File 20100520.0900: Notes from classified telecon on 5.0 CT&E this morning (YF SCIF):

Attending: Kevin Miller, Ian McGlothlin, myself, Olav, Dan Griffin, Kevin Fullerton, Dan Nichols, Orville Brown, Dave Aushman (sp?) from I173, Dennis Bowden, Charissa (sp?), and others.

The purpose of the call was to go over three things: list of findings extracted from SSC Charleston report, the results summary (pen testers' report), and Lockheed's responses.

Charissa: looking at the CT&E report, asked about the xterm issue. Ian replied that the OS will not audit that even no matter what the developer tries to do; the OS audits every other invocation of xterm but something about the way that xterm is invoked [classified details] makes it just not get invoked. The developer is going to open a trouble ticket with the OS vendor (Sun/Oracle) at the recommendation of Orville. The way that xterm was invoked was closed and is not possible any more.

Orville: we have a lot of work to do during the regression period.

Phyllis had to leave early today, so the telecon moved quickly on to her main topic. Regarding data link, there is a philosophical difference between CT&E and ST&E; we have always depended heavily on FAT and IV&V testing to validate. Phyllis then asked, besides digitally signing an arbitrary blob and auditing, what does WinDDS actually do? [She believes it adds no security because the CT&E configuration of RM 5.0 does not specify and enforce use of a particular viewer for RHR.]

Kevin Miller: the viewer is whatever the *accreditor* chooses.

Phyllis is upset because RM advertises RHR but it does not deliver. such functionality. Other guards advertise it, and they come with specific functionality that can be tested by CT&E. Most CDS provide specific tools, *eg* Purifile. RM uses a different model. Phyllis does not agree with that model and will continue recommending that WinDDS be dropped from 5.0 in the UCDMO baseline list.

Another person [not sure whom, but he noted that 'we' are also a voting member of the CDTAB] said it doesn't really matter what's in the baseline. What is important is to have either a resolution or a POA&M for every one of the findings before going to the CDSG. CDSG is reluctant to take an incomplete body of evidence to the CDTAB because of the risk of the body of evidence not being accepted.

Phyllis said that ST&E cannot guarantee that a site won't choose a stupid RHR tool, for example Notepad, for a viewer. Phyllis would prefer that RM enforce a choice of tools, to guarantee that no site uses a weak tool.

Ian and Kevin Miller both responded that it is not the site that chooses. It is the accreditor who chooses. If the accreditor is not satisfied that the residual risk of using a particular tool is low enough, the accreditor will not sign off the site accreditation.

Orville said that both Paul Livingston [recently retired from the DSAWG] and Frank Sinkular helped design this architecture—it is not something LM just made up.

Resolution for today: have to come up with a response that will satisfy Phyllis, who is a voting member of the CDTAB.

Colours in the document:

black original

blue Lockheed's response

green NSA's reply

red Programme Office and LM's final response

(The last two colours in that list might be swapped.)

Proceeding through the IC world is currenrly green light. Proceeding through the SABI world is red light.

Ian: 'that completely defeats the purpose of the UCDMO.'

A lost of CRs associated with specific findings would be classified. If the list of findings could be unambiguously numbered across all test reports, then the list of CRs could be unclassified.

Need to put together a way ahead for the SABI world. Next telecon next week will be unclassified, and shorter. I asked Kevin Miller to let me know when it is if it's scheduled not for Thursday at 0800.

References