IST Information Services & Technology

Home / Services And Resources / Backup

TSM at MIT: Security Notes on TSM (Tivoli Storage Manager)

On this page:

Overview

If you have sensitive data on your hard drive, you should be aware of the relative level of security provided by Tivoli Storage Manage (TSM) before you decide to use the service for backing up your data. Members of MIT's IT/Integration Team and the Service Team have spoken to representatives from Tivoli, a subsidiary of IBM, to discuss the security level in the product. In this document, we'd lik to start with a quick summary of our assessment of security in TSM, and then go into a more detailed explanation. The detailed explanation will start with some issues to keep in mind when evaluating the security level of any client/server software, and then follow up with our assessment of TSM in light of these issues.

Is TSM Secure? - The Short Answer

TSM is designed to authenticate each user using a proprietary challenge-response mechanism, without sending passwords over the network. Presuming that the vendor has not made any serious mistakes in their implementation of authentication, we believe that the TSM system should provide secure authentication without the risk of users' passwords being intercepted on the network. This should thwart the easiest and most common type of attack from network intruders.

By default, the data from users' hard drives, are sent over the wire unencrypted, and could be intercepted by a serious and motivated intruder.

TSM has a feature that allows you to encrypt your data before it is sent over the network. (Data are also stored in encrypted form if this feature is turned on.) If some of your files are sensitive, we recommend that you use the encrypt function of TSM. For more information on the encryption facility, see TSM at MIT.

Alternatively, you could exclude files or directories containing sensitive data from the TSM backups. You must weigh the risks and decide whether some of your data should be encrypted or excluded.

General Security Concerns for Client/Server Software

TSM, a network-based system for backing up data on individual workstations, is a sort of client/server system. Like other instances of client/server server software, there are a number of potential ways that the data handled by the software could be vulnerable to attac by unscrupulous people on the Internet, particularly if there are design problems in either the client or server components of the software. We can group the potential vulnerabilities into four main areas:

- **Exposing the user's password as it travels over the network**
  A client/server system should not send a user's secret password over the network in cleartext (i.e., unencrypted). Since network attackers have access to sniffers that are able to intercept and store passwords sent over the network, running client/server software that transmits unencrypted passwords over the network is almost always unacceptable at MIT.

  Some client/server software encrypts passwords before sending them over the network. If this is done, the software must be carefully designed so that no one can easily break the encryption scheme. If the software scrambles the password in a simple way or uses an encryption key that can be discovered by reverse-engineering the client component, then the password is still vulnerable to attack. Poorly-implemented encryption of a password sent over the network is better than no encryption at all, but once one person has discovered how to break a poorly-implemented scheme, that knowledge is likely to become available to many potential intruders. Well-designed and well-implemented code for encrypting passwords sent over the network can be very secure, but there are many mistakes that a software developer can make that can open up vulnerabilities. Some systems avoid sending a secret password over the network altogether by using tickets (as in Kerberos) or public/private key pairs (as in PGP or RSH). These schemes should be secure, if properly implemented by knowledgeable software developers who avoid making subtle mistakes that open up vulnerabilities.

- **Exposing data (other than passwords) traveling over the network**
  If client/server software does not reveal a secret password while it travels over the network, then the software has avoided the vulnerability most likely to be exploited by intruders. We next turn our attention to the data itself being sent over the network by the client/server software. An unscrupulous user might try to gather the packets containing sensitive data as they go over the network hoping that he will find something interesting or damaging. Or, he might try to "hijack" a session, sending his own packets of information to the server to try to masquerade as the client.

  Both of these techniques are a lot harder than simply discovering a secret password, and a would-be intruder is less likely to go to the trouble of using these techniques. However, for very valuable or sensitive information, it might be worth someone's trouble to attempt such an attack. Also, one cannot rule out the possibility that someday, someone may develop and disseminate a "toolkit" for intercepting data or hijacking sessions that could be used for a specific kind of client/server session.

  These sorts of attacks can be thwarted if all the data between the client and server are protected by strong encryption.

- **Opening a "backdoor" or other vulnerability to exploitation in the software through inappropriate or poor design**
  It is possible for a software vendor to either deliberately or accidentally include a "backdoor" in their software that could open an access path to information on the client machine. A vendor might use such a backdoor to install upgrades, get information about the client, or help the user if the user calls for support. Even if the vendor's intentions are good, such a backdoor is safe only so long as the "secret" is not revealed or discovered by an unscrupulous user. It is also possible for a vendor to make a design mistake that opens up an unintended path to access the client or server software over the network.

  One would hope that a vendor would avoid intentional or unintentional backdoors to their software that might expose their users to network attacks. However, in proprietary software where the source code cannot be examined, and the license precludes reverse-engineering the program binaries, one cannot be absolutely certain that there are not intentional or unintentional vulnerabilities in the software.

- **Vulnerability of the server itself, due to problems outside of the particular client/server package under consideration**
  Even if the particular client/server package under consideration is well-designed and well-implemented for maintaining security, it is still dependent on the protection provided by the operating system running on the server itself. If the server is poorly maintained, or there are vulnerabilities in the operating system that have not been addressed by its vendor, then a potential intruder might break into the server machine itself and thereby gain access to data used by the client/server system.

  In a backup system, data from users' hard drives are stored on disk, tape or other media. Both the server and the media on which the data are stored must be protected in order to protect the data.

How Does TSM Stack Up in the Four Areas of Potential Vulnerability?

- **Exposing the user's password as it travels over the network**
  In our conversations with Tivoli representatives, they have described the authentication system used in their software, which they tell us is "modeled after Kerberos." Their challenge-response authentication design is based on a sound approach. The client uses its password as part of an encryption key, and does not send the password over the network. Each session key is unique, so replaying a session stream will not result in a signon to the server. As we've mentioned, to develop good secure code, it takes a

skilled developer who knows how to avoid several possible mistakes. We at MIT cannot guarantee that the authentication component of the TSM software is free of mistakes, but we believe that there are some skilled developers at IBM who should knov how to do it right.

- **Exposing data (other than passwords) traveling over the network**
  By default, the data from your hard drive are not encrypted as they are sent over the network to the TSM server. If the encryption feature of TSM is not turned on, data backed up from your hard drives are sent over the network as cleartext.

  If your data are sensitive, you should turn encryption on within TSM to encrypt the data. Alternatively, you could exclude certain files or directories from the backup list. You need to make the judgment on the sensitivity of your data and determine if it should be encrypted or excluded.

  It is also worth noting that once you choose to encrypt data to protect the data in transit over the network, your data will also be stored in encrypted form, and cannot be retrieved if you lose the original encryption key.

- **Opening a "backdoor" or other vulnerability to exploitation in the software through inappropriate or poor design**
  We have no reason to believe that there is a backdoor or other vulnerability in the client or server software, but we have no way of proving that such a vulnerability does not exist.

- **Vulnerability of the server itself, due to problems outside of the particular client/server package under consideration**
  At MIT, the TSM servers run on Sun servers, managed by IS&T's Administrative Systems Services Team (ASST), who are responsible for configuring the servers appropriately and applying security patches to the operating system whenever patches become available from Sun. Thus, reasonable efforts are made to protect the servers from known security problems, which should make the risk of intruders breaking into the servers themselves a fairly low risk.

  The data from users' workstations are stored on hard disk staging areas and tape cartridges. The data are not stored in encrypted form unless the encryption feature was used on the TSM client. We believe that reasonable precautions are taken to protect the media. However, for sensitive data, we recommend that you turn on the encryption feature in the TSM client, and then your data will be stored in encrypted form on the staging disks and tape cartridges. This would protect your data from intruders in the event of a break-in to the server or a theft of the storage media.

Back To Top