Government models of security

Doug Tygar (doug.tygar@gmail.com)

October 31, 2005

cs161.org

Military models of security

- "Need to know"
- Three models of security
  - Classification
    - unclassified, classified, secret, top secret
  - Compartmentalization
    - nuclear, crypto, weapons specific
  - Discretionary access control
    - Distribution lists

What clearance means

- Clearance is primarily a restriction on what you can release
- Declassification = permission to discuss
- Everyday example: Non-disclosure agreements
- Advice: Be careful before agreeing to clearance or NDAs

Two ways to rank systems

- How much do they protect military models of classification?
- What is the strength of mechanism

History

US
  Orange book (Trusted Computer Security Evaluation Criteria) → TCSEC Rainbow Series

Europe
  Harmonized Criteria (UK, Germany, France, Holland) → ITSEC

Canada
  CTCPEC

Internationalization
  Common Criteria (now on version 3.0)

US levels

D : minimal protection
C1: discretionary access control
C2: controlled access control
B1: labeled security protection
B2: structured protection
B3: security domains
A1: verified design
A2: verified implementation (never achieved)

Key ideas

- Bell-Lapudula
- We trust people, not processes
- Small "trusted computing base" (TCB)
- Includes a "security kernel"
- Processes "read down"
- Processes "write up" (star property)

More on the star property

- Star property acts as a "King Midas" touch
- Once a process reads a classified file, its security level is boosted to that of the file
- Then everything it writes (modifies, deletes, etc.) is at the same security level

Problem: covert channels

- There is more than one way to leak information
  - Existence of a file
  - System load
  - Paging behavior
- Example: TENEX passwords

Covert channels

- Covert channels are virtually impossible to remove entirely
- So we restrict the bandwidth of what can transmitted
- This means that high-classification processes are heavily restricted

What killed the Orange Book?

- System performance was poor
  - Often 1,000 to 10,000 times worse than unsecure operating systems
- Using special hardware was expensive
- Formal methods for evaluation never really worked
- User interface was horrible
- Evaluation took years (and was expensive)

The last great evaluated system

- Windows NT was evaluated at the C-2 level of security … as long as you didn't hook it up to a network.

Today's problems & the Orange book

- Problems we face today seem strangely distant from the Orange book
- Denial of service, worms, privacy, aggregation of data … none of these are addressed

Common Criteria

- Protection Profile
- Security Target

Common Criteria Levels

- EAL 1: functionally tested (US between D & C1)
- EAL 2: structurally tested (US C1)
- EAL 3: methodically tested & checked (US C2)
- EAL 4: methodically designed, tested, & reviewed (US B1)
- EAL 5: semiformally designed & tested (US B2)
- EAL 6: semiformally verified design & tested (US B3)
- EAL 7: formally verified design & tested (US A1)