SAND2015-8704C

Exceptional service in the national interest

Sandia National Laboratories

Photos placed in horizontal position with even amount of white space between photos and header

TE Framework

A Framework For Securing COTs Applications

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Sandia National Laboratories

"The 21st century has been bombarded with technological innovations aimed at a tech savvy youthful market and communication is getting more open in a world that is truly getting smaller by the day; we are living in a global village."
~Abayomi Oloko , *Information Security in the Enterprise and Modern Challenges*

Introduction

Sandia National Laboratories

- Increased usage of COTS and GOTS software(s) across organizations
  - These software(s) can pose a security risk for organizations
- Rapid Cybercrime growth
  - OPM breach
- Evolution of Information Security Management
  - Exists in most organizations now, whereas previously did not
- Cyber-security is ever evolving

TE Framework

Sandia National Laboratories

- Designed to assist engineers and developers in strengthening an organizations security posture when integrating COTS software
- Broken into two areas:
  - TE Analysis
  - TE Architecture
- Focuses on the entire life-cycle: design to decommission
- Not all components are necessary for all cases
- Can be used to address the three core fundamental principles of all security systems: confidentiality, integrity, and availability

TE Analysis

- Broken into four parts
  - Brainstorming Sessions
  - TE Baseline Assessment of Cyber Risk
  - TE Design Assurance
  - TE Security Engineering

Brainstorming Sessions

Sandia National Laboratories

- These sessions can help an organization to better understand the scope and effort needed for their particular situation
- All brainstorming sessions may not be needed to be utilized for each organization
- For these sessions one must ensure all stakeholders and responsible parties are in attendance so that a 360-degree view can be achieved.
  - Ex: System Administrators, Security Engineers, Hardware Engineers
- Can be broken into three Brainstorming Sessions:
  - Questions Brainstorming Session
  - Operational Challenges Brainstorming Session
  - Malicious Actors Brainstorming Session

Questions Brainstorming Session

Sandia National Laboratories

- Types of Questions to Answer:
  - What are we trying to secure?
  - Which key approach should be the focus in how we address the security of this system: security depth or breadth?
  - Even though we cannot solve all cyber-risks, are there things that we can design or implement within the system that will reduce the external risks?
  - Should the security design apply the same approaches and techniques for all functional areas of the system, or should the strategies and techniques be tailored to the functional area?
  - How many different security domains are necessary?

Operational Challenges Brainstorming Session

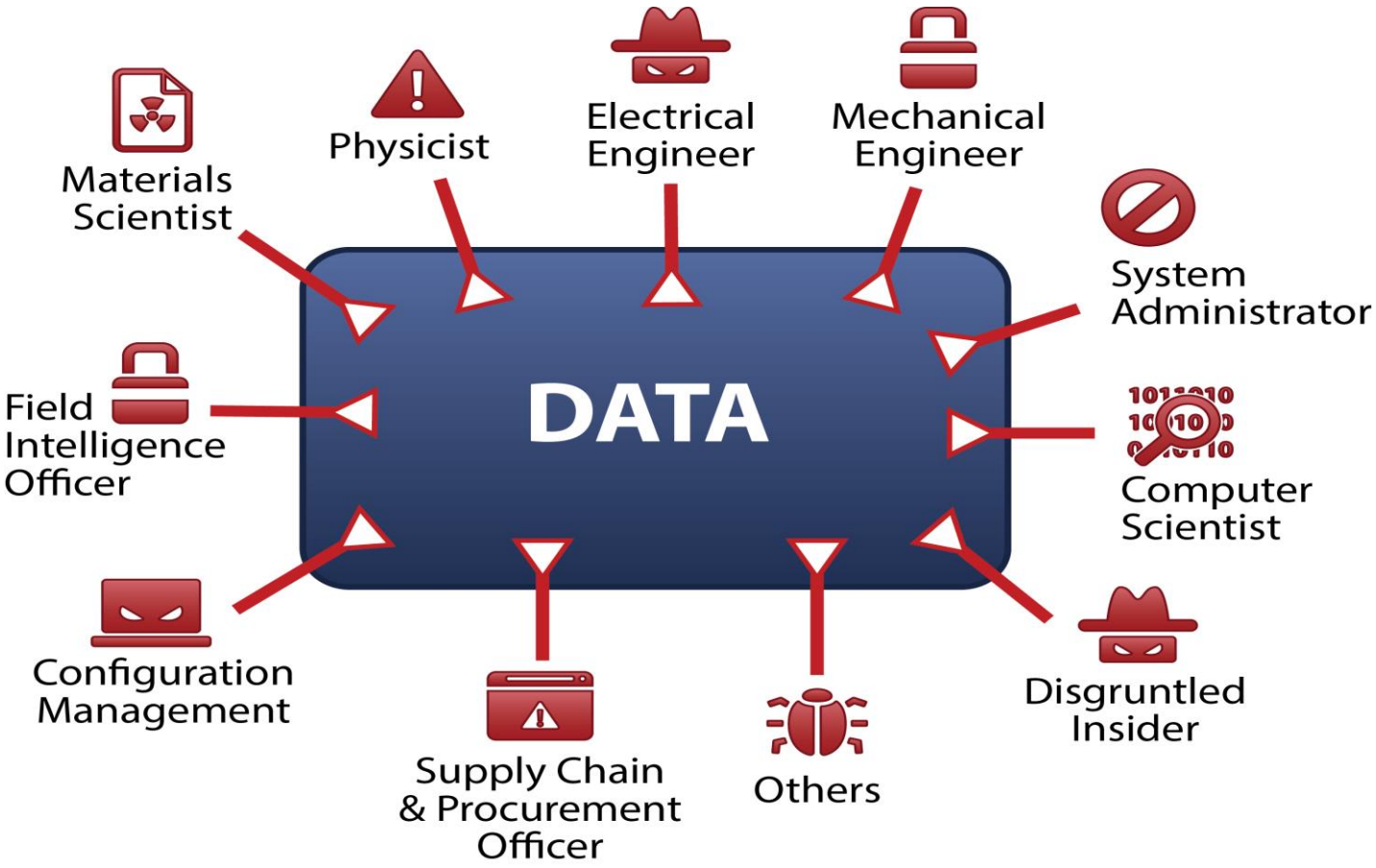
- Includes the following types of questions:
  - Evaluation of an organization's current or proposed environment for key critical systems, including possibly numerous COTS and custom applications
  - Evaluate current methods used for managing the systems. Management of these systems can be by using standalone, custom information technology systems and/or processes optimized to support the organization's unique mission/goals.
  - Evaluate data that is stored and the enterprise-information architectures. An organization's enterprise-information architectures and information systems may collect, process, store, and transmit large amounts of data.
  - Evaluate the combination of varying applications that may create a complex architecture with many interdependencies. As the number of interdependent applications increases, it becomes exponentially more difficult to secure the system because of the many inflows and outflows.

Malicious Actors Brainstorming Session

Sandia National Laboratories

- Many types of malicious actors seek different kinds of information; each with a different intent
- Sometimes they may not be the individuals that carry out the exfiltration, but may be the end user of the information gained through subversion
- Important to fully understand the risk and possible malicious actors to an organization's system(s)
- Design decisions should be made so that an increase in system security posture is realized
- If an engineering decision reduces the system's security posture, the change should not be incorporated

Malicious Actors



Defining Trust Brainstorming Session

Sandia National Laboratories

- Trust engineering is a relatively new term in information technology (IT)
- Government agencies, who have significant interest in ensuring data confidentiality, integrity, and availability, were some of the first proponents of the approach now called **trust engineering**.
- “The problem with COTs products”, says Alexander, “is that organizations have to grapple with untrusted components to get the functionality needed to make the business run smoothly”

Trust Engineering

Sandia National Laboratories

- Software has now become “the unwitting delivery mechanism for network attacks” due to a number of factors:
  - Computers have made it possible to do far more interesting things with information than merely communicate it, and the appetite for new functionality has become insatiable.
  - Protection of information is not the killer app for most customers of the newer functionalities, and information technology vendors.
  - A flatter world has produced a dynamic, global IT supply chain offering state-of-the-art functionality much more cheaply than it can be obtained from vetted providers.[2]

TE Baseline Assessment of Cyber Risk

Sandia National Laboratories

- A baseline assessment should be conducted so that system owners may be aware of possible risk areas from within the COTS solution
- Helps to understand the extent of the potential issues and work towards specific mitigations to address them
- Conducting a cyber-risk baseline assessment applies the Trust Engineering principles and characterizes the system or COTS solution so that the potential risks are fully understood and mitigations can be engineered to reduce the attack surface

TE Design Assurance

Sandia National Laboratories

- Definition and application of design assurance greatly varies between design teams, organizations, companies, and even government entities
- The end goal of design assurance is to follow a well-defined process to increase the security posture throughout the design phase through disposal of the product
- Possible activities during Design Assurance:
  - Run COTS vulnerability analysis tools, fault tree analysis, code reviews looking for weak validation of function parameters, extensive testing using statistical-based test pattern
- Simplified design assurance characterization and analysis process (iterative in nature) should contain the following: Planning, Data Collection, Characterize, Analyze, Report, and Engage
- Red-teaming can be used to acquire an independent and adversarial-like view of the areas of vulnerability and concern for an organization.

TE Security Engineering

Sandia National Laboratories

- System designers and security engineers need to accomplish all of the below major tasks:
  - Least-privilege security model,
  - System architecture assessment,
  - Adversary threat model,
  - System monitoring and intrusion detection technology assessment,
  - Information protection technology assessment,
  - Security system requirements definition and meta-model,
  - Baseline cyber-risk assessment and design assurance red teaming,
  - Trusted architecture design and system mitigations,
  - Cyber-security acceptance test plan & tests, and
  - Cyber-security maintenance plan.

Security Threat Model

Sandia National Laboratories

- Primarily identifies issues that challenge the system's confidentiality, integrity, and availability
- Will include a number of generic attacks that apply broadly to many networked information systems
- Applications can have many specific threats associated with it
  - The identified specific threats, vulnerabilities, and weaknesses may be from previous studies on the existing system as well as new ones discovered during the baseline assessment and interim testing.

TE Architecture

Sandia National Laboratories

- Information gleaned during TE Analysis is a direct input into the TE Architecture
- A system can be broken down and defined into a number of functional zones within the system where cyber-protection technologies should be implemented
- Nine primary factors that provide a unique view on the security of the system or subsystem:
  - System monitoring & analysis,
  - Hardware,
  - Network,
  - Virtual environments (virtual machines, virtual networks, etc.),
  - Software security (including operating systems, applications, middleware, etc.),
  - Human Factors,
  - Patches and upgrades,
  - Configuration management, and
  - Post-incident forensics
- The TE Architecture focuses on the key areas of a containered/enclave approach to system security, defense-in-depth, layered defense and least-privilege.

TE Architecture

Sandia National Laboratories

- There are many areas that the TE architecture can help better secure a system they are as follows:
  - Containered/Enclave Approach
  - Least Privilege
  - Defense-in-Depth
  - Network Defenses
    - Network Enclaves
  - Monitoring
  - Operations
    - Procedures and Policies
    - Trusted Software Process

Containered/Enclave Approach

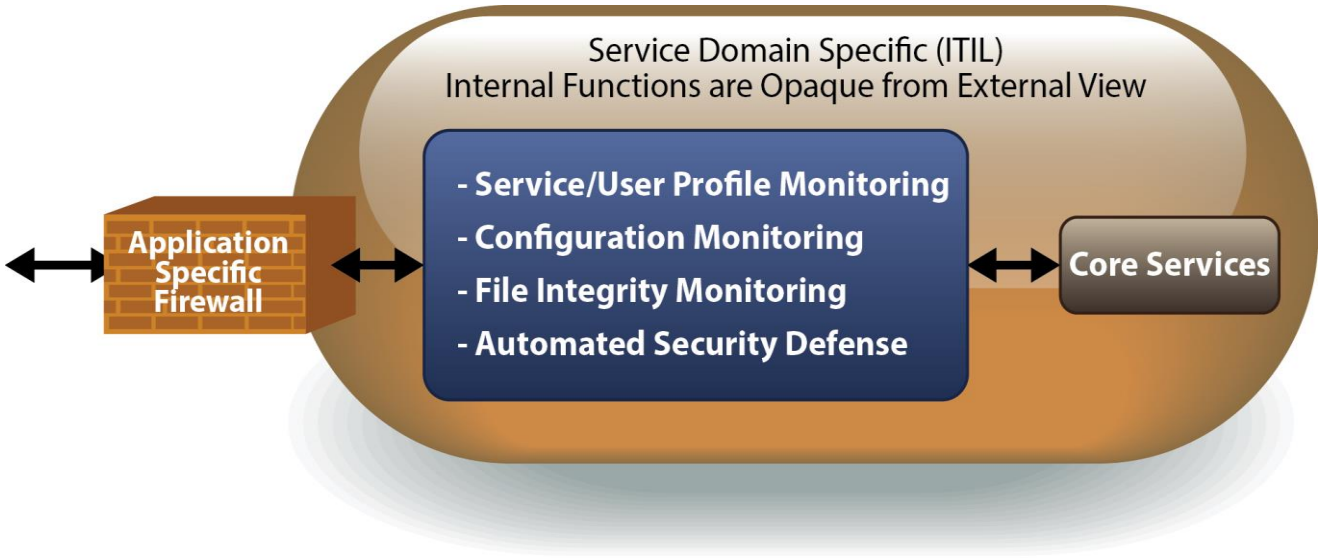
Sandia National Laboratories

- For the Container/Enclave it is important to:
  - Containerize (physically isolate) COTS system (Hardware, Application, Middleware, Database), critical environments;
  - Implement application firewall(s) with advanced monitoring and detection;
  - Encapsulate all internal processes, operation, and monitoring from external view;
  - Continual and ongoing internal testing of files and software to ensure system integrity;
  - Implement a least-privilege model - limit container personnel access;
  - Tightly control configuration management of entire system (Hardware, Software, and People); and
  - Securely manage upgrades and patches to reduce possibility of introducing new vulnerabilities.

Containered/Enclave Approach

Sandia National Laboratories

- Approach allows the container to protect the file integrity, utilize service/user profile monitoring, provide automated security defenses, and offers configuration management and monitoring



Least-Privilege and Defense-in-Depth

Sandia National Laboratories

- Least-privilege security model starts with complete lock-down of a system, and incrementally adding access or communication capability to the desired level of functionality, but not more
- Defense-in-depth is a multi-layered defense approach where the system does not rely solely upon a single cyber-defense mechanism
  - There should never be a single point of failure for a security system

Network Defenses

Sandia National Laboratories

- TE Architecture is created with flexibility and application visibility in mind by creating an architecture that contains two key elements:
  - Application traffic visibility in the form of SSL Intercept or Forward-Proxy, and
  - The creation of containers, in the form of zones using networking technologies.

Monitoring

Sandia National Laboratories

- Many tools used can be used monitor the network traffic, encrypted and un-encrypted
- It is important to also monitor the software activity:
  - Monitoring software was created at SNL that uses multiple data sources to draw an in-depth look and analysis at user and software behavior in order to form a profile
- The TE framework can easily integrate with the tools currently used by an enterprise to monitor their network

Operations

Sandia National Laboratories

- Procedures and Policies
  - The TE Architecture suggests the implementation of policies and procedures for limiting access to the machines within the defined enclaves
  - All access of an administrative nature to the enclave should be through one central point
  - Different types of administrative users, such as application administrators should be created and utilized
- Trusted Software Process
  - A process should be created to dictate how new software and patches should be integrated into the enclave
  - Tools should be used to scan new patches and necessary files for introduction in the enclave for malware

Why the TE Framework?

Sandia National Laboratories

- Helps an organization to develop a new system or re-architect an existing system.
- Helps an organization define the risks and areas of concern
- Helps an organization to define the necessary number of functional zones within a system where cyber-protection technologies should be implemented
- TE Framework is a Framework
- TE Framework is tailorable to an organization
- Has been utilized at Sandia National Laboratories

Questions

Sandia National Laboratories