

Re: OS Partitioning and security

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2004-02/0655.html>

From: Walter Roberson (roberson_at_ibd.nrc-cnrc.gc.ca)

Date: 02/28/04

Date: 28 Feb 2004 18:04:01 GMT

In article <4040cee8\$1@news.012.net.il>, Tsvi Gad <tsiky@mail.com> wrote:

:I am looking for information about the following issue:

:A client I work for is going to use a single hardware for the Development

:and Production servers by using the machine ability of OS Partitioning. It

:means that every OS has its own hardware except the bus that is common.

:The problem is that for security reasons there is a need to separate the two

>*servers and it also has different sets of data.*

:I am sure every vendor will confirm that kind of architecture as safe but my

:guts says otherwise.

I would want very strong assurances from the vendor that a privileged user on one partition could not snoop the bus for traffic on another partition. For example, is the data on the bus cryptographically protected by a key specific to the partition? But if it is, then there has to be a per-partition key negotiated with the peripheral controllers (e.g., hard disks): is the key exchange protocol secure against main-in-the-middle that can see every byte transferred both directions? A facility like that certainly isn't included with any SCSI or ATA or EIDE controller that I am familiar with.

What is the Orange Book rating of the equipment involved? If it is C2 then you absolutely cannot trust the setup for the circumstances you envision: C2 only protects against non-root users. You need at least evaluated at B1, and although my knowledge of B1 is weak, I don't recall that even B1 would be enough. I seem to recall that at least B2 would be needed, and more likely A1. There are very few systems at the B2 level or above.

According to <http://www.dynamoo.com/orange/summary.htm>

you'd need Cryptek VSLAN, Trusted XENIX (both B2),

Getronics/Wang Federal XTS-300 (B3),

Boeing MLS LAN, Gemini Trusted Network Processor, Honeywell SCOMP (all A1)

--

Those were borogoves and the momerathsoutgrabe completely mimsy.