Remote Control White Paper

Network Efficiency and Security – Getting the Most Value from Your Remote Control Solution

Edited by Nancy Richards & Mark Krueger

CrossTec Corporation
500 NE Spanish River Blvd.
Boca Raton, FL 33431
(800)675-0729 / (561)391-6560
www.CrossTecSoftware.com

Abstract

You may have heard your grandparents use the idiom: "Time to tighten your belt." Given the challenging current economic situation; one area that cannot be sacrificed is an organization's security posture. Yet, that is exactly what is happening. We all understand that budgets are not growing, or are even declining. Risk mitigation is essential, and it needs to balance with the efficiency required to run an organization effectively.

Remote control software is one way in which a company can expand usability and centrally administer the network in an efficient and effective manner. Remote control software links a keyboard, mouse, and screen to any PC that needs to be controlled. Many solutions on the market today enable the administrator to also support PCs across the operation due to a wealth of information which goes beyond basic remote access. These features help in pinpointing problems, while also obtaining a real-time view of the hardware and software installed on Windows and Linux machines. The network and company can continue to operate at maximum potential as employees can access technical support in a matter of seconds without picking up a phone or filling out paperwork.

Remote control programs also need to support a variety of different operating systems, since many departments within companies are utilizing different platforms and protocols. For example, most high-level graphic design is done on a Macintosh; Excel and Word are Windows based, CE devices are optimal for portable management, and Linux/Unix are long standing systems in corporate IT departments. Also, with the increasing Help Desk and Call Center Industrial outlets and more employees traveling and/or working from remote locations, securely transmitting information is essential in the corporate world of today.

The right remote control product makes all this possible while creating a barricade of security against would-be attackers. No one wants to be caught with their pants down.

Management Challenges

Technical support solutions are predicated upon good communication for problem resolution. Good communication requires the right tools. However, these tools can come at the expense of security measures. Instead of increasing security measures, today's budget restrictions, hiring freezes, downsizing, governmental compliance regulations, and increased cost-cutting pressure - force a *do more with less approach* to IT asset monitoring.

Unfortunately, remote control software often creates vulnerable points-of-entry into the network when sufficient security is not implemented to protect all remote control sessions.

How does an administrator balance the increasing need for security measures with the need to efficiently run an IT department? Moreover, policies relating to critical (often proprietary) information access can be at risk if these are not clearly discussed or controlled. The compromising of this data through theft or attack can not be understated. A good mission-critical infrastructure by the CIO will help to alleviate the external and internal vulnerabilities which demand sound security measures. Some applications go way beyond passwords and encryptions to offer several different levels of security.

A Successful Strategy

At CrossTec Corporation, the developers recognize the need to balance security and efficiency. CrossTec Remote Control software has many security options to protect all data streams, utilities, and points of entry used to access external machines via the Internet. CrossTec has been designed around customer feedback, suggestions, and needs; resulting in a highly comprehensive enterprise solution for securely accessing and controlling remote, cross-platform machines. Recognizing the importance of protecting corporate data, the developers took security and privacy very seriously when designing CrossTec Remote Control.

Secure Remote Connections

There are several communication components that must be secured in order to protect a network. Let's take a look at how CrossTec restricts Control and Client access and protects data streams.

Remote Control software works by having Client software present on all computers involved in a remote control session, as the Control application controls the application installed on the end user's machine. The Client application operates on the controlled machine, enabling the Control to establish a connection to the Client and control activities on the machine. Once a connection is established, the data is streamed between the two machines to enable the Control to take over the Client. In order to protect a remote control session, all data streams must be secured and Control and Client access must be restricted to authorized users.

CrossTec Remote Control utilizes Windows Active Directory (AD) to enable an administrator to centrally manage all users' access privileges, machine rights, unique user IDs, and passwords. Many remote control applications do not let an administrator use the centralized authentication tools they already use, such as AD Users and Computers. This creates a disadvantage by introducing additional management consoles to provide the same functionality.

Each AD Group is assigned privileges pertinent to the job responsibilities. For example, some IT employees need access to all applications and computer information in order to troubleshoot when problems arise. Other supervisors may

have limited access to only monitor his/her employees, so they do not need remote control functionality. By limiting the Control's access privileges, a network administrator can restrict who has access to confidential documents such as patient records or employee payroll.

Corporate networks are typically layered with tight security to protect confidential data. For instance, the common perimeter and desktop firewalls restrict network traffic to specified ports and applications. Unfortunately, these are also the same communication doorways that attackers use to gain access to private networks. This is why many IT departments work very hard to minimize the number of ports that are opened on their network. The more open ports, the easier it is for an attacker to break into a network. Remote control software requires that a port be opened to transmit data between two machines participating in the remote control session. CrossTec developers recognized this long ago and realized the inherent security risk, so they created the CrossTec Gateway Server to resolve this issue. The CrossTec Gateway Server acts like a traffic patrol officer, directing network traffic through a designated port to enable network administrators to define a specific port for all remote access communication, usually HTTPS (443), an encrypted TCP port. No additional ports are opened to expose the private network to outside attackers.

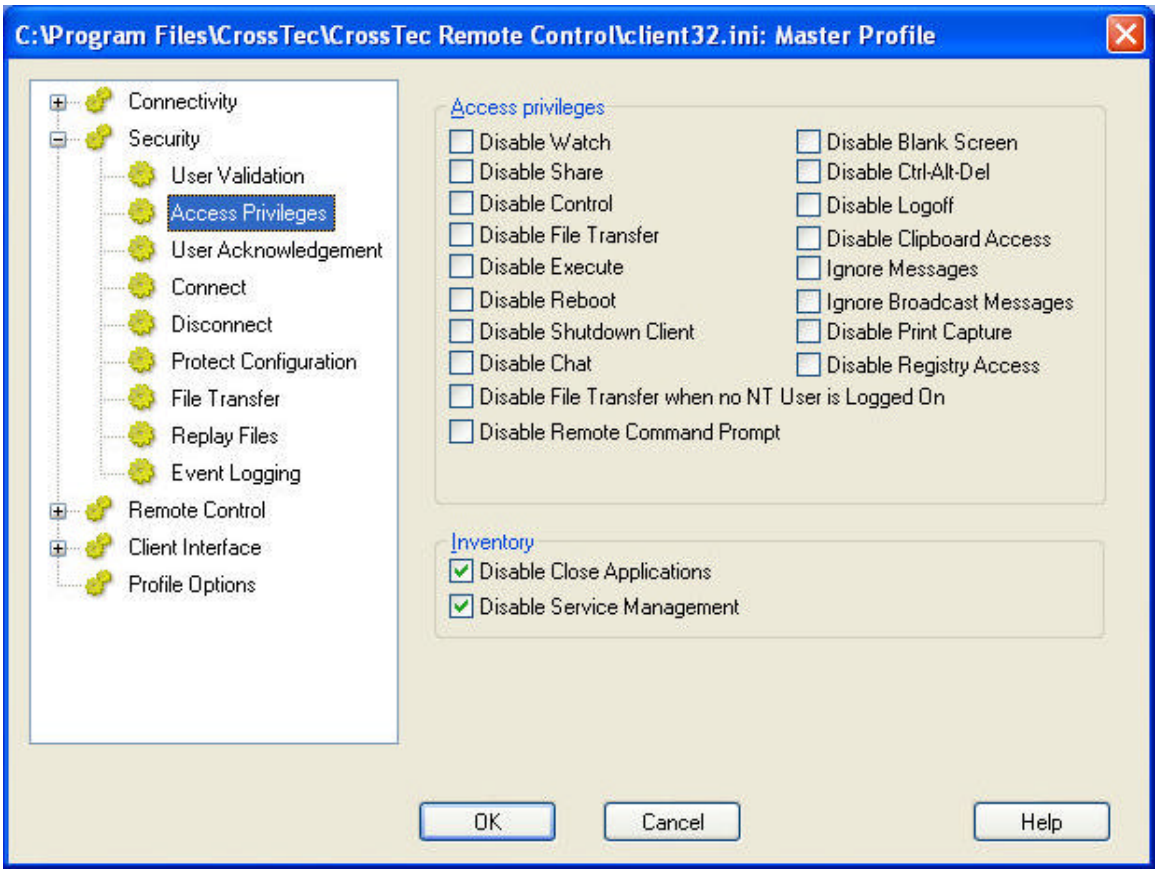
Access Restriction and Control

Unfortunately, due to an ever increasing number of security threats, nothing is a sure thing. So what happens if an attacker manages to break into your network? All they need to do is pirate a Control computer and access every Client machine on the network. CrossTec Remote Control restricts access to Clients machines. Network administrators can rest assured that even if an attacker were able to commandeer a Control computer, they would not be able to remotely connect to Client machines containing important data - even with an administrator password.

If machine passwords have been assigned, Control users are prompted for a password that will either grant or deny them access to the Client machine(s). These passwords can be assigned individually to give each computer a *separate* password for every Client machine. Control's access security can also be integrated into current network authentication schemes such as Active Directory, or local Windows security. The CrossTec Client can be configured a number of different ways to give the Client's user complete control over whoever is trying to access their machine. Whoever is using the Client machine determines how access to the Client will be configured. For example, if a CEO is working with the Client computer, he/she may want to restrict who and when someone is accessing that machine. However, a sales rep, whose Client machine is monitored by a supervisor, does not need to know when he/she is being monitored or who is doing the monitoring.

CrossTec's authentication feature alerts the Client's user when a Control attempts to connect to that machine. The Client has the discretion to grant or deny Control access, because CrossTec enables Clients to be configured to only accept remote connections from a designated list of users. By creating Profiles on the Client

machines, and associating these Profiles to AD Groups, it is easy to create multiple sets of permissions depending on which Windows AD Group member is controlling the Client. For example, this allows an administrator to assign remote control permissions for the Help Desk group that are lower than those of the Domain Admins group when connecting to the same Client.



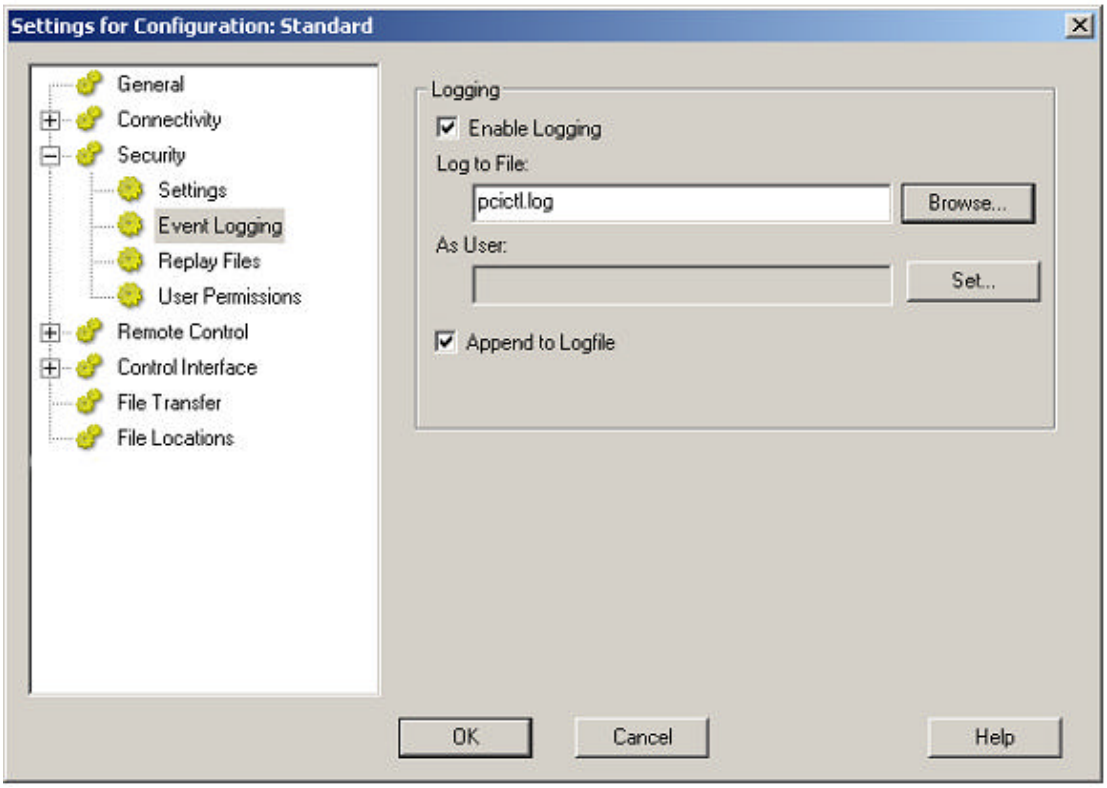
Serial Keys

The Serial Key feature augments Client restriction. Customers who choose to implement a Serial Key create a unique password that is embedded in every deployed license. Only Controls with the correct Serial Key can access Clients with the unique embedded password. Outside users are prevented from gaining access to the company network via a separately purchased CrossTec Remote Control application or a trial license. For instance, if an IT employee is fired, he/she still has knowledge of company passwords and the whereabouts of confidential information. All he needs to do to hack into the network is install his own CrossTec Control and access the Client machines using the company's passwords for clearance. If the employer deployed a Client configured to use Serial Keys, the dismissed employee lacks the unique embedded password on the Control. He is not allowed access to the employer's Client machines even if he has the correct Windows credentials.

Encryption
Information on a hard drive can be protected with firewalls and virus scanners. However, once that information leaves a computer to travel through cyberspace, it has the potential to be accessed and, possibly, manipulated. Any attacker could intercept the data in transit and access a network. A doctor remotely accessing patient records poses the risk of leaking that information to unintended parties, so it is extremely important to encrypt all data that is transmitted over the Internet.

CrossTec Remote Control provides the highest level of encryption in the remote control software industry. Encryption is the process of converting data into an incomprehensible form, and ensures that any efforts to interpret intercepted transmissions will fail. Every CrossTec connection is protected with the government standard 256-bit AES encryption, the most current method of securely transmitting data over the Internet.

Accountability
When using remote control software on a network, information is constantly being accessed by numerous individuals. In the event of an intrusion, it is nearly impossible to identify who accessed what information without the ability to log remote sessions. With CrossTec, every Client logs and documents all Remote Control activity to the Event Log of the Clients machine. This is beneficial for investigating intrusions or suspected malicious activity.



Experienced hackers can simply go in to these local logs and erase their footsteps, so there is no record of them ever being on the Client machine. The CrossTec Client can provide a solution in this scenario by centrally logging all activities to a secure location that is password-protected. Attackers cannot erase their footsteps without the mandatory administrative password used to access the protected activity log on the network.

With the government enforcing strict punishments for corporate security and confidentiality violations, pinpointing a guilty party may shift the blame from the entire corporation to the specific individual who committed the act.

Summary
Experts recommend that IT administrators conduct security audits and penetration tests to identify potential vulnerabilities to their network. Once identified, these vulnerabilities can be eliminated with additional security, or the replacement of non secure applications.

Remote control software is one type of application that has the ability to threaten the security of a network by creating network vulnerabilities. Remote control applications are widely utilized amongst IT departments for saving time, money, and wasted hours of down time by minimizing time for software support. Having the embedded security to protect remote control sessions ultimately balances that need for network efficiency with security.

More information on CrossTec Remote Control and CrossTec's complete line of integrated network and IT asset management solutions can be viewed at www.CrossTecSoftware.com.

CrossTec Remote Control's Comprehensive Security Features:

- Password protection at Client and Control.
- User present acknowledgement required at Client.
- Connection audit trail.
- Disable file transfer or specific files and directories.
- Limit functionality depending on which workstation is connecting.

- Allow a Control to watch only.
- Restrict file transfer to specific drives, directories and files.
- Dial-back to different numbers according to password.
- Restrict connections to named Controls.
- Customize Control and Client profiles to enable and disable virtually every feature depending on the security level of the signed on User.
- Set Unique Security Keys on both Control and Client.
- Integrates with existing NT profiles & security.
- DES/AES Encryption.