Global Information Assurance Certification Paper

Wireless Security: Blackberry by Research In Motion

Jeff Danielson
February, 18 2002
Version 1.3
Resubmission

Personal Data Assistants (PDA's) have quickly become a required tool for the corporate executive. It has been previously used for calendar and contact management and storage purposes. However, these PDA's have quickly been promoted to wireless email and confidential information mobile storage devices. This has created a large security vulnerability problem for Information Security Professionals worldwide. This paper presents an introduction to the Blackberry Wireless Email devices as well as suggestions to help Information Security Professionals minimize the risk of using such devices.

As these devices continue to grow in popularity as well as storage features, the companies creating these devices should have a responsibility for also creating bigger and better security features. The Blackberry wireless devices have taken the correct steps to minimize informational theft, but there are still some issues that Information Security Professionals as well as corporate executives need to consider before they are purchased.

I. Introduction

Blackberry mobile units are wireless email devices designed and produced by Research in Motion Ltd (RIM). Originally developed for use in the United States and Canada, RIM has recently expanded its coverage to those in the United Kingdom and the Netherlands (See. www.blackberry.net/europe or www.blackberry.net/netherlands).

Founded in 1994 and publicly held in 1997, Waterloo Ontario based RIM provides many different wireless solutions for corporate and home use. Blackberry was first released in 1999 across the United States and Canada.

Specifications

RIM has currently created 2 different models of the Blackberry Mobile units, with a third on its way. The first model, 850 or 950 depending on the network, is designed similarly to that of a generic paging device. At 4.1oz (without battery) and 3.4"x2.5"x0.94" this model features a 4 MB Flash memory as well as 512 kB of RAM. The screen on the *50 is a full graphic LCD, 132 x 68-pixel resolution, that holds 8 lines by 25 characters of text or graphics. This model also features a 31-key QWERTY style keyboard, and has two power sources. This fail-over feature requires one AA Alkaline battery for normal use and includes a rechargeable internal lithium ion cell to protect the information when the user

replaces the AA Alkaline battery.

The second model, 857 or 957, is designed more like a generic handheld or PDA. This model features 5MB of flash memory with 512KB of RAM. The screen is a larger one, containing a 160x 160-pixel resolution and has a layout similar to that of a Palm Pilot or Handspring with graphical Icons to portray links to features and third-party programs. A 33-key QWERTY keyboard and a fully rechargeable lithium ion cell battery is featured as well.

Both models include a thumb-operated track wheel, for easier navigation. A real-time clock, audible alarm, Autotext and Address Book are also featured on both models. The Blackberry connects to its users computer with a RS-232 compatible serial port that operates to speeds up to 115,200 baud.

In North America, the Blackberry currently uses 4 different wireless networks throughout the world. The four networks are: GPRS (General Packet Radio Service), Datatrac, Mobitex, and the Nextel IDEN network. While in Europe, Blackberry uses the global GPRS network. The wireless devices are named per network that it was designed for; for example, Blackberry 957 uses the Bellsouth Mobility Mobitex Network while the Blackberry 857 uses the Motient Datatrac (formerly ARDIS) network. The same is true for the Blackberry 950 and 850, respectively.

As the de-facto standard of wireless email devices, Blackberry is currently used by over 7,800 companies with more than 2,300 of them use the Blackberry Enterprise Server which is built into an organizations Email Architecture.

II. Wireless Network Architecture Overview

Blackberry uses multiple different backbones to deliver the required information packets over the wireless network. These backbones include, Microsoft's Exchange Server, Lotus Notes Domino as well as Internet Only Email systems.

Microsoft Exchange Server

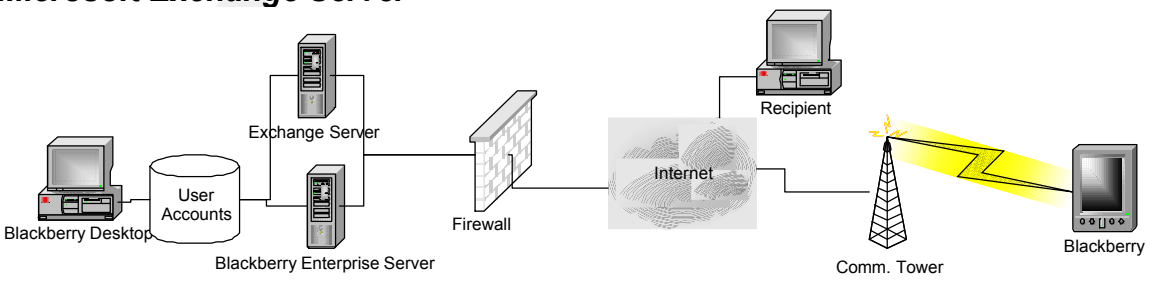

Figure 1

At the center of the backbone is RIM's proprietary Desktop Manager. This

software package stores the configuration information and synchronizes the handheld to a docking station connected through a serial connection to the users main desktop computer. The synchronization process includes tasks, contacts, calendar, email, time, as well as the initial encryption key that will be detailed out later in this report. After the initial synchronization, the Blackberry will link up to the Blackberry Enterprise server to monitor the user's inbox for new mail, compress and encrypt the message to deliver them to the Blackberry handheld or decompress and decrypt messages originating from the handheld. These two software packages then integrate into the Microsoft's Exchange Server and Outlook for email delivery to the recipient. The figure 1 illustration shows the path that the information moves through the computer network for the Microsoft Exchange Server backbone. Please keep in mind that this is a two way diagram, the email starts at the mobile unit, moves through network to the blackberry desktop and out again to the recipient.

Lotus Domino Server

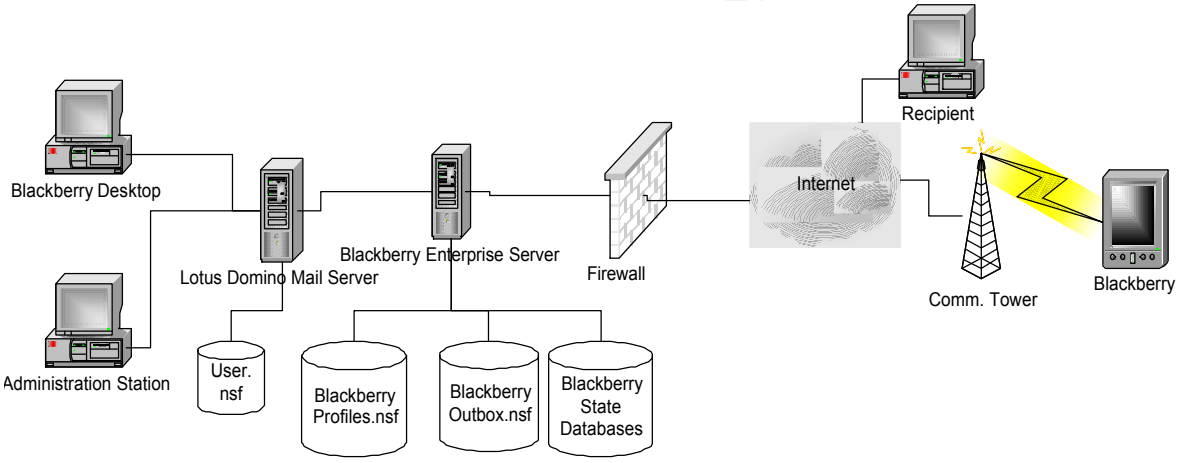

Figure 2

Lotus Domino's architecture is similar to the architecture around the Microsoft Exchange server, however, there are many differences. For example, The Blackberry Enterprise server is the center of the backbone rather than the Desktop Software. The reason for this is the Blackberry Enterprise Server creates two separate Lotus Domino databases for wireless email. The three separate databases illustrated below, Blackberryoutbox.nsf, Blackberryprofiles.nsf, and blackberry state databases holds all information for wireless email rather than relying on the mail server. The Blackberryprofiles.nsf database contains the configuration information as well as the security information, specialized forwarding rules and handheld identification information.

Internet Only Architecture Overview

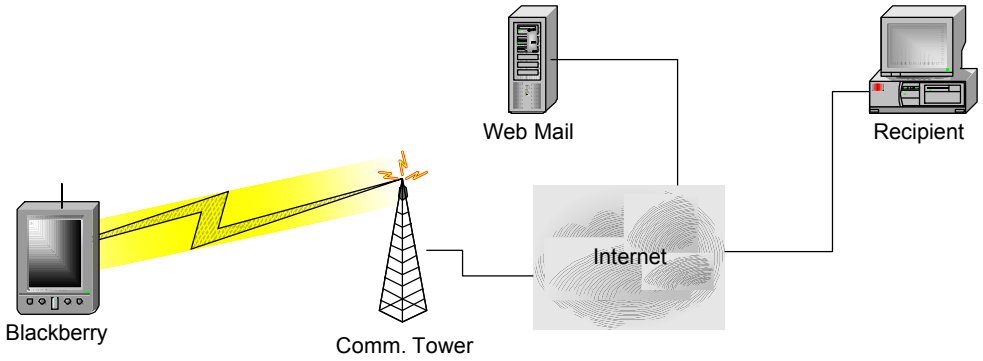

Figure 3

RIM built the Internet Only Blackberry device and contracts it out to many different companies to provide the service required allowing it to work. The service providers sell the brand name Blackberry under their own name; provide the wireless service, and also provides multiple other services that integrate into the Blackberry unit. Because of this design, the service providers are tasked to include the needed security for their customers. Figure 3 illustrates the network architecture for the Internet only devices. Starting with the Blackberry unit, the device transmits the information to an online web mail station provided by a specific service provider, who then sends it through the Internet to the final recipient. Specific service providers also allow the blackberry unit to connect to other web mail devices, like hotmail, to send and transmit information.

III. Blackberry Security Features

Wireless devices have now become an essential component to a corporate executives or technical workers arsenal. Due to the information that is now being transmitted and literally falling out of the sky, the term end-to-end security is no longer a selling point, rather a requirement. Because of this increased security, Research in Motion developed the Blackberry architecture to ensure multiple different security objectives. These objectives include:

1. Protecting data on the handheld
2. Securing the wireless link
3. Minimal user impact

Information Security individuals have been inundated with wireless devices that promise security outwardly, but have little to show for it. Security Issues that surround the wireless device include eavesdropping, physical theft of equipment and information, viruses, DoS attacks, and spoofing and hijacking. The following list of security features will be sorted by RIM's stated objectives and compared to the issues and vulnerabilities surrounding wireless networks.

Protecting data on the handheld

Two of the main problems surrounding mobile devices are theft and/or loss. In the situation that an employee carrying sensitive information leaves a device at an unknown location, it is necessary that the device be protected from others having access to that device's internal memory. RIM felt that the information stored on the handheld should be as secure as the information stored on the company local area network (LAN.) To do this, they implemented a password feature integrated into the handheld. The password feature allows a user to set a custom password between 4 and 14 characters long. The Blackberry also rejects weak passwords such as identical characters or those of a natural sequence. With the password set, after a specific period of inactivity, the Blackberry activates a screensaver and requires the user to input the password to access the information on the handheld.

The password on the handheld in of itself is protected from being broken. The password is stored on a encrypted SHA-1 hash store. Using this method of encryption makes cracking the password on the handheld difficult, even if they have the contents of the memory. Unfortunately, this is not a requirement for handheld use, and the user has the ability to disable this feature.

For any corporate security or network administrator, physical theft of equipment should be taken extremely seriously. For corporate executives or those employees that are privileged users regarding information access, this feature should be stated as a common usage policy. Also, it is recommended to audit the handheld periodically to make sure the devices have the password feature enabled and using strong authentication. Last, the user or administrator should back-up the information located on the handheld often. This will reduce the risk of corporate informational assets being completely gone.

Securing the Wireless Link

Due to the basic nature of wireless technology, information is pushed and literally flying through the air. This creates a security problem that physical wired networks do not have. Physical wired networks are limited to the location that the wires extend to. Wireless, however, is only limited to the area the wireless networks cover, which is currently around 98% of the American city and urban population. To keep the user's informational assets integrity and confidentiality, RIM has integrated the encryption method of triple Data Encryption Standard (DES).

The original DES was approved by the United States government on March 17, 1975 but is now considered insecure due to its somewhat small key length of 56 bits that results in 2^{56} possible different keys. DES was first cracked in 1997 from the RSA Challenge. It took around 5 months to crack. Today, with a relatively small equipment fee (around 1 million dollars), a dedicated DES

cracking device can review all the DES crypto-variables in 3.5 hours.

Triple DES, however, uses a symmetric key system that applies the DES algorithm three times using two different secret crypto-variables. This 192-bit (24-character) key gets broken up into three sub keys of 64-bit chunks, however, due to the incorrect parity, the key is an effective 56-bit sub key with a 168-bit total encryption key. This data is then encrypted using the DES algorithm three different times using the three sub keys. Decryption uses the same process only in reverse. The encrypted data gets decrypted three different times using the three sub keys to get the plain text message on the blackberry. Triple DES is also three times slower, but the latency that wireless brings currently is not a noticeable factor for users.

The encryption key is located on both the handheld and the desktop. This key is generated from the random use of mouse movements on the user's desktop computer to generate the key. The key is then transferred from the desktop to the handheld from the physical docking station connected to the computer from a selected port. This is considered a symmetric key encryption due to the secure key exchange provided from the physical access to the users desktop. The key is confidential and authenticated due to this exchange.

If the Blackberry Enterprise Server is being used, a copy of the key is stored on the server instead of the desktop and also the handheld. This key is required for messaging to be possible. This key also allows the decryption to be performed at the server level, protected from the outside world with a firewall, allowing end-to-end security. If the server is not being used, then the information from or to the wireless handheld is not decrypted until it moves to the desktop. This also allows the message to be decrypted end-to-end, from the handheld to the desktop.

With the Blackberry Enterprise Server or desktop secured behind a corporate firewall, this encryption method should currently satisfy the issue of wireless eavesdropping from the wireless device to the corporate email system.

Minimal User Impact

Information Security professionals face a daunting task; to make employees feel the same way about security as they do. In fact, security professionals rely on their peers at their corporation to implement and follow through on the security policies that they provide. To help these employees who are not trained in security concepts, the security professionals best tool is a tool that provides minimal user impact. Unfortunately, the technology has not yet arrived, or is too expensive to implement, to make security invisible. For example, if the user does not enable the password-protected feature of the Blackberry, the information that the user receives, or has already received, is available to those who steal or acquire freely. This does not work well within the information

security industry.

Minimal user impact allows users to send information securely, without having to follow a list of procedures. Due to social engineering and other human error, minimal user impact allows information security professionals to feel somewhat secure in the fact that their users cannot accidentally or purposively remove many security features built into their wireless handheld.

IV. Other Security Features

RIM included these other security features to decrease the risk of a network intrusion through its Blackberry Enterprise Server software. It should be noted that these security features are not implemented in the Internet Only Architecture.

Microsoft Exchange Version

RIM has included many security features to defend the wired, physical link as well as the wireless. To maintain a constant direct TCP/IP connection to the wireless network, Blackberry Enterprise server requires a change in the local or corporate firewall(s). To keep this connection, the port 3101 needs to be opened in an outbound-initiated only configuration. This feature keeps an attacker from using this port to connect into the secured internal network.

Looking at the architecture for the Exchange Server illustrated at the beginning of this report, the information travels from the mail server and gets redirected to the recipient. This is an important concept since there is no information store directly from the Blackberry Enterprise Server. Thus, there is no access to messaging information in any kind located on this server to be exploited by an attacker. Also, the information being received by the Blackberry Enterprise Server must be encrypted and decrypted with the valid encryption key. Thus, any information from the exchange server or from the outside not encrypted using the correct encryption key will not be accepted.

Lotus Domino Version

The Blackberry Enterprise Server is configured similarly to the exchange version, except that there is extra information on the server. As the architecture section states above, the Blackberry Enterprise server does contain information as it holds three different databases, the Blackberryprofiles.nsf, the BlackberryOutbox.nsf and the Blackberry state databases. However, no inbound traffic is accepted from anything other the source host. This outbound-initiated only uses the authentication method of a challenge/response mechanism. Other features mirror the Microsoft Exchange version as stated above.

Using the authenticated key, combined with Triple-DES and outbound-initiated

only TCP-IP connections should be able to satisfy the requirements for spoofing and hijacking. Only users with the same handheld serial #, encryption key, and username/email address could possibly spoof or hijack that address using the Blackberry handheld.

Blackberry currently has no known viruses that affect the unit, however, since it relies on other mail systems to complete the delivery, any messages that affect those mail systems have the opportunity to affect other receivers. The Blackberry has the ability of receiving and viewing of specific attachment types which give the user the ability to view, forward, and infect without knowing of the problem. This can be especially dangerous with PDF or DOC virus attachments.

Since the Blackberry relies on other mail systems, the completion of the delivery is determined by the state of those systems. For example, if a Blackberry user sends a message and the corporate email account is down, that message would not be received by the intended recipient resulting in a denial of service issue.

V. Operation WhiteBerry

Operation Whiteberry was developed in response to solve multiple problems found within the wireless data transfer systems of Wireless Application Protocol (WAP) and Blackberry Mobile Messaging system. Due to the security issues surrounding these protocols, Operation Whiteberry is built upon to compete against those industries that promote closed and proprietary solutions such as RIM's Blackberry. Instead of reviewing the complete project, the issue of security that Operation Whiteberry promotes should better help to see the problems that Blackberry faces.

It would be wise to understand the concept of end-to-end in RIM's definition instead of the logical definition. Operation Whiteberry is a project that defines end-to-end as messaging from the point of origin to the point of destination or from the blackberry to the intended email address. It is an important "point of view" difference when related to security. RIM's definition of end-to-end is defined as messaging from the point of origin to the point of corporate email redirection or from the blackberry device to the corporate mail system. Operation Whiteberry also takes into account the proprietary or closed nature of its messaging architecture, as this prevents the use of other independent or third party security mechanisms.

All of these are important points. If the user or customer thinks that the Blackberry wireless device provides security from the handheld to the receiver of the email, they are only partially correct. Blackberry was built to be used by other email servers, thus the security Blackberry provides is from handheld to the point of decryption at the corporate mail system. After that, the email is sent

using the corporate mail system to the intended receiver, without any encryption, thru the Internet.

Last, Blackberry users have the ability to send electronic messages to other blackberry users without connecting to the email system. This "direct-connect" feature does not support full encryption and thus the information being sent and received wirelessly is more easily accessible. It is important to remove this ability or add a statement to your wireless policy revealing this information, and that no confidential or corporate information be passed in this fashion.

VI. Conclusion

During the terrorist attacks of September 11, 2001, while other lines of communication failed, cell phones, pagers, telephones and such, Blackberry didn't. In fact, it has been getting rave reviews for its performance during those horrible times. Remarkable stories have poured out from Blackberry users that used the technology to stay in touch of loved ones, evacuate employees, or save informational assets when no other source of communication was available.

On the day of those attacks, Congressman Robert Ney, R-Ohio used his Blackberry to communicate with his assistants and family. As a result, he ordered 435 Blackberry devices for each member of the House so those representatives could communicate to their assistants and families during emergencies. As an indirect result reports Congressman Ney, they have become more productive throughout their normal workload.

If it's good enough for the government, is it good enough for you? The answer may be yes, if the correct policies and procedures are in place to maximize the security benefits that Blackberry provides. The key to any secure environment, wireless devices included, is to maximize the security features that each device has available. Following these procedures and policies, as well as auditing users to make sure these practices are followed should mitigate the risk that wireless devices apply. Of course, not having these at all would be the optimal choice for security, but that is not always possible. Wireless devices have an extremely far distance to travel to be considered secure, but at least The Blackberry by Research in Motion has been shown to be more secure than most wireless devices currently in production.

References

1. "Blackberry Installation and Users guide: Internet Edition". Waterloo: Research in Motion Limited, 4 June 2000. 16,19-22,171-172

2. "RIM 950 and RIM 957" Blackberry Installation and Starters guide: Enterprise Edition. 7 July 2001 URL: http://www.blackberry.net/support/pdfs/mb_950_957_guide.pdf (19 February 2002)

3. "Technical White paper for Blackberry Security: Microsoft Exchange" 2.1 2001. URL: http://www.blackberry.net/support/pdfs/EnterpriseServerTechnicalWP.pdf (19 February 2002)

4. "Technical White paper for Blackberry Security: Lotus Notes Domino for Version 2.0 with Service Pack 2" 2001. URL: http://www.blackberry.net/support/pdfs/BlackBerrySecurityTechnicalWhitePaperforDomino.pdf (12 February 2002)

5. "Triple DES Encryption" URL: http://www.tropsoft.com/strongenc/des3.htm (18 Jan 2002)

6. Beachum, Frank "9/11: What worked, What Didn't" 17 October 2001. URL: http://www.tvtechnology.com/features/Net-soup/f-fb-whatworked.shtml (18 January 2002))

7. Mohsen, Banan. Hammoude, Andrew "Creation of a Truly Open Mobile Messaging Solution" Operation Whiteberry 2.4. 2 August 2001. URL: http://www.freeprotocols.org/operationWhiteberry (18 January 2002)

8. Schwartz, Ephraim "Congress going Wireless" 11 October 2001 URL: www.infoworld.com/articles/hn/xml/01/10/11/011011hncongress.xml (18 January 2002)

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS