File 20100924.1356: Notes from the RM 5.0 CT&E telecon this morning:

Larry Sampson sent out the following agenda:

- POA&M Review
- Report on CDTAB Discussions on RM 5.0
- Deliverables Update
- Update on CD CSTG Meeting, Wednesday, 29 Sep 2010
- Review of open action items

Before the meeting, a slide deck from Charissa Robinson (NSA Lead, CDS T&E) was sent out. It was titled 'Radiant Mercury 5.0 Joint Testing CT&E' and I wonder if it was presented at CDTAB or elsewhere. It defined the following roles and responsibilities:

- UCDMO: test coordinator/facilitator
- DNI: test director and review
- NSA: test review and penetration
- SPAWAR Atlantic: test conductor
- IV&V RM Team: IV&V testing
- PMW 160: RM programme management

History:

- October 2009: NIST SP 800-53 controls vetted by community
- 18 Nov 2009: Test Readiness Review meeting
- November 2009: Alpha/IV&V testing at LM
- 04 Jan 2010: Security Design Review
- 22 Jan 2010: recommended controls sent to community
- 08 Mar 2010: test procedures sent to community
- 29 Mar 2010 through 23 Apr 2010: CT&E at SPAWAR
- 28 Jun 2010 through 23 Jul 2010: CT&E regression testing at SPAWAR and pen test finding regression testing by I733
- 02–13 Aug 2010: ST&E at STRATCOM performed by DIA

The Joint Test Approach leveraged Alpha and IV&V testing. It incorporated lab-based testing to provide DoD evidentiary requirements and to perform potentially 'destructive' tests. It accomplished Beta 2 and ST&E testing to satisfy IC requirements and DoD mitigation requirements. It was the prototype usage of 800-53 controls for CDS; will not 'certify' in absence of 800-53a; used for test organisation and reporting understandable to the community. The controls will be tested to provide evidence necessary for utilisation by all communities. It will address additional NSA-submitted controls not yet adopted into 800-53 (i.e., Flow Enforcement).

Controls to Test Objectives will be a one-to-many relation. The results of 'certified' evidence will be used by communities to assess control implementation in the context of their security accreditation.

> 'Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.' [Source: NIST SP 800-37]

Testing Evidence Used:

- Alpha/IV&V testing
- POA&M Validation Report—RMPMO
- CT&E Report with regression test results (SPAWAR with I173 oversight)
- I733 pen testing
- Beta 2 ST&E report (DNI/CAT)

TORA: Target of Risk Assessments

- RM 5.0 only
- FSR (October)
- RM 5.0 with SNMP (October)
- RM 5.0 with WinDDS (October)
- RM 5.0 with Remote Management (October)
- RM 5.0 with WinDDS and Remote Management (October)

Source: 'Radiant Mercury 5.0 Joint Testing CT&E' by Charissa Robinson. Undated, Unclassified//-FOUO. Acquired 24th September 2010 at LM Deer Creek Facility from Larry Brown, but emailed out by Larry Sampson earlier the same day, or the night before.

Present on the call today were Kevin Miller, Russ Savage, Joe Loughry, Larry Brown, Craig Christensen, Kori Phillips, Larry Sampson, Mia ?, Orville Brown, Kevin Gallicchio, Dennis Bowden, Dave Oshman (NSA), Charissa Robinson, Atri Amin and Corinne Castanza. Rob Drake was missing. The main topic was a document titled 'Dana's notes' from Dana Pipkin comprising her personal impressions and minutes from the CDTAB deliberations on 21st September. The CDTAB this time considered only the first of six TORAs (Target of Risk Assessment) that are planned to be reviewed. We have not seen the RM 5.0 TORA yet; it will be sent through the low-side email soon, probably Monday when Amy Arroyo gets back.

There were four sections in the first TORA; a 'high' technical risk rating on any two triggers a 'high' rating for the entire CDS.

1. Role separation is not being done at the kernel level; it is done in the application.

2. MAC policy is not implemented sufficiently; unauthorised communication between zones; `setlabel` command exists—if a user could get access to it, they could downgrade files. [The developer is of two minds on this one; firstly, a user cannot get to *setlabel* unless they could get to a shell, and the developer asserts that they can't (despite Corinne's claim). On the other hand, the developer is willing to remove *setlabel* as it is not needed.

3. Solaris 10 resource pools are not being used for resource management. Too many admin activities are being done by the `rmuser` account.

4. The *root* role still exists after installation. It is dormant and could be removed entirely. It is dangerous and not necessary to have around; it could be used to violate MAC policy.

Charissa is sending across the Technical Risk report; the board wanted it shared with the developer and the government Programme Office. Dan Griffin is unhappy with the 'high' technical risk rating; he wanted to know if there would be an opportunity to rubut.

Atri explained that historically, the rating stays where it is, unless there was some serious error. It would be necessary to request another review to have a chance of getting the rating changed.

Kevin Miller put the rating in perspective. RM 4.0.5 received a 'high' rating, which did not slow down adoption. The later RM 4.5 received a 'medium' rating. The 'high' rating of RM 5.0 suggests that the CDTAB rating process is inconsistent at best. The board also specified some additional ST&E tests that they would like to see run, for their own assurance.

Corinne, Atri and IV&V were with Charissa in the CDTAB meeting. They brought with them all the evidence to the board. Dana Pipkin later sent Charissa an email; they want the developer to submit their ticket now.

Dan Griffin asked, ‘So now, with this high technical risk rating, how is this going to play with SABI?’ If we want to get the risk rating changed, it will be necessary to use the Navy CDMO for leverage. The developer is not permitted to contact the board directly; the developer must go through the Navy CDMO, which goes to the board, and the board then contacts Atri’s people. Only the board can contact Atri’s people. I173 needs to have a ticket before they can work on anything.

Dan Griffin asked about bringing additional evidence to the board. I173 said please provide the missing evidence to us so it can be included in the evidence provided to CDTAB and the Community Jury. Developers cannot present evidence to the board. The developer must give the evidence to I173.

Lots of systems get a ‘high’ technical risk rating. It is not a bad rating. I173 would be very surprised if the rating changed.

Corinne then amplified on her remarks during CDTAB that she had ‘almost been able to get to a window’. She said she had managed to minimise some of the widgets, and was playing with the Help window. There are too many of the default Solaris components left in; the OS was not stripped enough. DNI and NSA agree on that. They are also not happy that the guard crashed several times at STRATCOM. They did not expect to see stability issues this late in the CT&E.

The telecon on 1st October will discuss whether a Version 5 POA&M is needed; the board’s recommended additional ST&E procedures will go in the updated POA&M and be added to the ST&E plan for DoD sites.

Larry Sampson said there will be a CD-CSTG meeting next week, on 30th September. A number of briefings are slated, on the new risk management framework, RM 5.0 CT&E, and talking about moving forward with the CSTG. He next brought up the issue of closing down the RM 5.0 testing effort. Dan Griffin noted that the only thing left is the response to the pre-CDTAB report.

The IC risk assessment is still to come. Need to keep going with these telecons for the time being. They can wrap up in October. The 19th or 20th is when CDTAB meets again.

Dan Griffin asked if a knowledgeable LM engineer could be standing by outside the room where CDTAB meets, to answer questions in support of IV&V representatives inside the room.

Dennis Bowden asked if Rob Drake is on track to provide an accreditation letter by 30th September. Kevin Miller asked at what point will RM 5.0 be on the UCDMO baseline. Answer: pending triage of the CDTAB report, pending everyone sending in their final reports, and one ATO from either DoD or IC. Atri reported that the lab has expended all their funds; nothing is left to support any more testing. There is barely enough for one more trip to attend.

After the telecon ended, Larry Brown expressed concern that a ‘high’ technical risk rating will necessitate provision of screening routers, anti-virus, etc. at sites. Russ Savage commented that none of that helps the RBAC problem anyway. Craig Christensen said he is concerned that if sites see two solutions, one with a ‘medium’ risk and one with a ‘high’ risk then the site will choose the lower risk. Larry and Russ countered that after the initial period when a product is first introduced, no one looks at the risk rating. Like GPA, in the evaluation of an experienced candidate it will be forgotten, Craig asked, can we get through the initial period? Russ pointed out that for SEW, JCDX and shipboard duties, nothing else but RM can do the job.

Kevin asked, so can we fix the RBAC issue now? Russ Savage advocated pushing out the 5.1 patch to next Spring. ‘Stop this patch business now’. Root is only used for debugging in the field. Sites use debug capability all the time. Larry suggested putting all tools needed for debugging on a CD-ROM. Get them off the hard disk. The tool CD can reside in a safe, and that will satisfy the CDTAB’s complaint about RBAC and OS minimisation. Kori Phillips pointed out that changing passwords requires the root role. It cannot be eliminated.

Kevin Miller: the core issue is RBAC. If software tools are used, then a person with a shell can use them, but the core issue is whether Corinne can get her window open in the first place.

Joe Loughry suggested to make it so the site has to take a CD-ROM out of the safe and put it in the machine before they can change passwords. Kevin: that’s ridiculous. Joe: yes, it is, but it would satisfy CDTAB.

Larry Brown suggested that we define a debug rôle. It will have all the same capabilities as root, but at least it’s a different rôle and can be audited separately.

Meeting adjourned to Craig Christensen’s office at 1000. Larry Brown advocated for a 5.1, 5.2, 5.3 release schedule every six months; get them disseminated so that customers start demanding the 5.1 capabilities. Every six months a new one is released; maybe only every third one gets certified.

At 1000 the developer called Dennis Bowden regarding the patch. Engineering does not see anything in the patch currently that addresses any of the CDTAB concerns; the developer wants to redirect patch testing effort to focus on the new issues. By pushing the patch out to a later date, call it 5.01, it could take care of more of the issues important to the CDTAB.

Expecting report from CDTAB and Corinne's report on Monday.

Dennis Bowden: nobody, not CDTAB, not UCDMO is pushing for a patch. The next significant activity is the test event for the current patch. Delay the test event, and a single later test can cover a better patch, without requiring a second test event to take place.

Dan Griffin: we should wait for the reports to arrive on Monday.

Kevin Miller: remember, the October TORA reports will come out afterwards. Suggest we hold off the entire test event until those other TORA reports come out. They will likely generate new issues.

Dan Griffin: I am not ready to do that. Want to have the 5.01 patch available in case UCDMO says RM 5.0 cannot field without it. We will wait until Monday and meet formally again then.

Discussion of what to do. The developer's recommendation is that the October TORAs will almost certainly generate new CRs. In addition to those, address Corinne's issues. Push all of those back from now into a single, better patch and test it once.

Dan Griffin: still concerned that UCDMO might come out and say RM 5.0 cannot field without this small patch. RMPMO is willing to pay for a second test event for a larger patch if and when it becomes a necessity (which is likely).

My notes from Dana Pipkin's document:

Charissa Robinson and her team, NSA: very neutral, just provided the facts.

Dave Oshman, NSA: very neutral; provided technical information only, no opinions.

Corinne Castanza, pen tester: opponent to RM, claimed she was sure she could open a window given a little more time; came late, left early; did not show up at all on the second day. It appeared that her only intent was to drop her bomb and leave.

Phyllis and associate, pen testers: advocate for RM, provided technical information when asked.

[Note the role reversal in the previous two. Phyllis has always been the bete noir of RM in the CT&E telecons, with Corinne much more reasonable. In the CDTAB it was as if they'd switched personalities.]

Glenn Learn, CDTAB?: neutral, provided guidance on Risk Decision Acceptance Criteria (RDAC).

[Note: I think Mr Learn is Navy, not CDTAB. Navy CDMO, maybe.]

Dan ?, CDTAB Chairman: statements would seem to imply that he was not a proponent.

Jay C. and associate, UCDMO: neutral, quiet.

Dave Bowman, Army CDSO: advocate, voice of reason.

Unknown, Marine CDSO: neutral, very quiet.

Rick Perkins, AF CDSO: opponent to RM, very vocal.

Atri and sidekick, SPAWAR testers and Navy CDSO rep: waffled between neutral and opponent to RM. At first they tried to stick to the test evidence, but over time jumped on the bandwagon with the other more vocal members of the board.

General comments: a decision was made to divide the Technical Risk Review (TRR) into different TORAs. A TORA is the baseline architecture that is being evaluated. Because they didn't want the risk rating for certain high-risk subsystems necessarily to affect the overall risk rating of the system. This TORA covered generic guard only without any bells and whistles. The TORAS for Filter Strength Review (FSR), SNMP, WinDDS, Remote Management, and WinDDS with Remote Management will be held in October.

Individual Ratings: areas they looked at.

1.1 network isolation

1.2 interface isolation

1.3 screening: this is where Corinne said she was 'close' and also where RBAC was discussed.

1.4 packet handling

Category 1 roll-up: moderate.

2.1 process access control

2.2 trusted subject

2.3 least privilege

2.4 shared resources

Category 2 roll-up: minimal (which is not so good)

3.1 separation of account duties
3.2 account access control
3.3 permission authentication
Category 3 roll-up: minimal
4.1 hardware architecture security
4.2 physical access control
4.3 software architecture security
4.4 least network functionality
4.5 configuration controls
Category 4 roll-up: moderate

According to the RDAC Roll-Up charts, two moderates and two minimals roll up to a 'High' technical risk rating.

Impressions from the pre-CDTAB meeting: the board asked very technical questions, but did not allow any technical people from the developer into the meeting. The board wanted to rely completely on what the testers knew, but if testers did not know something, the board counted it against the guard.

There are a few members of the board who are extremely vocal and negative, and the other members tend to go along with whatever they say.

The board does not like it when the developer or the government Programme Office decides, after due consideration, not to address a particular issue. The board interprets this as not listening to the board's feedback.

The board does not take into account things that have been fixed during CT&E. If something was broken once, then repaired, the board treats it as forever broken.

The board discounted recommendations from DIA to close certain findings as fixed during CT&E. DIA's opinion did not count.

The board discounted anyting that was done at site during ST&E, because those risk mitigations are not in the baseline delivered to a site prior to ST&E. If it was not in the system at the beginning of CT&E, it was considered not to exist.

No consideration was given to installation in a physically secure environment with cleared users. The only consideration was the guard itself as it was delivered to CT&E.

The board did not take TSOL 8 EOL considerations into account.

References