Lesson 7.4: Programming Condition

SECURITY VULNERABILITIES IN C/C++ PROGRAMMING

Programming Condition

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

UCDAVIS
Continuing and Professional Education

Slide 1: Finding Problems

Finding Problems

Look for places where untrusted users can alter files

- Temporary files created in world writable directories
  - /tmp, /usr/tmp, /var/tmp, others
- Sub-directories of world writable directories
  - Can move unwritable sub-directories
- Consider groups, too

Slide 2: Example: *sendmail*

Example: *sendmail*

Programming condition tested on v8.6.10

- Used the “quick and dirty” method

24 positives found

- 19 clearly false positives
- 2 allow redefinition of “class”
  - Require file containing definition of class to be untrustworthy
- 2 allow listing of files with names of form “qfnnnnnx” or “dfnnnnnx” and in protected directories
  - Again, require directory to be untrustworthy

Slide 3: But

But

1 allows file protection modes to be altered

- Requires “dead.letter” to be in untrustworthy directory (normal state of affairs if real user cannot be identified)

Slide 4: Amusing Aftermath

Amusing Aftermath

Problem reported to Eric Allman

- When reported, *sendmail* v8.6.12 had just been released
- *Hobbit* had found it just before we did
  - The sixth race condition…

Slide 5: About the Script

About the Script

A perl program written in under 3 hours

- Rumor was the grad student had begun learning PERL the day before he wrote it

Run over a vendor's source

- Found numerous problems
- Reported to vendor and subsequently fixed

Script ported to other vendors' systems

- Required changing the list of system calls to look for
- Enumerating these was the most painful