

REVIEW of PAPER # __22__ BY REVIEWER # __25__

Fill in each _____ with a number on a scale of 1-5.

(1=Poor) (2=Fair) (3=Acceptable) (4=Good) (5=Excellent)

1. Presentation: __3__

1.1. Organization: __4__

1.2 Grammar and spelling: __2__

2. Completeness (Strength of Content- Missing key items?): __3__

3. Technical Correctness: __3__

4. Proper Referencing: __2__

5. "Coolness" / Originality: __3__

6. Comments to Author (Suggestions for Improvement):

The style of the paper and content is a bit vague. While the main topics are covered, many details to firmly support these topics and opinions/analysis upon them are missing or loosely mentioned. Thus, the paper is not very in depth.

Some areas seem technically incorrect:

Page 1, section 2: The use of "virtualization", while following the suggested topic to cover, should had been specifically addressed as Xen (as seems to be referenced). Additionally, virtualization is herein described specifically by what Xen and related hypervisors achieve. It is incorrect to define virtualization as the same as a hypervisor, as virtualization is a much broader topic.

Page 3, section 3.2: "The significance of risk of a compromised operating system is not well established". Here the opinion that operating system code is not significantly at risk of attack is very questionable. Citing that many people may be looking at this code does not justify ignoring security of the system.

Page 3, section 3.2: The topic of locks and Virtual Ghost seems out of context. At least direct citation to a reference would be useful to back up the claims that Virtual Ghost is unable to secure against compromised locking.

There a few noticeable spelling and grammatical errors:

Page 1, section 2.1 : curruption

Page 2, section 2.2: wasy

Page 3, section 3.2: [?] and involed

Page 4, section 5.1: "Visualization" should be "Virtualization"

Page 6: The formatting of the references is not consistent, lacks needed commas, and the use of the bracketed names and year in the beginning of every reference is unconventional.

Some use of language is too informal (as indicated by the italicized word):

Page 1, sections 2.1, "*somewhat* isolated..."

Page 2, section 2.1, "client machine is *stolen*"

Page 4, section 5, "The most important *thing*..."

Page 4, section 5.1, "...just affecting different *people*"

Some ideas need to be further explained or developed (even just an additional sentence would be helpful) :

Page 1, section 2.1, " Improper implementation can completely ...": Here "improper implementation" needs to be elaborated.

Page 2, section 2.1, " restore that system to its previously secure state": How is this restoration achieved?

Page 2, section 2.1, " virtualization..reduce...hardware...This can help to reduce the overall security burden": How does the reduction in hardware equate to reduction in security burden?

Page 2, section 2.2, "increased impact of any security breaches...": It needs to be explained how providing a hypervisor lends way to more insecurity.

Page 2, section 2.2, “when the system has been configured properly”: What specifically does “configured properly” mean? An example would be helpful.

Page 2, section 2.2, “share information between systems”: What are examples of shared information?

Page 3, section 3.2, “few types of attack that virtual ghost does not protect against”: What are these attacks?

Page 3, section 3.2, “the application code must also be written to take specific advantage of the hidden memory space”: Is this referring to the use of bit-code and virtualization in Virtual Ghost?

Page 4, section 4: More can be described about Exokernel. Of all three systems, this one is very lightly described; this is also the case in section 5.

Page 5, section 5.2, “Virtualization ... does so at the cost of creating new potential risks”: Name some of these risks here.