Feb 23, 2005 -- Lecture 15

22C:169
Computer Security

Douglas W. Jones

Department of Computer Science

Gate Crossing

Domain, definition:

An access right allows
an operation to be applied to an object

A capability is
an object handle bundled with
a set of access rights

A domain is
a set of capabilities

C-lists implement domains

Definitions, continued

A secure system must

prevent use of objects outside domain

prevent operations not in capabilities

Capability-based addressing

for memory:

each C-list is a virtual address space

for file systems:

each C-list is a directory

State of the Marketplace

Capability-based addressing for memory
one virtual address space per process

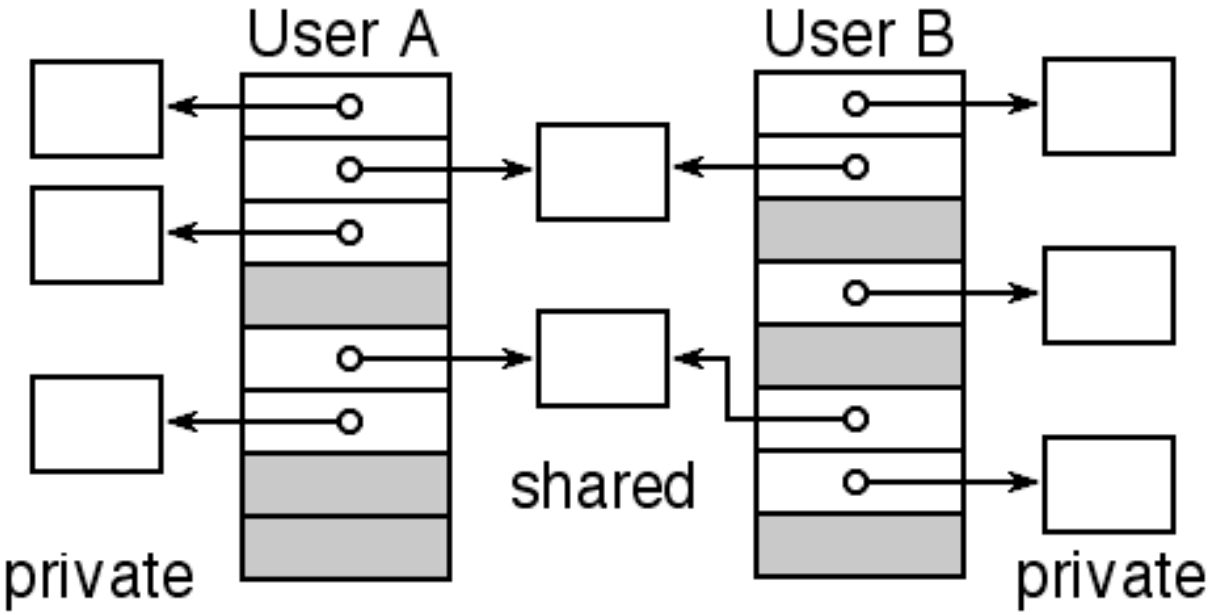
Capability-based addressing for open files
one open-file table per process

ACL protection model for files

Risk: You can name a file that you cannot access

Capability based addressing problem:

Virtual address is not constant



Solutions

Tagged architecture so that

all pointers are full-scale capabilities

IBM AS 400

Plessy System 250

Cambridge CAP computer system

Intel iAPX432

64-bit address space so that

all objects have unique virtual address

HP-UX and several others

Gate Crossing

Control Transfers between domains

User code calls system code

User calls method of proprietary object

System calls user's exception handler

Common implementation:

ban interdomain calls

use message passing instead

hide this decision behind RPC stubs

Mach kernel does this

Access-rights amplification problem

Anita K. Jones, Protection in Programmed Systems, 1973

Problem:

User U has capability C for object O
C gives U no rights to O representation

U passes C to method M of class of O
M must gain access to O representation

Example:

O is an open file
M is the read method of the file system

Solution to the amplification problem

The Unix SETUID bit

Object O is a file with owner P

Application U runs in domain Q

U has limited or no access to O

Application M has owner P, SETUID

U runs M with parameter O

M runs in domain P

M gains owner access to O!

System V and successors break it

Solution to the amplification problem

Cambridge CAP sealed objects

Wilkes and Needham, 1979

Morris, Protection in Programming Languages, CACM, 1973

Capability C for object O is sealed with K

K is a capability not in domain of U

Domain of U contains capability to call M

Call M always enters domain of M

Domain of M contains K

U calls M, passing C

M may unseal C using K

M gains owner access to O!