A Trusted Open Platform

P. England

B. Lampson

J. Manferdelli

M. Prinado

B. Willman

IEEE Computer 36:7, July 2003 , pp.55-62

18/10/2004

Presented by: Mingfeng BAO

Summary

“The NGSCB system aims to provide *security* and *openness* ……”

The article introduces us how Microsoft NGSCB works and some applications running above NGSCB system.

Next – Generation Secure Computing Base

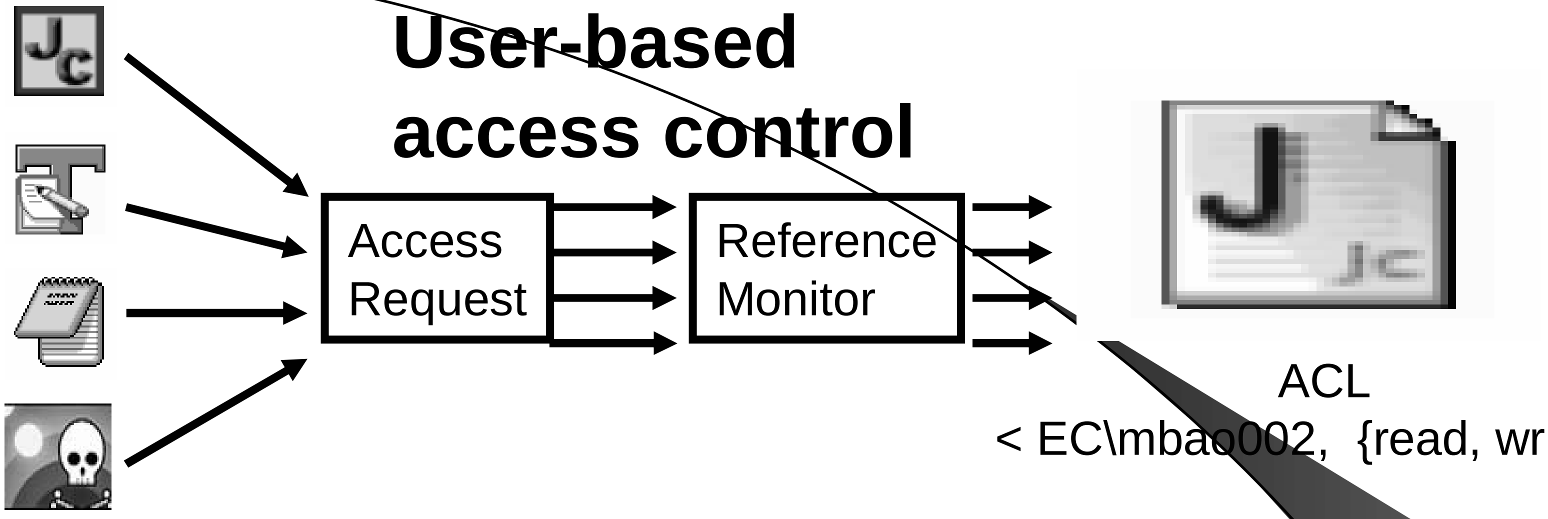
APPRECIATIVE COMMENT(1)

It gives us a very good explanation on how to achieve openness securely

- SCP & authenticated operation
- code ID (cryptographic digest, hash)
- code based access control model
- Virtual Machine Monitor (VMM) isolation

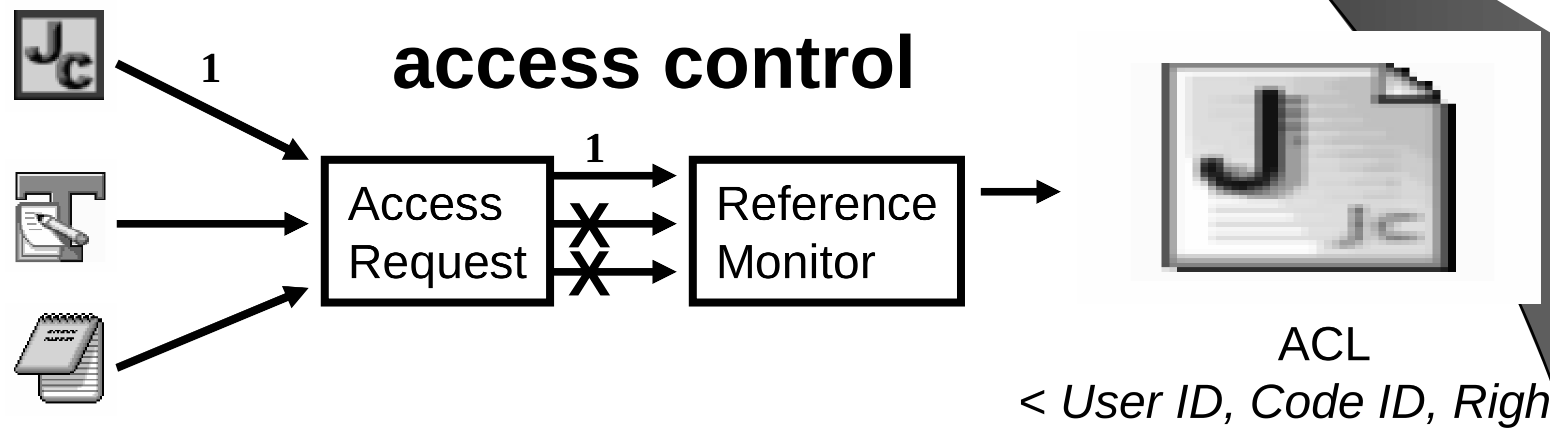
SCP -- Security Coprocessor

User-based access control



ACL
< EC\mbao002, {read, write} >

Code-based access control



ACL
< *User ID, Code ID, Rights* >

Trust Chain

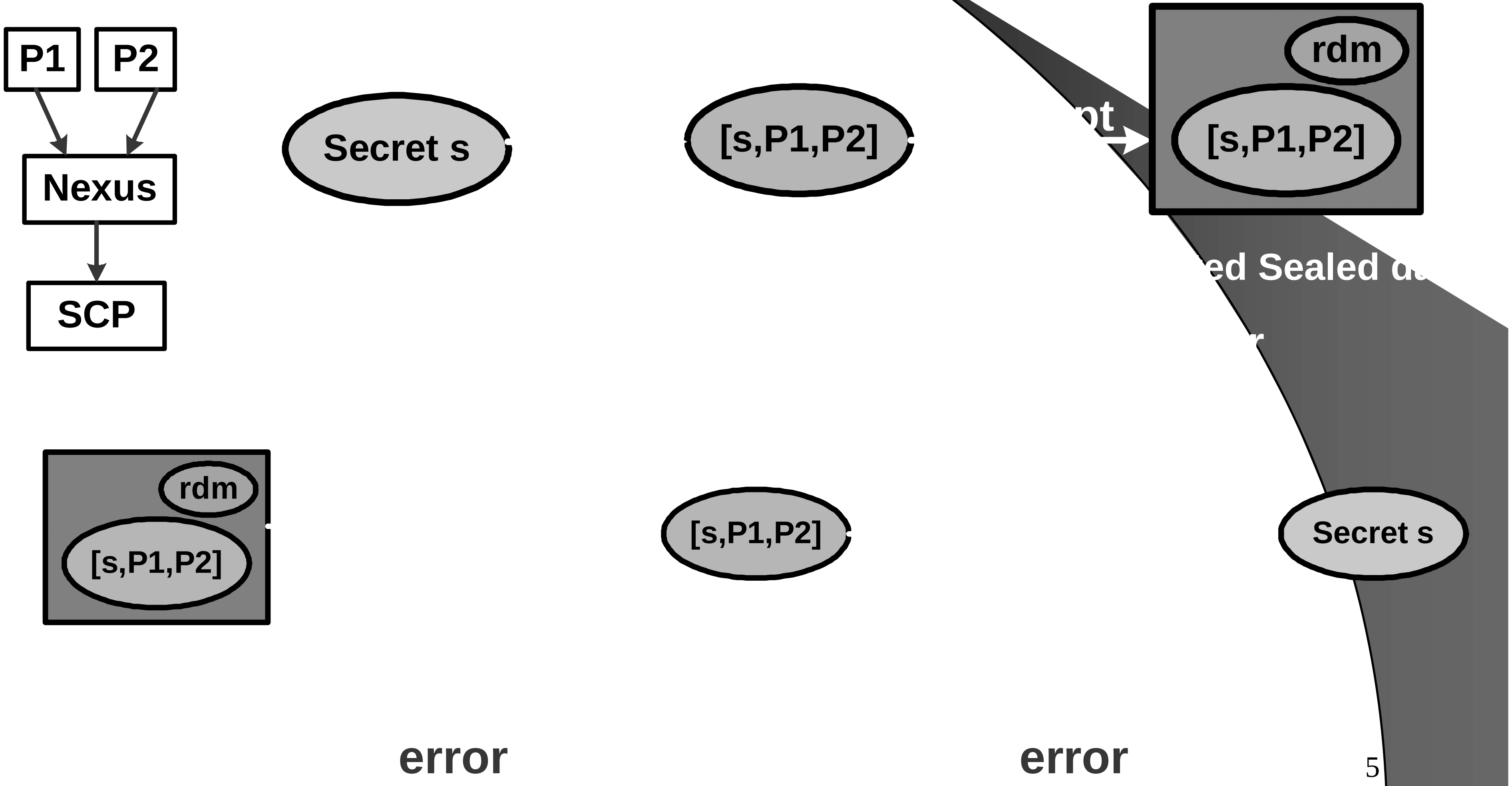
Security
Co-Processor
(SCP)

Operating System
Kernel (Nexus)

Programs

APPRECIATIVE COMMENT(2)

Clearly illustrates how **sealed storage** works



Criticism:

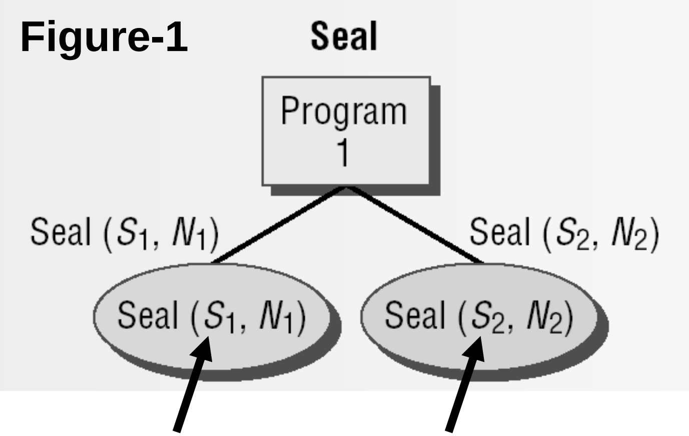


Figure-1

- What is the meaning for $\boldsymbol{S_1}$, $\boldsymbol{S_2}$?

They were sealed by the same program, but have a different sealer’s ID.

- VMM & Main OS, which one boots first ?

“ NGSCB platforms allow a lightweight boot of a machine monitor from within an already running operating system.”

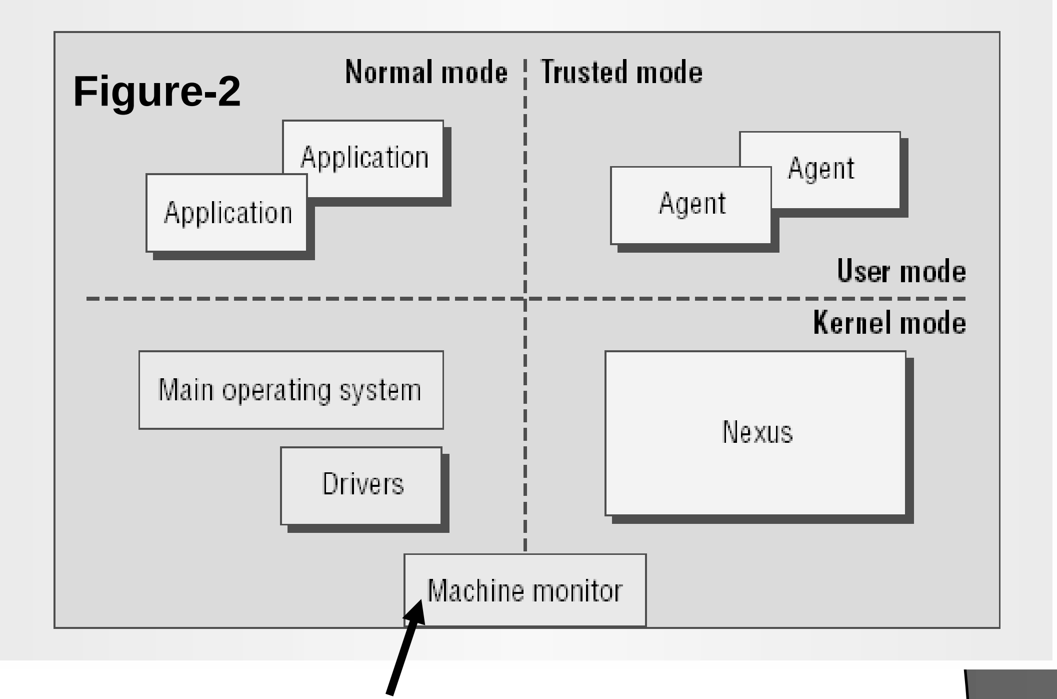


Figure-2

Questions:

- NGSCB has done a lot in improving system confidentiality; does it make improvement on its availability as well?

- Can we trust NGSCB fully, considering intentional back doors in OS and Applications?