Data and Network Security in Windows - Threats & Countermeasures

Harsh Vikram Singh
Department of Electronics Engineering
Kamla Nehru Institute of Technology
Sultanpur -228118, India
harshvikram@gmail.com, harsh@knit.ac.in

ABSTRACT: *Information and Communication Technology (ICT) revolution over the past two decades has been facilitated multimedia data transfer over commonly available public domain open channel networks. Such public domain network environment is open to all across the world and thus necessitates security measures to ensure multimedia data confidentiality, authenticity, and integrity to the intended recipient. Organizations of all sizes want secure network connectivity to their business data and applications. The need to connect and collaborate with partners, customers, and remote/mobile employees anytime and anywhere has expanded network connectivity requirements beyond traditional wired LANs to include dial-up remote access, virtual private networks (VPNs), as well as Wi-fi, WiMAX and other wireless networks. This paper discuss the commonly used Windows operating systems for enabling superior access to the open networks and other related issues like security, management complexity, and cost.*

Keywords: Information Security, Windows Operating Systems, Rights Management

Received: 11 October 2012, Revised 19 November 2012, Accepted 27 November 2012

1. Introduction

Enterprises are competing globally to provide access to information, to enhance productivity, and to deliver services promptly with the lowest possible expenditure. The capability to communicate and collaborate with partners, suppliers, customers, and employees anytime and anywhere is now a requirement. Open channel public domain networks (i.e. Internet) offer public channels to deliver and exchange information for cost effective and fast data transfer. Such open public networks have long been known for being insecure while at the same time technological developments for the perfect reproduction, ease of editing, access and sharing of multimedia data have resulted in greater concerns of copyright infringement, illegal distribution, and unauthorized tampering. Therefore, data security to ensure authorized access of open channel digital information and fast delivery to a variety of end users with guaranteed Quality of Services (QoS) are important topics of current relevance [1].

The advent and acceptance of new computing technologies and the Internet have changed the way information is stored, accessed, and shared. Companies have implemented a more open and distributed information model resulting in benefits that include [2]:

(i) **Increased Employee Productivity:** Enables employees to be flexible, make better decisions, and respond quickly to the changing demands of the marketplace by providing secure access to the information they need anywhere at anytime.

(ii) **Lower Cost:** Decreases costs and increases efficiency by safely leveraging the power of collaboration and network connectivity.

(iii) **Integrated Business Processes:** Increase sales by enabling closer relations with customers and partners through secure communications and collaboration.

If you have an operating system (OS) running on a locked-down box, isolated in a secure room with no network connections, and it is running a single application, then most of today's OSes can be considered secure. But most OSes don't operate in that environment. Security protection in Windows perhaps isn't as comprehensive as was first thought, and is unlikely to ever be unbreakable, but the layers of protection used in Vista are still effective at mitigating many attacks and preventing the exploitation of vulnerabilities in server processes [3].

Today, many Windows users run with administrative privileges in both the enterprise and the home. Running as an administrator results in a desktop that is hard to manage and has the potential for high support costs. Deploying desktops with standard user permissions can result in cost savings because a non-administrative user no longer has the ability to accidentally improperly configure the network or install an application that might affect system stability. Windows XP and earlier versions of Windows are vulnerable to offline attacks that attempt to obtain a user's data on lost or stolen computers. Windows Vista includes an agent that can prevent a Windows Vista-based client from connecting to your private network if it lacks current security updates, lacks virus signatures, or otherwise fails to meet your computer health requirements [3]. Network Access Protection (NAP) can be used to protect your network from remote access clients as well as LAN clients [4]. The agent reports Windows Vista client health status, such as having current updates and up-to-date virus signatures installed, to a server-based Network Access Protection enforcement service. NAP can enforce health requirements for mobile computers, remote computers, and computers directly connected to your private network. The personal firewall built into Windows Vista builds on the functionality that is included with Microsoft Windows XP Service Pack 2. It also includes application-aware outbound filtering, which gives you full, directional control over traffic. Many potentially risky applications, such as peer-to-peer sharing client applications that might transmit personal information across the Internet are designed to bypass firewalls that block incoming connections. Windows Vista's firewall enables enterprise administrators to have the ability to set Group Policy settings for applications that should be allowed or blocked, giving them control over which applications can communicate on the network. Windows Vista has improved support for data protection at the document, file, directory, and machine level.

The integrated Rights Management client allows organizations to enforce policies around document usage [5]. The Encrypting File System, which provides user-based file and directory encryption, has been enhanced to allow storage of encryption keys on smart cards, providing better protection of encryption keys. In addition, the new BitLocker Drive Encryption enterprise feature adds machine-level data protection [6, 7]. On a computer with appropriate enabling hardware, BitLocker Drive Encryption provides full volume encryption of the system volume, including Windows system files and the hibernation file, which helps protect data from being compromised on a lost or stolen machine.

An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

2. The Need for Security

The need to connect and collaborate with partners, suppliers, customers, and employees anytime and anywhere has expanded network connectivity requirements beyond traditional wired LANs to include dial-up remote access, VPNs, and wireless networks. When addressing secure network connectivity, administrators need to consider the following:

Security: Employees not only work from corporate offices, but also from branch offices, home offices, or from the road. Providing remote connectivity requires solutions that are secure, standards-based, and manageable.

Management complexity: Many vendors offer dedicated product solutions with little integration with other products and infrastructure. Setting up wireless clients with centralized authentication and policies can be a challenge unless there are integrated solutions.

Lowering cost: Secure networking can be expensive if there are multiple products and technologies with separate licensing, support contracts, and training.

For example, a secure VPN implementation may require separate certificate authority for PKI, separate authentication model, client-side software, and additional server gateways and firewalls. By addressing these key secure connectivity challenges, organizations can achieve greater employee productivity, decrease costs, and improve business integration [8].

2.1 Security

Whereas the LAN once formed a de facto security boundary, it is now common for companies to open parts of their internal networks to suppliers, business partners, and other stakeholders. By providing greater network access, companies will need to increase their level of security to safeguard against unauthorized access and usage of internal assets. Security challenges to consider include:

Security procedures and policies that are adequate to protect LAN data may be ineffective when the network is opened to outsiders.

Weak authentication used on external networks can compromise network entry points and allow unauthorized access.

Sensitive data sent over the Internet or wireless networks can be compromised without the proper level of encryption.

Application-aware firewalls are necessary to ensure traffic is filtered before being allowed onto the internal network since hackers are now using more sophisticated application-layer attacks.

2.2 Management Complexity

Expanding network connectivity brings a set of technology and process management challenges that make it difficult for administrators to provide a centralized and consistent approach to network access. Management challenges to consider include:

Consistent network access control: This requires synchronizing and managing across multiple network access points such as Internet, extranets, leased lines, wireless LANs, VPN and dial-up access, etc.

Access policies: Different users require different levels of access rights and permissions. Administrators should consider enforcing policies based on identity, time, location, and device type.

Single authentication model: A single method for authentication regardless of the type of access (dial-up, wireless, VPN, etc.) is highly desired for ease of management.

2.3 Lowering Costs

Providing secure network access can increase employee productivity and expand business integration; however, deploying, managing, and maintaining the necessary network access can be costly. Cost challenges to consider include:

Administrators will spend significant time and effort if each access method has to be managed separately with separate authentication and access control databases.

Security systems are frequently expensive to acquire, difficult to manage, and obtrusive to end users' workflow. This may encourage users to find ways to circumvent systems, or administrators to minimize their safeguards, leading to *less* security instead of more.

In systems with distributed authentication databases, customers and partners who need access to data may be forced to wait while the network staff creates and manages their credentials, leading to productivity loss.

3. Solutions for Secure Network Connectivity

Microsoft® Windows 2000 Server, with its rich feature set that includes Active Directory®, Certificate Authority, and RRAS (Routing and Remote Access Service) in combination with other Microsoft products, such as Windows XP, ISA Server, and Microsoft Exchange, provide the foundation that companies can use today to provide secure network communications to employees, partners, and suppliers [9]. These technologies and products work together to provide three fundamental capabilities that help deliver secure communications and address business concerns around security, management complexity, and cost.

3.1 Securing the Network Perimeter

The network access points of corporate networks must be secured against hackers and unauthorized access. Blocking traffic and shutting down ports are not sufficient or feasible in an Internet-connected organization. Having security solutions that "*look inside*" network traffic to validate application-specific requests mitigates risks. ISA Server, Microsoft's Enterprise firewall, provides organizations with the stateful-packet inspection and application-layer firewall protection required to protect against today's sophisticated attacks. With ISA Server's application-level filtering technology, attacks such as Code Red and Nimda can be mitigated at the firewall before entering company networks [10].

ISA Server integrates with Microsoft Management Console (MMC) and Active Directory to provide a single directory to validate and manage all access requests for application data or services. This enables consolidation of access control and authorization policy in a centrally managed, replicated, and secure repository. ISA Server is also designed to work best with Microsoft Exchange 2000 and Internet Information Services (IIS) to provide fast and secure access to e-mail and web content.

3.2 Providing Strong Authentication and Encryption

Accessing the corporate network requires administrators to enforce strong authentication to validate identity as well as provide strong encryption to prevent data from being communicated "*in the clear*". Whether using VPN or wireless LANs, Microsoft's Windows 2000 and Windows XP provide the authentication and encryption infrastructure to enable secure connectivity. With Windows 2000 built-in VPN server and Windows XP VPN client, organizations can take advantage of secure standards-based VPN directly "*out of the box*". Because Microsoft supports VPN standards such as L2TP/IPSec and smart card authentication, organizations have access to the encryption, authentication, and interoperability that best meet their VPN security needs. While VPNs are often used to encrypt traffic over the Internet between users and the corporate network, encryption can also be implemented between any Windows 2000, Windows Server 2003, and Windows XP machine. Since Microsoft has full standards-based support for the IPSec security extensions, organizations can provide robust encryption of all network traffic, without requiring cumbersome changes to deployed applications, servers, or network hardware.

In addition to strong encryption, authentication requirements can be met through Windows 2000 support for the IEEE 802.1x authentication protocol. This allows network clients and servers to securely authenticate each other using digital certificates. 802.1x provides port-level control that can stop interlopers from connecting to the network and thus prevent any malicious activity [11]. Companies that want to build an integrated authentication system that securely authenticates users against a single directory, regardless of the access method or device they are using can take advantage of Windows 2000's Internet Authentication Service (IAS) [12]. This built-in industry-standard RADIUS server interoperates with network access devices from a multitude of vendors.

3.3 Securing Wireless Access

In addition to adding remote access connectivity, customers are also exploring wireless LANs to provide their mobile laptop users with anytime, anywhere access. Authentication and encryption concerns as well as security weaknesses in the IEEE 802.11b protocol have slowed the adoption of wireless LANs [13]. Microsoft has tackled the WLAN security problem in Windows 2000 and Windows XP by working within the 802.1X standard to support EAP-TLS (Extensible Authentication Protocol – Transport Layer Security). EAP-TLS provides certificate-based, mutual authentication for clients and access points. This counters the rouge access point threat and supports dynamic session keys that minimize the key theft problem. EAP can also be used with smart cards and biometric authenticators to provide added security. Windows Vista includes many security features and improvements to protect client computers from the latest generation of threats, including worms, viruses, and other malicious software (collectively known as *malware*). Windows 7 extends BitLocker drive encryption support to removable storage devices, such as flash memory drives and portable hard drives [14].

Organizations can take advantage of Microsoft's technologies and products to enable: secure Internet connectivity, secure messaging, strong user authentication, VPN and wireless LAN access to corporate networks. All these solutions can be controlled by a common management interface and can be administered using Active Directory policies. This ensures consistent and complete application of policies to all access requests, regardless of where they originate. Although, it is virtually impossible to build a completely safe operating system that accommodates literally hundreds of thousands of different programs, scripts, applets, etc., written by many different vendors whose developers may be good or average. However, by providing advanced security technologies, common management, and lower cost through integrated solutions, Microsoft can enable businesses to take advantage of the network connectivity. Enterprise users with computers with appropriate enabling hardware benefit from protection of data on lost or stolen computers with BitLocker™ Drive Encryption. Windows Vista includes new authentication architecture that is easier for third-party developers to extend. Biometrics enhancements include easier reader configurations, allowing users to manage the fingerprint data stored on the computer and control how they log on to Windows 7 [14].

4. Conclusion

To take advantage of the networked world, organizations must prevent unauthorized users from accessing their networks, and at the same time, ensure that authorized users have access only to authorized assets with current available OSes. Together, these security improvements will make users more confident in using their PCs. Whether or not the presented security mechanisms can be used easily for Windows must be examined for each kind of multimedia data and OSes applications separately. This paper presented security threats in data transfer over open channel network environments and their solutions with countermeasures available in different visions of Windows OSes. Their merits and limitations of data security are discussed. It is explained that there is no single universal technique for either achieving robust multimedia data security or providing guaranteed success in the secure transmission of such multimedia objects and thus these are still open problems requiring further investigations.

References

[1] Harsh Vikram Singh, A. K., Singh, Anand Mohan. (2006). Minimizing Security Threats in Multimedia Systems, *In*: Proc. of 2nd IEEE International Conference on Distributed Framework for Multimedia Applications, p. 1-5, Penang, Malaysia.

[2] Available: *http://technet.microsoft.com/en-s/library*

[3] Sangani, K. (1996). Review - living with windows vista, *IEEE Engineering & Technology*, 1, p. 52 – 54, Aug.

[4] Kumar, L. N., Douligeris, C. (1996). Demand and service matching at heavy loads: a dynamic bandwidth control mechanism for DQDB MANs, *IEEE Transactions on Communications*, 44, p. 1485-1495.

[5] Kohali, S. S., et al. (2008). The impact of wireless LAN security on performance of different Windows operating systems, *In*: *Proc. of IEEE Symposium on Computers and Communications*, p. 260- 264, July**.**

[6] Hayes, D. R., Qureshi, S. (2008). A framework for computer forensics investigations involving Microsoft Vista, *IEEE Long Island Systems, Applications and Technology Conference*, p. 1-8, May.

[7] http: www.technet.microsoft.com/en-us/library/cc507844.aspx

[8] Al-Khayatt, S., et al. (2002). A study of encrypted, tunneling models in virtual private networks, *In: Proc of IEEE International Conference on Information Technology: Coding and Computing*, p.139 – 143, April.

[9] Routing and Remote Access Service (Remote Access), Windows Server 2003 Networking Recipes. (2006). Chapter 4, p. 141-189, Springer publication.

[10] Kyle Schurman, Hard HAT AREA, X-ray Vision: Virus Penetration, Computer Power User Artical.

[11] Narayan, S., et. al. (2008). The Influence of Wireless 802.11g LAN Encryption Methods on Throughput and Round Trip Time for Various Windows Operating Systems, 6*th* *IEEE Annual Conference on Communication Networks and Services Research Conference* - 2008, p.171-175, May.

[12] Internet Authentication Service, Windows Server 2003 Networking Recipes, Chapter 6, p. 243-287, Springer publication.

[13] Nam, J., et. al. (2006). Load modulation power amplifier with lumped-element combiner for IEEE 802.11b/g WLAN applications, *Electronics Letters*, 42, p. 24-50, January.

[14] Sangani, K. (2009). Lucky seven?, *IEEE Engineering & Technology*, 4, p. 32-33, March.