Goverlan v7

Security Information

PJ Technologies, Inc.®
Software Solutions for IT Professionals

Synopsis

The Goverlan Remote Administration Suite v7 and the Goverlan Remote Control v7 software products are powerfull tools. If you are considering the purchase of Goverlan, or if you already own Goverlan and need to implement it, you may require a better understanding of how secure this solution is.

Our products have been designed to answer the highest security requirements of corporate networks. This paper is an overview of the security model and architecture implemented in Goverlan, including its encryption, authentication and authorization mechanisms.

Table of Contents

Publication Information

This document was written by Pascal Bergeot, Chief Technology Officer of PJ Technologies, Inc.

Published by
PJ Technologies, Inc.
2655 S LeJeune Road S1001
Miami, FL 33134

Overview

Goverlan is a software based solution which is installed on each administrator's machine. It is designed to be implemented within your corporate infrastructure with minimal changes involved.

Our solution doesn't use a third party web-service tier which needs to process its own authentication and authorization. Instead, Goverlan uses the native Windows security layer to authenticate and authorize every transaction.

The Goverlan Agents, which are used to provide remote administration services to the Goverlan Management Console, are installed on each client machine (this process can be automated by Goverlan). Every communication between the agents and the console is encrypted and securely authenticated before being processed.

Securing Enterprise User & Desktop Management

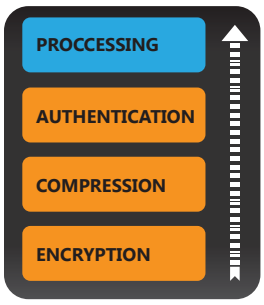
An important aspect of the Goverlan Security Model is that no proprietary security or authentication process is done while executing a task in Active Directory or on a remote machine. Every transaction is performed under the credentials of the Goverlan user (or specified alternate credentials) and is approved/rejected and audited by the native Windows security layer. If a user doesn't hold the necessary privileges to perform an action, Goverlan simply returns an Access Is Denied message.

Essentially, Goverlan doesn't provide its user with any more privileges than the ones allocated to them in Active Directory.

Encrypted Communication and Secure Authentication

Most remote administration tasks such as software deployment, remote assistance or asset management require communication between the client's machine and the administrator's machine.

The Goverlan agents (the software agents installed on the client machine) directly communicates with the Goverlan Management Console (installed on the administrator's machine) via a single TCP port (by default, port number 21159). There is no middle web-service tier involved between the administrator and the client.



To ensure a secure connection and protection against malicious hacking, our communication protocol encrypts all data transmitted between the client and the administrator at the lowest level. Goverlan uses the 128-bit RC4 stream cipher* from RSA Security.

Once the data frame is decrypted on the client side, the frame is then securely authenticated using Microsoft SSPI (Security Service Provider Interface). The Microsoft SSPI Technology allows client and server to establish and maintain a secure channel, provide confidentiality, integrity and authentication. Using SSPI, Goverlan guarantees the identification of the administrator to the client and impersonates the administrator's credentials locally to authorize the request**.

Note: You can view the information of the encryption cipher used during a connection to a client machine in either the Goverlan Management Console's System Information window or in the Goverlan Remote Control's Encryption Information section of the Optimization tab.

** "In cryptography, RC4 (also known as ARC4 or ARCFOUR meaning Alleged RC4 is the most widely-used software stream cipher and is used in popular protocols such as Secure Sockets Layer (SSL) (to protect Internet traffic) and WEP (to secure wireless networks)..." **extract from Wikipedia***

*** Authentication via SSPI is not used during a remote assistance session by design since it is the client which places the request to be connected.*

PKI Compliance - Using Smart Card Logon

Some of our clients, in particular, financial institutions and the U.S. military, have a highly secure and lock-down infrastructure that uses Public Key Infrastructure (PKI). Smart Card Logon is used exclusively for authentication.

Goverlan fully supports Smart Cards. With Goverlan, you can authenticate and authorize a task using a smart card logon certificate. The Goverlan Remote Control product supports Smart Card Logon Redirection, a process by which the administrator can use his/her local smart card reader to execute an interactive logon on a remote machine via a remote control session.

Centralization

A large number of settings can be used to fine tune the behavior of Goverlan both on the client and administrator's machine. For instance, machines can either be configured to prompt the local user for approval before a remote control session is initiated or not to display any visual notification.

These settings can be controlled centrally using a Scope Action or a Group Policy Object. If these methods of distribution are not considered secure enough for your environment, they can also be distributed and enforced using the Goverlan Central Server.

Auditing & Traceability

Accountability and traceability are essential to a remote administration solution. The Remote Control and Remote Assistance features of Goverlan provide an audit trail of every session initiated on a machine. Goverlan records an audit event in both the Windows application event log and in a proprietary log which can be queried remotely. Optionally, an audit event can be registered centrally in a log file, via email notification or via the Goverlan Central Server.

During a remote control session, the administrator can also record a video of the session on their local machine.

Note: Other Goverlan remote administration features, such as domain account management, are not recorded and audited by Goverlan. However, Microsoft's Windows Security Auditing features can be used to record most of these events.

Remote Assistance Security

The Goverlan Remote Assistance feature allows an administrator to take control of a client's machine no matter where they are. It is designed to assist users connected to a public network.

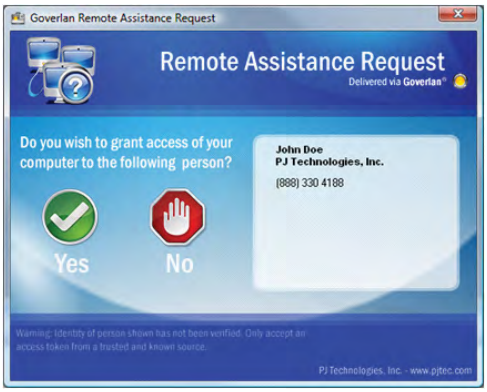
Unlike most remote assistance solutions on the market, Goverlan doesn't use a third party web-service tier between the administrator and the client. The implementation of the Goverlan Remote Assistance session is very simple and straightforward, alleviating the security requirements involved in other more complex solutions.

The corporate network hosting the administrator's machine is configured to accept connections on a particular network address and port number and to port-forward the connection to the administrator's machine. The administrator then generates an encrypted Remote Assistance Request token which is emailed to the client.

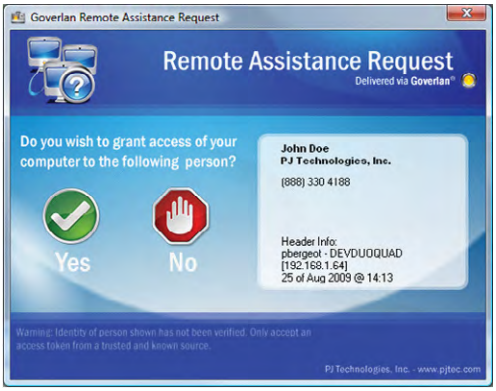
The client then downloads and installs a light-weight, passive Goverlan Remote Assistance Agent, opens the token and approves the connection. The Goverlan Agents on the client machine connects to the pre-configured corporate network address and establishes a connection to the administrator's machine. All communication to/from the client is encrypted (see *Encrypted Communication and Secure Authentication*).

Securing the Remote Assistance Transaction

The encrypted Remote Assistance Request token sent to the client provides complete information on the identity of the source for review and approval. By default, the identity information displayed is what is provided by the administrator, but it can be opened in extended mode which shows the username, machine name and IP address.



Default View



Extended View

Additionally, a token can be configured with a password or a pin which the client has to enter in order to continue with the request.

Conclusion

The Goverlan Remote Administration Suite v7 has been designed to fulfill the IT needs of many diverse business cultures while preserving security and integrity. It does this by integrating with and using the existing security infrastructure instead of adding a proprietary layer of authentication and hosted credential stores. Every communication is encrypted and then authenticated before being processed. Every remote control session is audited and can be traced. Finally, the security settings controlling the behavior of Goverlan can be securely distributed and controlled centrally.

We believe that the level of security provided with the implementation of Goverlan surpasses the requirements of most companies. Please contact me if you have any questions/concerns or have a security requirement which is not being currently addressed.

Pascal Bergeot - Chief Technology Officer
pbergeot@pjtec.com

PJ Technologies, Inc.