Relying on $CMON as a security brings your system at risk!

Dear GreenHouse tool users,

some of you may believe - or be made to believe by so called experts - that $CMON is a quality security base of your NSK system which you can rely on.

The bad news is, and always was: It never was and still is not!

$CMON became invented in the 197x time frame, when COMINT was the interactive interface into a Tandem system. Its intention was to have a kind of first level control over a user, e.g. to deny commands (such as ALTPRI), to control the start of a resource, or to translate command abbreviations into real commands (COMINT did not know about macros etc.).

The $CMON interface was carried forward with TACL.

Since SAFEGUARD exists – and that is since 1985 - there is no good reason for using $CMON left. Even the load balancing can easier and much more efficiently be accomplished by using the GreenHouse ShareWare product LAUNCHER.

And here are the reasons why $CMON is NOT a security base you can rely on:

1. $CMON gets only involved from a standard TACL.
   Even worse: A TACL object file can easily be manipulated in a way, that the $CMON interface is disabled, allowing a complete bypassing of measures provided by a running $CMON process.
2. GUARDIAN procedure calls used in applications other than TACL, such as
   - User_Authenticate_
   - AltPri
   - etc.
   are NOT seen by $CMON at all!
   This means: When you do not like to get $CMON involved in your activities – write your own small command interpreter – or use the tools explained below.

To demonstrate the weakness of $CMON, I have prepared a TACL object in a way, that it no longer talks to $CMON and bypasses all $CMON actions.

1. Download the TACL available from this location (in binary mode), and name it e.g. **`NOCTACL`**.
   When it is loaded outside of $SYSTEM.SYSnn then you need to install a TACL environment in that location. When not doing it, TACL will not execute its environmental variables.
2. Make sure the file code of the down loaded file is set to 100 (**`FUP ALTER NOCTACL,CODE 100`**).
3. There is nothing special necessary, because TACL does not need any license or system manager interaction: It is a simple program! (OK – not THAT simple…)

4. … and here we go: All interactions of this TACL are no longer seen by the running $CMON process.

Give it a try and you get a pretty good understanding why $CMON is NOT a security base for NSK systems at all! Real security products should NOT rely on $CMON, but on operating system provided mechanisms.

A second method to circumvent $CMON is to bind the also provided TACLLIB library to your TACL program by executing this command:

```
[run] TACL/NAME $name, PRI pri, ..., LIB TACLLIB/
```

This library is **independent** of any TACL version, and works for all current as well as future TACL programs.

You think that using this TACL or library is a security breach?
I believe, that using $CMON as a reliable security base is the security breach. Real security systems can not be bypassed so easily!
The conclusion is: Get rid of security products, relying on $CMON!

Have fun and limit your exposure,

Carl
23Oct2003