Evaluating System Security
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

Evaluating Program Security

- What if your task isn't writing secure code?
- It's determining if someone else's code is secure
  - Or, perhaps, their overall system
- How do you go about evaluating code or a working system for security?

Secure System Standards

- Several methods proposed over the years to evaluate system security
- Meant for head-to-head comparisons of systems
  - Often operating systems, sometimes other types of systems
  - Usually for HW/SW, not working systems

Some Security Standards

- U.S. Orange Book
- Common Criteria for Information Technology Security Evaluation
- There were others we won't discuss in detail

The U.S. Orange Book

- The earliest evaluation standard for trusted operating systems
- Defined by the Department of Defense in the late 1970s
- Now largely a historical artifact

Purpose of the Orange Book

- To set standards by which OS security could be evaluated
- Fairly strong definitions of what features and capabilities an OS had to have to achieve certain levels
- Allowing "head-to-head" evaluation of security of systems
  - And specification of requirements

Orange Book Security Divisions

- A, B, C, and D
  - In decreasing order of degree of security
- Important subdivisions within some of the divisions
- Required formal certification from the government (NCSC)
  - Except for the D level

Why Did the Orange Book Fail?

- Expensive to use
- Didn't meet all parties' needs
  - Really meant for US military
  - Inflexible
- Certified products were slow to get to market
- Not clear certification meant much
  - Windows NT was C2, but that didn't mean NT was secure in usable conditions
- Review procedures tied to US government

The Common Criteria

- Modern international standards for computer systems security
- Covers more than just operating systems
  - Other software (e.g., databases)
  - Hardware devices (e.g., firewalls)
- Design based on lessons learned from earlier security standards
- Lengthy documents describe the Common Criteria

Common Criteria Approach

- The CC documents describe
  - The Evaluation Assurance Levels (EAL)
    - 1-7, in increasing order of security
- The Common Evaluation Methodology (CEM) details guidelines for evaluating systems
- PP – Protection Profile
  - Implementation-independent set of security requirements

Another Bowl of Common Criteria Alphabet Soup

- TOE – Target of Evaluation
- TSP – TOE Security Policy
  - Security policy of system being evaluated
- TSF – TOE Security Functions
  - HW, SW used to enforce TSP
- ST – Security Target
  - Predefined sets of security requirements

What's the Common Criteria About?

- Highly detailed methodology for specifying :
  1. What security goals a system has?
  2. What environment it operates in?
  3. What mechanisms it uses to achieve its security goals?
  4. Why anyone should believe it does so?

How Does It Work?

- Someone who needs a secure system specifies what security he needs
  - Using CC methodology
  - Either some already defined PPs
  - Or he develops his own
- He then looks for products that meet that PP
  - Or asks developers to produce something that does

How Do You Know a Product Meets a PP?

- Dependent on individual countries
- Generally, independent labs verify that product meets a protection profile
- In practice, a few protection profiles are commonly used
- Allowing those whose needs match them to choose from existing products

Status of the Common Criteria

- In wide use
- Several countries have specified procedures for getting certifications
  - Some agreements for honoring other countries' certifications
- Many products have received various certifications

Problems With Common Criteria

- Expensive to use
- Slow to get certification
  - Certified products may be behind the market
- Practical certification levels might not mean that much
  - Windows 2000 was certified EAL4+
  - But kept requiring security patches . . .
- Perhaps more attention to paperwork than actual software security
  - Lower, commonly used EALs only look at process/documentation, not actual HW/SW