达95%。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com