Software Security Lifecycle Professional Credentials:
The Case for Secure Software Lifecycle Education and Certification

Patricia A. Myers, CISSP-ISSMP
The Dawn of a New Certification

• Why is security critical in software?
  ♦ Defining the Problem
  ♦ Proposing the ‘Right’ Solution

• Why the CSSLP?
  ♦ Goals and objectives of CSSLP
  ♦ Early Support
  ♦ CSSLP – By the Numbers
Defining the Problem

• Total number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005 is estimated between 34.4* and 226MM.

• David Rice, author of “Geekonomics: The Real Cost of Insecure Software” puts the total cost of security holes in software at around $180 Billion USD a year!”

• A holistic approach to security requires that we go beyond just installing firewalls and network monitoring.

• We need defense-in-depth with security applied all along the attack vector, up to and including applications and sensitive data elements. Here’s why…

*Source: Privacy Rights Clearinghouse  Chronology of Data Breaches
Defining the Problem

- De-perimeterization of networks place increased burden on the security of individual computers and applications.

- Malware increased by 64.3 %, (compared with over 50% last year) according to the November 2009 CSI Annual Report.

- Experts agree that more data breaches could result in greater government oversight and regulation.

  - 43 states in US have now enacted breach disclosure laws.

- $202 USD per record lost (not including reputation damage and loss of trust).*

*Ponemon Institute’s Fourth Annual US Cost of Data Breach Study, January 2009
Vulnerability Rates 2004 - 2009

FIGURE 88. Industry-wide vulnerability disclosures by half-year, 1H04–1H09

Insecure Software: *People* Problem

- Three primary conditions create information security vulnerabilities in enterprise software applications:
  - *Inexperienced* developers writing code
  - *Experienced* developers writing code with inadequate training in ‘Good Practices’ for security
  - Designers and managers consistently failing to include security considerations in business requirements
  - Influencers lack basic understanding of information security issues pertaining to the software lifecycle

*Source: (ISC)² Secure Software Market Study*
Insecure Software: Process Problem

Developer unawareness of need for basic data security controls:

- Protection from disclosure (confidentiality)
- Protection from modification (integrity)
- Protection from destruction (availability)
- Request validation, e.g., who’s making a request? (authentication)
- Request rights and privileges, e.g. what can they see and do? (authorization)
- Creating historical evidence (auditing) and managing configurations, sessions and exceptions
- Putting these controls into practice during implementation
Insecure Software: *Policy* Problem

Software developers are driven to deliver functionality within deadline and scope constraints because of:

- Lack of time
- Rush to market
- Expense
- Limited personnel resources
- Lack of awareness or appreciation for the value of security
Proposing the ‘Right’ Solution

• A dilemma:

♦ Do we wait for security breaches get to the point that governments force a licensure of application developers?

OR

♦ Do we adopt a pro-active approach that establishes industry standards and certification to improve application security?
Proposing the ‘Right’ Solution

• In Q307, the (ISC)^2 Board was asked to consider creation of a new certification aimed at solving this dilemma. ‘Seed’ funding was granted; validation and acceptance of the basic concepts by the community was undertaken.

• A global market study, numerous focus groups were held and a business case established. Full funding for the new cert was granted by the board in ’08.

• 2009 saw the first CSSLP exam held.
Goals & Objectives of CSSLP<sup>CM</sup>

Establish a comprehensive program that educates, certifies knowledge of, and experience in the 7 domains of the CSSLP CBK®:

1. Secure Software Concepts
2. Secure Software Requirements
3. Secure Software Design
4. Secure Software Implementation/Coding
5. Secure Software Testing
6. Software Acceptance
7. Software Deployment, Operations, Maintenance and Disposal
Secure Software Concepts - CSSLP<sup>CM</sup>

- Confidentiality, Integrity, Availability Authentication, Authorization, and Auditing
- Security Design Principles
- Risk Management (e.g., vulnerabilities, threats and controls)
- Regulations, Privacy, and Compliance
- Software Architecture (e.g., layers)
- Software Development Methodologies
- Legal (e.g., Copyright, IP and trademark)
- Standards (e.g., ISO 2700x, OWASP)
- Security Models (e.g., Bell-LaPadula, Clark-Wilson & Brewer-Nash)
- Trusted Computing (e.g., TPM, TCB)
- Acquisition (e.g., contracts, SLAs and specifications)
Software Lifecycle Stakeholders

- Top Management
- Business Unit Heads
- IT Manager
- Security Specialists
- Application Owners
- Developers/Coders
- Software Lifecycle Stakeholders
- Auditors
- Business Analysts
- Technical Architects
- Project Managers/Team Leads
- Client Side PM
- Industry Group Delivery Heads
- Quality Assurance Managers

Influencers
Primary Target
Secondary Target
Early Supporters of CSSLP

- Symantec
- Microsoft
- Xerox
- SANS
- SAFECODE
- Accenture
- BASDA
- NASSCOM
- SRA Int’l
- Cisco
- ISSA
CSSLP -- By the Numbers

• Statistics on early adoption, as of September 30, 2009:
  - 894 Experience Assessment Applications (EAA)
  - 854 CSSLPs granted from EAA process
  - 12 Exams Scheduled
  - 27 Seminar seats reserved
  - 857 CSSLPs to-date, representing 50 countries
Building in security should be second nature

Take a lesson from Mother Nature and apply it to your own business. Begin building security into every aspect of your software’s lifecycle!

Start today by becoming an (ISC)² Certified Secure Software Lifecycle Professional (CSSLP®).
For Additional Information:

Contact Jessica Smith: jsmith@isc2.org  (727-785-0189 Ext. 243
www.isc2.org
CSSLP dISC contents

ISC_CSSLP_CD_2009.exe.ink