IBM 2105 ESS / IBM TotalStorage ESS Master Console Remote Access and Call Home Security

Version 5.2

January 18, 2002

Thomas Fiege

IBM
SSD-RAS San Jose
5600 Cottle Road
San Jose, California 95193

Document Control Information

Owner: Thomas Fiege

Owner Userid and Node: Thomas Fiege/San Jose/IBM

Owning Department: DDJA

Filename: enc2_security052.lwp

Location of source file: Shark RAS Documentation Library on SNJLNT02

Documentation Retention: TBD

Documentation Review Schedule: Whenever updated.

Document Review/Approval By:

Name	Dept	Review/Approve	Lotus Notes ID	Date
Steven van Gundy	87TA	Version 3.0	Steven van Gundy/San Jose/IBM	08/14/01
Steven van Gundy	87TA	Version 5.0	Steven van Gundy/San Jose/IBM	09/07/01

Change History

Version	Date	Flag	Summary
Original Version 1.0	07/16/2001	None	Initial Version composed using the existing 2105 security letter, Ed Hickman's input and the actual implementation
Update Version 2.0	07/20/2001	None	Added skelleton, Ferriers' input
Update Version 3.0	07/27/2001	None	Finalized with input from SVG (add privileged access for 2105, grouped items for the technical description)
Update Version 4.0	08/31/2001	None	Added detailed ftp description
Update Version 5.0	09/07/2001	None	Final changes per SVG's request
Update Version 5.1	10/02/2001	None	Removed minor details
Update Version 5.2	01/18/2002	None	Declassified (announced + GA)

IBM 2105 ESS / IBM TotalStorage ESS Master Console
Remote Access and Call Home Security

The following is a description of the security IBM provides with respect to remote access and call home functions in the IBM 2105 ESS / IBM TotalStorage ESS Master Console. There are two types of descriptions. The first is the technical description that is intended for the network specialist and the second is intended to be used for other than a network specialist.

The third part of this document contains detailed information about the ftp process that is used to send PE packages and dump/trace data from the customer site over the Internet to the IBM ftp server.

Technical description:

The IBM 2105 ESS, later referred to as 2105, and the IBM TotalStorage ESS Master Console, later referred to as Console, is designed to conform IBM's Corporate Standard "ITCS204 - Security Standards for Providers of Network and Computing Services" and therefore to ensure maximum security in a networked environment.

Applicable to both 2105 and the Console:

1. All non-trusted network commands and services are either crippled or completely removed (i.e. the Berkeley r-commands, Sun rpc commands, ftp and telnet clients).
2. As recommended in the US Department of Energy CIAC bulletin, all nonessential Internet daemons are either not installed (ftp, telnet), turned off or crippled.
3. All unused Internet ports are disabled.
4. All nonessential TCP/IP commands have been removed.
5. The root user is not a login user.
6. For 2105 and the Console a non-authenticated user does not have access to a command line or shell.
7. In order to gain privileged access to a 2105 or to the Console an expiring challenge/key password is used that ensures that only current IBM employees can gain access.
8. Neither Domain Name Service (DNS) nor any standard TCP/IP services (ftp, telnet) are available for remote connections.
9. The serial port connection from the Console to each attached 2105 is a terminal connection and does not support TCP/IP. It is used for logging into the 2105.
10. The ethernet connection between a 2105 and the Console is used for transfering trace and log information only. The transfer is done via proprietary socket communication, no higher protocols (e.g. ftp, telnet) are available.

Applicable to 2105:

1. The only non-authenticated user (service) cannot access a 2105 over a network.Only direct connection via ASCII terminal or login from the local Console via the serial connection is possible.
2. On 2105, the only privileged user (IBM Product Engineering) has a machine generated password that expires after 7 days. For actually gaining privileged access an expiring challenge/key password scheme is used.
3. On 2105, the WEB server is running as user-nobody, having very restricted access. It is not server-root, which is more typical for WEB servers.

Applicable to the Console:

1. The only non-authenticated user (service) cannot access the Console over a network.Only local login is possible.
2. Remote services connections (dial-in) via the modem connected to the Console only allow logins to the Console and attached 2105s. No customer data can be transfered over the modem. The remote user cannot access the customer's LAN because no network commands are available. The dial-in connection is a terminal connection and does not support TCP/IP.
3. Call Home connections (dial-out) are made over a point-to-point TCP/IP dial-up connection into a secure IBM network. The data transfer is done over a plain point-to-point socket connection using a proprietary protocol over the TCP transport layer.
4. There is no IP traffic between the dial-up adapter and the network adapter installed on the Console. Thus no direct IP traffic is possible between a 2105 and another network connected to the Console via a second network interface (eg. modem/ppp dial-up).
5. The modem connected to the Console is a secured modem: Before presenting a login screen the caller must enter a modem internal password.

In addition, IBM continuously monitors the CERT (Computer Emergency Response Team) bulletins for news about security problems, just to be certain that other people haven't discovered problems with features, functions, operating system components, or program products used by the 2105.

Non-Technical description:

1. An on-site CE only has access to "service menu" functions and must be directly connected via his service terminal or the Console to the 2105, ie. the CE must be physically present where the 2105 and Console is located.
2. Remote access to the customer's network is not possible via modem.
3. TCP/IP functions to access the network have been removed from the 2105 and from the Console.
4. The remote connection into the Console via modem and into the 2105 via serial connection is a "remote terminal" session that does not support TCP/IP functions.
5. No customer data can be transferred from a 2105 to an attached Console.
6. The authentication schemes utilized for connecting into the 2105 and into Console are independant from eachother, ie. successfully authenticating with the Console still requires an additional authentication for each attached 2105.
7. There are two levels of remote access to a 2105:

   1. The Support Level access authorization option is set by an on-site CE. The standard support access password is part of the "Call Home Record" sent to IBM. An optional remote access password is known only by a on-site CE and the customer. User "support" can only view the machine's configuration, settings, and logs.

   2. The Product Engineering (PE) Level access requires a password to be supplied by the customer or an on-site CE. The password expires after 7 days. PE Level access has a higher authority than Support Level access has and can change 2105 configuration and settings. In order to get privileged access to the 2105, PE Level access must overcome an expiring challenge/key password scheme.

8. There are two levels of remote access to the Console:

   1. The Support Level access authorization option is set by an on-site CE. The standard support access password is part of the IBM internal support structure.
   The standard support access password can be changed to be unique for each customer. The support level access does only allow to view items, nothing on the Console and on the 2105 can be changed.

   2. Product Engineering (PE) level access requires authorization by the customer or an on-site CE. The password used is a challenge/key password and expires after 48 hours. PE is a "privileged user" and can change the Console's configuration and settings.

9. Any local or remote system/resource access attempt to the Console is logged, regardless if it was successful or not.
10. Only a privileged user can change the security settings of the Console.

Description and security considerations of the ftp data offload process:

Product Engineering data can be sent to IBM using the Internet and IBM's anonymous ftp server. This option is intended for those customers who desire significantly faster data offload times than is possible using the Console's modem connection, but this process should only be used when there is a network firewall between the ESS Network and the Internet.

1. It is the customers responsibility to provide a secure access to the Internet for the Console. Secure access means the customer providing a ftp firewall server installed between the ESS Network and the Internet.
2. Using the ftp transfer method does not require ftp servers to be installed on the Console or on the 2105.
3. The ftp transfer method has to be enabled and configured on the Console before using it. By default, the ftp transfer method is disabled.
4. The Console can be configured to talk to several kinds of ftp firewalls provided by the customer.
5. Whenever Product Engineering data has been requested by IBM Product Engineering personnel it will be sent from the 2105 to the Console using a proprietary protocol over a TCP/IP socket connection.
6. On the Console, data is stored in a specific directory. It will not be directly sent from the 2105 to the IBM ftp server using the Console as a router. The Console does not have any routing / IP forwarding capabilities.
7. From the Console data is retrieved from the directory and sent using a ftp client to the IBM ftp server via the customer provided ftp firewall server.
   This process takes place automatically and does not require human intervention.
8. The ftp client on the Console can only be used by the automated process. During normal operation the client is not visible and not available from the command line, even for a privileged user.
9. If successfully sent Product Engineering data is erased from the Console.

The 2105 and the Console are designed, and have been tested by IBM, to be secure from unauthorized user access when connected to a network in its default field configuration. Using the ftp data offload process does not change the configuration of the 2105 or the Console.

During data offload the ftp client will be visible and usable on the Console. Therefore it is possible for someone monitoring the 2105's network to use the ftp client and login to other machines on the network. Due to the fact that no servers are installed on the 2105 this exposure is merely theoretical. Under no circumstances can any actual customer data be altered or transferred to, or from the 2105.

The responsibility for network security is the responsibility of the customer's network administrator. It is the customer's responsibility to provide a secure connection between their ESS network and the Internet. Typically this means providing a network firewall between the ESS network and the Internet that supports some form of outbound ftp firewall service while blocking all other inbound forms of network access.

Note: Using the ftp data offload process can reduce the offload time from several hours to approximately 40 minutes. When a secure firewall is used as suggested above the security exposure is mostly hypothetical and limited to the time the Console's ftp client is active.