Teaching Computer Security

Matt Bishop
Department of Computer Science
University of California at Davis
Davis, CA 95616-8562

phone: (916) 752-8060
fax: (916) 752-4767
email: bishop@cs.ucdavis.edu

Multi-Disciplinary?

Yes; the field includes various aspects of:

- operating systems
- networking
- databases
- theory of computation
- programming languages
- architecture
- computer/human interaction

Incorporation

How do you incorporate the other disciplines into a computer security curriculum effectively?

More interesting question …

How do you incorporate computer security into the other disciplines?

Matt Bishop
Dept. of Computer Science
UC Davis

Example: Second Programming Course

- Program design from a set of requirements
  - ☞ Treat going from requirements to specification as an exercise (also allows students to be creative)
  - ☞ Design to meet the specifications
- Program implementation from design
  - ☞ argument checking (types, validation)
  - ☞ input/system checking (bogus data from server, bad command arguments)
  - ☞ buffer overflows (bounds checking)

Matt Bishop
Dept. of Computer Science
UC Davis

Testing

- Verification and validation
  - Mathematical verification of binary sort
  - Test with respect to properties
  - Test data generation
  - Stress testing
  - If it “can’t happen,” fake it

Matt Bishop
Dept. of Computer Science
UC Davis

Conclusions

- To improve the quality of security-sensitive software, we have to teach security principles in non-computer security courses.
- Computer security is a multi-disciplinary subject, but one that can be taught with other disciplines as well as teaching other disciplines in a course on computer security
- No-one is expert in all areas; so draw on experts in the other areas

Matt Bishop
Dept. of Computer Science
UC Davis