

Securing Remote Control: Fundamentals for security in remote environments

By Mike Baldwin

IT administrators now have to find a secure and effective way to handle the increased workload created by remote offices.

In today's enterprise environment, many organizations depend on budget-strapped IT administrators to provide efficient and effective support to an ever-increasing number of users. These companies may number in the tens or tens of thousands, but one thing remains the same: The number of employees who spend 100 percent of their time in the office is decreasing. Users access the office remotely while on business trips; some work remotely all the time. No matter what the reason, IT administrators now have to find a secure and effective way to handle the increased workload created by remote offices.

IT administrators turn to remote control software as a powerful tool to quickly solve problems and keep the network available to authorized users. Just as administrators can leverage remote control to help manage and support their multi-platform IT infrastructures, IT professionals can use it to provide customer support without leaving their offices.

A good remote control solution serves as a powerful tool, opening new avenues and possibilities. With these opportunities come new risks, and more and more organizations demand tools that offer the advanced security they need to protect their information assets and meet industry and government regulatory requirements. To meet these demands, remote control programs must provide a secure environment for resolving helpdesk issues, managing remote computers, and working across multiple platforms.

Remote workers may be less likely to follow security procedures because the problems and policies at corporate headquarters often seem far away. In fact, issues with security are often the most important factors in determining whether to implement remote control technology in the corporate environment. However, by addressing necessary security requirements in specific areas, such as authentication, authorization and access control; perimeter and data-transfer security; and administration, a remote control solution can provide IT organizations with a secure and cost-effective helpdesk tool.

Why remote control?

Remote control software easily enables a user to see the desktop of another system and to control that system by passing mouse move-

ments and keystrokes to it. Remote control includes file transfer, remote access, and often remote management capabilities. These capabilities offer more freedom to executives and IT administrators alike.

Traditional remote control programs offer a point-to-point solution, creating a direct connection between two computers. This type of solution provides control over the connection, where the data is going, and which ports are open. The traditional model of remote control enables IT administrators to retain the ability to control traffic as needed, based on corporate IT policies.

Remote control is also now available as a hosted Web service, giving users access to a host PC from remote devices that have Internet access. These highly convenient, subscription-based or free services are typically easy to use and require minimal installation. However, the hosted service model may pose security concerns, especially for enterprises faced with demonstrating compliance with industry or government regulations for information security.

Improving security in the remote environment

While remote control offers businesses and IT administrators the freedom to log on to another computer from a remote system, it also brings special security challenges. These obstacles can be overcome by performing and utilizing these key functions:

Integrity Checking – Integrity checking is critical. Remote control software with integrity checking identifies changes made since the original installation. If changes are detected, indicating potential rogue installations, the program will not function.

Alerts and Logs – Administrative features such as alerting and logging are also essential to a secure environment. Secure remote control programs generate alerts when a number of unsuccessful attempts to connect to a host PC are detected; this permits real-time monitoring of suspicious activity from a network management console. A secure remote control program also generates audit logs of all remote control transactions, enabling the administrator to monitor activity and detect unauthorized attempts to access systems. Some programs also enable these audit logs to be secured to prevent hackers from altering them in order to hide their tracks.

Controls – Authorization and access controls are also effective deterrents to security breaches. Mandatory authentication measures help reduce unauthorized access by verifying a user's credentials against a directory or access list to determine if that user is authorized to connect to the system. Flexible remote control software can leverage either its own features or existing OS policy to further limit users' rights to certain drives on the host, or to specific application functionality.

Lastly, secure remote control programs will enable administrators to limit access to computers within a specific subnet or to specific TCP/IP addresses, or conversely to prevent connections from specific addresses. Serialization also protects remote control sessions by allowing IT administrators to embed a security code into the host and remote components of a remote control solution. Serialization ensures that connections are only accepted between computers containing matching serial numbers. In support situations, the host user should be able to confirm or deny access.

Keeping data secure at all points

IT administrators make sure that the data they protect remains secure on the network, but they also know that securing the data stream in transit is just as important as preventing unauthorized access. Remote control software should support both symmetric and asymmetric (public key) encryption services, to prevent eavesdroppers from intercepting data during transmission.

Remote control users should pay attention to current industry and government data encryption standards. If they do, they will see that the AES encryption algorithm is something to look for in a remote control product. AES (or Rijndael) is one of only four symmetric-key encryption algorithms approved against the National Institute of Standards and Technology's (NIST) Federal Information Processing Standard (FIPS) 140-2 standard. It provides encryption at the 128-bit, 192-bit, or 256-bit cipher strengths.

AES is, by definition, exponentially stronger than the previous DES and 3DES algorithm standards, and is considered to be faster and less resource-intensive as well. It should be set as the standard across all product components of your remote control solution. The NIST FIPS 140-2 validation allows products to be purchased by federal agencies and other organizations that require stringent security standards to protect sensitive information.

FIPS 140-2 is also required by federal agencies in Canada, recognized in Europe and Australia, and being adopted by numerous financial institutions worldwide. It is a tremendous indicator of product encryption security. Secure remote control products will support encryption of both the data stream and authentication credentials. For full effectiveness, remote control software should also support Virtual Private Network (VPN) technology to permit secure Internet connections over an extended corporate intranet.

Remote control security across platforms

The typical IT environment today is composed of everything from Windows desktops to Linux servers to handheld computing devices. And IT organizations are responsible for keeping this heterogeneous infrastructure functioning at all times. That's why a growing number of organizations are turning to remote control solutions that offer true cross-platform support. The use of remote control solutions across platforms demonstrates another reason that security within these solutions is important.

Compliance and security

Ongoing legislation continues to change the landscape of compliance and regulatory standards, making security a boardroom issue in any organization. From the Health Insurance Portability and Accountability Act (HIPAA) of 1996, to Sarbanes-Oxley (SOX) of 2002, to California's Notice of Security Breach Act, these regulations call upon organizations to evaluate and address issues of data reliability, integrity and security, even as government institutions face mandatory requirements.

Regulatory compliance is one driver for organizations reevaluating their remote access tools. As remote access software might inadvertently put the confidentiality of sensitive data at risk, organizations will demand more sophisticated remote control solutions, including support for existing security infrastructure, and advanced security functionality and features. Support for a variety of strong encryption also helps mitigate the risk of information exposure, enabling regulatory compliance. Performance

Another expectation an organization should have for its remote control solution is high performance and availability. To be effective, even the most secure cross-platform remote control solutions must also offer high performance in an enterprise environment. To ensure such performance, features such as bandwidth auto-detection can be used, enabling users to detect the actual connection speed or bandwidth of each connection and then adjust settings that impact performance in lower-bandwidth connections. In doing this, administrators are able to ensure the availability of their now-secured data.

The bottom line

Numerous recent data breaches have demonstrated the many ways that security can be compromised within the enterprise. No matter the method of loss, these types of security lapses can ultimately cost millions of dollars. Ensuring the security of remote offices provides a way for organizations to increase efficiency while adding a much-needed layer of protection to the data and the network.

To continue to play an integral part in any IT infrastructure, remote control software solutions should foster a secure environment for managing remote computers, working across multiple platforms, and resolving helpdesk issues. With a secure remote control solution, organizations have a powerful tool for keeping their environments up and running no matter what.

About the Author

Mike Baldwin is a Senior Product Manager within Symantec's Data Management Group. He has primary responsibility for Symantec's remote control, IT inventory and asset management solutions. Prior to joining Symantec in early 2003, Baldwin held product management positions at leading technology companies including Sonic Foundry, Inc. and Marconi Corporation PLC. Baldwin began his career as an active-duty communications officer in the US Army, where he led multiple platoons charged with missions varying from satellite communications to combat photography. He earned his undergraduate degree from James Madison University and his graduate business degree from Carnegie Mellon University.