# Global Information Assurance Certification Paper

# Smart Cards:
## Understanding Security Implementations

Richard Gallagher
GIAC Security Essentials Certification Practical
Version 1.4b
Option 1
December 29, 2003




## Abstract

A smart card is a small plastic card, resembling a credit card, which contains within its makeup a small microprocessor. These cards are used in a variety of applications. This paper briefly discusses some of those applications. The physical characteristics of a smart card are analyzed, with a special emphasis on physical security of smart cards. Physical vulnerabilities are presented, as well as possible measures to avoid exposure to these vulnerabilities.

Smart cards are also used widely in the area of user authentication. This application for smart cards is addressed at length and the specifics of smart card use for password, token, and biometric authentication are evaluated. The advent of biometric methods such as Parasitic Authentication and Pressure Sequencing has expanded the potential for smart card use in computer security. However, these techniques are still in development, and the benefits of these methods have yet to be realized. Some of the security and implementation advantages of these methods are reviewed and recommendations for further development are made.


## Introduction

It has always been a trend in the computing industry to make devices progressively smaller and faster. Moore's law (which has held true since 1965) provides proof of this: According to Gordon Moore, the number of transistors that can fit on a chip doubles every few years.[1] This same concept is trickled down to the embedded application industry, although it has to do with much more than simply chip size. Devices such as cellular phones, radios, and many others shrink in size and expand in power each day. Chips have also found their way into many household items that were previously all mechanical, such as refrigerators and washing machines. One relatively new application of a microprocessor is inside common objects such as credit cards and identification cards. Dubbed *Smart Cards*, these devices provide a multitude of uses, ranging from providing an electronic purse to securing building access. Although they

seem simple at first glance, the smart card is actually highly complex. In the following sections important issues involving smart cards will be discussed including the physical layout and design of a smart card, security methods employed by and with smart cards, and some practical applications implemented using smart cards.

## Current Smart Card Usage

Smart cards are used as a tool to facilitate the transfer of information required in many arenas, including electronic payment, access control, healthcare, and identification.

Electronic Payment is one of the most widely used applications of the smart card and is the most familiar among the average user. There are several different types of smart cards in this category, all of which deal with currency or a fiscal value. This type of smart card provides an additional level of security (public key encryption) to protect the assets of the bearer as it is frequently the type of card issued for credit and debit purposes.

Smart cards can also be used for access control by facilitating the authorization and authentication to physical sites or resources. They are widely used in the military, corporate, and government environments as means of authorization or authentication. Because they are an excellent tool for identification, smart cards are often also used in schools, corporations, and governmental agencies to identify students and employees. In addition, they can be used to thwart intruders and ensure a safe working environment. Most of the identification smart cards are also useful as photo ids, which have an interface that allows them to be used in vending machines, laundry machines, meal payment plans, libraries, medical care and office security. In addition, smart cards can be used in gaining access to lab equipment, telecommunication equipment, vehicles, and machines.

The field of communications has been using smart cards for years as a means of payment for services such as subscriber cards, mobile phones, and public phones. In Europe, smart cards are commonly used in cellular phones to purchase pre-paid airtime at vending machines. These smart cards are an integral part of the telephone itself.

Smart cards are extensively used by the healthcare industry, especially through an individual's health insurance card. This card holds crucial information on the patient's personal health history, as well as contacts and policies of the insurance company legally bonded to cover the patient's medical costs. This type of smart card is also found in applications such as a patient medical record card, holding information about the patient such as allergies, blood type, special needs, etc. Through the use of these smart cards, the healthcare industry

benefits by significantly reducing the chances of fraud while, at the same time, shortening the time needed for claim processing.

Overall, the multiple uses of smart cards are widely spread across domains, industries, education, law-enforcement and banking. Technological advances will allow more powerful smart cards to replace the ones in use now, and at the same time they will become more secure and robust against fraud.

## Smart Card Physical Aspects and their Security

At first glance one would assume that a smart card is just a regular credit card or photo ID. Essentially a smart card is just that with the addition of a small "chip" or microprocessor embedded into the surface of the card. This chip is used to store data such as financial or personal information, perform calculations such as encryption schemes, and has Input/Output capabilities to be able to communicate with reader devices. One of the key reasons to use smart cards is for portability of data and ease of access to data stored on the chip. Since the data on the chip may hold sensitive personal data or financial information, it is important that no one except the authorized cardholder gain access to it. To do this, steps must be put in place to ensure that the chip is tamperproof.

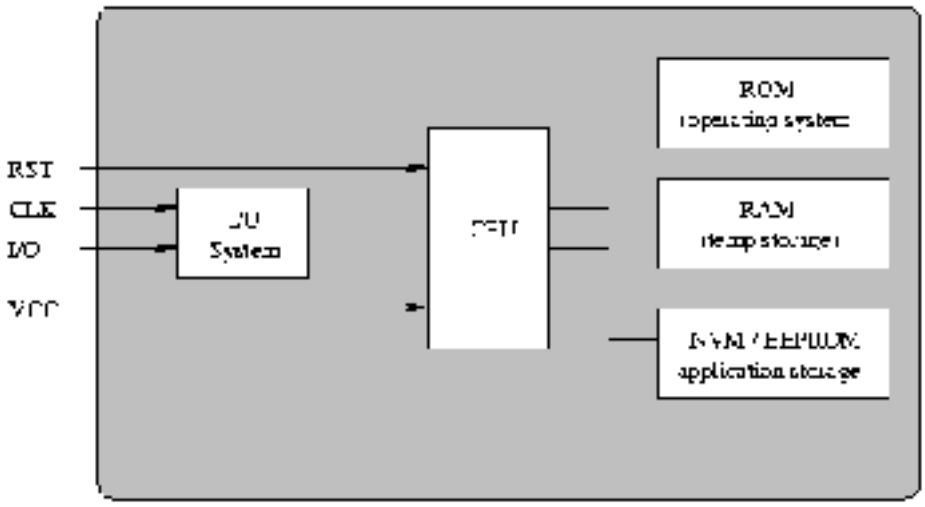


Figure 1. Architecture of a Smart Card. RST, CLK, I/O, and VCC illustrate the electrical connections to the I/O bus and CPU. [2]

Although physical attacks against smart cards are rare due to the length of time required to attempt breaking into the chip and the equipment needed in the process, it is important to recognize the possible threats. Physical attacks may be either passive, where the attacker simply observes and analyzes the cyphertext in an attempt to break the encryption code on the smart card, or active, where the attacker will try to tamper with data transfer or the microcontroller. These threats may occur at any time during the production cycle including development and manufacturing or even after the card has been put in

use. By identifying these potential risks, measures may be put in place to protect against them, such as providing screens in the workplace to prevent visual spying during PIN configuration and assuring that no programmer has solitary access to the chip code during production.

To perform a physical attack the attacker would need tools such as a microscope, a laser cutter, focused ion beams, chemical etching installations, and most likely the knowledge that there is data on the card that holds value to the attacker (other than the mere prestige among certain groups for breaking the card). The first step would be in removing the chip from the card without damaging it and removing the epoxy resin that coats the chip. Sensors are often installed on the chip and are used to detect high temperatures associated with the resin removal process, or to detect light sources from a microscope when viewed. These sensors, when activated, can automatically delete the data from the chip. One problem with this method is that without being near a power source the sensors can not delete any data.

Dummy Structures are sometimes used in the design of the chip. In this method extra semiconductors that have no function are installed on the chip. These semiconductors are simply put there to confuse an attacker who is attempting to visually inspect the surface of the chip for data.

**Smart Card Microprocessors**

The main element of smart card chips is the 8-bit microprocessor, located in the center of the chip layout. Typical speeds are currently within the tight range of 3 to 5 megahertz, with the most common CPU designs in the industry being derivatives of the Motorola 6805 or Intel 8051 architectures. Both processors are very cheap to build and relatively simple in design. Specialty processors also exist, for very high-speed applications. They can execute up to 1 million instructions per second, as opposed to the typical 400,000 instructions per second boasted by a standard processor such as the Motorola or the Intel.[3]

**Smart Card Input/Output**

The I/O on a smart card can work in one of two ways: they are either contact cards or contactless cards. Smart cards are subject to physical characteristics determined by International Standards Organization (ISO) 7816 standards, which specify the actual dimensions of the card, the location of the chip on the card, and where electrical contacts are to be placed on the card, among numerous other things.[4]

With a contact card the chip on the card communicates with a smart card reader through a set of eight electrical connections on the surface of the card with the following uses[5]:

| | |
|---|---|
| 1 – VCC | Operating voltage |
| 2 – RST | Reset connection |
| 3 – CLK | Clock |
| 4 – N/A | Reserved for future use |
| 5 – GND | Ground |
| 6 – VPP | Programming voltage |
| 7 – I/O | Data Input/Output |
| 8 – N/A | Reserved for future use |

With contactless cards the smart card need only be within a certain range of the reader, transmitting a signal that is picked up by the reader.[6] The chip gets its power to run either through one of the connections or from a magnetic field produced by the smart card reader.

### Smart Card Chip Size

A critical aspect to remember when considering the functional layout of a smart card is the chip size. A chip that is too small will not provide optimal performance due to wasted potential (its size will not be close enough to its torsional limit, the degree the chip may flex before breaking), and a chip that is too large will be too fragile for everyday use. Additionally, many smart cards are kept in their owner's flexible wallets and purses, which can lead to disaster if a larger chip undergoes too much deflection during storage. Optimum chip size, according to the smart card industry, has a surface area of about twenty-five square millimeters. This size limitation puts a great burden on smart card architects; they must determine a way to increase the performance of a smart card beyond that of a single twenty-five square millimeter chip while still preserving chip durability. Two methods are currently in existence for accomplishing this goal: the use of multiple chips (in an arrangement similar to multiple processor servers or desktop computers) and the development of a chip that has a higher density.

### Risks of Multiple Chip Design

Multiple chip designs raise an immense security issue. The transferring of data between multiple chips requires a small "data bus" to carry the data between locations which is susceptible to sniffing by would be attackers. An individual could access someone else's secure information by tapping into the data lines and performing various operations on the card, intercepting data as it passes by. Since smart cards are currently used for many financial applications, this attack can have devastating consequences. One method of securing the data bus on a smart card would be to add encryption to the data as it goes from chip to chip, but this adds overhead to the transmission, and may outweigh the performance gained by multiple chips. When this is combined with the drawback of high cost, smart card designers are left with only one option - higher density chips. A denser chip structure allows more functionality to be added to a design without changing size, leading to greater performance. This is the current trend

among smart card manufacturers, who attempt to increase the density of a chip as much as possible while still remaining within cost and fabrication limits.

### Types of Smart Card Memory

Directly connected to the processor on the smart card chip are three types of memory, all with a unique size and purpose. The first type of on-card memory is Read Only Memory (ROM), which usually contains the operating system information and other utility routines. Its size ranges between 8KB and 96KB for an average card, and is filled with its data during the manufacturing process. The information stored in the ROM remains unchangeable during the card's lifetime as the read-only name suggests, and rightfully so; certain modifications made to an on-card operating system or routines could possibly lead to incompatibility with the devices designed to interface with the card.

The second type of memory is Random Access Memory (RAM). Smart card RAM functions very similarly to that of a PC; it is excellent for storing data for a short amount of time but it is unsuitable for long term storage due to its volatile nature. Typical on-card RAM size is a few hundred bytes, which can sometimes lead to it becoming a bottleneck during processing.

Finally there is Electrically Erasable Programmable Read Only Memory (EEPROM), which is a type of nonvolatile memory where variable data is stored. It can be read from and written to on multiple occasions during a card's lifetime, and functions as a RAM substitute when necessary to avoid the aforementioned processing bottleneck. The EEPROM retains its information even when power is not available to the card, thus making it very attractive for holding long term data such as account numbers and usage information, which should not be lost when the card is extracted from a system. The amount of EEPROM memory capacity is typically .5K to 16K, with more memory coming from increased sizes and higher prices. EEPROM memory is usually what most affects the pricing of a chip.

### Securing Smart Card Memory

The chip may be designed with all busses for ROM, EEPROM, and RAM built internally in the chip, preventing access to the bus without dismantling the chip. It is possible to visually inspect the ROM on a chip with a powerful microscope and read the contents of the ROM bit by bit. Once read, bits can be assembled into bytes and read to complete the ROM code. Building the chip with the ROM in the lower layers of the chip would make it impossible to read the ROM through visual inspection.

### Variations on Smart Card Design

In addition to the three types of memory on a chip there are other chip features, meant to customize a particular chip for a specific application. Some of these features include but are not limited to: specialty communications hardware for contactless communications, coprocessors for faster security encoding and decoding, long registers which allow larger keys for encryption, and secret key escrow and storage registers for electronic purse applications. All of these added features are necessary for some cards, but not for others. For example, the secret key escrow and storage registers are present on cards that are used for transactions, but are unnecessary on smart cards such as those used for access control to a secure building. As the space on smart cards is limited, extraneous features can be removed from one card and replaced with other necessary ones, which is relatively simple to do.

## The Role of Smart Cards in User Authentication

Assuming that the smart card has made its way safely into the hands of the user, authentication of the cardholder becomes critical. The security of the smart card is only as good as the security of its user authentication system. For this reason, it is critical that the security measures go well beyond that of the physical security of the card itself.

With any type of security system there are three main categories of authentication:

1) Knowledge of a secret (password)
2) Possession of an object (token)
3) Bodily feature (Biometric)

### Password and PIN Use

Passwords for smart cards are known as Personal Identification Numbers (PINs) or sometimes referred to as Cardholder Verification (CHV). A PIN is usually a four digit number, never containing letters because not all card terminals have alpha-numeric keyboards. Because it only contains numbers, a four digit PIN has a total of 10,000 possible combinations. While time consuming, this four digit PIN could be cracked by an individual who manages to acquire the card. This technique is left over from the procedures that were followed when all plastic cards were magnetic stripe only.

With smart cards, the chip on the card may be programmed to disallow certain “easy” PIN combinations such as “1234”,”0911”, and any others that may coincide with the user’s birth date, anniversary or other significant value. Smart cards also sometimes have what’s known as “Super-PINS”, or PUKs (Personal Unblocking Keys). PUKs usually have more than 4 characters and can be used

to reset the retry counter if an incorrect password has been entered too many times. At the same time, a new PIN is entered since the cardholder has probably forgotten the original PIN.[7]

### Using Smart Cards as Tokens

Tokens are an inexpensive and easy way to authenticate users. One of the most common forms is the RSA Secure ID, where a user has a small device that displays a numeric value. This number changes every 60 seconds and only the authenticating server knows what the current value to be displayed should be. When logging into a network or accessing a facility the user will be prompted for the displayed number and will be denied access if an incorrect value is entered.[8] However, they are not used often in conjunction with smart cards, but rather the smart card itself may be the token. When used for security purposes (i.e., entrance into a secure building) a smart card can be used along with a PIN before granting access to the premises. This works especially well when used with biometrics.

### Biometrics

Biometrics is a method of comparing physical attributes of a person with a stored copy of those attributes. These can be facial features, hand geometry, a fingerprint, retinal scans, and many other traits. When a smart card is issued to a cardholder, the attributes of that person are stored in the EEPROM of the smart card. By comparing features it can be determined with great certainty that the person in possession of the card is indeed the person who is authorized to use the smart card. Using biometrics with a password protected smart card introduces all three factors of authentication simultaneously. One downside of biometrics is that it uses a non revocable trait, and once compromised may become forever invalid for that user. Additionally, there are social issues regarding biometrics and the storage of an individual's personal information in a central location.

### Parasitic Authentication and Pressure Sequencing

Research is currently being performed on additional smart card security measures such as Parasitic Authentication and Pressure Sequencing. With Parasitic Authentication the smart card relies on another device that must stay in close proximity to the smart card in order for the smart card to function. This works by using radio frequency identification (RFID) between the two units. RFID is mostly used in retail applications and for tracking items or people. A small transponder is attached either to a product or an individual. Transponders may be either active, where it is battery operated, or passive, in which case it will be powered by an electro-magnetic field created by a reader when the transponder comes within a certain range. There are also semi-passive transponders which have a battery operating the circuitry of the device but will

not communicate with a reader until the broadcast equipment is powered by the reader. Once powered, the transponder emits a radio signal that broadcasts information, possibly a serial number, item name, or other pertinent data.[9]

When used in conjunction with a smart card, an active transponder may be mounted inside a unit as small as a button, pendant, or an earring. This transponder broadcasts a signal that will only reach a very limited distance. The smart card is built with a receiver which constantly monitors for the presence of the transponder and once the smart card is out of the broadcast range from the transponder it will cease to function. Because of the possibility of the transponder being built into several different items, it would be much more difficult for someone to acquire the smart card and to identify the transponder. It also would be possible to program the smart card to work for a specified duration of time after losing its signal from the transponder so the smart card could be "recharged" once a day when the cardholder is at a certain verifiable location making it even less likely that the smart card and transponder both to be stolen by not having them both in possession by the cardholder, thus reducing the total loss or damages if the card is lost or stolen.[10]

The typical smart card biometric system uses equipment external to the smart card for checking the physical measure against the data on the card. Pressure Sequencing uses a device that is installed directly on the smart card and is independent of external hardware. This device incorporates a press pad and a piezo-electric layer to adjust electrical current between two electrodes, all of which are installed directly on the card. When the card is first issued, the cardholder can press the pad in a sequence (maybe a favorite jingle) that will fluctuate the current running between the electrodes and that the cardholder can repeat later. Data is stored in the smart card that holds information about the length, strength, and duration between each finger press, all computed by the fluctuations in current. If the stored data is not a match for the input given, access to the card's resources is denied.

This behavioral biometric has been shown to be as unique as fingerprints. While still in its infancy, initial experiments have shown Pressure Sequencing to be 97% accurate in identifying individuals.[11] Though not yet foolproof, this concept of the biometric authentication device built directly onto the smart card would enable any smart card reader to use the biometric confirmation without the additional overhead of specialized equipment and without the cardholder having the concern of where their biometric information is being stored.

## Conclusion

As long as Moore's Law continues to be upheld, smart cards and similar technologies will become more prevalent in everyday life for all people, technical or non. Devices will continue reducing in size and will be invisible to many people. The increased computing power of smart cards will greatly expand their

capabilities and applicability into new arenas. Identity, resource, and data theft are issues to be dealt with now and in the future. Developing ways to assure that only authorized people are able to obtain access to critical areas is crucial.

Those responsible for designing and managing smart card systems must not only focus on the technical features and advancements, but also on the environment in which the cards will operate. It takes much longer to build a consistent infrastructure for smart cards than to develop individual applications that will employ the use of the card. To ease the burden of creating a complex and expensive infrastructure, measures will need to be put in place to allow authentication of users without the need for specialized equipment in multiple locations. The use of a smart card that can do its own form of authentication be it biometric or otherwise will greatly enhance the applicability of smart cards in their existing and ever-expanding venues.

## References: Cited Works


[1] "Moore's Law." Intel Corporation. URL: http://www.intel.com/research/silicon/mooreslaw.htm (Dec. 27, 2003).

[2] Bezakova, Ivona, Pashko, Oleg, and Surendran, Dinoj. "Smart Card Architecture" Fall 2000. URL: http://people.cs.uchicago.edu/~dinoj/smartcard/ (Dec. 25, 2003).

[3] Jurgensen, Timothy M. and Guthery, Scott B. Smart Cards - The Developer's Toolkit. Upper Saddle River: Prentice Hall 2002.

[4] "Executive Summary of Government Smart Card Interoperability Specification (GSC-IS)" URL: http://www.smartcardalliance.org/pdf/alliance_activities/DSI_GSC_Paper.pdf (Dec. 29, 2003).

[5] Haghiri, Yahya and Tarantino, Thomas. Smart Card Manufacturing. New York: John Wiley and Sons, 2002.

[6] "Smart Card Overview." Java Card Special Interest Group. URL: http://www.javacard.org/others/smart_card.htm (Dec. 26, 2003).

[7] "National Security National Concerns" URL: http://www.sspsolutions.com/files/SSP_-National_Security_National_Concern.pdf (Dec 23, 2003).

[8] "RSA Security | RSA SecurID Tokens" URL: http://www.rsasecurity.com/products/securid/tokens.html (Dec. 27, 2003).

[9] "RFID Journal – Frequently Asked Questions" URL: http://www.rfidjournal.com/article/articleview/207#anchor#002 (Dec. 28, 2003).

[10] Ebringer, Tim, Zheng, Yuliang, And Thorne, Peter. "Parasitic Authentication." Smart Card Research and Advanced Applications. London: Kluwer Academic Publishers, 2000: 307 – 326.

[11] Henderson, N.J. and Hartel, P.H. "'Pressure Sequence' – A Novel Method of Protecting Smart Cards." Smart Card Research and Advanced Applications. London: Kluwer Academic Publishers, 2000: 241 - 256.

## References: Other Resources

Hendry, Mike. Smart Card Security and Applications. Norwood: Artech House, 2001.

Rankl, W. and Effing, W. Smart Card Handbook. New York: John Wiley and Sons, 2000.

Weidong Kou, Payment Technologies for E-Commerce. New York: Springer-Verlag, 2003.

Last Updated: July 26th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS Boston 2017 | Boston, MA | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| Community SANS Omaha SEC401* | Omaha, NE | Aug 14, 2017 - Aug 19, 2017 | Community SANS |
| SANS New York City 2017 | New York City, NY | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS Salt Lake City 2017 | Salt Lake City, UT | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| 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 |
| Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style | Virginia Beach, VA | Aug 21, 2017 - Aug 26, 2017 | vLive |
| SANS Chicago 2017 | Chicago, IL | 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 |
| Community SANS Albany SEC401 | Albany, NY | Sep 11, 2017 - Sep 16, 2017 | Community SANS |
| Mentor Session - SEC401 | Ventura, CA | Sep 11, 2017 - Oct 12, 2017 | Mentor |
| 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 |
| 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 |
| 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 Sacramento SEC401 | Sacramento, CA | Oct 02, 2017 - Oct 07, 2017 | Community SANS |
| SANS DFIR Prague 2017 | Prague, Czech Republic | Oct 02, 2017 - Oct 08, 2017 | Live Event |
| Community SANS Charleston SEC401 | Charleston, SC | Oct 02, 2017 - Oct 07, 2017 | Community SANS |
| Mentor Session - SEC401 | Arlington, VA | Oct 04, 2017 - Nov 15, 2017 | Mentor |
| Community SANS Indianapolis SEC401 | Indianapolis, IN | Oct 09, 2017 - Oct 14, 2017 | Community SANS |