Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Security Assessment of the Ricoh Afcio 450E Multifunction Device

There is an increasing use in the business community of multifunction devices that provide network printing, scanning and faxing. These devices are frequently being deployed within business with little thought of the security implications of devices that bridge the network and phone line, potentially offering a backdoor to both the network and confidential information via "cross channel" communications. This paper provides a Security Assessment of the Ricoh Afcio 450E multifunction device.

Copyright SANS Institute

Author Retains Full Rights

AD

A Security Assessment of the Ricoh Afcio 450E Multifunction Device

Version 1.0 9th July 2003

SANS GSEC Practical Version 1.4b Option 1

David L. Garrard

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

There is an increasing use in the business community of multifunction devices that provide network printing, scanning and faxing. These devices are frequently being deployed within business with little thought of the security implications of devices that bridge the network and phone line, potentially offering a backdoor to both the network and confidential information via “cross channel” communications.

This paper examines the security of the Ricoh Aficio 450E Multifunction device (hereafter known as Ricoh 450E) that provides the following functions:

- Manual and optional network faxing
- Network printing
- Manual and network scanning
- The ability to store faxes, scans & print jobs to memory
- The ability to archive to hard disk
- The ability to store and forward received faxes

A security assessment of the Ricoh 450 E reveals many of the security issues encountered with workstations and servers. These issues can endanger the confidentiality, integrity and availability (CIA) of data passing through the device. These issues require implementation of countermeasures appropriate for the business environment.

Introduction

After reading Kevin Smith’s paper (Smith) on the security analysis of a Sharp AR-507 Imager, the paper by Daniels et al on the Penetration testing of the Xerox DC 230ST (Daniels et al) and the paper by Orvis on the general security issues with multifunction digital devices (Orvis et al), I decided to examine the potential security risks associated with a common multifunction device that is used in Australia.

I am employed as an Information Technology Contractor and have worked in various Commonwealth Government Departments in Australia. After discussion with my counterparts in various departments, I decided to assess the security of a Ricoh 450E Facsimile/Network Printer/Scanner. Although this particular Ricoh model is no longer sold in Australia, it is still in use in many Commonwealth Government departments, including at least one whose network carries data classified as highly protected.

Unfortunately, the systems I had access to were production systems. Consequently, the custodians of these systems were keen to minimize any outages and limited the actual tests I was permitted to perform. As a result, the majority of the analysis presented in this paper is based on publicly available information concerning the Ricoh 450E.

Methodology

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

I took a three pronged approach to look for vulnerabilities that could compromise the confidentiality, integrity and availability (CIA) of the system and data.

The first phase was to visit hacker Web sites and perform a search for Ricoh, Afcio, 450E, Facsimile machine and photocopier to see if there were any published works that had already analyzed the Ricoh 450E. The search produced no result. The results using the standard Internet search engines Google and AltaVista were similarly unfruitful (Google), (AltaVista).

The second phase was to visit the following online vulnerability databases and repeat the above searches:

- The Mitre Common Vulnerability Exposures database (Mitre)
- The X-Force vulnerability database (X-Force)
- The Bugtraq mailing list (Bugtraq)

These searches also produced no results

The final phase was to look at what publicly available information on the operation and servicing of the Ricoh 450E was available, assess the results of tests I was permitted to perform and use a threat vector list to determine possible avenues of attack and formulate countermeasure strategies (Cole et al, pp.827-875).

Using the quick search facility on the Google Search Engine I was able to locate free copies of the Ricoh 450E operational and servicing documentation. The Ricoh 450E operations manual is freely available from the Ricoh US Web Site (Ricoh 4). There are also numerous Web sites, which for a nominal fee will, sell online copies of all Ricoh manuals. For a nominal donation to a charitable organization, I was able to obtain the following manuals (Service Manuals):

- Ricoh 450E service manual
- Ricoh 450E parts manual
- Ricoh 450E Operations manual system settings
- Ricoh 450E Facsimile reference manual

The service manual was particularly useful, providing a great detail of information on how to override or reset every security control built into the Ricoh 450E.

The threat vector list used is as follows:

1. Attack from malicious code
2. Insider Attack – Internal Host
3. Insider Attack – Internal Network
4. Outside Attack - Phone
5. Outsider Attack – Internet

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1. Attack from malicious code

There is no information readily available to indicate that a virus, trojan or worm has been written to target the Ricoh 450E. The device is, however, a fully functioning computer with memory, hard disk, storage, OS and a network protocol stack. It certainly would not be impossible to write a boot sector or file infector virus or a trojan to target the Ricoh 450E that could render the device unavailable or allow storage of information passing through it to memory or hard disk for later retrieval

A more likely scenario though, would be an attack from a virus, trojan or worm written in the printer control language Postscript. There are reports of trojans written in Postscript (Harley). Postscript is a powerful interpretative language with file input/output capabilities and the ability to reside in memory. It is conceivable that a Postscript program could be written to either make the machine unavailable or to retain copies of data.

The following countermeasures would reduce this vulnerability:

- Turn off the ability to submit files for printing via FTP without any authentication thus providing an auditable trail of who submits files.
- If Postscript support is not required then turn this feature off
- Include this device in normal anti-virus protocols as per any server

2. Insider Attack – Internal Host

The Ricoh 450E has the ability to archive documents to hard drive in its three operational modes. If the device is in a physically insecure room then the hard drive can be removed for retrieval of information. The Ricoh 450E service manual shows in full detail how to do this in six steps with nothing more then a screwdriver (Ricoh 1, pp.50-56).

The countermeasures to apply here are:

- Put the Ricoh 450E in a monitored secure room
- Use some third party locking mechanism to increase the difficulty of removing the hard drive
- If the hard disk archiving feature is not required then have the hard drive removed

There are two-security control mechanisms available via the console of the Ricoh E450:

- Key Operator code
- User Codes

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The Key Operator code allows access to the configuration of the machine and is equivalent to the console root password of a server. Users can be tracked and their access limited by assigning user codes with ID information. The assigning of user codes is performed via the Key Operator code. The default Key Operator code is “0000” and distinct User codes are not by default enabled. However, even if the Key Operator code is set to a non default this can be overridden as detailed in the service manual by entering service program mode, pressing the interrupt key then 107 on the keypad and finally, holding down the <c> key for 3 seconds (Ricoh 1,pp.4-5). No authentication is required. Once in this mode, all system parameters including the Key Operator code can be reset to factory defaults. This not only allows the machine to be made inoperable but also allows data to be archived to the hard disk or memory, allowing data retrieval at a later date. An alternative way to achieve the same result would be to open the machine, reset the systems NVRAM, automatically resetting the machine to factory defaults.

The Ricoh 450E has a Fax capability option called ‘forwarding’ which allows faxes from registered numbers to be printed and then retransmitted to a different Fax number. The use of this feature is controlled by the use of User codes, the assignment of which is controlled by the Key Operator code, which has been shown to be vulnerable. This is an obvious confidentiality attack. If this option is installed, I recommend having it disabled/removed or at the very least implement regular audit reports of inbound and outbound faxes and investigate the validity of retransmitted faxes.

The fax machine by default prints out the first page of every fax sent leading to the possibility of confidential information being left in the machine. This feature is enabled by default and should be disabled.

The Ricoh 450E also has the capability to print out reports detailing the number of pages printed, scanned and number of pages faxed along with fax numbers. Although this seems an innocent recording tool that can provide users with confirmation of successful faxing, it could also provide valuable business information to a competitor by the analysis of frequency etc. This is an inference attack against the CIA of data passing through the Ricoh 450 E The counter measure for this vulnerability is to limit the use of this default function via User codes, which are controlled by the vulnerable Key operator code.

The Ricoh 450E’s functionality is controlled by its firmware. This firmware can be copied and altered through the use of a special card obtainable from Ricoh. The details on how to perform this upload and download are described in the Ricoh 450E service manual. All that is required is to place the unit into service program mode. Such a modification could enable the bypassing of security controls with no audit trail, thus allowing the compromising of the CIA of information passing through the system. To exploit this vulnerability would require a great deal of technical sophistication.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3. Insider Attack – Internal Network

The Ricoh 450E has three network protocols enabled by default - AppleTalk, Novell IPX and TCP/IP. While there are security vulnerabilities in both AppleTalk and Novell IPX, I restricted my examination to TCP/IP. The board that provides network connectivity (the NIB 450E) is in several Ricoh devices and is listed on the Internet as being in other manufacturer's devices. This is not surprising as Ricoh provides multi function devices that are often re-badged and sold by other manufacturers. An Internet search reveals that other manufacturer's multi function devices containing the NIB 450 card have reported security vulnerabilities (Duchemin).

The manual of the NIB 450E lists the following TCP/IP services:

- TELNET
- FTP
- HTTP
- SNMP (not enabled on the Ricoh 450E)
- LPR/LPD

A port scan with the Nmap utility showed the following TCP/IP services:

- telnet, 23
- ftp, 21
- http, 80
- lpd/lpr, 515
- unknown, 10001

The port of '10001' was confusing as all manuals simply referred to this as the default TCP/IP port. I was told via email conversation from the Ricoh support site in the US, that this port was used for "TCP/IP communication and lpr printing". I would assume that this is used for a non lpr installed spooler and to support lpr in what the NIB 450 E manual refers to as "host mode where the an lpr spooler installed on the work station communicates via TCP/IP to the NIB interface board" (Ricoh 6).

Telnet is used to access a configuration screen for setting the interface card parameters. It has two accounts:

- User name "guest" with no password by default, this account allowing viewing of settings and submitted print jobs.
- User name "sysadmin" with a default password of "sysadmin".

The "sysadmin" account can be used for changing all network parameters. The default system administration account and password is published on the US Ricoh Web site as well as in the NIB 450E user manual. The countermeasure to limit this vulnerability would be to change the password on a regular basis. There is no indication in the manual or through the Ricoh Web support Web site that the "guest" account can be

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

disabled. Even though the “sysadmin” account password can be changed, this password can be reset to the factory default of “sysadmin” as outlined in the NIB 450E service manual (Ricoh 7). The countermeasure to apply here would be to place the Ricoh 450 E in a secured monitored room. These configuration screens are also accessible by an inbuilt Web Server using the same default passwords. The third method that can be used to change all network parameters is to download readily available software from the Ricoh Web site.

FTP is used to upload files to the printer. This can be done using the account name “port1” with no password. This is listed in the NIB 450E manual (Ricoh 6). This would be a perfect delivery vector for viruses. Similarly, a web browser-using FTP can drag and drop files to the printer with no authentication required.

Although SNMP is not enabled on the Ricoh 450E, the manual for the NIB 450E network interface card indicates the card is capable of supporting it in enabled printers (Ricoh 6). An Internet search looking for SNMP enabled printers that contain the NIB 450E card found a printer in manufactured by Lanier (a German subsidiary of Ricoh). This multi function device is SNMP enabled a community string of ‘public’ (Lanier, pp. 29). It is likley the SNMP write string is the well know default of ‘private’. This would allow the listing and alteration of the printer settings using readily available SNMP utilities. This is an indicator of a security vulnerability for SNMP enabled Ricoh multifunction devices that contain the NIB 450E card.

The final step in assessing the vulnerability of the Ricoh 450E to internal network based attacks would be to look for vulnerabilities in the TCP/IP stack (Daniels et al, pp.6), the available network services and any embedded systems and software. The steps to undertake are as follows:

1. Connect to the open TCP/IP ports via telnet and see if any information sent to the telnet client can identify the emended systems or software. Use this information to search online vulnerability databases looking for known security issues.
2. Look for common vulnerabilities in the TCP/IP stack such as the FTP Bounce attack (high level protocol attack), urgent data attacks such as “Winnuke” and ip fragmentation attacks such as “Jolt” or “Teardrop” (denial of service attacks) (Huygen).
3. Check if Buffer overflow attacks against the network protocols make the machine unavailable or perhaps put it into an administrative mode that can be used to launch attacks. Searching the Mitre CVE Database using the search phrases “lpr buffer overflow”, “Telnet buffer overflow”, “ftp buffer overflow” and “http buffer overflow” produced over 128 items.

The major concern with the Ricoh 450E’s network capability is the lack of authentication and control over who can connect to the devices TCP/IP services. The preferred countermeasure here is to put the Ricoh 450E behind a firewall and restrict services based on port numbers and IP addresses. For services that allow the configuration changes, enforce strict authentication. Similarly, configure the firewall to restrict what IP

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

addresses and TCP/IP ports the Ricoh 450E can connect to and from on the internal network. This would mitigate the risk of the device being compromised via the telephone and using cross channel communication to attack other hosts on the network.

4. Outside Attack - Phone

There is no mention of the Ricoh 450E having dial in diagnostic capability. This was confirmed by the Ricoh support Web site. To test this I tried to connect to the fax machine from an external data modem. I was unable to connect the system. This test also allowed me to search for any information that may identify the embedded software and software used. This could then be used to search online vulnerability databases looking for possible vulnerabilities. This test, however, was unsuccessful.

I was able to connect to the Ricoh 450E from an external line using the above data modem in Fax mode and commercial fax software. The Ricoh fax capability may be vulnerable to sending abnormally long station ID's (Daniels et al, pp.5), however, I was unable to obtain permission to test this theory.

5. Outsider Attack - Internet

The risks here are the same as identified in the section "Insider Attack Internal host". The countermeasure to apply is the same as the above section, along with the normal protections when providing Internet connectivity to an internal network i.e. use a firewall to restrict traffic in accordance with local security policy and authenticate users to the network.

In the event that Internet connectivity to the Ricoh 450E is required, it should be noted that the lpr protocol send data in clear text (McLaughlin). Consequently, to protect confidential information sent to the Ricoh 450E via the Internet use of a VPN.

Conclusion

The vulnerabilities outlined above demonstrate that there are many points where it would be possible to attack the security of the Ricoh 450E. Much of this information was obtained without actually performing any tests on the Ricoh 450E. Based on these results I recommend that users of this device perform a risk assessment with the appropriate business units' input on the data that will pass through the device and the data/systems potentially accessible from the network to which this device will be connected. Based on this assessment, perform the following:

1. Disable all features that are not required, especially archiving to memory/hard disk and fax store and forward.

2. Install the standalone management software if possible. It provides greater capability to lock down the machine and monitor its usage.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3. Update (or implement) a security policy with appropriate compliance checking that at a minimum, encompasses the following:

    - Define acceptable use of the device, especially with respect to storage and retransmission of data

    - Define what will be done with the unit's hard disk if the system is being sent out for service or disposed of

    - Define the protocols for an acceptable key operator code, administration password and user codes. This should specify who can change these items, how often they are changed, the acceptable format for these items and where these items will be stored

    - Define a configuration management protocol for the machine linked to your companies change management and configuration protocols.

    - Define the level of audit to perform, who is authorized to perform these audits and how often the audits will be performed. This audit should verify the key operator code, user codes, enabled features and the configuration of the enabled features. Any variation identified by the audit that cannot be related to authorized changes through the company's change management protocol should be treated as a possible security incident.

4. Ensure the appropriate operational security controls are in place so that any servicing of the Ricoh 450E is by authorized personnel in accordance with appropriate configuration and change control protocols.

5. Update (or implement) incident handling procedures that define the response to any change in the Ricoh 450E's configuration that cannot be directly related to an authorized request via your company's change and configuration management protocols.

To Ricoh and other manufactures of similar multifunction devices I would recommend applying some basic information security principles into the design of these devices. At the very least the following would greatly enhance the security of these devices:

1. Limit the network operating systems enabled out of the box. There is no reason for the Ricoh 450E to be enabled for three network operating systems. The most common network protocol is TCP/IP - when the machine is turned on for the first time, this only should be enabled. If other network protocols are required the user should have to specifically enable these protocols

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

2. Have all unnecessary network services turned off by default. If users need to make use of other services such as FTP or HTTP, then require the user to enable these services. Have strong authentication enabled on all services by default.

3. Have strong authentication enabled by default for any device functionality allowing the accessing or changing of services and parameters. While default passwords are required the first time the machine is booted up, at this stage have the machine enforce changing these passwords. Similarly, have a default mechanism built in forcing the user to change critical passwords on a regular basis. For SNMP enabled machines choose non guessable community strings and have a mechanism in place for forcing the SNMP community strings to be changed the first time the system is booted and on a regular basis.

4. Make the removable hard drive more physically secure.

5. Require stronger authentication to put the machine in user service mode. Being able to put the machine in user service mode and override all console security controls is a major security issue with the Ricoh 450E.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Glossary of Terms

Confidentiality	Information is available only to authorized personnel
Integrity	Information can only be changed by authorized personnel
Availability	System or Information is available to authorized personnel when they need access to the system/information.
Threat Vector	Mechanism via which a threat is delivered
Vulnerability	A weakness in a system that allows a threat to be realized.
Threat	An event that could cause harm to an information system or data
Authentication	Process to determine that somebody or something is who they purport to be
NVRAM	Nom Volatile Ram, computer memory that retains information written to it unless specifically reset.
Highly Protected	An Australian Federal Government classification for data. The Australian Federal Government classifies as Top Secret, Secret, Highly Protected, Protected and commercial in confidence.
RFC	Request For Comments a series of informational Internet documents and standards.
SNMP	Simple Network Management Protocol a protocol for managing network devices and the function of such devices in a TCP/IP network. Version 3.0 of this protocol is defined in RFC 3410 (ftp://ftp.rfc-editor.org/in-notes/rfc3410.txt)
FTP	File Transfer Protocol a TCP/IP based protocol for transferring files across the network. This protocol is defined in RFC 959 (ftp://ftp.rfc-editor.org/in-notes/rfc959.txt)
HTTP	Hypertext Transfer protocol a TCP/IP protocol used for transferring web pages across the Internet. This protocol is defined in RFC 2616 (ftp://ftp.rfc-editor.org/in-notes/rfc2616.txt)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Telnet	A protocol for remote logins via TCP/IP network from one host to another. This protocol is defined in RFC 854 (ftp://ftp.rfc-editor.org/in-notes/rfc854.txt)

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

Cole Eric, Fossen Jason, Northcutt Stephen, Pomerance Hal.
"SANS Security Essentials with CISP CBK Version 2.1 (Volume 1).
SANS Press, 2003. 827-875

Ricoh 1. "NAD 30/40 Service Manual". Ricoh Corporation

Ricoh 2. "Afcio 340/350/450 Operating Instructions Systems Setting". Ricoh Corporation

Ricoh 3. "NAD 30/30S/40 Parts Catalogue". Ricoh Corporation

Ricoh 4. "Aficio 450E Operator Reference Manual". Ricoh Corporation.
URL: http://www.ricoh-usa.com/support/manuals/bw/aficio450e.pdf

Ricoh 5. "Fax Option Type 450, Operating Instructions Facsimile Reference". Ricoh Corporation

Ricoh 6 "Network Interface Board Nib 450-E Owners Manual". Ricoh Corporation.
URL: http://www.lanier.de/C1256BAA0035F203/ContentByKey/GCOI-4V9EVG-DE-p/$file/OG-NIB450.pdf

Ricoh 7. "Service Manual: (A855), Network Interface Board Type 450-E". Ricoh Corporation.
URL: http://www.google.com.au/search?q=cache:dvKMVQJs-lAJ:extranet.rex-rotary.cz/%2Bdata/Servis/0104_DIG2/options/nib450/s_nib450.pdf+NIB+450-E+Service++Manual&hl=en&ie=UTF-8

Duchemin Gregory. "Nashuatec printer, 3 vulnerabilities found".
URL: http://lists.insecure.org/lists/bugtraq/1999/Oct/0166.html

McLaughlin L."Line Printer Daemon Protocol", August 1990.
URL: ftp://ftp.rfc-editor.org/in-notes/rfc1179.txt

Smith Kevin K. "Do you copy? Security issues with Digital copiers".
16 Sep 2000.
URL: http://www.giac.org/practical/gsec/Kevin_Smith_GSEC.pdf

Daniels Thomas E, Kuperman Benjamin A, Spafford Eugene K.
"Penetration Analysis of a XEROX Docucentre DC 230ST". October 2000.
URL : http://csrc.ncsl.nist.gov/nissc/2000/proceedings/papers/034.pdf

Orvis William J, Van Lehm Allan L. "Data Security Vulnerabilities of Facsimile Machines and Digital Copiers". January 1995.
URL: http://www.ciac.org/ciac/documents/CIAC-2304_Vulnerabilities_of_Facsimilie_Machines_and_Digital_Copiers.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Harley David . ”Viruses and the Macintosh FAQ”. August 2000.
URL: http://www.sherpasoft.org.uk/MacSupporters/macvir.faq

Service Manuals. “Web Site where Ricoh Service Manuals were obtained”.
URL: http://user-service-manuals.com/

Lanier 1. “Technique Information fur die Lanier-Series 5000”.
URL: http://www.lanier.de/C1256BAA0035F203/ContentByKey/LHON-4UMHNG-DE-p/$file/NICNIB.pdf

Huegen Craig A. “Network based Denial of Service Attacks”.
URL: http://www.pentics.net/denial-of-service/presentations/msppt/19980209_dos.ppt

Nmap port scanner. URL: http://www.insecure.org

Default Password Nib 450E. URL: http://ricoh.custhelp.com/cgi-bin/ricoh.cfg/enduser/std_adp.php?p_sid=g9iNAXKg&p_1va=3003&p_faqid=2887&p_created=10443839:

Goggle Internet Search Engine.
URL: http:// www.google.com

AltaVista Search engine.
URL: http://www.altavista.com

Mitre Common Vulnerabilities and Exposure Database.
URL: http://www.mitre.org

Butraq Computer Security Mailing List.
URL: http://www.securityfocus.com/archive/1

X-Force Security Advisories.
URL: http://xforce.iss.net/xforce/search.php

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: March 12th, 2014

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Secure Canberra 2014	**Canberra, AU**	**Mar 17, 2014 - Mar 22, 2014**	**Live Event**
ICS 410@ Sydney 2014	**Sydney, AU**	**Mar 24, 2014 - Mar 28, 2014**	**Live Event**
SANS Munich 2014	**Munich, DE**	**Mar 31, 2014 - Apr 05, 2014**	**Live Event**
SANS 2014	**Orlando, FLUS**	**Apr 05, 2014 - Apr 14, 2014**	**Live Event**
FOR518 Mac Forensic Analysis	**Vienna, VAUS**	**Apr 22, 2014 - Apr 27, 2014**	**Live Event**
SANS Abu Dhabi 2014	**Abu Dhabi, AE**	**Apr 26, 2014 - May 04, 2014**	**Live Event**
US Cyber Crime Conference	**Leesburg, VAUS**	**Apr 27, 2014 - Apr 28, 2014**	**Live Event**
SANS Austin 2014	**Austin, TXUS**	**Apr 28, 2014 - May 03, 2014**	**Live Event**
Security Leadership Summit	**Boston, MAUS**	**Apr 29, 2014 - May 07, 2014**	**Live Event**
SANS Security West 2014	**San Diego, CAUS**	**May 08, 2014 - May 17, 2014**	**Live Event**
SANS Secure Europe 2014	**Amsterdam, NL**	**May 10, 2014 - May 24, 2014**	**Live Event**
SANS Melbourne 2014	**Melbourne, AU**	**May 12, 2014 - May 17, 2014**	**Live Event**
SANS ICS410 London 2014	**London, GB**	**May 12, 2014 - May 16, 2014**	**Live Event**
SANS Malaysia @MCMC 2014	**Cyberjaya, MY**	**May 12, 2014 - May 24, 2014**	**Live Event**
SANS Bahrain May 2014	**Manama, BH**	**May 17, 2014 - May 22, 2014**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**May 26, 2014 - May 31, 2014**	**Live Event**
Digital Forensics & Incident Response Summit	**Austin, TXUS**	**Jun 03, 2014 - Jun 10, 2014**	**Live Event**
SANS Rocky Mountain 2014	**Denver, COUS**	**Jun 09, 2014 - Jun 14, 2014**	**Live Event**
SANS Northern Virginia 2014	**OnlineVAUS**	**Mar 17, 2014 - Mar 22, 2014**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**