Raytheon

Customer Success Is Our Mission

# Building Secure Systems

Antony Selim, CISSP, P.E.

Cyber Security and Enterprise Security Architecture

13 November 2015

# Antony Selim - Bio

- 1997 B.S. in Engineering and a B.S. in Physics from Harvey Mudd College (HMC)
- 1998 Masters in Engineering from HMC with an emphasis in Communication Theory
- Licensed Professional Engineer (PE) in the State of California
  - Electrical Engineering
- Certified Information System Security Professional (CISSP)
- 1997-Pesent Raytheon Company in Fullerton, California
  - First 8 years working on wireless communication systems
  - More recently working on the security of large integrated computer systems and the networks that support them

# So what's the problem?

- Government organizations and major businesses are frequently being compromised
  - 2015 June, U.S. Office of Personnel Management (OPM)
  - 2015 February, Anthem
  - 2014 November, Sony
  - 2014 September, Home Depot
  - 2014 July, JPMorgan Chase
  - 2014 May, eBay
  - 2014 April, Michaels
  - 2014 January, Target
  - 2013 October, Adobe
  - 2011 March, RSA

- These breaches have several impacts
  - Loss of Intellectual Property (IP)
  - Paying for credit monitoring for customers
  - Class-action lawsuits from customers
  - Damage to reputation = Loss of business

# How do we begin to address this problem?

- Designed and build computing systems and networks with security in mind
  - Secure by design, not as an afterthought

- Consider a two pronged approach
  - Follow robust processes for the development of secure systems
  - Utilize people who are well trained in cyber security

# Robust Processes for the Development of Secure Systems

- National Institute of Standards and Technology (NIST)
  - Risk Management Framework (SP 800-37)
  - Security Controls (SP 800-53)
  - Risk Assessment (SP 800-30)
  - Supply Chain Risk Management (SP 800-161)
  - System Security Engineering (SP 800-160)

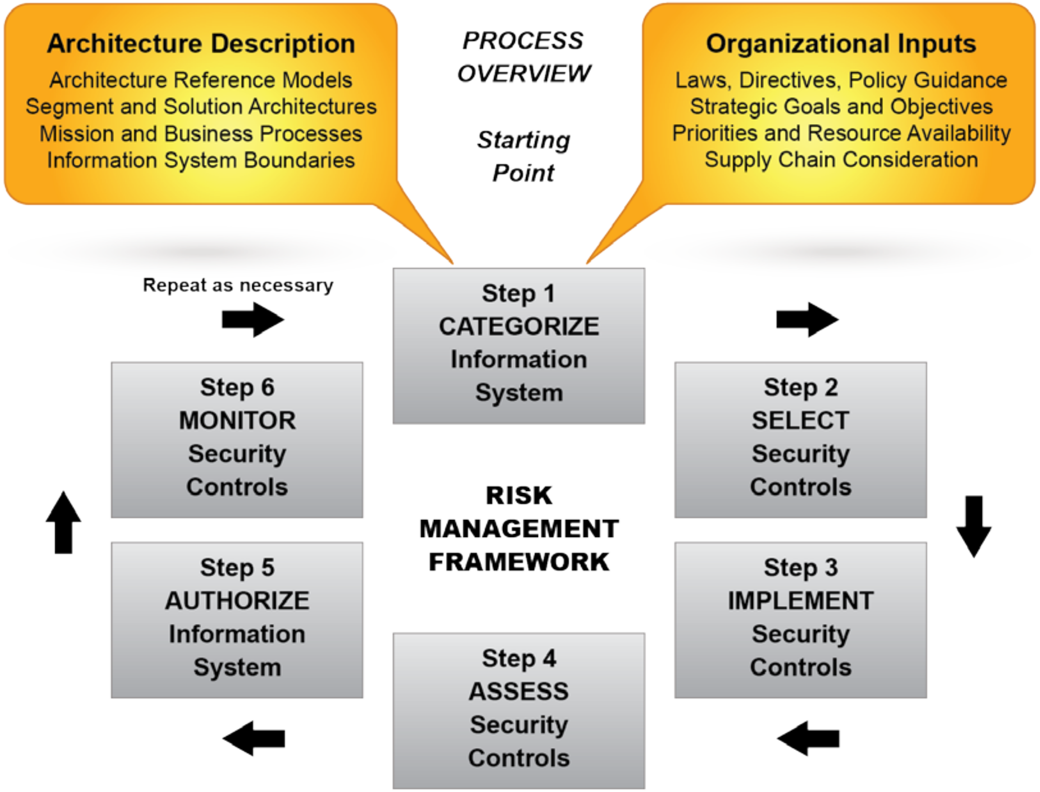
- SANS Institute
  - 20 Critical Security Controls for Effective Cyber Defense

- The Mitre Corporation
  - Common Weakness Enumeration (CWE)
  - Common Vulnerabilities and Exposure (CVE)

# Risk Management Framework
# SP 800-37

Raytheon
Integrated Defense Systems

- Governing document for the overall design, development, assessment and authorization of a secure system within the context of an organization
  - References many of the other documents


Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Consideration
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

# Security Controls
# SP 800-53

- 18 Control Families
  - Each family has dozens of controls (eg. AC-24, IA-11, PS-4)
  - Security Architecting should consider each of these controls

| ID | FAMILY | ID | FAMILY |
|---|---|---|---|
| AC | Access Control | MP | Media Protection |
| AT | Awareness and Training | PE | Physical and Environmental Protection |
| AU | Audit and Accountability | PL | Planning |
| CA | Security Assessment and Authorization | PS | Personnel Security |
| CM | Configuration Management | RA | Risk Assessment |
| CP | Contingency Planning | SA | System and Services Acquisition |
| IA | Identification and Authentication | SC | System and Communications Protection |
| IR | Incident Response | SI | System and Information Integrity |
| MA | Maintenance | PM | Program Management |

# Risk Assessment
# SP 800-30

- Step-by-step guide
  - How to prepare for risk assessments
  - How to conduct risk assessments
  - How to communicate risk assessment results
  - How to maintain the risk assessments over time
- Identification of threats
  - External
  - Internal
- Determination of asset criticality
- Evaluation of currently deployed controls
  - Effectiveness
  - Pervasiveness
- Assessment of residual risks

# Supply Chain Risk Management
# SP 800-161

- Supplier Interface
  - Assessment of supplier computing system and network
  - Access controls on supplier access to buyer’s system
  - Monitoring or supplier interface (email, VPN)

- Supplied Hardware
  - Inspection and testing
  - Determine providence (origin along with the history)
  - Implement configuration control
  - Detect counterfeit parts

- Supplied Software
  - Evaluation and testing
    - Commercial Off The Shelf (COTS) software
    - Free and Open Source Software (FOSS)
  - Determine providence
  - Implement configuration control and maintenance plans
  - Detect software defects
  - Detect malicious code insertion

# System Security Engineering SP 800-160

- System Engineering Process with a focus on Security
  - Requirements definition
  - Requirements analysis
  - Architectural design
  - Implementation
  - Integration
  - Verification
  - Transition
  - Validation
  - Operation
  - Maintenance
  - Disposal

# SANS Top 20 Critical Security Controls for Effective Cyber Defense

- An alternative list of Security Controls to consider when Security Architecting

- CSC 1: Inventory of Authorized and Unauthorized Devices
- CSC 2: Inventory of Authorized and Unauthorized Software
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges
- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 7: Email and Web Browser Protections
- CSC 8: Malware Defenses
- CSC 9: Limitation and Control of Network Ports, Protocols, and Services
- CSC 10: Data Recovery Capability
- CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- CSC 12: Boundary Defense
- CSC 13: Data Protection
- CSC 14: Controlled Access Based on the Need to Know
- CSC 15: Wireless Access Control
- CSC 16: Account Monitoring and Control
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 18: Application Software Security
- CSC 19: Incident Response and Management
- CSC 20: Penetration Tests and Red Team Exercises

# Mitre Databases

- Common Weakness Enumeration (CWE)
  - List of poor software coding structures/practices
    - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
    - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
    - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

- Common Vulnerabilities and Exposure (CVE)
  - List of known product vulnerabilities
    - CVE-2014-0160: Heartbleed
    - CVE-2014-6271: ShellShock
    - CVE-2014-3566: Poodle

# Developing Well Trained People

- Certified Information Systems Security Professional (CISSP)
  - Administered by International Information System Security Certification Consortium (ISC)$^2$
  - Most widely recognized
  - 8 security domains
    - Security and Risk Management
    - Asset Security
    - Security Engineering
    - Communications and Network Security
    - Identity and Access Management
    - Security Assessment and Testing
    - Security Operations
    - Software Development Security
- Certified Ethical Hacker
  - Administered by EC-Council
- General user training
  - Security Awareness Briefings

# Jobs at Raytheon

- General website
  - http://www.raytheon.com/
- General jobs website
  - http://jobs.raytheon.com/
- Cyber website
  - http://www.raytheoncyber.com/
- Cyber jobs website
  - http://www.rtncyberjobs.com/
  - Includes cyber challenges on the website