Products: R&S Spectrum Analyzer FSP, FSU, FSQ

Instrument Security for
R&S® FSP, R&S® FSU and R&S® FSQ
Spectrum Analyzer

Application Note

This application note describes the different memory types and locations that user information can be stored in a spectrum analyzer R&S® FSP, R&S® FSU or R&S® FSQ, as well as the different ways in which it can be erased/cleared for security reasons.

ROHDE & SCHWARZ

Contents

1 Overview

In many cases it is imperative that the R&S® FSP, R&S® FSU or R&S® FSQ spectrum analyzers are used in a secured environment. Generally these secured environments will not allow any test equipment to leave the area unless it can be proven that all devices capable of maintaining memory have been thoroughly erased. This, in conjunction with the Windows® operating system, requires some measures when the spectrum analyzer has to be transported to a non-secure environment, e.g. for calibration.

This application note describes the types of memory used in the spectrum analyzers R&S® FSP, R&S® FSU and R&S® FSQ and describes a method to maintain security under these conditions. Please note that some of this information is dependent on the revision of the CPU board and the Windows® operating system used in your spectrum analyzer. For purposes of this document, these are divided into "Windows® NT" and "Windows® XP" instruments.

2   Instrument Models Covered

R&S Spectrum Analyzers

R&S® FSP	R&S® FSU	R&S® FSQ
FSP3	FSU3	FSQ3
FSP7	FSU8	FSQ8
FSP13	FSU26	FSQ26
FSP30	FSU46	FSQ40
FSP40	FSU50	

3   Warnings

Be sure that all information stored by the user in the instrument that needs to be saved is properly backed-up before attempting to clear any of the instrument memory. Rohde & Schwarz cannot be held responsible for any lost files or data resulting from the clearing of memory.

In most cases there will be no user prompts to confirm the clearing or deleting of files or instrument memory. Be sure to read this document entirely before proceeding with any file deletion or memory clearing.

4   Battery Information

There are no batteries in the R&S® FSP, R&S® FSU and R&S® FSQ spectrum analyzers other than the one on the CPU board used to power the clock in the chipset and the CMOS-SRAM memory (Windows® NT instruments only).

5   Types of Memory

SDRAM

The R&S® FSP, R&S® FSU and R&S® FSQ spectrum analyzers have 64 – 512 MByte of SDRAM in one or two SODIMMs on the CPU board. SDRAM is volatile memory and it loses its memory as soon as power is removed. **This is not a security concern.**

EEPROM

Each board assembly has one serial EEPROM device. These devices hold 256 Bytes up to 32 kByte and contain information related to the installed hardware, such as board serial number, options, correction constants, etc. and are not generally user accessible. This data is required to make the spectrum analyzer functional. This data can be changed only by factory or by service personnel when performing adjustments. **No user data is stored in these locations.**

FLASH

The CPU board of the R&S® FSP, R&S® FSU and R&S® FSQ spectrum analyzers has one 512 kByte flash memory device which contains the BIOS. The BIOS is used by the Windows® operating system. **No user data is stored in the flash memory.**

On Windows® XP instruments the BIOS enables the usage of the USB ports. To prevent this there is an alternative BIOS with disabled USB ports available (see section USB below).

CMOS-SRAM

This 128 kByte memory device resides on the CPU board of Windows® NT instruments. There is no CMOS-SRAM memory on Windows® XP instruments. The CMOS-SRAM stores system information like last state settings, remote interface configuration and printer settings. This memory is battery backed-up, so it is not lost when power is removed from the instrument. **This is a security concern.**

Hard Drive

The main non-volatile device is the hard drive. Hard drives vary from 4 GByte up to 40 GByte. The hard drive is used to store:

- Ø Instrument operating system (Windows® NT or Windows® XP)
- Ø Instrument firmware and firmware options (measurement personalities) with option license keys
- Ø Instrument states and setups
- Ø Trace data
- Ø Limit Lines, Transducer tables
- Ø Screen images

The hard drive content is non-volatile, so nothing is lost when power is removed from the instrument. **The hard drive is a security concern.**

Compact Flash Memory

For the R&S® FSP and R&S® FSU spectrum analyzers there is an option available which uses Compact Flash memory instead of the mechanical hard drive (Option FSP-B20 and FSU-B20). This option is not available for the R&S® FSQ.

The flash disk is comprised of two compact flash memories and it's overall size varies from 512 MByte to 1GByte. The information stored on the flash disk is the same as on the hard drive (see above). **The compact flash disk is a security concern.**

6 Maintaining Security

Clearing the different types of memory

SDRAM

This memory is volatile. All you have to do is remove the power from the instrument and all data stored in it will be lost.

CMOS-SRAM

This is volatile memory that is kept alive with an internal battery, and the battery cannot be removed to clear the memory without taking the instrument apart. However, there is a procedure that can be used to have the instrument clear this memory itself:

Cold Boot procedure

To clear the CMOS-SRAM memory follow these steps:

- Ø Turn the instrument Off
- Ø Turn the instrument back On while holding down the decimal point key [.] on the number keypad on the front panel
- Ø Continue to hold this key for 10 seconds after pressing the "On" button
- Ø The instrument will now clear it's CMOS-SRAM memory and then power up

This procedure will clear any last state information and forces the instrument to power up with the factory default settings. Information such as the current time and date will not be erased by this procedure.

Note that this procedure is necessary for Windows$^®$ NT instruments only since there is no CMOS-SRAM memory on Windows$^®$ XP instruments.

Hard Drive / Compact Flash Memory

All user specific data like

- Ø Instrument states and setups
- Ø Trace data
- Ø Limit Lines, Transducer tables
- Ø Screen images

are stored on the internal hard disk / flash disk. Simply deleting these files is not sufficient from a security perspective.

For deleting files there are several Windows programs available to "shred" files according to the DoD 5220 standard which are working with the NSA approved algorithm. One example of these that has been tested by Rohde & Schwarz is FileShredder - see operating manual for details on installing Windows software on the instrument.

The FileShredder program works by overwriting the file seven (7) times with an alternating pattern of bits which not only stops all software programs from retrieving data contents, but also helps to prevent physical magnetic data sensors from retrieving a proper image of the data. This is standard government regulation for secure data erasure and conforms to Department of Defense specification DOD-5220.22.

Point your browser to the following web site for download and additional information: http://www.winappslist.com/security/file_wipers1.htm

Removable Hard Drive

Erasing all user data on a hard drive without also destroying the operating system is a tedious and cumbersome task. The best method for maintaining security, when the R&S® FSU or R&S® FSQ spectrum analyzer must be removed from a secure area, is to replace the hard drive with a "non-secure" hard drive. i.e. a drive that has never had any sensitive data placed on it. This allows the spectrum analyzer to still function properly in non-secured areas or for use when servicing.

For this purpose the Option FSU-B18 and FSQ-B18 'Removable Hard Disk' is available from Rohde & Schwarz in conjunction with a second hard disk (Option FSU-B19 and FSQ-B19). Note that this option is not available for the R&S® FSP.

As shipped from the factory, all R&S® FSU and R&S® FSQ spectrum analyzers have very little unique information stored on the hard drive. This allows one hard drive to function on most any instrument assuming it is the appropriate type of analyzer.

However, for the R&S® FSQ with the option B72 (I/Q Bandwidth Extension) there is an instrument-specific file which contains factory correction data. This file named "cal_freq_resp_b72.bin" which resides in the directory "D:/R_S.FW/Instr/EEPROM/CAL" must be copied to whichever hard drive is being used (see installation instructions of FSQ-B19 for more details). Whenever a new R&S® FSQ with option B72 is received, this file should be backed up to a floppy disk. It is recommended to label the disk with the model/serial number.

Step-by-Step Security

Purchase the appropriate spare hard drive (B19) and keep it in a non-secure area. It is recommended to clearly mark this hard drive as "Unsecured" together with instrument model/serial number information.

For a R&S® FSQ with option B72 copy the appropriate cal file to a floppy disk. This disk should be maintained together with the spare hard drive in a non-secure area.

In the event the secure R&S® FSU or R&S® FSQ needs to be used elsewhere, or, if it needs servicing:

- Ø In case of a Windows® NT instrument clear the memory (CMOS-SRAM) as described above.

- Ø Remove the secure hard drive (label it as secured if desired) and keep it in the secured area.

Ø Remove the instrument from the secured area and install the "unsecured" hard drive.

Ø In case of a R&S® FSQ with option B72 copy the appropriate cal file from the floppy disk to the "unsecured" hard drive.

The R&S® FSU or R&S® FSQ can now be used elsewhere or sent for servicing without fear of leaking any sensitive information.

If the R&S® FSU or R&S® FSQ needs to be returned to the secured area, follow the steps below:

Ø In case of a newly calibrated R&S® FSQ with option B72, copy the appropriate cal file from the "unsecured" hard drive to a floppy disk.

Ø Remove the unsecure hard drive and keep it in a non-secured area.

Ø Transport the R&S® FSU or R&S® FSQ to the secured area and install the secured hard drive.   In case of a R&S® FSQ with option B72 copy the appropriate cal file from the floppy disk to the "secured" hard drive.

Ø Perform the Cold Boot procedure as described above. This forces newly updated correction data to be copied from the EPROM to the hard disk.

Ø Start the self alignment procedure by pressing the CAL key and the softkey CAL TOTAL.

USB

USB ports can pose a security threat in high-security locations. Generally, this threat comes from small USB pen drives (a.k.a. memory sticks, key drives, etc) which can be very easily concealed, yet can quickly read/write up to 2 GByte of data. To a lesser extent, portable USB hard drives, zip drives, and CD-ROMs also present some risk, but these devices are much bulkier and cannot be concealed as well. The built-in floppy drives can also be an issue, but solutions such as floppy locks, already exist for this.

USB is an issue with Windows® XP instruments. Windows® NT does not support USB at all. This document describes a method to increase security by preventing access to USB ports.

Disable USB Ports

The R&S® FSP, R&S® FSU and R&S® FSQ spectrum analyzer BIOS can be updated with an alternate BIOS with disabled USB Ports. This is available from Rohde & Schwarz as Option FSP-B33, FSU-B33 and FSQ-B33 w/o any charge.

Please follow the detailed instructions for BIOS installation. Make sure you are using the appropriate BIOS for your type of analyzer. After installation of the BIOS option B33 any access to USB devices is blocked even if these devices were used previously with the instrument.

7 Additional Information

Please contact your support center for comments and further suggestions:

Hotline Europe

Telephone: +49 180 512 4242
Fax: +49 89 4129 63778
Internet: Contact us

Hotline America

Telephone:1-888-TESTRSA (1-888-837-8772) selection 2
From outside the USA: +1-410-910-7988
Email: customer.support@rsa.rohde-schwarz.com

Hotline Asia

Telephone: +65 6846 3716 (9am-6pm, Mon-Fri, excluding Public Holiday)
Fax: +65 6846-0029
E-mail: info@rssg.rohde-schwarz.com

ROHDE & SCHWARZ