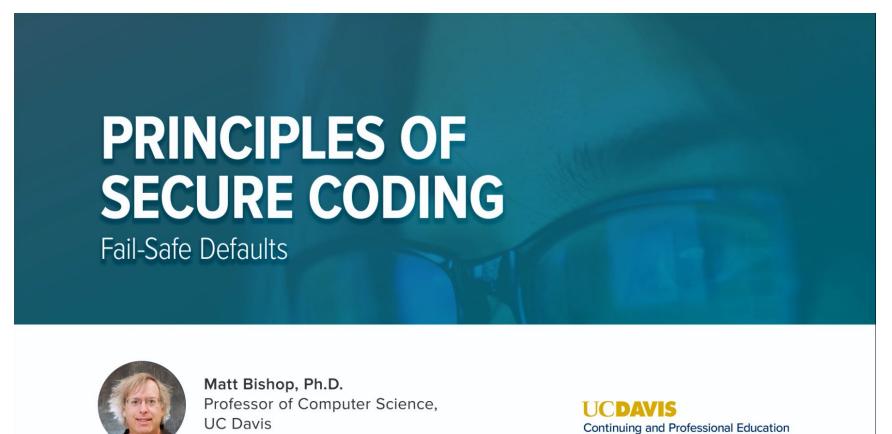
Lesson 2.3: Fail-Safe Defaults



Copyright ©The Regents of the University of California

Slide 1: Fail-Safe Defaults

## **Fail-Safe Defaults**

Default action is to deny access

If action fails, system as secure as when action began

## Puzzle

Your program will pass input to a second program that will act based on the input. The characters ", ', \$, !, ?, \*, I, and ; are known to mean special actions

- For example, the second program treats "I" as a command separator
- Letters, digits, and "-" will not cause these special actions

How should the first program sanitize its input to remove characters that may cause the second program to act specially?

If the only characters needed are letters, digits, and "–", then reject any others. Otherwise, make sure it is very easy to change the list of metacharacters