File 20100817.1250: Notes from Systems Engineering meeting today at 11:00 a.m.:

The developer considers the UCDMO conference to have been very useful. There was one session about the RM 5.0 CT&E which was well-attended and positive in tone; the presenters did not go into detail about problems encountered, just the overall plan and outline of the CT&E effort. RM is considered to have six competitors: ISSE, BAE's DataSync Guard, the Raytheon High Speed Guard, HardwareWall, the General Dynamics Tactical Cross Domain Solution (TCDS), and TMAN.

(Not included in weekly activity report) GD got in trouble for claiming that TCDS is compatible with Radiant Mercury MAG: the developer believes that GD stole it from a joint project.)

TMAN is on the UCDMO baseline list which means they have both SABI and TSABI approval. SABI considers their threat environment to include the entire internet, so certification to SABI level takes about a year and a half, compared to half a year for TSABI. Now, under the combined process, everything takes a year and a half. TMAN boasted during the UCDMO conference of a six-month release cycle, leading the RM developer to conclude that TMAN wants to get off the UCDMO baseline list soon.

Virtualisation of guards was the biggest topic at the UCDMO conference this year. NSA was pushing it; Boyd Fletcher is the most visible proponent of virtualisation. He is very influential. Perceived advantages are two-fold: firstly, the ability to run ten guards on two boxes is a win from a SWAP perspective; secondly, virtualisation of hardware stabilises the hardware environment that guards need to run in and be certified on; short hardware manufacturer product cycles have always been a problem for certified systems.

Phyllis Lee's two assistants gave a presentation on all the attacks that they perform on CDS test articles. It was widely considered the best presentation at the conference. They are sending out a white paper as a follow-on to the presentation soon. They described their test methodology as being based on the CVE, which the developer is interpreting as a good indication of how to test internally in future. By giving this clue to the CDS vendors, NSA are making their job more difficult, they observed. The impression given me by the developer was that guard vendors at the UCDMO conference thought of this a wonderful piece of competitive intelligence. But personally I wonder if the reason it was delivered was intended as a stinging indictment against all the vendors, who—it seems apparent—are not paying attention to the CVE. If that is so, I think NSA's message was only partly understood.

(Not included in weekly activity report) The UCDMO presentation was enjoyable to watch, because it was done in a lighthearted manner, and they did not name any names, but it was clear that a lot of the vulnerabilities NSA finds—in all the guards—are still straight out of the CVE. In future, the RM developer's testing methodology will change to include tests for all the CVE items, plus a bunch of new performance-oriented requirements. If the RM requirements contained a requirement to support fifty concurrent DDS sessions, then problems such as the one found at STRATCOM this week could have been avoided. Silly things that seem obvious to everyone and consequently never have requirements written against them ('the guard shall recover from an unexpected TCP termination') end up causing problems—RM crashes in that particular situation; it ought to handle it—end up being caught in CT&E. It is not just the RM developer; all the guards are being caught short by this. [Editorial note: I agree; several of the findings from CT&E were elementary secure programming mistakes straight from the CVE. The RM software writers are not at all familiar with the CVE, and that could be remedied easily.]

References