IBM 2105 ESS
Remote Access and Call Home Security

Version 5.1

October 02, 2001

Ed Hickman

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

Document Control Information

Owner: Ed Hickman

Owner Userid and Node: Ed Hickman/San Jose/IBM

Owning Department: DDJA

Filename: enc1_security051.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 5.0	Steven van Gundy/San Jose/IBM	09/07/01

Change History

Version	Date	Flag	Summary
Original Version 1.0	1999	None	ICreate
Update Version 5.0	09/07/2001	None	Final changes per SVG's request Use Template
Update Version 5.1	10/02/2001	None	now non IBM confidential

IBM 2105 ESS
Remote Access and Call Home Security

The following is a description of the security IBM provides with respect to remote services provided in the 2105 product. There are three sections: First is the technical description of the 2105 Network Security features that is intended for the network specialist; Second is a less technical description that is intended to be used by someone less familiar with networks; Third is a description of the security aspects of the optional high-speed ftp process for sending 2105 product engineering data back to IBM via IBM's anonymous ftp server.

Technical Description

The 2105 is designed to conform to IBM's Corporate Standard "ITCS204: Security Standards for Providers of Network and Computing Services" and network security is a very important part of the 2105's design.

1. All non-trusted network commands are crippled (i.e. the Berkeley r-commands, and Sun rpc commands).
2. All nonessential internet daemons are turned off (as recommended in the US Department of Energy CIAC bulletin).
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 (cannot login).
6. The only privileged user (IBM Product Engineering) has an machine generated password that expires after 7 days. For actually gaining privileged access an expiring challenge/key password scheme is used.
7. The WEB server is running as user-nobody, having very restricted access (It is not server-root, which is more typical for WEB servers).
8. The serial port connections from the modem is a terminal connection and does not support TCP/IP.
9. Remote connections via the modem only allow user logins. No data can be transferred while a user is logged in, and the user cannot access the customer's LAN from a 2105 because no network commands are available, per items 1 through 4 above.

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. The "on site" CE only has access to "service menu" functions and MUST be directly connected to the 2105 and able to view and enter a password displayed on the 2105's Panel.
2. Remote access is controlled by customer or "on site" CE via PASSWORDs.
3. Remote access to a customer's network is NOT possible via the 2105 modem connection.
4. TCP/IP functions to access the network from 2105 have been removed.
5. Remote connection via the modem is as a "remote console" which does not support TCP/IP functions.
6. No data can be transferred from the 2105 when a remote connection is active.
7. There are two levels of remote access:

   Support Level

   - Support Access authorization option is set by "on site" CE.
   - Standard Support access password is part of "Call Home Record" sent to IBM.
   - Optional Remote access password known only by "on site" CE and customer.
   - Support "user" can only view machine configuration, machine settings, and logs.

   PE Level

   - PE Access requires that a machine generated PASSWORD be relayed to a PE by either the customer or an "on site" CE. This PASSWORD will expire after 7 days.
   - The PASSWORD allows the PE to remotely login to a 2105, but without having access to privileged functions.
   - Access to privileged functions requires the ability to respond to a special challenge whose response can only be generated by a proprietary program.
   - Access to this proprietary challenge response generator program is restricted to a small number of designated IBM personnel.
   - The challenge response for privileged functions expires at midnight of the following day.

Security Considerations when using the manual 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 2105's modem connection, but this process should only be used when there is a network firewall between the ESS Network and the Internet.

The exact details of how to configure and use the ftp process is described in other documents. This document deals with the security issues and responsibilities involved when using the manual ftp data offload process to transfer data from the 2105 to the 2105's ESS Network Console, and then forwarding that data via a customer supplied ftp proxy firewall to IBM's anonymous ftp server.

The 2105 is designed, and has been tested by IBM, to be secure from unauthorized user access when connected to a network in its default field configuration. Activating the ftp server temporarily changes the default configuration to allow an authenticated PE user to login to the 2105's ftp server via the network and use ftp subcommands to perform a data transfer. The PE user is the only user who can login to the ftp server, all other users are restricted from using ftp, including root user.

The 2105's ftp server does not use data encryption. Therefore it is possible for someone monitoring the 2105's network to discover the PE password and login to the ftp server while it is active and use the ftp subcommands to alter the 2105's Licensed Internal Code, or modify files used by the 2105's Licensed Internal Code. Under no circumstances can any actual customer data be altered or transferred to, or from the 2105. To prevent any unauthorized activity, it is imperative that there be a firewall between the 2105's local area network and other networks so that ftp usage is restricted to only those personnel who are in the actual vicinity of the 2105 and authorized to be doing the ftp data transfer.

- ✍ All of the IBM product engineering personnel who have the capability to activate the ftp server are fully aware of the small, but manageable security exposure of having the ftp server active. They make every attempt to turn off the ftp server when the data transfer is completed to keep the exposure window to a minimum. If for some reason the PE is unable to login and deactivate the ftp server, it will automatically deactivate 24 hours after it was activated

- ✍ 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 proxy 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 2105 ftp server is active.