Assurance in Operating Systems

Tom Kelliher, CS 325

Nov. 3, 2006

1 Administrivia

Announcements

Assignment

Read 6.1, 6.2.

From Last Time

Secure operating system design.

Outline

1. Assurance.
2. Flaws.
3. Assurance methods.

Coming Up

Security in databases.

2 Assurance

What is assurance?

How does an OS vendor create assurance in an OS?

3 Flaws

1. Typical sources of flaws:

   (a) I/O devices — consider video drivers.

   How has Microsoft sought to remedy this?

   (b) Ambiguity in access policy. Isolate user's data, but allow sharing of system libraries, etc.

   Which is it, is the system open or closed?

   Examples: default umask settings; sharing in Windows XP.

   (c) Incomplete mediation.

   (d) Generality.

4 Assurance Methods

1. Testing. Problems with testing.

2. Penetration testing.

3. Formal verification.

4. Validation, as part of a software engineering methodology.

5. Can a proprietary nature (Solaris, formerly), and low market penetration increase assurance?

6. Reputation and experience — OpenBSD.

   "Only one remote hole in the default install, in more than 10 years!"

7. Open source, pros and cons.

8. Evaluation — "Orange Book."