SANS ANALYST PROGRAM

Sponsored by Netop

Compliance and Security Challenges with Remote Administration

A SANS Whitepaper – January 2011

Written by Dave Shackleford

Introduction

Remote administration of IT systems is not a new concept. Over the years, many organizations have looked for ways to make systems administration and troubleshooting more efficient. Remote administration offers a cost-effective way to add systems management capabilities while reducing travel costs and minimizing downtime.

There are many types of remote administration tools and methods available from which organizations can choose. Some are built into operating systems, like Microsoft's Remote Desktop capability,[1] while others are available as commercial or open-source solutions, such as Virtual Network Computing (VNC).[2]

There are, however, many shortcomings associated with most remote system administration tools. For example, many tools do not scale well. It's difficult for administrators to work across fast and slow network links in a secure manner.

Another major consideration with remote administration tools is multiplatform support. Most organizations today run a variety of applications and operating systems, including Windows, Linux, and Mac OS X—all of which need to be supported. They also need remote support for mobile platforms such as the iPhone and Blackberry.

Using separate tools with varying capabilities and performance levels for each of these systems makes remote administration impractical. It also makes the organization less secure because each administration system and corresponding administration tool presents numerous authentication, encryption and access challenges that fall under multiple regulatory requirements.

To begin with, remote administration means IT users may have super user access to the systems being administered—systems that may be processing and storing financial and other personal data on customers. Employees, contractors and vendors may all be entrusted with administrative access to ATMs, kiosks, store systems, internal systems and remote end points. They can also be doing so from their own mobile devices, such as the iPhone, which the organization may or may not have approved.

Remote administration is subject to the same laws and requirements found in most privacy regulations. This paper focuses on remote administration of systems with regulated data falling under the Payment Card Industry Data Security Standard (PCI DSS). Like other regulatory requirements, DSS is now specifying access controls, encryption, multifactor authentication and vulnerability management as they apply to remote administration tools and processes where payment cards are processed.

[1] http://en.wikipedia.org/wiki/Remote_Desktop_Protocol
[2] http://en.wikipedia.org/wiki/Virtual_Network_Computing

Compliance Control Points

It is not uncommon to have numerous employees and nonemployees accessing networks, devices and applications remotely for legitimate business reasons. For example, many vendors are permitted to access applications for troubleshooting and remote support of their solutions. Distributed network architectures with remote offices spread out over large geographic areas have also given rise to remote administration. Many of these offices are devoted to specific business functions, such as sales or marketing, but they still need support. In addition, many retail and financial businesses have point-of-sale (POS) systems or ATM machines with network connectivity in remote locations, all of which need to be accessed from afar by IT staff for updating and troubleshooting.

Another obvious use case is teleworkers, or remote employees, who work from home full time or part time—or who work from the road due to travel requirements. Thanks to the United States government's Telework Enhancement Act of 2010, the number of teleworkers will continue to grow.[3] Their systems also need remote troubleshooting and administration. They will need to be patched and have their configurations kept up-to-date; applications will need to be updated for partners and employees; and vendors will need a secure method of gaining access to internal systems from afar.

Another strong use case for remote administration security is IT staff logging in with administrative privileges when they are off premises, even from smart phones, to manage or troubleshoot servers and end point systems inside the organization. Figure 1 illustrates one application for the iPhone that can be used for these purposes.

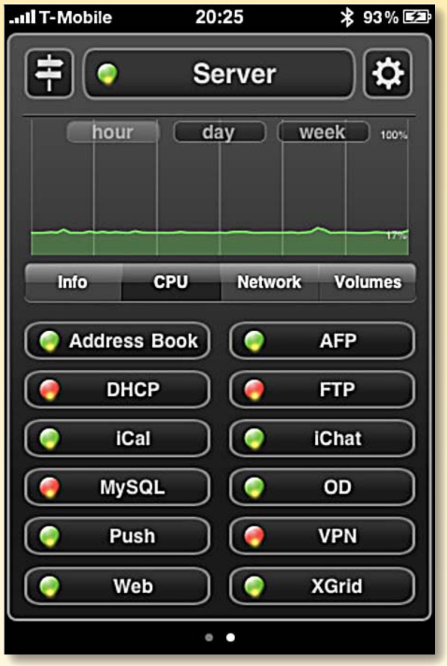

Figure 1. This remote server administration application is sold in iTunes store.[4]

[3] www.chcoc.gov/transmittals/TransmittalDetails.aspx?TransmittalID=3246
[4] http://itunes.apple.com/us/app/server-admin-remote/id300347476?mt=8

If any of these systems being remotely administered have sensitive data on them or can access sensitive data, compliance rules apply. Most privacy compliance mandates, including the PCI DSS, the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley and others, have specific or implied requirements around controlling and monitoring who can access and modify systems that house or interact with sensitive data—including maintaining audit trails of all access to sensitive data and critical systems.

Although the PCI DSS requirements are fairly explicit, they represent the intent of many other compliance mandates and regulations, all of which focus on a baseline security standard to adequately protect sensitive data. PCI DSS requirements that impact remote administration fall into several categories, including encryption, roles and access privileges, authentication, configuration management and logging. The specific requirements of the PCI DSS are referenced in the following sections. In most cases other compliance mandates can also be satisfied with similar controls.

Encryption

For communication between different types of systems, ensuring proper encryption key exchange and use of well-known, highly-scrutinized encryption protocols and standards are paramount. Any weaknesses in the implementation or technology used could lead to an attacker discovering the encryption keys and breaking them to intercept and potentially modify sensitive data.

PCI DSS version 2.0 Requirement 4, Encrypt transmission of cardholder data across open, public networks, specifies that strong encryption should be in place in payment card environments. Requirement 4.1 is applicable for remote access and remote administration scenarios, because these could easily be occurring over the Internet or wireless networks—for example, when vendors connect into the environment or support teams work with remote staff on the road or at home. PCI DSS section 4.1 states the following:

> ***4.1:*** ***Use strong cryptography and security protocols (SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks***

With many widely used remote administration tools, meeting PCI DSS requirements could be problematic. Most built-in, free or open-source remote administration tools do not have adequate cryptographic key management and verification measures to suit auditors. Neither do they support strong, tested cryptographic algorithms. For example, many products incorporate Microsoft's Remote Desktop Protocol (RDP) but do not distinguish between a low encryption level (40-bit) and a high-encryption level (128-bit). Although RC4 is a trusted encryption method, the 40-bit method is not sufficient for PCI compliance and does not meet general best practices; whereas, the 128-bit method does have sufficient key length. Some low-cost remote administration tools offer 128-bit AES encryption to secure the connection between host and client systems. However, many of these types of programs don't allow for customization or easy manipulation of the keys used to negotiate the connection. For organizations that need strict control of key lifecycle (creation, maintenance and revocation), management of specific keys will need to be implemented, either with add-on management technologies or as part of their remote access applications.

Another common tool for remote administration, Virtual Network Computing (VNC), is used in many forms. One of them, TightVNC, only encrypts VNC passwords with 56-bit DES (no longer considered secure), and all other traffic is sent unencrypted. UltraVNC, another free VNC option, can leverage open-source plugins from the Data Stream Modification (DSM) Plugin system for encryption, but these are neither updated often nor supported in any way. One commercial version of VNC, RealVNC, does offer strong encryption with 256-bit AES; however, it lacks the granularity in assigning rights and privileges that is required in some large, enterprise environments.

Another critical encryption component for a remote administration tool is key exchange. Section 4.1.b of the PCI DSS standard states:

> ***4.1.b: Verify that only trusted keys and/or certificates are accepted***

Key exchange allows both sides of the session to securely transfer encryption keys to create an end-to -end encrypted tunnel for communications. The common standard for best practices today is 2,048-bit RSA keys exchanged using Diffie-Hellman or another secure key exchange method. Any remote administration tool used to connect to systems storing, processing or transmitting payment card data should adhere to best practices for key exchange when establishing encryption for the connection.

The third major element of any remote administration tool's encryption capabilities should be verifying message integrity. This is often accomplished by using hashing algorithms such as MD5 or SHA-1. Because both of these protocols have been shown to have demonstrable weaknesses, however, stronger hashing algorithms such as SHA-256 should be implemented. Currently, the PCI DSS does not mandate the use of a specific hashing algorithm; instead, it relies on current knowledge of security best practices for meeting compliance.

Access Roles and Privileges

PCI DSS Requirements 7.1 and 7.2 focus on restricting access to systems and applications in the payment card environment to users with well-defined roles. One common problem with remote administration tools is the lack of granularity in assigning rights and privileges for performing only specific actions. Remote support teams and vendors are commonly granted administrative privileges to systems, even if this level of access is not required. Section 7.1.1 of the PCI DSS requires:

> ***7.1.1:*** ***Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities***

PCI DSS compliance dictates that organizations use demonstrable controls around how the remote administration software is installed, what privileges its users have, what user context the software will operate in, and what individual access credentials will be required for all privileged users. In addition to the control of administrative users and privileges, specific delineation of a user's role is necessary for the access rights granted, as required in section 7.1.2:

> ***7.1.2:*** ***Assignment of privileges is based on individual personnel's job classification and function***

Consider a system that requires remote access by both internal IT support teams and outside vendor support. Internal teams may require much more extensive access in order to patch the system, change operating system configuration settings, and so on. An outside vendor will likely require access only to particular settings related to specific installed software that they are troubleshooting. As a result, any more privilege would be in violation of the standards. Privileges for remote administration access need to be granular enough to comply with a need-to-know access policy, as well as be demonstrable for audit and compliance.

To maintain this policy, PCI DSS mandates the use of a "deny all" security posture unless a specific need exists for the user to have access:

> ***7.2:*** ***Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed***

To verify this, a PCI auditor would need to verify that all defined remote administration roles had no access to begin with and that specific privileges are added as needed. Most remote administration tools do not allow for granular role definition to begin with, and even those that do may not start with a "deny all" role definition that builds from this posture.

Strong Authentication

Several requirements of the PCI DSS call for the use of technologies to protect authentication to any systems or applications within the payment card environment. The primary requirement that addresses authentication specifically is Requirement 8, Assign a unique ID to each person with computer access. The first section of Requirement 8 specifically mandates the use of unique User IDs:

> ***8.1:*** ***Assign all users a unique ID before allowing them to access system components or cardholder data***

This means that each remote administrator will require a unique User ID when connecting to systems that interact with payment card data.

In many traditional support scenarios, IT administrators connect to a user's system using a local Administrator account. Many POS and retail terminal technologies also have a common local account that remote technical support teams use for access (over a web-based interface or using Secure Shell [SSH] connection). To satisfy PCI compliance, each administrator needs to provide a unique username for remote administration to any system in scope for PCI. Unfortunately, many embedded systems, for example, POS terminals, do not provide native support for centralized user account repositories like Active Directory or another Lightweight Directory Access Protocol (LDAP) store. This can be an issue because creating and maintaining unique local usernames and passwords is difficult. Without proper management, organizations have old or rarely-used accounts with too many privileges they don't know about on their systems. Particularly in large organizations, centralized account creation, maintenance and deletion are important protections for account lifecycle procedures and maintenance.

The next section of PCI DSS Requirement mandates the use of an authentication secret:

> ***8.2:*** ***In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:***
>
> - ***Something you know, such as a password or passphrase***
> - ***Something you have, such as a token device or smart card***
> - ***Something you are, such as a biometric***

For remote administration users, this means any authentication to systems needs to consist of a unique username and something else, such as a password, a fingerprint, or a token or smart card of some sort. Unfortunately, most remote administration tools cannot accept anything but passwords, which is still the most common authentication technique in use today.

To protect authentication passwords, PCI DSS 8.4 requires the use of "strong cryptography" for password storage and transmission:

> ***8.4: Render all passwords unreadable during transmission and storage on all system components using strong cryptography***

The PCI Security Standards Council's definition of "strong cryptography" specifies particular algorithms such as AES (128 bits and higher) and RSA (1,024 bits and higher).[5] Many remote administration tools do not provide this level of security for transmission of data, as previously discussed. In addition, most remote administration tools with proprietary password storage do not meet this requirement. For example, many versions of VNC store passwords on Windows systems as a weak hash (often using DES encryption or a variant) in a registry key.

For any remote administration originating from outside the network, more than one of the methods specified in Requirement 8.2 is called for in what is known as two-factor or multifactor authentication. PCI DSS requirement 8.3 states:

> ***8.3: Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties***

For remote administration of a system by a vendor, service partner or off-site IT administrator, the administrator must use a password and some additional form of authentication, such as a token with changing passcode values or a smart card with an embedded digital certificate. For example, a vendor providing remote support for POS terminals or an IT support member accessing a system running commercial payment processing software would need more than just a password when remotely administering such systems. Microsoft's Remote Desktop can support smart cards and passwords, whereas most VNC versions support nothing other than passwords. To use these tools in environments where compliance mandates apply, additional controls may be needed.

[5] www.pcisecuritystandards.org/security_standards/glossary.php#S

Patching, Logging and Auditing

In payment card systems, all software components need to be patched and updated in a timely manner. PCI DSS section 6.1 requires:

> ***6.1: Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release***

Remote administration tools that are components of the operating system may be more easily managed and maintained, because patches for these components are usually supplied with OS patches by the same vendor. However, organizations using third-party tools need to ensure that their remote administration software is patched and updated. This process usually requires obtaining patches from the specific vendor or open-source team and applying them separately from traditional OS patches.

In addition to patching, PCI DSS Requirement 10 calls for a number of auditing and logging controls to monitor who has access to sensitive data and protect against tampering. Specifically, Requirement 10 includes:

> ***10.2: Implement automated audit trails for all system components***
>
> ***10.5: Secure audit trails so they cannot be altered***
>
> ***10.5.2: Protect audit trail files from unauthorized modifications***

Requirement 10.2 includes a number of specific events that should be logged, including all privileged user access, invalid logical access attempts, and individual access to cardholder data.

Although operating system and application logging can be enabled properly for many of these, there may be some discrepancies in how remote administration tools generate logs or interact with existing logging and audit mechanisms. For example, successful authentication via VNC installed on a Windows system may not generate a Windows event, and remote graphic control of a system may not generate logs if a user simply copies data elsewhere or accesses resources in a "read-only" fashion.

Putting It All Together

To successfully meet PCI DSS and other compliance mandates, a remote administration solution should:

- Meet strong requirements for encryption and authentication.
- Allow flexible use of two-factor authentication tools such as smart cards and hardware tokens.
- Provide for granular role definition and privilege/permission assignment.
- Facilitate the need for detailed audit events for all actions taken during a remote administration session.
- Encompass multiple operating platforms, such as Microsoft Windows, Mac OS X, and UNIX/Linux variants, and allow for simple patching and updates.

In order to show how all these functions should work together, the following sample remote administration scenario includes all of the security controls needed to meet best practices and compliance requirements.

> ACME Corporation is a midsized company that sells fine widgets at 200 retail locations throughout North America. From its central headquarters, five IT Support team members maintain support for the organization's retail stores, 200-employees at the main office, and another 30 employees who work from home and take phone and Internet orders for widgets.
>
> The home-based employees use their own computers running a mix of Mac and Windows operating systems, while all the retail stores run Windows systems and have embedded Windows POS kiosks that allow customers to make purchases on their own and create frequent shopper profiles, which are stored for promotional and marketing purposes. The company currently falls under PCI Merchant Level 1 due to the large number of credit card transactions they process annually.

Given the size of the organization, troubleshooting and upgrade operations are frequently handled remotely. In addition, the software running on the POS terminals in the stores occasionally needs to be accessed by vendor technical support personnel. The team has installed remote administration software that works on Windows and Macs and configured the following parameters for the software:

- The organization uses Microsoft's Active Directory for centralized user authentication. The remote administration software support has been configured to look up provided user credentials in a Windows Domain Controller. The IT Support team members are all in a privileged domain group that allows them to access all systems in the company and perform patching and configuration tasks.
- The team previously used OpenSSH for remote access and had specific RSA 2,048-bit keys configured for authentication. The remote access program is configured to use Diffie-Hellman key exchange with the configured RSA 2,048-bit keys. The remote session is protected using 256-bit AES encryption for the tunnel.
- Roles are defined for IT Support and vendors. The IT Support team is allowed full access to the systems but no access to payment card applications or related storage. The outside vendor role is permitted access only to the payment card application on the POS terminals but no access to any data in those applications.
- In addition, the vendor role requires the use of a second factor authentication method. The system is configured to use a built-in RADIUS server and hardware token when these users access the system.
- Patching for the remote administration software is automatic for all home user systems and is manually initiated for POS terminals from a central console after testing. The software will only accept digitally-signed patches from the remote administration software vendor.
- The remote administration program keeps extensive logs, which are automatically sent to a central server. This data is then synchronized with existing log management and SIEM tools. The software can also record the entire remote administration session for playback, but this is only enabled on POS terminals for vendor access.

Figure 2 is a diagram of ACME's remote administration structure:

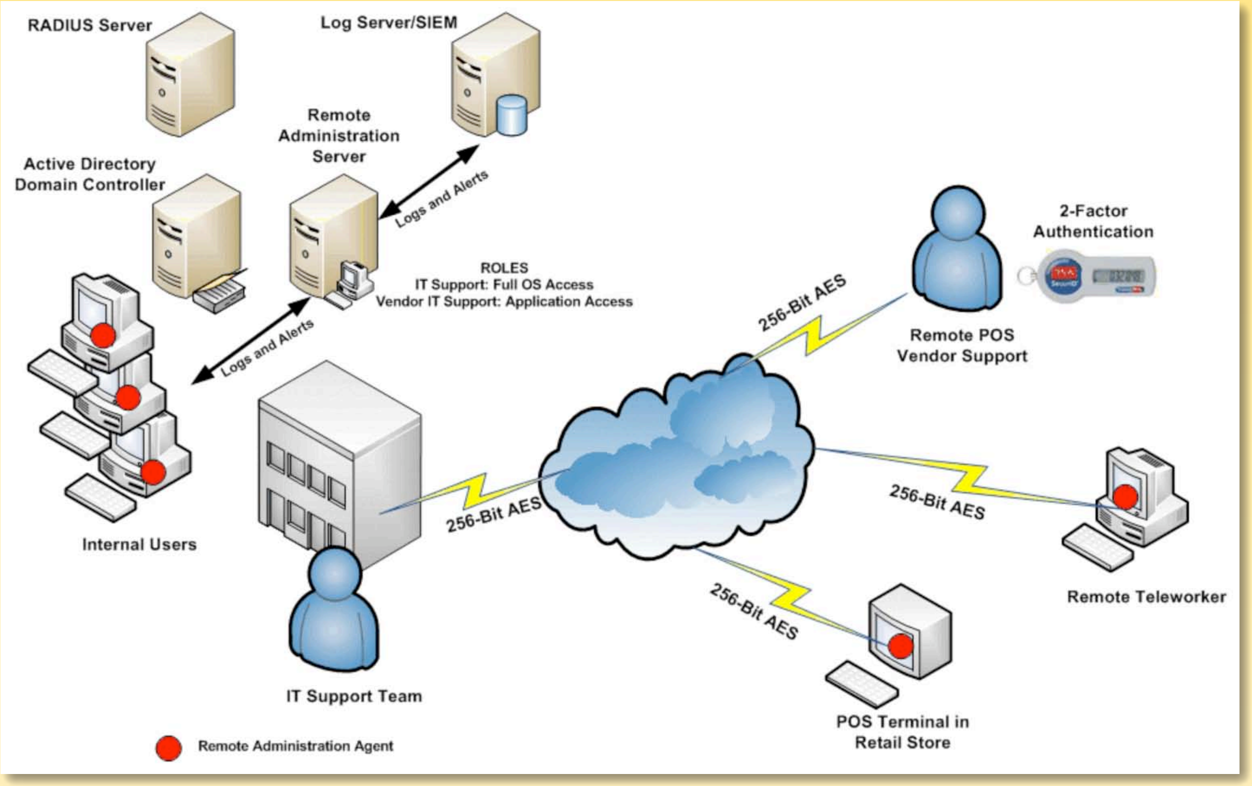
RADIUS Server
Log Server/SIEM
Remote Administration Server
Active Directory Domain Controller
Logs and Alerts
Logs and Alerts
ROLES
IT Support: Full OS Access
Vendor IT Support: Application Access
2-Factor Authentication
256-Bit AES
Remote POS Vendor Support
Internal Users
256-Bit AES
256-Bit AES
Remote Teleworker
256-Bit AES
IT Support Team
POS Terminal in Retail Store
● Remote Administration Agent

Figure 2: A Sample Remote Administration Architecture

By implementing this remote administration software with robust security in place, the IT Support team at ACME is able to meet PCI compliance requirements and easily manage and maintain all systems within their environment, whether local or remote.

Conclusion

Remote administration is important for improving IT team efficiency in managing and maintaining systems throughout distributed environments in a cost-effective manner.

For systems in environments that need to meet and maintain compliance requirements, remote administration software must have strict security controls. Programs used to facilitate remote administration must include strong encryption, robust authentication, granular role definition and privilege assignment, along with auditing and logging capabilities in order to meet security best practices and compliance mandates. Remote administration programs should also be patched and updated easily in a trusted manner that doesn't require significant manual effort.

Many remote administration tools in use today may not offer these capabilities. Commercial third-party products, such as identity and access management tools, can also be developed to include remote administration compliance. Remote access tools, themselves, are also improving their security. Organizations looking for security and compliance capability within their remote access tools should consider how strong those features are and how well they meet compliance and best practices.

About the Author

Dave Shackleford, founder and principal consultant with Voodoo Security, is a SANS analyst, instructor and course author, as well as a GIAC technical director. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert, and has extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft, CTO for the Center for Internet Security.

SANS would like to thank its sponsor

Netop