Lesson 8.5: Cryptography Basics

SECURITY VULNERABILITIES IN C/C++ PROGRAMMING

Cryptography Basics

Matt Bishop, Ph.D.
Professor of Computer Science,
UC Davis

UCDAVIS
Continuing and Professional Education

Slide 1: Policy

Policy

Assume your policy requires you to use encryption to protect data

- Passwords, etc., covered elsewhere

What does “protect” mean?

- Keep the data confidential?
- Protect it from unauthorized changes?
- Be able to tie the data to someone?
- All this, or some combination?

Slide 2: Basics

Basics

2 types of cryptosystems

Secret key

- Symmetric
- Sender, recipient have the same key
- We'll call key the "secret" key

Public key

- Asymmetric
- Sender, recipient use different keys
- Each has 2 keys: one to encipher, one to decipher
- Enciphering key is public
  - Nope, we'll not discuss PKI here!