Certification: Good, Bad, or Indifferent?

Matt Bishop
Dept. of Computer Science
University of California at Davis

December 9, 2009
Certification and Security

• Certification assists in strengthening security when:
  – You know what the person certified knows
  – You can arrange job functions so that the most appropriate people get each task
This Requires ... 

• Knowing a common body of knowledge appropriate to the task
  – Contents of a CBK for secure software development not agreed upon
  – “Best practices” may not always be “best”

• Ability to communicate
  – Must know (or be able to figure out) what information is needed
How to Do a CBK

• People agree graduates should know basic facts, applications
  – Focus on principles that hold always
  – Avoid facts, applications that change rapidly

• Degree certifies some level of mastery of subject
  – Students may take tests, do projects
  – What is mastered depends on CBK of awarding institution
How It Gets Adopted

• Slowly!
• Faculty members must accept it
• Do not try to force adoption of a CBK using threats or cuts in funding
  – You lose all the program, even those parts that are good
  – Your CBK may not meet my needs
Limits of Certification

• Implies someone has been exposed to a set of material
• States someone has passed one or more hurdles designed to demonstrate mastery

⇒ does not assure that they have really mastered the material!
Contact Information

Matt Bishop
Department of Computer Science
University of California at Davis
1 Shields Ave.
Davis, CA 95616-8562

phone: +1 (530) 752-8060
fax: +1 (530) 752-4767

email: bishop@cs.ucdavis.edu
www: http://seclab.cs.ucdavis.edu/~bishop