

# REMOTE CONTROL AND SECURITY

By: Pushpendrasinh Jhala  
For: NIVID LTD



As most IT organizations know, security is the most important factor in determining whether to implement remote control technology in the corporate environment. That's because remote control is often viewed as a backdoor to bypass security and gain access to a computer and the network. For remote control to be widely and effectively adopted within any organization, it must provide multiple levels of security to ensure that only authorized users can connect. This article looks at how some necessary security requirements can be used to help IT organizations evaluate the potential of remote control software.

### Doing more with less

Today's IT organizations are expected to support a growing number of users, many working remotely, who are using increasingly complex hardware and software. At the same time, IT budgets are being curtailed. IT organizations must therefore find a way to handle the increased workload securely and effectively.

Remote control software, which enables a helpdesk professional to assume control of a user's PC over a network, provides a way for a helpdesk to handle more calls without additional resources. But in order to allay fears that it could expose data to unauthorized use, remote control software must address security requirements in the areas of authentication, authorization and access control, perimeter and data-transfer security, and administration.

- **Authentication:** While no authentication technique is foolproof, requiring the use of passwords or other form of authentication before a remote session commences discourages unauthorized access. When evaluating a remote control solution, make sure it supports authentication methods that your organization is already using. Support of multiple, standard authentication methods allows IT staff to leverage existing user/password lists. Support for RSA SecurID provides a two-factor authentication process. This model presents the legitimate user with a security code that changes every 60 seconds. RSA SecurID support will be of particular interest to the federal government and the financial services industry.
- **Authorization and access control:** Remote control software should be able to limit access to computers within a specific subnet or to specific TCP/IP addresses. Another effective way to block unauthorized access is by embedding a "serialization" code into the host and remote portions of the remote control product. A host that has been serialized will accept connections only from a remote computer with the same serialization number.

If the serialization number does not exist, the connection cannot be established. In support situations, the host user should be able to confirm or deny access. Callback capabilities, in which the host disconnects the call and then calls the remote back at a specified number, help prevent unauthorized access.

- **Perimeter and data-transfer security:** Remote control software should support Virtual Private Network (VPN) technology to permit secure Internet connections through a firewall as well as over a corporate intranet. Securing the data stream in transit is just as important as preventing unauthorized access. The software should support encryption services and public key encryption to prevent eavesdroppers from intercepting data during transmission.
- **Administration:** The software's administration tools should help IT professionals plug security holes by scanning network and telephone lines to identify unprotected remote access hosts. In addition, since thorough alerting, logging, and reporting are essential to a secure environment, the remote control software should generate an audit log of all remote control transactions, including disallowed attempts at connection. This enables administrators to monitor activity and detect unauthorized attempts to access systems. Integrity checking, meanwhile, can ensure that the host and remote objects, DLL files, executables, and registry settings have not been modified since the original installation. Additional security options In addition to the

security requirements listed above, an effective remote control solution should address the latest security developments, such as:

- a) AES encryption algorithm. AES (or Rijndael) is one of only four symmetric key encryption algorithms approved against the National Institute of Standards and Technology's FIPS 140-2 standard. It provides encryption at the 128-bit, 192-bit, or 256-bit cipher strengths. AES is 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.
- b) FIPS 140-2 Level 1 validation. Has the remote control solution's cryptographic module received Federal Information Processing Standard (FIPS) 140-2, Level 1 validation from the NIST? This allows products to be deployed 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, is recognized in Europe and Australia, and is being adopted by numerous financial institutions worldwide.

- **Financial benefits of remote control software**

While the security issues related to remote control software cannot be overstated, it should also be noted that the financial benefits of this software can be significant, in some cases lowering helpdesk costs by 6 to 13%, according to Symantec. Cost savings can result from reducing size of the helpdesk staff, solving problems faster, and fielding fewer support calls. Forrester Research Inc. has found that an organization with 20,000 end users and a \$2.9 million helpdesk budget could save approximately \$338,000 through the use of desktop remote control software.

## Conclusion

Despite the frequently cited benefits of remote control software -- such as increased productivity and reduced support costs -- some IT organizations have been reluctant to install it out of concern for potential security risks. By addressing necessary security requirements in the areas of 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.

## About us

NIVID's Remote and Managed Services provides proactive monitoring—and even onsite management—to ensure your Microsoft, Novell technologies and leading-edge Linux systems are always running smoothly. These services help you make the most of your technology investments and your IT staff.

You can select the appropriate services you need to manage your networks efficiently and turn over the responsibility for day-to-day network activities to NIVID remote Network Management Services are ideal if you are looking for a single source of support for your communications networks yet still want to maintain a certain amount of control. NIVID will work with you to establish Service Level Agreements that define your expected levels of service. With the advanced processes, tools, and methodologies from NIVID, you can experience support services at a level that matches your needs.

NIVID has the people and resources to deliver best-in-class services. Please visit [www.nivid.net](http://www.nivid.net) for information on our services and our company. Alternatively you can reach us on 0207 101 9233 to speak to our IT Consultant.

#### Related links

Symantec pcAnywhere 11.5

<http://sea.symantec.com/content/product.cfm?productid=16>

Webcast: "Reducing Support Costs Through Secure Remote Control"

<http://ses.symantec.com/content/webcastinfo.cfm?webcastid=136>

#### **Disclaimer**

This article in whole or in part may not be duplicated, reproduced, stored or retransmitted without prior written permission of NIVID Ltd and its author. All opinions and estimates herein constitute our judgment as of this date and are subject to change without notice. Any product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.