Software Solutions Symposium 2017
March 20–23, 2017

Secure Software Workforce Development Panel Discussion

Girish Seshagiri
Nancy Mead
William Newhouse
James Over

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
Agenda

Introduction

• Community Initiative Center of Excellence for Secure Software (CICESS)

• Software Assurance Curriculum Project

• The NICE Workforce Framework & Software Development

• Software Quality and Security

Discussion
Secure Software Workforce Development Panel Discussion

Community Initiative
Center of Excellence for Secure Software

Girish Seshagiri
Executive Vice President | CTO
Ishpi Information Technologies, Inc.
Why We Are Here

Vanishing middle class jobs
High youth unemployment and large number of under-employed
Student debt > 1.0 trillion
1.5 million cybersecurity jobs currently unfilled
Increasing number of cyber attacks against critical infrastructure
Workforce capable of developing software which is secure from cyber attacks
Apprenticeships for skill building and talent pipeline
Takeaways

Defective software is insecure

Sense of urgency to solve cybersecurity skills gap and create hundreds of thousands of middle class jobs

Leverage and build upon existing resources – software assurance curriculum, cybersecurity workforce framework, high maturity processes for use by individual programmers and agile teams

Connect education directly to a job through a dual learn and earn registered apprenticeship program

Develop skilled workforce based on validated competencies and industry standard certifications

Apprenticeships are good for business with positive return on investment
Cybersecurity Workforce Demand

1.5 Million
MORE cybersecurity professionals will be needed to accommodate the predicted global shortfall by 2020.

Source: ISCS 2015 Global Information Security Workforce Study

On average, 52%
of IT professionals surveyed stated fewer than 25% of all applicants were qualified.


The biggest skill gaps of today’s cybersecurity professionals:

- 72% Ability to Understand the Business
- 46% Technical Skills
- 42% Communication Skills


Fastest cybersecurity demand sectors are in industries managing consumer data:

- 40% Professional Services
- 30% Industries Managing Consumer Data
- 16% Finance and Insurance
- 14% Manufacturing and Defense
- Other


Cybersecurity job postings took 9% longer to fill than IT job postings overall.

Source: ISCS 2015 Global Information Security Workforce Study

Expertise required for various cybersecurity roles in demand:

- Information Security
- Network Setup
- Auditing
- Network Protocols
- Core Database, Coding, and Scripting
- Systems Administration

Source: Job Market Intelligence: Cybersecurity Jobs, 2015

Approximately 10% of the current cybersecurity workforce are comprised of women.


18% Growth
Computer and mathematical occupations will grow much faster than the average job during 2012–2024.


Fastest growing skills in cybersecurity job postings:

- Python
- HIPAA
- Risk Management
- Internal Auditing
- Audit Planning

Source: Partnership for Public Service

Hardest to fill skills in cybersecurity job postings:

- Software Architecture
- Network Attached Storage (NAS)
- Software Issue Resolution
- Internet Security
- Legal Compliance
- Data Communications
- Platform as a Service (PaaS)
- Computer Forensics
- Internal Auditing
- Apache Hadoop


nist.gov/nice
## Cost of Status Quo

<table>
<thead>
<tr>
<th>Item</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two-year and four-year college</td>
<td>$400 billion per year</td>
</tr>
<tr>
<td>Workforce education and on-the-job training</td>
<td>$600 billion per year</td>
</tr>
<tr>
<td>Skills gap</td>
<td>$160 billion per year</td>
</tr>
<tr>
<td>Time for new employees to reach full productivity</td>
<td>&gt; Five months on average</td>
</tr>
<tr>
<td>Replacing an employee</td>
<td>Ranges from 6 to 24 months of the position’s salary</td>
</tr>
</tbody>
</table>
Common Benefits of Apprenticeship

Production
- Output during the apprenticeship at a reduced wage
- Higher post-apprenticeship productivity relative to similarly tenured employees
- Reduction in mistakes or errors

Workforce
- Reduced turnover
- Pipeline of skilled employees
- Better matching of employee skills and character with employer needs and firm culture
- Lower recruiting costs
- Development of future managers

Soft Skills
- Employee engagement and loyalty
- Greater problem-solving ability and adaptability
- Reduced need for supervision
A Unique Collaboration – Industry, Government, Academe
Goals

One of the largest available skilled workforce for secure software
Direct connection between education and a job without accumulating debt
World-class education providers with core common standard curriculum offerings
A standard competency-based, registered, apprenticeship program with uniform guidelines
Central Illinois is the destination choice for an exciting career
A skills formation and workforce development model scalable to other occupations and other communities across the nation
The Swiss Dual Track Model

Apprenticeships
Switzerland's business-driven & labor market-oriented training system

230 Types of Apprenticeships to Choose From

Global Innovation Index

Number 1

How does the system work?

Funding Sources

The Future Awaits

60% Private Sector

10% Vocational Education

30% Higher Education

20% Apprenticeship

Career Choice

Age 14 - Career Counseling

Age 16 - High School Graduation

Aged 18-20 - Earn Federal Diploma

Aged 19-20 - Earn Apprenticeship (3-4 years)

The Swiss Dual Track Model

Retention

Innovation

High Productivity

Best Results

Value to Companies after the training period.

Tuition paid by cantons (states).
Apprentices earn a progressive wage.

Yes student debt.
No student debt.

Skills & knowledge align with labor market demands.

A prestigious education pathway.

Retention

Innovation

High Productivity

Best Results

Value to Companies after the training period.

Tuition paid by cantons (states).
Apprentices earn a progressive wage.

Yes student debt.
No student debt.

Skills & knowledge align with labor market demands.

A prestigious education pathway.

Productive Apprentice Output

Companies see a direct net benefit

$450 Million

$5.65 Billion

$5.2 Billion

Who benefits? Everyone.

Among Swiss High School Graduates

Choose a General Education

Choose Vocational Education & Training
CICESS Design – 1

Standard academic curriculum leading to first-in-the-nation AAS Degree in Secure Software Development

Berger Aptitude Test (B-Apt) for Computer Programming for entry to the apprenticeship program

Standard apprenticeship curriculum based on Carnegie Mellon University Software Engineering Institute (CMU/SEI) process models

Validate secure software development competencies – (ISC)^2 CSSLP, SEI PSP Developer certifications
CICESS Design – 2

Alternating blocks of weeks of academic instruction and apprenticeship on-the-job training in the dual model

Recurring and one-time-only fees from participating employers for ongoing program administration, apprenticeship curriculum development, and train-the-trainer materials

Guidelines for minimum hourly wages for the apprentices with flexibility to meet varied human resources practices of participating employers
Alignment with Federal Initiatives

NIST Cybersecurity Workforce Framework
NIST National Initiative Cybersecurity Education
NSA Centers of Academic Excellence
DoL American Apprenticeship Initiative
DoL Registered Apprenticeship standards
CICESS Value Proposition

Augmentation of your current workforce development methods

Ability to plan for and satisfy future needs for hard-to-fill secure software developers

Ability to build a secure software talent pipeline that includes women and minorities who are trained, mentored, and certified

A cost-effective solution to training and retaining new workers in secure software development

High retention rates when apprentices become full-time employees
Takeaways

Sense of urgency to address unsustainable trends and exploit rare economic development opportunity to create hundreds of thousands of middle class jobs

Industry/government/academic coalition led by industry to address cybersecurity “skills gap” and talent pipeline

Connect education directly to a job through a dual learn and earn registered apprenticeship program

Develop skilled workforce based on validated competencies and industry standard certifications

Apprenticeships are good for business with positive return on investment
Software Solutions Symposium 2017

Secure Software Workforce Development Panel Discussion

Nancy R. Mead
SEI Fellow and Principal Researcher
Carnegie Mellon Software Engineering Institute
Copyright 2017 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM-0004332
Definition of Software Assurance

We used the following definition of software assurance:

*Application of technologies and processes to achieve a required level of confidence that software systems and services function in the intended manner, are free from accidental or intentional vulnerabilities, provide security capabilities appropriate to the threat environment, and recover from intrusions and failures.*
Software Assurance (SwA) Curriculum Project

Initially sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD)

Goals

• Develop software assurance curricula.
• Define transition strategies for future implementation.
Timeline

Goals: Develop software assurance curricula
Define transition strategies for implementation

Community Outreach
- 20+ published papers
- 7 SEI reports
- 20+ talks, webinars, podcasts, media
- Thousands of downloads
- LinkedIn group of 500+ members
- Course materials and videos

Integrated Into Course Offerings
- Carnegie Mellon University
- Stevens Institute of Technology
- US Air Force Academy
- University of Detroit Mercy
- University of Houston
- (ISC)²

Transition
- Degree offerings
  - Polytechnic U. of Madrid—full MSwA Fall 2014
  - Illinois Central College Community College Program Fall 2015
- SwA Courses
  - Assurance Management
  - Assured Software Development 1
  - exec course
  - practitioner version of ASD1
- SEI SwA Certificate Program
  - under development in 2017

August 2010 | March 2011 | Fall 2011 | 2012 | March 2013

Master of Software Assurance Reference Curriculum
Undergraduate Course Outlines
MSwA Syllabi
Community College Education
Software Assurance Competency Model

Professional Society Recognition
IEEE
ACM

[Distribution Statement A] This material has been approved for public release and unlimited distribution.
Objectives

Improve the state of software assurance education.

- Develop a Master of Software Assurance Reference Curriculum (Volume I).
- Identify educational offerings at other levels:
  - undergraduate (Volume II)
  - MSwA syllabi (Volume III)
  - Community College (Volume IV)
  - integration with IS curricula (SEI report)
  - SwA Competency Model

[Distribution Statement A] This material has been approved for public release and unlimited distribution.
Audiences

Faculty responsible for
  • design, development, and maintenance of degree programs focusing on software assurance knowledge and practices

Those in development and acquisition organizations responsible for either
  • staffing positions in software assurance
  • providing current software engineers with increased software assurance capabilities

Those who assess software assurance oriented programs
Book Published in Late 2016

Secure Software Workforce Development Panel Discussion

Community College Program
SwA Curriculum Community College Recommendations

Volume IV in the SwA Education Curriculum Reports

- Modifications to Computer Science I, II, and III
- Additional recommended courses
  - Introduction to Computer Security
  - Secure Coding
  - Introduction to Assured Software Engineering

SwA Curriculum webpage

- www.cert.org/curricula/software-assurance-curriculum.cfm
Timeline for the Community College and Industry Apprenticeship Program

- **2012**
  - Fall 2012, SEI Software Assurance Community College Report

- **2013**
  - March 2013, SEI Software Assurance Competency Report
  - September 2013, Meeting of industry/government/academic stakeholders in Peoria, Illinois
  - November 2013, Initial CICESS discussions with the SEI

- **2014**
  - May 2014, CICESS steering Committee established
  - October 2013, Community core group formed to develop a strategy
  - February 2014, CICESS goals established

- **2015**
  - January 2015, Initial ICC discussion with the SEI
  - Spring 2015, ICC announces first-in-the-nation AAS degree in Secure Software Development
  - May 2015, $3.9 million grant awarded to fund the Illinois Advanced Apprenticeship Consortium (IAAC)
  - April, 2015, CICESS regional summit of industry/government/academic stakeholders
  - Fall 2015, First cohort of students starts coursework in Secure Software Development at ICC
Illinois Central College Implementation

CS I: Programming in Java
CS II: Programming in Java
CS III: Advanced Programming in Java
Structured Query Language
Introduction to Relational Database
C# Programming
Mobile Application Programming
Introduction to Computer Security
Secure Coding
Introduction to Assured Software Engineering
Database Administration
Structured System Analysis
Two electives in computer programming, web, or networking, depending on employer needs
General education courses (19 credit hours)

[Distribution Statement A] This material has been approved for public release and unlimited distribution.
Contact Information

Nancy R. Mead
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213

nrm@sei.cmu.edu

www.sei.cmu.edu/about/people/profile.cfm?id=mead_13121
Secure Software Workforce Development Panel Discussion

The NICE Workforce Framework & Software Development

Bill Newhouse
Deputy Director, National Initiative for Cybersecurity Education, NIST
National Initiative for Cybersecurity Education (NICE)

- The NICE strategic plan [http://csrc.nist.gov/nice/about/strategicplan.html](http://csrc.nist.gov/nice/about/strategicplan.html)

Resources

  - Forum to identify and share best practices that help us as a nation make progress towards the NICE Strategic goals and objectives.
- NICE provide a grant to support the creation of Cyberseek [http://cyberseek.org/](http://cyberseek.org/)
- NICE provided grants for the creation of 5 Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS)
NICE Strategic Goals

Accelerate Learning and Skills Development
• *Inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cybersecurity workers*

Nurture A Diverse Learning Community
• *Strengthen education and training across the ecosystem to emphasize learning, measure outcomes, and diversify the cybersecurity workforce*

Guide Career Development & Workforce Planning
• *Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent*
NICE Strategic Goal #3: Guide Career Development and Workforce Planning

Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent

Objectives:

3.1 Identify and analyze data sources that support projecting present and future demand and supply of qualified cybersecurity workers

3.2 Publish and raise awareness of the NICE Cybersecurity Workforce Framework and encourage adoption

3.3 Facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs

3.4 Promote tools that assist human resource professionals and hiring managers with recruitment, hiring, development, and retention of cybersecurity professionals

3.5 Collaborate internationally to share best practices in cybersecurity career development and workforce planning
Specialty Areas (33) – Distinct areas of cybersecurity work;
Work Roles (52) – The most detailed groupings of IT, cybersecurity or cyber-related work, which
include specific knowledge, skills, and abilities required to perform a set of tasks.
Tasks – Specific work activities that could be assigned to a professional working in one of the
NCWF’s Work Roles; and,
Knowledge, Skills, and Abilities (KSAs) – Attributes required to perform Tasks, generally
demonstrated through relevant experience or performance-based education and training.

Audience:
Employers
Current and Future Cybersecurity Workers
Training and Certification Providers
Education Providers
Technology Providers
# Securely Provision (7 Specialty Areas, 11 Work Roles)

<table>
<thead>
<tr>
<th>Category</th>
<th>Specialty Area</th>
<th>Work Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securely Provision</td>
<td>Risk Management</td>
<td>Authorizing Official/Designating Representative</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Control Assessor</td>
</tr>
<tr>
<td></td>
<td>Software Development</td>
<td>Software Developer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure Software Assessor</td>
</tr>
<tr>
<td></td>
<td>Systems Architecture</td>
<td>Enterprise Architect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Architect</td>
</tr>
<tr>
<td></td>
<td>Technology R&amp;D</td>
<td>Research &amp; Development Specialist</td>
</tr>
<tr>
<td></td>
<td>Systems Requirements Planning</td>
<td>Systems Requirements Planner</td>
</tr>
<tr>
<td></td>
<td>Test and Evaluation</td>
<td>Testing and Evaluation Specialist</td>
</tr>
<tr>
<td></td>
<td>Systems Development</td>
<td>Information Systems Security Developer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Systems Developer</td>
</tr>
</tbody>
</table>
# Software Development Specialty Area

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>KSAs</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software Development (DEV)</strong></td>
<td>Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Software Developer (SP-DEV-001)</strong></td>
<td>Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.</td>
<td>621</td>
<td>Click to view KSAs</td>
</tr>
<tr>
<td><strong>Secure Software Assessor (SP-DEV-002)</strong></td>
<td>Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.</td>
<td>622</td>
<td>Click to view KSAs</td>
</tr>
<tr>
<td>Securely Provision (SP)</td>
<td>Software Developer (621): Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Knowledge</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0001</td>
<td>* Knowledge of computer networking concepts and protocols, and network security methodologies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0002</td>
<td>* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0003</td>
<td>* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0004</td>
<td>* Knowledge of cybersecurity principles.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0005</td>
<td>* Knowledge of cyber threats and vulnerabilities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0006</td>
<td>* Knowledge of specific operational impacts of cybersecurity lapses.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0014</td>
<td>Knowledge of complex data structures.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0016</td>
<td>Knowledge of computer programming principles such as object-oriented design.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0027</td>
<td>Knowledge of organization's enterprise information security architecture system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0028</td>
<td>Knowledge of organization's evaluation and validation requirements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0039</td>
<td>Knowledge of cybersecurity principles and methods that apply to software development.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0044</td>
<td>Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0051</td>
<td>Knowledge of low-level computer languages (e.g., assembly languages).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0060</td>
<td>Knowledge of operating systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0066</td>
<td>Knowledge of Privacy Impact Assessments.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0068</td>
<td>Knowledge of programming language structures and logic.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0073</td>
<td>Knowledge of secure configuration management techniques.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0079</td>
<td>Knowledge of software debugging principles.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0080</td>
<td>Knowledge of software design tools, methods, and techniques.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0081</td>
<td>Knowledge of software development models (e.g., Waterfall Model, Spiral Model).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0082</td>
<td>Knowledge of software engineering.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0084</td>
<td>Knowledge of structured analysis principles and methods.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0085</td>
<td>Knowledge of system and application security threats and vulnerabilities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0086</td>
<td>Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0105</td>
<td>Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0139</td>
<td>Knowledge of interpreted and compiled computer languages.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0140</td>
<td>Knowledge of secure coding techniques.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0152</td>
<td>Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0153</td>
<td>Knowledge of software quality assurance process.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0154</td>
<td>Knowledge of supply chain risk management standards, processes, and practices.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0170</td>
<td>Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0179</td>
<td>Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0199</td>
<td>Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0202</td>
<td>Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0219</td>
<td>Knowledge of local area network (LAN) and wide area network (WAN) principles.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0260</td>
<td>Knowledge of Personally Identifiable Information (PII) data security standards.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0261</td>
<td>Knowledge of Payment Card Industry (PCI) data security standards.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0262</td>
<td>Knowledge of Personal Health Information (PHI) data security standards.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0263</td>
<td>Knowledge of information technology (IT) risk management policies, requirements, and procedures.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0322</td>
<td>Knowledge of embedded systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0331</td>
<td>Knowledge of network protocols (e.g., Transmission Control Protocol (TCP), Internet Protocol (IP), Dynamic Host Configuration Protocol (DHCP)), and directory services (e.g., Domain Name System (DNS)).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0342</td>
<td>Knowledge of penetration testing principles, tools, and techniques.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K0343</td>
<td>Knowledge of root cause analysis techniques.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Securely Provision (SP)</td>
<td>Software Developer (621): Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Skills</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S0001</td>
<td>Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S0014</td>
<td>Skill in conducting software debugging.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S0017</td>
<td>Skill in creating and utilizing mathematical or statistical models.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S0019</td>
<td>Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S0022</td>
<td>Skill in designing countermeasures to identified security risks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S0031</td>
<td>Skill in developing and applying security system access controls.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S0034</td>
<td>Skill in discerning the protection needs (i.e., security controls) of information systems and networks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S0060</td>
<td>Skill in writing code in a currently supported programming language (e.g., Java, C++).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S0135</td>
<td>Skill in secure test plan design (e.g., unit, integration, system, acceptance).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S0138</td>
<td>Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S0149</td>
<td>Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S0174</td>
<td>Skill in using code analysis tools.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S0175</td>
<td>Skill in performing root cause analysis.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Abilities</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A0007</td>
<td>Ability to tailor code analysis for application-specific concerns.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A0021</td>
<td>Ability to use and understand complex mathematical concepts (e.g., discrete math).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A0047</td>
<td>Ability to develop secure software according to secure software deployment methodologies, tools, and practices.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Dramatically Reducing Software Vulnerabilities

Report to the White House Office of Science and Technology Policy

Paul E. Black
Lee Badger
Barbara Guttmann
Elizabeth Fong

Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8151

November 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director
• This plan starts by describing a well-known risk: current systems perform increasingly vital tasks and are widely known to possess vulnerabilities.
  – These vulnerabilities are often not easy to discover and difficult to correct.
  – Cybersecurity has not kept pace, and
  – The pace that is needed is rapidly accelerating.
• The R&D Strategic plan defines goals for the near, mid and long term.
• NISTIR 8151 addresses the first mid-term goal:
  – Achieve Science and Technology advances to reverse adversaries’ asymmetrical advantages, through sustainably secure systems development and operation. ...
  – This goal is two-pronged: first, the design and implementation of software, firmware, and hardware that are highly resistant to malicious cyber activities (e.g., software defects, which are common, give rise to many vulnerabilities) ...
The Goal of NISTIR 8115

- Present a list of specific technical approaches that have the potential to make a dramatic difference reducing vulnerabilities – by stopping them before they occur, by finding them before they are exploited or by reducing their impact.
  - Stopping vulnerabilities before they occur generally includes improved methods for specifying, designing and building software.
  - Finding vulnerability includes better testing techniques and more efficient use of multiple testing methods.
  - Reducing the impact of vulnerabilities refers to techniques to build architectures that are more resilient, so that vulnerabilities cannot be exploited for significant damage.
Defective Software Is Not Secure

James W. Over
Technical Director/Principal Engineer
Carnegie Mellon Software Engineering Institute
Defective Software Is Not Secure

Many vulnerabilities are caused by common software defects.¹

• buffer overflow, failure to validate input, logic errors, etc.

```c
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0) 
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0) 
    goto fail;
goto fail; /* MISTAKE! THIS LINE SHOULD NOT BE HERE */
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0) 
    goto fail;
```

Poor quality development practices are a principal cause.
From 1-5% of defects are potential vulnerabilities.¹,²

Practices to improve software quality are critically needed.

Software Quality State of the Practice

**Software Defect**: an engineering artifact, that if not changed, could cause improper design, implementation, test, use, or maintenance.

**Defect Density**: Count of the defects removed divided by product size. A measure of product quality that is related to the quality of the development process.

<table>
<thead>
<tr>
<th>Source</th>
<th>Defects per KSLOC</th>
<th>Defects per MLOC</th>
<th>Est. Vulnerabilities per MLOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADA and Beyond: Software Policies for the DoD; 1997</td>
<td>1.0000 7.0000</td>
<td>1,000 7,000</td>
<td>10 350</td>
</tr>
<tr>
<td>Delivered Defect Density by Maturity Level; C. Jones; 2003</td>
<td>1.0500 7.5000</td>
<td>1,050 7,500</td>
<td>11 375</td>
</tr>
<tr>
<td>Software Engineering Best Practices; C. Jones; 2010</td>
<td>1.1600 5.2933</td>
<td>1,160 5,293</td>
<td>12 265</td>
</tr>
<tr>
<td>SEI TSP Data; 2014</td>
<td>0.00092 0.5625</td>
<td>1 563</td>
<td>0 28</td>
</tr>
</tbody>
</table>
Improving Software Quality

“The only way for errors to occur in a program is by being put there by the author. No other mechanisms are known. Programs can't acquire bugs by sitting around with other buggy programs.” – Dr. Harlan Mills

Software development relies on testing to find and fix defects.
As a defect removal practice testing is
  • Expensive; 30% to 60% of development costs
  • Slow; 50% or more of schedule
  • Ineffective; removes 80% to 85% of defects (and some vulnerabilities)

Low defect content is an essential prerequisite to a quality software process, but testing only finds a fraction of the defects. The most effective way to reduce defects is with the individual software engineer. – Watts Humphrey
Software Engineer Quality Data

Defects found in test and injected during detailed design and coding

Source: PSP training data
Personal Software Process Quality Practices

**Personal Software Process (PSP)**

Process framework for developers.

Scaled to small projects

Developer controlled

Metrics to manage variation and speed improvement

Training and certification

**PSP Facts**

- Training – developers write 10 small programs
- PSP levels – 3; baseline, planning, quality
- Measures – size; development time; defects found
- Data – 50 data points/assignment; 10 assignments/developer; 3383 developers as of 2016

**Graph**

- 810 developers
- Defect reduction
  - 1Q: 80.4%
  - 2Q: 79.0%
  - 3Q: 78.5%
  - 4Q: 77.6%

**Defects/KLOC**

- 1st Quartile
- 2nd Quartile
- 3rd Quartile
- 4th Quartile
PSP-Trained Software Engineer Quality Data

Defects found in test and injected during detailed design and coding

Source: PSP training data
Xtreme Quality

Team Software Process (TSP)

Process framework for PSP-trained developers.

Scaled to medium to large applications

Team controlled

Metrics to support team management.

Coach training and certification

<table>
<thead>
<tr>
<th>Project</th>
<th>Type</th>
<th>Critical Defects in first 1+ year</th>
<th>Defect Density (MLOC)</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>Safety Critical</td>
<td>20</td>
<td>46.07</td>
<td>2.8 MLOC</td>
</tr>
<tr>
<td>D2</td>
<td>Safety Critical</td>
<td>0</td>
<td>4.44</td>
<td>.9 MLOC</td>
</tr>
<tr>
<td>D3</td>
<td>Safety Critical</td>
<td>0</td>
<td>9.23</td>
<td>1.3 MLOC</td>
</tr>
<tr>
<td>A1</td>
<td>Secure</td>
<td>0</td>
<td>91.70</td>
<td>.6 MLOC</td>
</tr>
<tr>
<td>X1</td>
<td>Secure</td>
<td>0</td>
<td>20.00</td>
<td>.1 MLOC</td>
</tr>
<tr>
<td>B1</td>
<td>Secure</td>
<td>2</td>
<td>66.67</td>
<td>.45 MLOC</td>
</tr>
</tbody>
</table>
A Path Forward

Improving software quality is a necessary part of the solution to software security.

The means of achieving improved quality are proven and available.

The challenges

• Educating the workforce
• Changing the behavior of software people
• Raising consumer awareness
What Government Can Do

Change industry behavior

• Software quality standards and policies that address reducing defect content in the software.
• Incentives for government software providers designed to produce continued, incremental improvements in quality.

Sponsor secure software development apprenticeship programs

• Training programs that emphasize software quality
• Hands-on demonstration of knowledge/skills transfer
• On-the-job application of knowledge/skills learned under the supervision of a qualified coach/mentor