Developing Applications on LOCK

R. O'Brien and C. Rogers, "Developing Applications on LOCK", in Proc. 14th Nat'l Security Conf., Washington DC USA, 147-156, 1991.

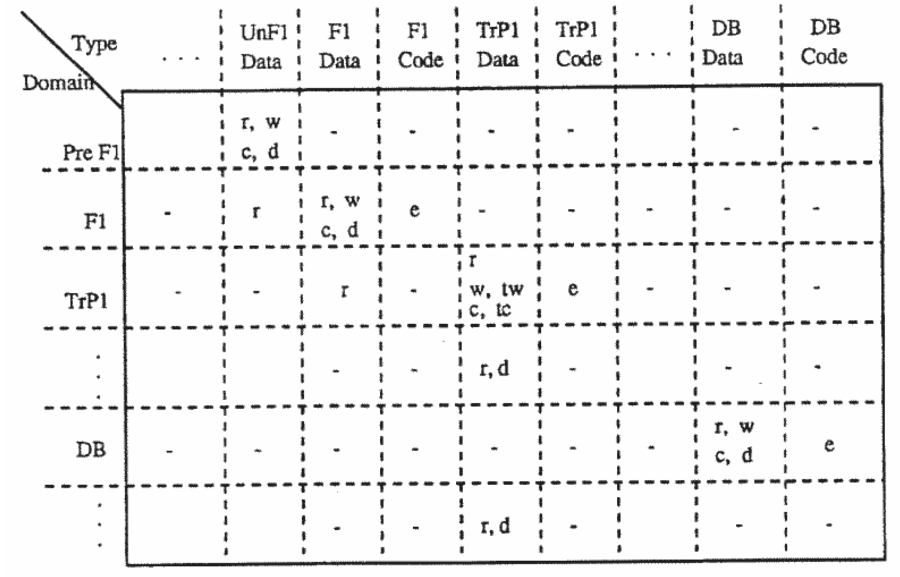
Presented by Heiko Voigt

What is LOCK

- Logical Coprocessing Kernel
- Research Project of NSA (U.S. National Security Agency)
- Goal: highly secure computing system
- Trusted computing base
  - Security Coprocessor called SIDEARM
  - Small set of assured primitives

Main Focus

- Type Enforcement and its possibilities in development
- Defined by Domain Definition Table



Type / Domain	. . .	UnF1 Data	F1 Data	F1 Code	TrP1 Data	TrP1 Code	. . .	DB Data	DB Code
Pre F1		r, w c, d	-	-	-	-		-	-
F1	-	r	r, w c, d	e	-	-	-	-	-
TrP1	-	-	r	-	r w, tw c, tc	e	-	-	-
. . .			-	-	r, d	-		-	-
DB	-	-	-	-	-	-	-	r, w c, d	e
. . .			-	-	r, d	-		-	-

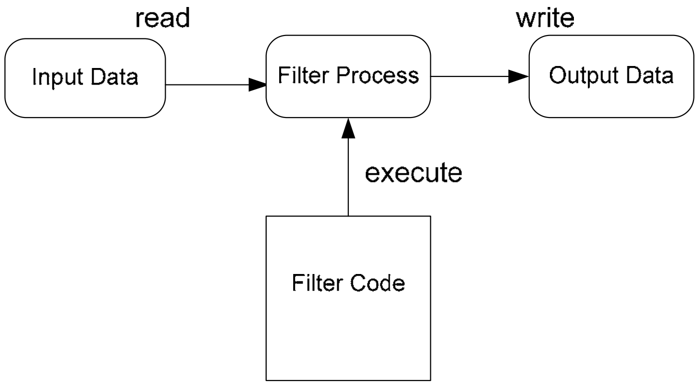
Source: Paper

Appreciative Comments

- Good Examples
  - Assured pipelines

Examples

- Assured Pipeline

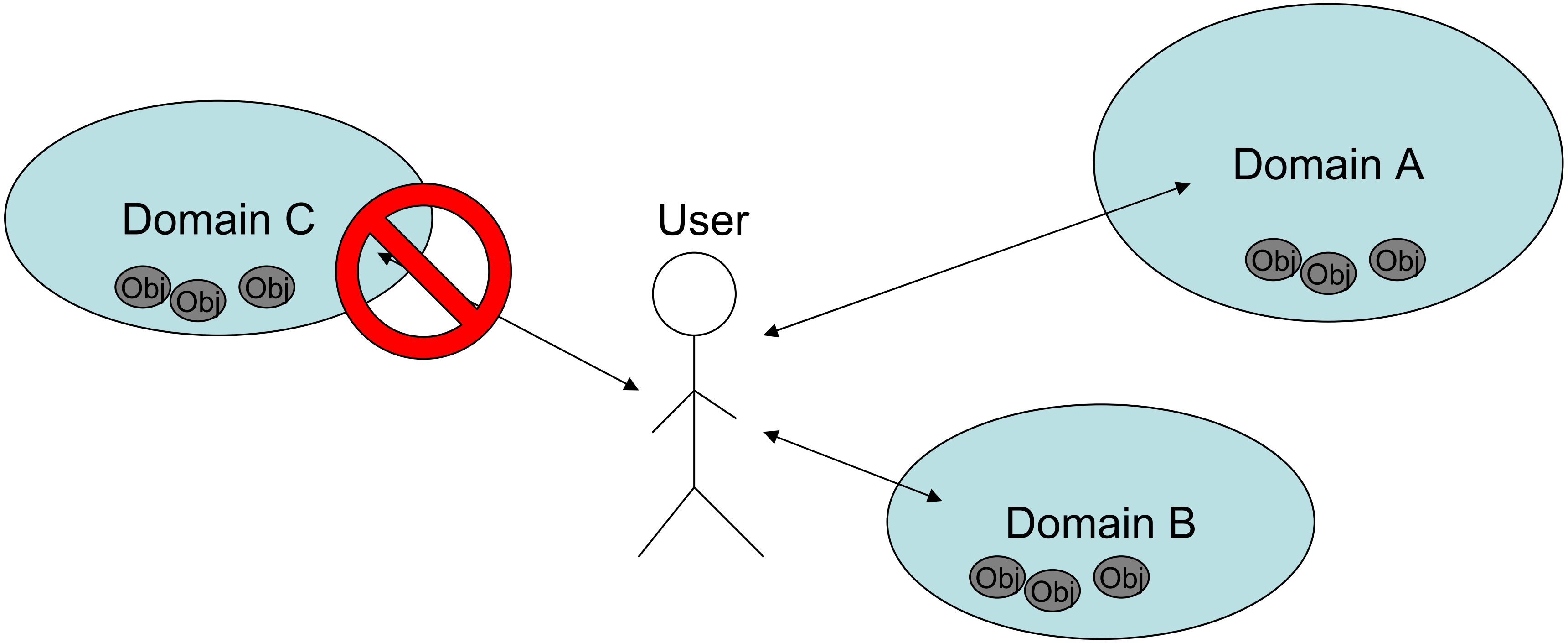


Appreciative Comments

- Good Examples
  - Assured pipelines
  - User roles

User roles

- Users can only act in certain domains



Appreciative Comments

- Good Examples
  - Assured pipelines
  - User roles
- Mentions unsatisfying points of current implementation
  - No debugger
  - TCB code has to be inserted using hardware level debugger

LOCK today

- Its not as scientific as you might think
- Many Results implementented in

“SELinux”

http://www.nsa.gov/selinux/

Criticizing Comments

- Missing Reference
- Trust:

“Trust on the LOCK System has a very specific meaning. It can be used to override the *-property and permit a subject to modify […] a lower level object, […]”

This is the first time the Author is using:

- Trust, *-property, lower level object

Criticizing Comments

- Recall:
  - User Role
  - Assured Pipelines
  - Theoretically secure
  - Does it work?

Question:

Would you feel comfortable in a User Role if that would eliminate all viruses but restrict your freedom executing programs?

☺