



Mangomind and the Security of Your Data on the Internet

Mangomind and the Security of Your Data on the Internet

Mangomind opens a whole new avenue for effectively conducting business. Mangomind lets you move your data to the Internet, yet have the access to the data appear as if it were local. Now your mobile or stay-at-home employees will be able to extend their offices, your B2B partners can collaborate without having to email multiple copies of documents back and forth, and setting up short lived directories for access by consultants becomes a snap. But even with these compelling features, you are not going to put your data on the Internet if you can't be sure that only you control who can see it! That is why Mangomind has been designed to offer the best in class security architecture. We like to think of it as the Swiss Bank of Internet storage. It is so secure, that not even the administrators of our disk farms can view your data. Only you and those you specifically invite, have the keys to the vault.

The Mangomind security architecture has two main components:

1. Connection Authentication

Connection Authentication validates and ensures that when a Mangomind client computer connects to the Mangomind server, both are who they say they are. This means that someone else cannot impersonate the Mangomind server, tricking your Mangomind software into sending it your data. A Mangomind client that has not been invited to the drive cannot trick the Mangomind server into sending it your data. This authentication is performed through a challenge and response protocol using the RSA Public/Private key pairs of both parties. Every new connection must successfully complete the challenge protocol.

2. Data Encryption

Mangomind encrypts your data using RSA 128-bit RC5 data encryption keys. Your data is encrypted with these keys on your Mangomind client just before it is sent to the Mangomind server. Once on the server, the information remains encrypted. At no point after leaving your computer can anyone view the clear text versions of your files. Most importantly, Mangosoft employs a unique key management system so that the usable keys are only available on the client computers. Only the client computer can download and decrypt the data. Since the usable keys are not available on the server, no one can view your files by looking at the data contained there. Even the names of your files are changed to meaningless characters strings on the server, so as not to hint at their contents.

By choosing Mangomind, you can be certain that the data you have stored on the Internet is just as secure, if not more so, than the data stored on servers in your private LANs. If you would like to understand more about Mangomind security, the next sections describe the Connection Authentication and Data Encryption components in greater detail.

Connection Authentication

Public/Private Key Primer

Public/private key pairs are a set of large encryption keys that are commonly used to validate identities. The keys are asymmetric, or one-way keys. This means that one key cannot be used to both encrypt and decrypt the same data. Data encrypted with one of the keys can only be decrypted with the other key. A public key, as the name implies is public; anyone in the world is allowed to know your public key. The private key, as the name suggests, should never be revealed. With this in place, anyone can take a string of data and encrypt it using your public key, and send it to you. Only you will be able to use your private key to decrypt the data.

Your RSA Public/Private Key Pairs

To perform the challenge and response protocol, your Mangomind client needs a RSA public/private key pair for each Mangomind drive you are using. The Mangomind software on your computer generates these keys when you first a new drive. The process is below:

First, you receive an invitation email to join a Mangomind drive. When you process your invitation, you do so on a HTTPS web page using the Secure Socket Layer (SSL) to access the Mangomind server. The Mangomind server is registered with Verisign. SSL asks Verisign to validate that you are communicating with the Mangomind service.

Once satisfied that it is communicating with the Mangomind server, the Mangomind software on your computer must prove to the server that it is presenting a legitimate invitation to a Mangomind drive. Your invitation to join a Mangomind drive contains a password that can only be used once. It also contains information specifying the drive you want to join, and which user you are. The Mangomind server validates that the specified drive exists, that the specified user has been invited but not yet joined the drive, and that the password you are presenting is valid.

Once all of the information has been confirmed, the server informs the client that the invitation has been accepted and transmits it public key to the client. The Mangomind client software now generates a public/private key pair. The public key is transmitted to the server and the private key is encrypted and saved on the client computer.

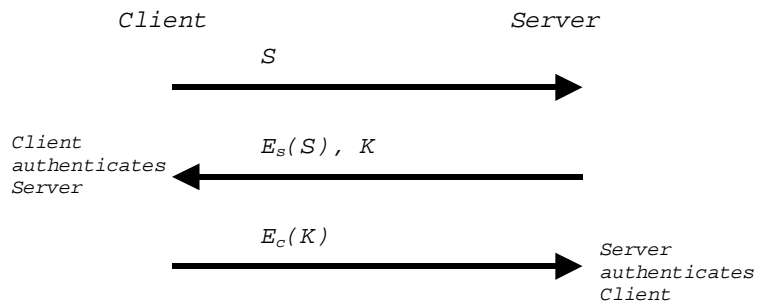
From this point forward, each new connection made to the Mangomind server for this drive will be authenticated using the key pairs.

The Challenge/Response Protocol

The challenge/response protocol is a mutual authentication protocol. This means that the protocol lets the client be certain that it is connecting to the server, and the server is certain that it is receiving the connection request from a valid client.

The client generates a cryptographically random string S , and sends it to the server. The server encrypts the random value using its private key and returns the result, $E_s(S)$, to the client. The client decrypts $E_s(S)$ using the server's public key, obtaining $D_s(E_s(S))$. If that value is equal to the original S , the client is satisfied of the server's identity.

Similarly, the server picks a random string K , sends it to the client, which returns $E_c(K)$ to the server. The server checks that $D_c(E_c(K))$ equals K and it thereby satisfied with the client's identity.



Data Encryption

The Mangomind client software uses RSA's RC5 algorithm to encrypt your data. This is a fast and cryptographically strong algorithm. There are two aspects of the Mangomind security architecture to consider with regard to data encryption:

1. How the keys are stored
2. How Mangomind uses the RC5 algorithms to encrypt and decrypt your data.

Key Storage

For each user on a Mangomind drive, a copy of the encryption key for the data is stored on the Mangomind server. Each copy has been encrypted with the public key of the user that placed it there. This means that only the user's private key can decrypt the key, and the user's private key can only be found on the user's computer.

When the encryption key for the data changes, the new data key must be added to the server storage for each user. The user that changes the data key has access to the public keys for each of the other users. This user encrypts the new data key with his public key and places it on the server. The same user then repeats this process for each user of the drive, using their public keys.

Encrypting and Decrypting Your Data

When you create a new file on your Mangomind drive, it is saved on your computer for caching purposes. The address of the key that will be used to encrypt the file is stored in metadata for the file. The file is then compressed, encrypted and transmitted to the Mangomind server in variable sized blocks; the block size depends on how well they compressed.

When you open a file that is not cached on your computer, your Mangomind client software requests that it be downloaded from the server. The data is delivered in the same-sized blocks used when uploading the file. The client software determines the key for the file from the metadata. If the key is not available locally, the client retrieves the key from the server and decrypts it using the client's private key. Now the key can be used to decrypt each block as they are read off the wire. The blocks are decompressed and returned immediately to fulfill read requests from your application. Should there be a loss of your Internet connection, the download can be restarted at the last chunk that had been processed.

Your Identity Profile

The design of the Mangomind security architecture guarantees that the keys for decrypting your data can only be used on the client computers. This is very powerful. Even Mangomind administrators with access to the disk farms holding your data have no way to view your data. Consequently, should something happen to your computer such that your keys are permanently lost, there would no longer be any way for you to view your data on that computer. Your Mangomind user id would become useless and another superuser on your drive would need to issue you a new invitation.

To protect yourself from this situation, we strongly recommend creating an Identity profile for each Mangomind drive you join. With this file, you can establish your security information on any computer with the Mangomind client software installed. If your computer's hard disk stopped functioning, you could replace the disk, reinstall the Mangomind client and provide your Identity Profile to restore access to your Mangomind drive. This is also a convenient way for you to access your drive from multiple computers. You can join the Mangomind drive on your work computer, and subsequently use your Identity Profile to access the drive from your home computer as well.

