Security Certifications
A Short Survey

Welcome

Stan Reichardt

stan2007@sluug.org

Disclaimer

- This is just a cursory look at what is out there.
- I believe certifications are good training tools, but not necessarily the best measure of ability.
  - I hold only a basic security certification
    - CompTIA's Security+ December 2005
    -

Definitions

- Certification
- Psychometric

Professional Certification

- A professional certification, trade certification, or professional designation often called simply certification or qualification is a designation earned bya person to certify that he is qualified to perform a job. Certification indicates that the individual has a specific set of knowledge, skills, or abilities in the view of the certifying body. Professional certifications are awarded by professional bodies and corporations. The difference between licensure and certification is licensure is required by law, whereas certification is generally voluntary. -- Wikipedia
- http://en.wikipedia.org/wiki/Professional_certification

Psychometric principles

- Psychometrics is the field of study concerned with the theory and technique of educational and psychological measurement, which includes the measurement of knowledge (achievement), abilities, attitudes, and personality traits.
- The considerations of validity and reliability typically are viewed as essential elements for determining the quality of any test. -- Wikipedia
- http://en.wikipedia.org/wiki/Psychometrics#Standards_of_quality

Focus on Issues

- Vendor-neutral vs Vendor specific
- Technical vs Managerial
- Certification vs No Certifications

Consider

- HR check list - Requirements
- Keeping Current
  - Environment changes
  - Continuing Education
- Fools Gold
  - Credentials
  - Training is not experience
  - Experience is too expensive

Something Extra

- Learning and continuing education
- Business card logos
- Job listing service by some

Certification in computer industry

- Vendor Specific
- Vendor-neutral
- Camp Folowers

Vendor Specific

- Oriented toward specific technologies, and managed by vendors
  - Checkpoint – certification program
  - Cisco Systems -- Cisco Career Certifications program
  - Citrix Systems -- the Citrix Certified Administrator program
  - IBM sponsors certifications
  - Juniper Networks -- Juniper Networks Technical Certification Program
  - Microsoft Corporation -- Microsoft Certified Professional program
  - MySQL -- certification program
  - Novell -- certification program
  - Object Management Group -- Certified Professional program for Unified Modeling Language
  - Oracle Corporation -- Oracle Certification Program
  - Red Hat -- Red Hat Certification Program
  - Sun Microsystems -- Sun Certified Professional program

Vendor-neutral

- Third-party organizations that sponsor certifications
  - Brainbench
  - Certiport -- Microsoft Office Specialist and IC3 certification (Internet and Computing Core)
  - CompTIA - Computing Technology Industry Association
  - EC-Council - International Council of Electronic Commerce Consultants
  - European Computer Driving License-Foundation -- European Computer Driving License
  - International ICT Council
  - ISC2 - International Information Systems Security Certification Consortium
  - Linux Professional Institute (LPI)
  - Planet3 Wireless -- Certified Wireless Network Administrator (CWNA)
  - Prosoft Learning Corporation offers CIW, CCNT, CTP, AssessPrep certification tracks
  - SAGE (organization) -- cSAGE program
  - SANS Institute -- Global Information Assurance Certification program

Camp Followers

- Additional Vendors – Non-affiliated
  - Transcenders - http://www.transcender.com/
  - List of legitimate practice test providers
    - http://www.certguard.com/reviews.asp
  - Brain Dumps
    - Some vendors provide illegally obtained information
    - http://en.wikipedia.org/wiki/Brain_dump

Community and Industry

- Professional Associations
  - CompTIA - Computing Technology Industry Association
  - ISC2 - International Information Systems Security Certification Consortium
  - ISSA - Information Systems Security Association
  - SANS Institute
    - GIAC - Global Information Assurance Certification -- www.giac.org
    - Certifications are offered in conjunction with a full 5 or 6 day SANS Training course

What Now?

- Too diverse and numerous for detailed survey
  - Some brochures
- A look at two examples
  - CompTIA - Security+
  - ISC2 - CISSP

CompTIA

- The Computing Technology Industry Association (CompTIA) is a non-profit trade association, founded in 1982, and is a provider of professional certifications for the information technology industry.
- Certificate programs
  - A+, Network+, Server+, Security+, HTI+, e-Biz+, CTT+, CDIA+, Linux+, I-Net+, Project+

CompTIA - Security+

- Security+ is a certification dealing with computer security topics such as cryptography and access control. Currently, according to CompTIA, there are more than 25,000 people around the world who have earned this certification.

ISC2

- The International Information Systems Security Certification Consortium((ISC)2) is a non-profit organization headquartered in Palm Harbor, Florida.
  - The organization is internationally recognized with over 42,000 information security professionals in more than 110 countries.
  - The organization maintains what it calls a **Common Body of Knowledge** for information security for the following certifications:

ISC2 Certifications

- Certified Information Systems Security Professional (CISSP ®)
- Systems Security Certified Practitioner (SSCP ®)
- Information Systems Security Architecture Professional (ISSAP ®)
- Information Systems Security Management Professional (ISSMP ®)
- Information Systems Security Engineering Professional (ISSEP ®)
- Certification and Accreditation Professional (CAP CM)

Common Body of Knowledge

- The CISSP certification tests the Common Body of Knowledge (CBK), acompilation of information for international Information Security professionals, comprising 10 security domains:
    - Access Control Systems & Methodology
    - Applications and Systems Development Security
    - Business Continuity Planning and Disaster Recovery Planning
    - Cryptography
    - Law, Investigation & Ethics
    - Operations Security
    - Physical(Environmental) Security
    - Security Architecture & Models
    - Security Management Practices
    - Telecommunications and Network Security

CISSP

- Certified Information Systems Security Professional (CISSP) is a vendor-neutral certification governed by the International Information Systems Security Certification Consortium (ISC)2.
- In granting the CISSP certification (ISC)2 operates in conformance with the requirements of the International Organization for Standardization (ISO) standard ISO 17024:2003 for certifying individuals.
- It is considered one of the premiere Information Security certifications.

CISSP

- CISSP is the flagship certification of (ISC)2.
- CISSP is a highly reputed Information Security Certification.
- The CISSP test includes information from 10 different domains which comprise the (ISC)2 Common Body of Knowledge® (CBK).
- The CISSP test is 250 questions taken in 6 hours.

How

- Course Objectives
  - Domains
- Self study
  - Books and Study Guides
  - Practice Questions
  - CDROMs
  - On-line
- Full Day Courses

Instructor Led Training Vendors

- Local Training (Missouri)
  - New Horizons Learning Centers - http://www.newhorizonsstl.com/
  - Premier Knowledge Solutions - http://www.premier-ks.com

Testing

- Test Content
- Test Administration
- Re-testing
- Re-certification

Test Content

- Primarily multiple choice questions
  - Multiple Choice with Single Answer
  - Multiple Choice with Multiple Answers
- Some Fill In The Blank written answers.
- Hands on segments for some

Test Administration

- Often on a computer based system
- Sometimes using a paper based test
- Through testing centers using a computer based system
  - Pearson VUE test centre
  - Thomson Prometric test centre.
- Sometimes at trade shows and conferences
- Sometimes after instructor led training

Re-testing

- Some vendor testing policies will allow a re-test within a limited time after first failure.
-

Re-certification

- Certifications only good for limited time
- Different times & changing requirements
  - LPI - Dec 2006 - policy change from 10 to 5 yrs
- Maintenance Fees
- Continuing Education requirements
- Re-testing
  -

Future (Money Talks)

- Expansions
  - SANS - Jan 2007 - Federal Information Systems Certification and Accreditation Process
    - NIST SP 800-37
    - Only training so far, no certification yet
    - ICS2 has CAP CM certification
  - LPI - The Ubuntu Certified Professional
  - LPI - MySQL Certification:
- Degree programs

The SANS Technology Institute

- Master of Science Degrees
  - MS in Information Security Engineering
  - MS in Information Security Management
- Licensed through the State of Maryland
- Full accreditation expected with MSCHE when complete candidacy period and graduate the first class of students.
  - http://www.sans.edu/accreditation.php

Internet References

- Compare Certifications
- http://www.cramsession.com/certifications/compare-certifications.asp
- CISSP Online
- http://www.cissponline.com/cissp.htm
- Rating Certifications
- http://www.certmag.com/articles/templates/cmag_feature.asp?articleid=170&zoneid=1
- My Top 10 Tips For Preparing and Passing the CISSP Exam
- http://certcities.com/editorial/tips/story.asp?EditorialsID=29
- 10 Hottest Certifications for 2006
- http://certcities.com/editorial/features/story.asp?EditorialsID=95
- Transcender Exam Preparation Software
- http://www.transcender.com/

Security Certifications
A Short Survey

Questions?

Stan Reichardt

stan2007@sluug.org