Security of Agilent Signal Generators Issues and Solutions

Application Note

Introduction

This application note describes the security features for the Agilent E4428C, E4438C, E8247C, E8257C, E8267C, E8257D, and E8267D signal generators. It also describes how to use these features in several common application environments.

Requires firmware revision:
E4428C: ≥ C.04.10
E4438C: ≥ C.03.40
E82xC: ≥ C.03.76
E82xD: ≥ 4.03

Instrument Security

To protect sensitive data, it is important for signal generator users to understand the generator's features. There are three main areas which must be considered when determining appropriate security measures in relation to the generator's use: the storage media, the display, and I/O ports.

Storage media

Storage media, or memory for user information, can be categorized into two groups: explicit and implicit. Explicitly stored information consists of data enter by the user. Implicitly stored information includes items such as IQ calibration data, user flatness, table editor files, and last state information. This information is stored in various memory devices within the signal generator. Understanding the memory devices used within the signal generator enables users to define best-practice security measures for their application needs.

Memory Description	Contents	Location	Persistence
DRAM	Running firmware code and temporary operational storage	Processor board, baseband	Memory contents are completely erased when powered off for longer than a few seconds
SRAM	Certain user-editable data (table editors), last state and last state backup, state storage	generator board	Memory contents do not get erased by turning off power because the memory is connected to a back up battery. (The battery is located on the processor board in the E82x7C, or on the mother board in the E4428C and E4438C)
CPU flash	User files including: flatness calibration, IQ calibration, instrument states, waveforms, modulation definitions, sweep lists, firmware code and factory calibrations	Processor board	Memory contents cannot be removed by turning off power. A low-level erase procedure will completely clean the contents in a single cycle. Note: since this memory contains both factory data and user data, a full chip erase is not desirable. However, user data areas can be selectively and completely sanitized
Other flash	Factory calibration and information files, code images, and self test limits	RF boards, baseband generator board, motherboard	Memory remains intact through power cycles, however, there is no security concern because there is no user information in this memory
Hard disk	User files including: flatness calibrations, IQ calibration, instrument states, waveforms, modulation definitions, and sweep lists. Note: the hard disk is an option and is therefore not present in some instruments. If it is present, the listed files are stored on the hard disk instead of in flash memory	Instrument chassis (controlled by processor board)	Memory contents cannot be removed by turning off power. The magnetic residue will require several rewrite cycles or drive removal and destruction

Display

The second element to consider in generator security is the display, as it can reveal sensitive information. To prevent unauthorized people from reading the instrument display, it can be blanked. In this mode, no information appears on the display. Once the display is blanked, one must cycle the power on the instrument to re-enable the display. In the reboot sequence, the Erase All action (described later in this document), is performed to remove all user information so that the stored states cannot be retrieved.

I/O ports

The I/O ports must also be considered, since they allow remote access to the instrument. These ports, which provide access to all user settings, user states, and display images, include the GPIB, LAN, and RS-232. To prevent remote access to these ports, the physical area around these connections must be tightly controlled.

There is also a “ping” service, which presently cannot be selectively disabled. The concern here might be that it is possible to discover IP addresses of connected instruments in order to query their setups over the Internet, or break into the code.

Application Environments

To illustrate how to safeguard the content on signal generators, four use scenarios are provided.

1. **The instrument is moved between users or shared by many users**
   In this instance, security measures may necessitate that all user files and information be cleared to prohibit other users from accessing this information through the instrument interface. In this scenario, we assume that other people will not take the instrument apart and analyze the internal chips or storage media. For this scenario, use the *Erase All* feature described in *Using Security Commands.*

2. **The instrument is used in a secure area**
   In this circumstance, people walking past should not be able to access the instrument or read any information from the display. Remote access through the I/O ports is limited or controlled. For this scenario, the front panel must be used to blank the display and access to the I/O ports must be controlled. (Refer to *Using Security Commands.*)

3. **The instrument is moved from a secure area to an insecure area**
   When the signal generator is relocated from a secure area to an insecure area, all user information must be removed. The information should not be recoverable even if someone takes the instrument apart and analyzes the storage media. For this scenario, use the *Erase and Sanitize All* feature described in *Using Security Commands.*

4. **The instrument fails in a secure area and must leave the secure area to be repaired**
   This case means that the instrument is not functioning and cannot clear its own storage media. None of the storage media can leave the secure area. The instrument without storage media can leave the secure area to be repaired. For this scenario, use the procedures noted in *Hardware Removal.*

Using Security Commands

The built-in security features of Agilent signal generators are accessed by various methods, depending upon the element of the generator to be secured.

Memory

Memory security features are accessible by softkey menus on the front panel and by SCPI commands through the remote interface.

Key entry
Options for erasing memory are obtained through a series of keystrokes.

Utility > Memory Catalog > More > Erase All > Confirm Delete
Utility > Memory Catalog > More > Erase and Overwrite All > Confirm Delete
Utility > Memory Catalog > More > Erase and Sanitize All > Confirm Delete

SCPI commands
To erase memory from a remote location, SCPI commands can be sent to the signal generator.

```
SYStem:SECUrity:ERASeall
SYStem:SECUrity:OVERwrite
SYStem:SECUrity:SANitize
```

These three commands perform as described below.

Erase All

This procedure removes all user files and user information so they are not accessible through the instrument interface. This action will remove only the file references and clear all table editors without sanitizing the memory. The instrument will appear in a similar state as it was shipped from the factory. The action will include all user files, table editor contents, user flatness calibration, and user IQ calibration. This action will be relatively quick, taking less than one minute. (Note: this is different than the current *Delete All Files* key under the **Utility** > *Memory Catalog* > *More* menu which deletes all user explicit files but not current table editor files.)

Erase and Overwrite All

The command includes the *Erase All* procedure from above. It then clears the memory according to the security standards defined by the United States' Department of Defense (DOD).

All addressable locations are overwritten with random characters in the SRAM, DRAM and hard disk. All addressable locations in the CPU flash also are overwritten with random characters, and then the flash blocks are erased. This is equivalent to erasing entire chip but is only done on the areas of the chip, which are no longer in use.

Erase and Sanitize All

The procedure undertakes the measures included in *Erase and Overwrite All* from above.

In clearing the SRAM, the user is required to wait at least the same amount of time the instrument was used in the secure area to comply with SRAM sanitation. Each overwrite must reside in memory for a longer period than the classified data resided in memory. (Alternatively, the SRAM battery could be removed and reinserted manually. See issues below.)

On the hard disk, all addressable locations are overwritten with a single character; its complement, then a random character, and then verified. (Note: this is insufficient for top secret data according to the DOD standard. For top secret data, the hard drive must be removed and destroyed.)

DRAM memory is overwritten with a single character; then the instrument must be powered off.

Display

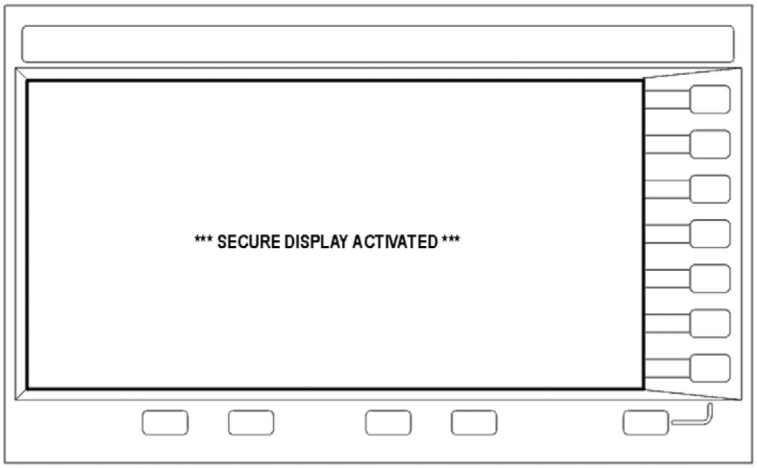
Blocking the display of sensitive data can be done using the generator's entry keys or using SCPI commands.

Key entry

Utility > *Display* > *More* > *Activate Secure Display* > *Confirm Secure Display*

SCPI command

```
:DISPlay[:WINDow][:STATe] ON|OFF|1|0
```



*** SECURE DISPLAY ACTIVATED ***

ESG/PSG Screen with Security Display Acivated

I/O Ports

While controlling access to the generator's ports is the leading security measure, the LAN port provides four services, which can be selectively disabled:

- http
- ftp
- sockets
- telnet

There is also a "ping" service, which presently cannot be selectively disabled. It should be noted that this service makes it is possible to discover IP addresses of connected instruments in order to query their setups over the Internet, or break into the code.

Hardware Removal

In the following circumstances, security measures may make it necessary to disassemble the instrument.

- If the instrument is non-functioning, the internal security features cannot be accessed. The storage media must be removed so the instrument can be sent to a repair facility
- If top-secret data has been stored, the storage media must be destroyed.

In these circumstances, the hard disk and the processor board must be removed. The assemblies can be reinstalled after the instrument has been repaired, or they can be destroyed.

Other Security Factors

Given that firmware commands are an inherent part of the virtually all electronic equipment, there are some security measures which may be impractical to implement. These relate to the following areas:

SRAM – according to DOD sanitize standards, a back-up battery should be removed; this requires opening the instrument (and thus voiding the warranty). The alternative is to perform a DOD clear and then wait for a period longer then the instrument was in use. Solutions include adding a software controlled “battery switch”, adding an externally removable battery tray, or describing how to disassemble and remove the battery.

FLASH – Since the factory calibration files are stored along with the user files, a “chip erase” cannot be performed. However, selective block erase achieves the same purpose.

DRAM – This area of memory is ignored in security features since its content is lost (erased) after powering down the instrument.

Conclusion

Aglient’s signal generators combine outstanding RF and microwave performance and baseband generation to deliver calibrated test signals at baseband, IF, and RF microwave frequencies. While the nature of the equipment requires the storage and use of data, generator features and operating practices can be combined to effectively safeguard data during the generator’s use. To ensure data protection in security-sensitive applications, the information is easily erased to DOD-standards using built-in utilities.

Related Literature

Agilent E4438C ESG Vector Signal Generator,
brochure, literature number 5988-3935EN

Agilent PSG Vector Signal Generators,
brochure, literature number 5989-1324EN

Web Resources

www.agilent.com/find/PSG

www.agilent.com/find/ESG

www.agilent.com/find/AD

This page left blank intentionally.

This page left blank intentionally.

Agilent Technologies' Test and Measurement Support, Services, and Assistance
Agilent Technologies aims to maximize the value you receive, while minimizing your risk and problems. We strive to ensure that you get the test and measurement capabilities you paid for and obtain the support you need. Our extensive support resources and services can help you choose the right Agilent products for your applications and apply them successfully. Every instrument and system we sell has a global warranty. Two concepts underlie Agilent's overall support policy: "Our Promise" and "Your Advantage."

Our Promise
Our Promise means your Agilent test and measurement equipment will meet its advertised performance and functionality. When you are choosing new equipment, we will help you with product information, including realistic performance specifications and practical recommendations from experienced test engineers. When you receive your new Agilent equipment, we can help verify that it works properly and help with initial product operation.

Your Advantage
Your Advantage means that Agilent offers a wide range of additional expert test and measurement services, which you can purchase according to your unique technical and business needs. Solve problems efficiently and gain a competitive edge by contracting with us for calibration, extra-cost upgrades, out-of-warranty repairs, and onsite education and training, as well as design, system integration, project management, and other professional engineering services. Experienced Agilent engineers and technicians worldwide can help you maximize your productivity, optimize the return on investment of your Agilent instruments and systems, and obtain dependable measurement accuracy for the life of those products.

Agilent T&M Software and Connectivity
Agilent's Test and Measurement software and connectivity products, solutions and developer network allows you to take time out of connecting your instruments to your computer with tools based on PC standards, so you can focus on your tasks, not on your connections. Visit
www.agilent.com/find/connectivity
for more information.

For more information on Agilent Technologies' products, applications or services, please contact your local Agilent office. The complete list is available at:

www.agilent.com/find/contactus
Product specifications and descriptions in this document subject to change without notice.

Phone or Fax

United States:
(tel) 800 829 4444
(fax) 800 829 4433
Canada:
(tel) 877 894 4414
(fax) 800 746 4866
China:
(tel) 800 810 0189
(fax) 800 820 2816
Europe:
(tel) 31 20 547 2111
Japan:
(tel) (81) 426 56 7832
(fax) (81) 426 56 7840

Korea:
(tel) (080) 769 0800
(fax) (080)769 0900
Latin America:
(tel) (305) 269 7500
Taiwan:
(tel) 0800 047 866
(fax) 0800 286 331
Other Asia Pacific Countries:
(tel) (65) 6375 8100
(fax) (65) 6755 0042
Email: tm_ap@agilent.com
Contacts revised: 1/12/05

Agilent Email Updates

www.agilent.com/find/emailupdates
Get the latest information on the products and applications you select.

Printed in USA, March 10, 2005
5989-1091EN

Agilent Technologies