

数字城市与网络信息安全

严春伟

2013 年 1 月 15 日

1 数字城市发展概况

数字城市是以计算机技术、多媒体技术和大规模存储技术为基础,以宽带网络为纽带,运用遥感、全球定位系统、地理信息系统、遥测、仿真-虚拟等技术,对城市进行多分辨率、多尺度、多时空和多种类的三维描述,即利用信息技术手段把城市的过去、现状和未来的全部内容在网络上进行数字化虚拟实现。^[1]

2 数字城市支撑技术

2.1 遥感技术

数字城市致力于将城市数字化建模.在城市数字化方面,遥感技术有很大的应用空间.

1. 拓展综合信息源. 现代城市中有极丰富的人文社会化信息,利用 GIS 和遥感集成技术将此方面信息整合起来,为宏观上探测城市的综合信息提供了技术可能.
2. 动态变化. 遥感技术可以动态更新,实现数据实时性,趋势性的要求.
3. 监测评估功能. 能够对城市资源,经济,人文实时监控.通过反馈评估,使城市健康高效运行.

2.2 信息技术

信息技术的发展能实现信息空间的扩展与城市空间的延伸.

1. 通过信息技术的支持,能集中城市经济规划与管理的职能,提供生产和消费市场的在线服务,消除信息互动的物质空间距离.
2. 提供便利的城市社会文化生活,为市民提供相关的服务.数字城市的管理中心能够便捷地与市民间实现便捷而方便的互动.
3. 促进虚拟社区的发展.强化了物质社区的功能,推动信息时代社区功能的全面复兴和发展.

2.3 网络技术

“数字城市”涉及到大量图形、影像、视频等多媒体数据,数据量非常大,目前的因特网难以胜任,必须使用宽带网络.城市宽带网技术发展很快,据报道,国内已有城市开始建立每秒 10G 的宽带网络.这种宽带网络可以满足“数字城市”的需要.

3 数字城市中网络信息安全的必要性

从数字城市的三个核心技术来看, 信息系统和遥感技术等产生繁多的数据, 而这些数据需要有强大而安全的存储系统, 而相关信息的传输以及整合便需要安全有效的网络技术的支撑。

那么关于数字城市中繁杂而频繁的网络信息的传输, 以及大数据的存储, 均需要有强大的网络安全技术支撑。

近年来发生在互联网上的安全事故频频发生, 据 IT 界企业团体 ITAA 的调查显示, 目前美国约 75 万的企业网的信息失窃, 25 万的企业损失高达 25 万美元以上。由此, 可以看到在信息安全比较脆弱环境下, 数字城市所面临的安全挑战。由于数字城市整个大系统中信息比较全面, 如果相关信息泄露会威胁整个城市框架中很多的运行核心信息的安全。

一个典型的事例就是, 城市中出现了一个劫持事件, 那么在城市的管理中枢(指挥中心)会尝试整合数字城市中各方面丰富的信息进行分析, 这些信息包括歹徒方向的, 卫星、监控录像、通话等等信息; 同时, 也会包括警察这方面的部署、人员配置等等方面的信息。我们不能想象如果歹徒能够窃取这方面的信息, 掌控了整个大局的后果。如此, 信息安全的重要性可见一斑。

在网络化信息化进程不可逆转的形势下如何最大限度地减少或避免因信息泄漏, 破坏所造成的经济损失是摆在我们面前亟需妥善解决的一项具有重大战略意义的课题。

4 中外安全技术支撑

4.1 病毒防范技术

数字城市健康运行需要庞大规模的计算机群的运行。如今, 计算机病毒能够经过系统穿透或违反授权攻击成功在系统中植入木马或逻辑炸弹等程序, 直接威胁到数字城市信息安全以及电子设施的稳健。

因此, 数字城市需要完善的病毒防范技术。

在这些方面国外的一些杀毒软件如 Norton McAfee 熊猫卫士等走在了前面, 而国内的大部分杀毒软件大都专注在单机版杀毒上。虽然有部分厂商推出了网络版的杀毒产品, 也只是在桌面端及文件服务器上防护, 防护范围依然较窄。所以国内杀毒厂商应及早加强在网关或邮件服务器上的防护, 只有有效截断病毒的入口, 才能避免电子城市的电子设施遭受病毒侵害。

4.2 加密型技术

采用加密技术, 能够保证电子城市的各职能部门间的信息安全。通过对网络数据的可靠加密来保护网络系统中包括用户数据在内的所有数据流, 从而在不对网络环境作任何特殊要求的前提下, 从根本上解决了网络安全的两大要求: 即网络服务的可用性和信息的完整性。

加密技术可以分为对称加密、不对称加密以及不可逆加密, 下面进行简单介绍。对称型加密使用单个密钥对数据进行加密或解密。这是比较传统的一种加密方法, 发信人用密钥将某重要信息加密后, 通过网络传给收信人, 收信人再用同一密钥将加密后的信息解密。这种方法的优点是计算量小加密效率高即使传输信息的网络不安全, 被别人截走信息加密后的信息也不易泄漏。

4.2.1 不对称型加密

其特点是两个密钥一个称为公用密钥另一个称为私有密钥。其中公用密钥在网上公布, 为数据源对数据加密使用, 而用于解密的相应私有密钥则由数据的收信方妥善保管。

由于密钥的分拆, 可以实现分布式的加密, 在互联网中可以有很大的应用。

4.2.2 不可逆加密

这种加密的特征是加密过程不需要密钥，且经过加密后的数据无法被解密，只有同样的输入数据经过同样的不可逆加密，算法才能得到相同的加密数据。

4.3 入侵检测技术

入侵检测系统是对计算机和网络资源上的恶意使用行为进行识别和响应的处理过程它不仅监测来自外部的入侵行为同时也对内部用户的未授权活动进行检测。

参考文献

- [1] 王家耀, 宁津生, 张祖勋. 中国数字城市建设方案及推进战略研究. 北京: 科学出版社.2008
- [2] 许奕锋, 试论数字城市建设与管理的三大技术支撑, 湖南省委党校, 湖南长沙
- [3] 沈昌祥, 张焕国, 冯登国, 曹珍富, 黄继武. 信息安全综述, 中国科学,2007