Global Information Assurance Certification Paper

Department of Defense
Public Key Infrastructure

Sandra Felton
January 19, 2004

SANS GIAC GSEC Practical Assignment version 2.7 option 1

Introduction

Federal agencies, including the Department of Defense (DoD), rely heavily on the Internet to provide on-line public access to information and services as well as to conduct internal business operations. While Internet-based applications offer enormous efficiencies in service and productivity, they also introduce significant security risks that threaten to impair national security. To achieve information superiority in a highly interconnected, shared-risk environment, DoD Information Assurance capabilities must contend with providing timely, accurate information to fulfill the everyday mission, while protecting the information from attack. To meet this objective, the DoD employs Defense-in-Depth, a technical strategy that underlies DoD information assurance in which layers of defense are used to achieve security objectives. No single countermeasure can provide adequate assurance independently. Defenses of varying strength and assurance levels must be overlapped to provide multiple countermeasures for protection of our sensitive information systems from those internal and external adversaries who would try to exploit them, thus achieving a balanced IA posture. An element of the Defense-in-Depth strategy is the use of a common, integrated, interoperable DoD Public Key Infrastructure (DoD PKI) to provide security services at multiple levels of assurance. The funding allocated for the DoD PKI for Fiscal Years 2001-2005 is nearly $1 billion. This paper overviews the DoD PKI implementation and examines the return on this hefty investment.

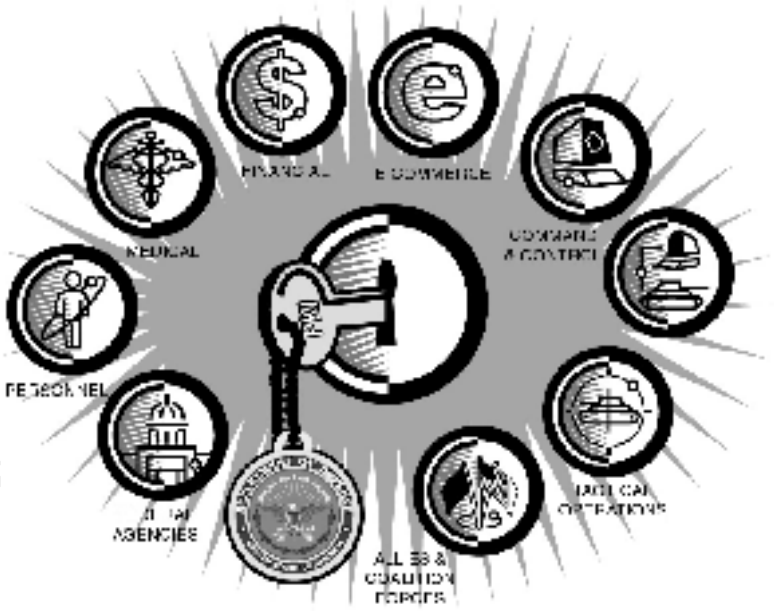

Figure 1. DoD Missions and Operations Relying on PKI [3]

PKI is the framework and services that provide the generation, production, distribution, control, tracking and destruction of public key certificates. The purpose of a PKI is to manage keys and certificates in a way in which an organization can maintain a trustworthy networking environment. PKI enables the

use of encryption, digital signature, and access authentication services in a consistent manner across a wide variety of applications. The DoD PKI will support directly the Department's desire to encourage the widespread use of public key (PK)-enabled applications throughout the Department's activities. The DoD PKI will evolve as an essential element of the overall Key Management Infrastructure (KMI) and will be realized as an integral part of DoD's KMI evolution. The National Security Agency (NSA) has initiated a DoD KMI program, with the support of the Defense Information Systems Agency (DISA), the Services and Agencies, Joint Staff, and the DoD contractor community. The DoD KMI will enable the provisioning of cryptographic key products, symmetric and asymmetric (public) keys, and security services. The DoD KMI will be implemented through a phased evolution delivering Capability Increments (CIs) every 18-24 months. The PKI is the primary component of the first CI, CI-1. This contract is the first in the incremental plan that is intended to provide the foundation for achieving the DoD's Key Management target architecture. Work to be completed includes the development and fielding of a Class 4 PKI certification management system that integrates multiple Certificate Authorities (CA). [3]

PKI Roadmap

The Public Key Infrastructure (PKI) Roadmap, latest version dated December 18, 2000, establishes the enterprise-wide target for the DoD PKI and outlines the evolution strategy along with an aggressive timeline for DoD PKI capabilities. This long-term strategy document also identifies critical risk management issues and defines roles and responsibilities of organizations involved with its realization.

The DoD PKI strategy recognizes that a traditional, Government-developed implementation will not be able to keep pace with a strategy based on commercial technology and services. To be successful, the DoD PKI must employ an incremental, evolutionary approach using open standards, based on commercially available products and services that can keep pace with the technological evolution of applications and standards commonplace in the Information Technology (IT) environment. Still, it must maintain required levels of security, facilitating secure interoperability internal and external to the DoD.

PKI Products and Services

PKI, as defined herein, refers to the framework and services that provide for the generation, production, distribution, control, revocation, recovery, and tracking of public key certificates and their corresponding private keys. The DoD PKI supports registration of users, dissemination of certificates, and a full range of certificate management services. This provides the critically needed support to individuals, applications, and network devices that provide secure encryption and authentication of network transactions as well as data integrity and non-repudiation. [3]

Certificates are trusted vehicles used to bind an identity to a public key. The initial deployment of the DoD PKI provides two types of certificates: identity certificates (used for authenticated access and digital signatures) and key establishment (confidentiality) certificates. There are profiles within these types that support certificates for servers, e-mail signature services, and e-mail confidentiality services. To achieve common certificates across the entire DoD, the DoD PKI identity, e-mail signing, server certificates, and encryption certificates have a minimum/common set of attributes as specified in the certificate profile section of the DoD X.509 Certificate Policy. Unique e-mail certificates are needed to support current versions of the commercial S/MIME protocol that requires an e-mail address to be embedded in certificates, but may not be necessary in the future. As it evolves, PKI operational requirements may dictate that additional certificate types be provided.

A Brief History

Since the mid 1980s, NSA has used PK technologies in a number of large deployment programs. In the next ten years, there was development of a hardware token (FORTEZZA) and an operational PKI under the Multilevel Information Systems Security Initiative (MISSI) to support organizational messaging under the Defense Messaging System (DMS) using Government-off-the-shelf (GOTS) technologies. The development of FORTEZZA hardware tokens and a Government-developed Certificate Authority capability, which required the use of Certificate Authority Workstations (CAWs) to register and issue certificates on the FORTEZZA token, were the basis of the Class 4 PKI designed primarily to support DMS. Approved for operational use in March 1995, the infrastructure has been updated to support subsequent releases of DMS. The latest CAW update provides the capability to support X.509 version 3 certificates, key recovery for private confidentiality keys, and security labeling compatible with DMS Release 3.0. [3]

In the mid 1990s, DoD decided to assess the value of the rapidly evolving commercial PKI technologies by deploying a commercial, Medium Assurance PKI and a series of application pilot programs that relied on it. In 1999, DoD policy called for making the Medium Assurance PKI pilot an operational (Class 3) capability, sustaining the existing DMS (Class 4) PKI, and planning for an evolution to the DoD PKI that would eventually replace both of these systems. The DoD PKI will be implemented as an integral part of DoD's KMI evolution. Beginning with Release 4.0, PKI releases will be integrated as part of the appropriate KMI capability increments. While the DoD PKI continues to evolve, existing PKI capabilities will remain operational to facilitate an efficient transition. [3]

PKI Components

Programs, which carry out or support the mission of the DoD require services such as authentication, confidentiality, technical non-repudiation, and access control. These services are met with an array of network security components such as workstations, guards, firewalls, routers, in-line network encryptors (INE), and trusted database servers. The operation of these components is supported and complemented by use of public key cryptography. As a system solution, the components share the burden of the total system security. The use of public key certificates does not add any security services in a poorly designed or implemented system.
Security management services provided by the PKI include:
• Key Generation/Storage/Recovery
• Certificate Generation, Update, Renewal, Re-key, and Distribution
• Certificate Revocation List (CRL) Generation and Distribution
• Directory Management of Certificate Related Items
• Certificate Update, Renewal, and Re-key
• Certificate token initialization/programming/management
• Privilege and Authorization Management
• System Management Functions (e.g., security audit, configuration management, archive, etc.)

PKI requirements to ensure the security of these services:
• Subscriber identification and authorization verification
• Control of computer and cryptographic systems
• Operation of computer and cryptographic systems
• Usage of keys and public-key certificates by Subscribers and relying parties
• Definition of rules to limit liability and to provide a high degree of certainty that the stipulations of this policy are being met

X.509 Certificate Policy

The United States Department of Defense Certificate Policy (CP) is the unified policy under which a Certificate Authority operated by a DOD component is established and operates. It defines the creation and management of Version 3 X.509 public-key certificates for use in applications requiring communication between networked computer-based systems. Such applications include, but are not limited to, electronic mail; transmission of unclassified and classified information; signature of electronic forms; contract formation signatures; and authentication of infrastructure components such as web servers, firewalls, and directories. The network backbone for these network security products may be unprotected networks such as the Internet or Nonclassified Internet Protocol Router Network (NIPRNET), or protected networks such as the Secret Internet Protocol Router Network (SIPRNET). [2]

Five distinct levels of assurance are defined within the Certificate Policy.
DOD Class 2: is intended for applications handling unclassified information of low value in a Minimally or Moderately Protected Environment. DOD CAs will not issue CLASS 2 certificates; the DOD shall issue CLASS 3 and CLASS 4 certificates exclusively. Access to DOD information resources shall never be allowed on the basis of CLASS 2 certificates. CLASS 2 certificates, (or non-DOD equivalent certificates) may be accepted by DOD relying parties for the purpose of authenticating or encrypting communication that does not access or process DOD information (meeting coordination, accessing web site information that has been cleared for unlimited distribution. etc.) These certificates may, for example, be issued by non-DOD commercial entities. [2]

DOD Class 3: is intended for applications handling unclassified medium value information in Moderately Protected Environments, unclassified high value information in Highly Protected Environments, and discretionary access control of classified information in Highly Protected Environments.
DOD Class 3 Hardware: is intended for applications handling unclassified medium value information in Minimally Protected Environments, unclassified high value information in Moderately Protected Environments, and discretionary access control of classified information in Highly Protected Environments. This level is also intended for all applications operating in environments appropriate for CLASS 3 but which require a higher degree of assurance and technical non-repudiation. This level is intended for applications performing contracting and contract modifications. [2]

DOD Class 4 is intended for applications handling high value unclassified information in Minimally Protected environments. Finally, DOD Class 5 is intended for applications handling classified material in Minimally Protected Environments, and authentication of material that would affect the security of classified systems. This policy does not currently define the requirements associated with CLASS 5 certificates. As National Manager for National Security Telecommunication and Information Systems Security (NSTISS), only the Director, NSA, may approve the use of a lower assurance certificate to protect classified material in a Minimally Protected Environment. Procedures for issuance and use of specific DIRNSA-approved certificates will be separately documented. [2]

The strategy to achieve the target DoD PKI is intrinsically linked to the overall DoD strategy for achieving IA. On November 10, 1999, the Deputy Secretary of Defense directed that the CAC be used as the DoD's primary platform for the PKI authentication token. A report to Congress, "Consideration of Smart Cards as the DoD PKI Authentication Device Carrier" dated January 10, 2000, was submitted in compliance with section 374 of the fiscal year (FY) 2000 Defense Authorization Act (Public Law 106-65), requiring the evaluation of the option of using the smart card as the DoD's authentication token. The report concludes the smart card is

the most feasible, cost-effective technology for the authentication mechanism to support the DoD PKI and to protect its critical information. [3]

A smart card is similar to a credit card with hardware token containing one or more embedded memory and/or microprocessor integrated circuit chips (ICC). The smart card may contain other data display, storage or transfer technologies such as a linear barcode, two-dimensional barcode, magnetic stripe, radio frequency antenna and biometrics. It can support multiple applications, such as storing personal data, calculating values, validating biometric identification, performing digital certification, and encrypting information.

In 1993, the DoD began conducting evaluations of smart card technology. Initially tested as an updateable individually carried data storage device, the Department's smart card requirement was expanded to an interoperable, backward compatible device for secure on-line data transfer and on-line transactions. In 1997, the Deputy Secretary of Defense (DEPSECDEF) established the Smart Card Technology Office to fully conduct and oversee smart card demonstrations of joint applications. The success of these pilots and Service-specific demonstrations, coupled with the Departments Public Key Infrastructure token requirements, resulted in the November 1999 DEPSECDEF directive to use smart card technology for multiple applications on a single platform, the Common Access Card. [4]

The Common Access Card

The DoD's smart card technology implementation is a Department-wide Common Access Card (CAC). The CAC is the standard identification card for active duty military personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel. The CAC will also be the principal card used to enable physical access to buildings and controlled spaces and for logical access to the Department's computer networks and systems. The CAC platform will contain the mandatory identification, physical and logical access capabilities and may also contain Department-wide and/or Component-specific applications such as manifesting, deployment readiness, food service, and medical/dental readiness.

Figure 2. Sample Common Access Card [8]

Over 4 million active duty military members, Selected Reserve, DoD civilians, and eligible contractors have received the CAC. An aggressive awareness campaign began in the summer of 2000 to ensure Department leadership, card recipients, and supporting vendors are educated on the value and benefits of the CAC. The CAC issuance began in October 2000 in selected regions; now the cards are being issued in approximately 945 locations in 27 countries and scheduled to be complete by March 2004.

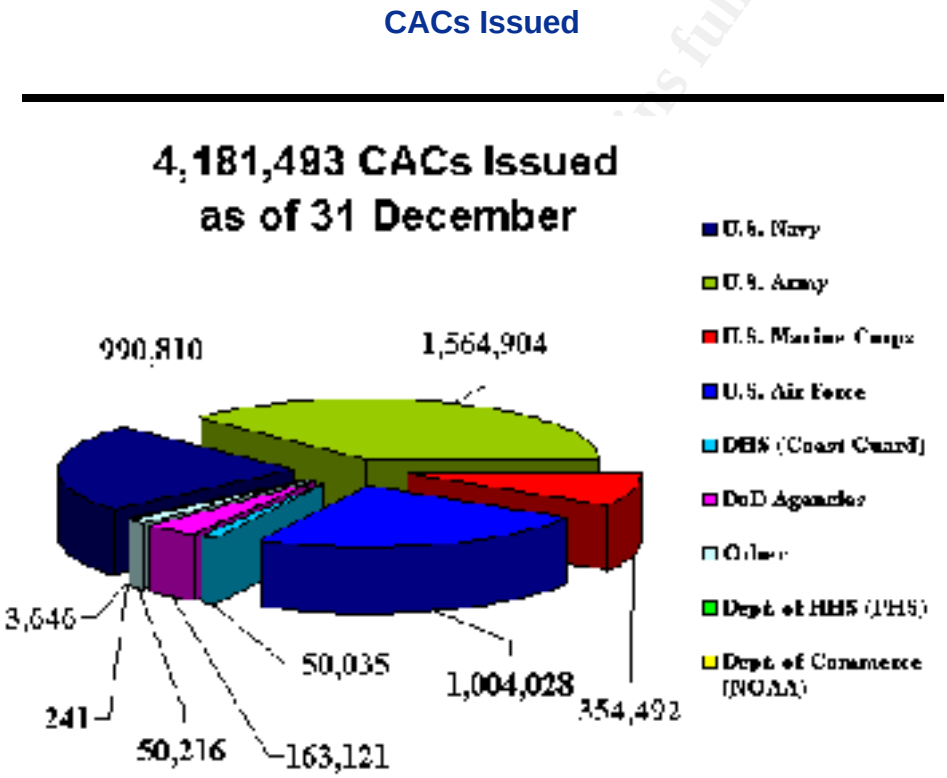

Figure 3. Common Access Cards Issued within DoD [10]

The CAC, as the hardware token for the DoD PKI, is an essential part of daily operations within the DoD, and it plays a key role in the information assurance defense-in-depth strategy for unclassified and sensitive but unclassified data. CAC recipients will gain appropriate access to computer systems and perform secure transactions over networks. Those failing to obtain a CAC will not be able to access their DoD computer at work, nor will they be able to access DoD private Web sites or send DoD e-mail.

The CAC has a number of security features that protect the data on the card including cryptographic services to secure personal information as well as information transmitted. The key components that enable these functions are the cardholder's PIN (6-8 digit person identification number), the PKI private keys generated and stored on the chip, and the associated PKI certificates that reside on the chip. Additionally, the CAC Cardstock Specification requires input voltage, input frequency, and temperature sensors that reset the card when an out of normal operating range condition is detected.

Access to the Department's public key enabled computers and systems will be granted only when all of the following are presented: the CAC, valid PIN, valid certificate, and authorization to that particular computer or system.
The current CAC has thirty-two demographic elements of data stored in the integrated circuit chip on the card. The majority of these elements are actually printed on the card. Gaining access to the data stored on the chip currently provides minimal information. The future data requirements, as well as the use of the card by services and agencies, may provide data that could be exploited. The card is not, however, a repository for classified data and it is expected that many applications developed to use the card will be web-based, vice data based. That is, the data will not actually reside on the card but will be securely accessed from a central source using the card.

To access the data on the chip, or utilize the certificates on the chip, a PIN must be entered. The card has a lockout function that activates after three incorrect PIN attempts. To reset the card, you must return to a CAC issuance station, present the card, show proof of identity as card owner, and verify your fingerprint against the one stored in the Defense Eligibility Enrollment Reporting System. The card can then be re-enabled. If the card and its PIN were available, access to the certificates and the information on the chip would be possible. However, the system has a procedure to revoke certificates on cards that are lost or stolen and on cards held by personnel in specific personnel categories, such as POWs and MIAs. Any application that reads and passes data to and from the card must be registered and digitally signed by the US Government. If the authenticated 'keys' for this process are not present, the integrated circuit chip on the card will not work and cannot be accessed.

The CAC shall be used to control access to DoD facilities, installations, and controlled spaces. This policy does not preclude the continued use of supplemental badging systems that are considered necessary to provide an additional level of security not presently afforded by the CAC, however, DoD activities are to plan for migration to the CAC for general access control using any of the CACs present or future access control capabilities.

Overcoming Obstacles

Initially, department officials considered satisfying the need for digital signatures by issuing software tokens on floppy disks. But this would have required the development and fielding of a complex and expensive face-to-face registration. Consulting with one of the nation's leading experts in smart card technology, the DoD converged the PKI and identity programs to leverage one infrastructure instead of two. But officials acknowledge that implementation will not be achieved as quickly as originally planned.

Few applications are being implemented with the rollout; others still are in the planning stage. Users are frustrated at times because the cards are being issued first, before the application infrastructure is in place. This generates a catch-22 scenario for application developers. If you have an infrastructure, but no one has a card, you can't change the applications over. Likewise, without public key enabled applications requiring the CAC for access, many users forget their PIN and must go through the hassle of resetting the card.

The project also had to overcome challenges with national security certification. DMDC and its industry partners broke new ground to meet National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 cryptography certification and National Security Agency (NSA) systems security accreditation. It proved to be a slow process. In addition, real world events abroad, and the resulting massive troop deployments affected the card distribution deadline. [8,9]

Although it's declining, the CAC issuance failure rate continues to be high, between 10 and 15 percent in 2002-2003. Printing problems and high personnel turnover are the main causes for the high rate. Replacing hardware on a three-year cycle, technological advances in printers, and training should lead to a reduction in the failure rate. [8]

CAC Failure Rates

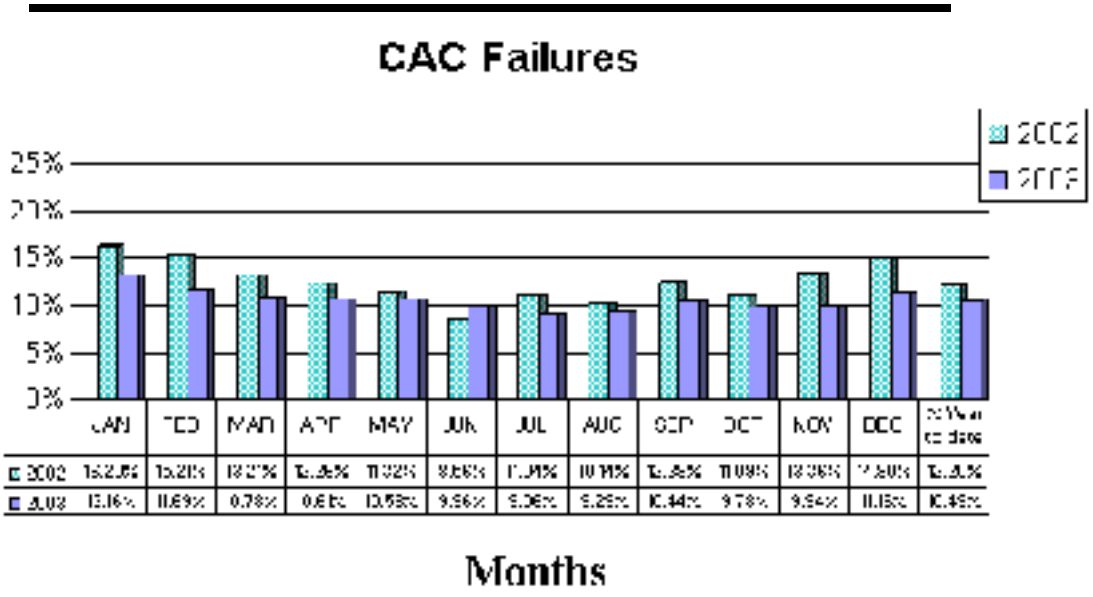

Figure 4. Common Access Card Failures [11]

The Next Wave of PKI

For the future, DMDC and its industry partners are looking at more centralization in issuing the cards. DoD wants to be able to apply best practices and raise the bar as far as strengthening the CAC as a credential, and the bar needs to be raised continually. Storing biometric data, such as fingerprints, on the CAC is being considered. Another possibility being explored is the use of contactless cards to save on the wear and tear of the CAC. [8]

The Defense PKI Program Management Office is looking ahead to the next wave of PKI for securing e-mail. Future enhancements include adding biometrics to the smart cards and use of 64K chips and more PKE applications. New Common Access Cards will be more hardened, more robust—to provide more functionality for DOD PKI users.

Looking even farther down the road, an external review conducted by the Joint Service Advisory Group to the DoD chief information officer had this to say: “The DoD CAC–a combination Military ID card and the host for the PKI hardware token—will eventually have the same national impact as the ARPANET did in leading to the Internet.” [8]

References

1. http://nsa2.www.conxion.com/support/guides/sd-1.pdf
   Defense in Depth, undated pdf

2. http://www.defenselink.mil/nii/org/sio/ia/pki/DOD_CP_V7.0_18Dec2002_R.pdf
   X.509 Certificate Policy for the Department of Defense, v7.0, 18 Dec 2002

3. http://iase.disa.mil/pki/dodpki-roadmap.doc
   PKI Roadmap for the Department of Defense, v5.0 18 Dec 2000

4. http://iase.disa.mil/pki/SMpolicy.pdf
   DoD Smart Card Adoption and Implementation, 10 Nov 1999

5. http://iase.disa.mil/pki/pkim0812.pdf
   Department of Defense (DoD) Public Key Infrastructure (PKI), 12 Aug 2000

6. www.gcn.com/vol1_no1/daily-updates/22553-1.html
   Dawn Olney, Def looks to new wave of PKI and smart card use, 24 Jun 03

7. www.sspsolutions.com/news/press_release.php?Article=122
   SSP Litronic Company Announcement, 26 Feb 2002

8. www.mit.kmi.com/archive_article.cfm?DocID=234
   Patrick Clark, Smart Card Security, 13 Oct 2003

9. http://infosecuritymag.techtarget.com/2003/may/dodid.shtml
   Neil Roiter, Who Are You DoD Gets Smart, May 2003

10. www.dmdc.osd.mil (private)
    Number of CACs Issued per Component

11. www.dmdc.osd.mil (private)
    Overall CAC Failure Rate

12. www.dmdc.osd.mil (private)
    CAC Issuance Mandate, 25 Sep 2003

Last Updated: July 22nd, 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
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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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 Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 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
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 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