File 20100716.0806: Weekly activity report 0145:

weekly activity report 145 (loughry)
Joe Loughry
Sent: 16 July 2010 08:06
To: Niki Trigoni; Andrew Martin; Joanna Ashbourn
Cc: otaschner@aol.com; anniecruz13@gmail.com; andrea@hpwtdogmom.org; chip.w.auten@lmco.com; edloughry@aol.com; diane@dldrncs.com; Joe Loughry; mmcauliffesl@comcast.net; tom.a.marso@lmco.com
Attachments:
Weekly activity report no. 20100715.1954 (GMT-7) sequence no. 0145, week 8+4 TT

I made a few changes to the draft ACM CCS workshop paper after suggestions by Dr Martin and technical reviewers at Lockheed (part of the approval-for-public-release process that I have to go through). I added a small amount of new material, clarified the claims in the paper, and made the distinction between current and future work more clear. I will talk about it at Security Reading Group next Wednesday.

I have been reading a couple of old papers on certification and accreditation (Neugent, 1988) that I found in a file box when moving my cubicle to a new location in the building the other day. I took home everything that appeared relevant to my thesis. I have also been reading some articles in the collection by Lewis (2008) on the Black--Scholes options pricing model, in regards to figuring out how to implement the solution described in the ACM CCS workshop paper. Black--Scholes is interesting because it was based on some assumptions that actually worked very well under steady-state conditions, but failed catastrophically at the exact point when they were most needed. It coincided with a point in time when the derivative of one of the assumptions went to infinity. I am studying it because it is a recent example of a market collapse, the opposite of an equilibrium, and relevant to the model I am trying to construct of residual risk in the assessment of accreditors of a cross domain system.

I am helping out with the 2010 Comlab DPhil Student Conference programme committee. The committee met last week to discuss calendar, deadlines, venue, funding, submission format, and publishing of the proceedings. I will help out the programme committee remotely as referee and EasyChair admin. We are investigating whether it is feasible to publish a bound proceedings through lulu.com.

I met with Dr Martin briefly to ask a question about a paper; we have a proper meeting scheduled for Monday. I misread the calendar and mistakenly thought our meeting was today; Dr Martin nonetheless made time for me on short notice. I appreciate that. I had to leave early to drive to the Lockheed facility in Deer Creek to attend the weekly certification telecon. As it happened, today's call was an important one. The certification is coming down to the wire, and tempers are beginning to fray. I observed a number of interesting behaviours amongst the participants.

Part of the reason today's telecon was interesting was because two important participants, one a senior penetration tester from NSA and the other accreditor for STRATCOM, were both present on the call. It is unusual to have either of these people on the telecon, to say nothing of both. Present on the call were Kim Frey, Olav Kjono, Kevin Miller, Joe Loughry, Dan Griffin, Larry Brown, Rob Drake, Don Flint, Dave Oshman, Emely Martinez, Corinne Castanza, Phyllis Lee, Charissa Robinson, and Larry Sampson.

Phyllis began by complimenting the developer for being responsive, but expressed frustration that the pen testers have been unable to finish all the tests they want to run, because they keep running into breakages. Testing stops while the developer fixes a problem, then testing picks up again. The pen testers are frustrated that previously identified findings are being found not to have been fixed, and new findings are found besides. It is slowing down testing.

The developer replied that in the TOE test scenario set up for the test labs to operate in, there are numerous factors that differ from the real world. In actual installations, a running configuration is very specific and tuned to do exactly what is needed. No matter how much the pen test team would like the system they test to reflect the real world, the exigencies of testing enforce an artificial environment. The developer strives to give testers the opportunity to perform significant and meaningful tests on the full scope of functionality of the system, but testing some features in combination is neither meaningful nor realistic.

NSA wants another week for regression testing. They will not accept any more code changes for a week. At the end of that week, the developer will provide a fix, and then NSA will determine what needs to be re-tested. Phyllis believes that the additional week of government regression testing will not adversely affect the schedule.

Emely: The pen testers not been able to look at key functionality because of problems that keep cropping up. Look at the history: CT&E started back in March. Since CT&E began, the test team has never been able to get the entire system up and running. They spent a week trying to install, debugging, changing mags on the fly. Not to fault the developer---it was a very aggressive schedule. But every time the team starts trying to test, something else breaks. LM has always been very responsive. But every time the testers try to test, it's back and forth, back and forth.

The developer protested that there is only a single issue that has been found but not fixed, and that is only because the developers were unable to reproduce it until recently. They keep hearing generalities about a large number of unfixed issues, but there is only one problem that has not been fixed yet.

NSA replied that repeated test stoppages have kept the pen testers from getting through all the tests they wanted to run. This was followed by a long classified discussion of specific tests.

Rob Drake asked: How many weeks of delay of ST&E at STRATCOM, which currently starts in August, are we talking about? Corinne replied: three weeks is the best case scenario.

Rob Drake: I want to talk to the other accreditors. Personally, I am still inclined to go forward on August 2nd and fix things later. My own risk assessment is that the risk is low.

Corinne: If you are willing to accept the risk based on the test results you have been given so far---which is not all the testing that NSA wanted to perform---then...

UCDMO spoke up: The agreement at the beginning was that Rob Drake would make the decision for this iteration. We should hold off the baseline until we get a common agreement.

Rob Drake: If, when we do ST&E at STRATCOM, we find any findings, then we should fix those and put the fixes into the baseline. I am still pressing to stay to the present schedule.

Points at the end that the developer stated they wished to make:

1. One more week is needed for NSA pen testers before a new code drop. After that, NSA will need one week additional for regression testing.

2. NSA pen testers are frustrated that they cannot perform testing non-stop without encountering issues. (This is where the original plan to have an RM engineer on-site during the entire test event would have been very beneficial.)

3. Phyllis used harsh words. It is crucial to recognize, however, that the NSA testers are looking at a completely unrealistic configuration. Their test system is a Swiss Army knife. It has every bell and whistle turned on, things that would not ordinarily be used in combination. Operational installations of RM are never configured that way.

4. Rob Drake is pushing strongly to stick to the original schedule.

5. [elided]

6. [elided]

7. LM will likely send Kori Phillips to NSA next week for support.

8. After many sharp remarks from Phyllis, in the end she seems to be OK with rating certain things as high risk and moving on as long as they are documented. The developer wants to ensure that only those specific items are rated poorly, and not the whole guard.

Other notes from the meeting:

SPAWAR SSC Charleston is working for NSA I173; Ft Meade is I733. The I173 group essentially re-run the developer's Factory Acceptance Test (FAT); they test to NIST SP 800-53 (or prior to this, DCID 6/3) requirements. The penetration testers in Ft Meade couldn't care less about 800-53; they have their own bag of tricks which they keep largely hidden. All the developer ever sees is the resulting wreckage; I733 do not usually reveal details of how or why they test certain things.

About 30 of the 101 findings had to do with not having a virus scanner.

The product is being evaluated to Confidentiality = High, Integrity = High, and Availability = Moderate. That means that most of the problems that will be found will be Denial-of-Service (DoS) attacks. Most any other form of successful attack, if found in testing, would kill a certification immediately. They have not found any such.

Security Reading Group this week discussed two papers: a whitepaper from Fortify Software on cloud computing security, and 'On Technical Security Issues in Cloud Computing' by Jensen, et al. Cornelius, John and I began discussing the Fortify whitepaper until Professor Song arrived. Being remote, I missed out on the fresh strawberries that Mingqiu brought.

I suggested that perhaps Fortify are putting forth their product to cloud customers in an analogy to car safety inspections. Unless customer software meets certain minimum security standards, it should not be allowed on the cloud. It is hard to tell from the white paper; it is light on details. Alternatively, Fortify might choose to offer their product as an additional service to cloud vendors, for the purpose of being used as a sort of driver's licence. Unless customer code is first scanned using Fortify 360 and shown to meet certain minimum security standards---resistance to buffer overflows, SQL injection, use of SSL, not establishing a session with SSL and then using HTTP unencrypted for the rest of the data, for example---then it will not be allowed to play in the cloud. I have used Fortify 360 at Lockheed and with the right analysis packs installed, it could perform this function.

Prof. Song asked about Trusted Computing. John said that TC is very good at encrypted storage, not quite so good yet at remote computation.

Google is known for quietly designing their own hardware for use in data centre installations. They work with system-board and chip set vendors to design rack-mount PCs having very efficient power supplies and high throughput disk I/O interfaces, but leaving out video circuitry as an unnecessary source of heat dissipation. I asked whether anyone knew if these high-density machines contain a TPM. (Little information is available about Google's data centre hardware, aside from a few papers published by Google Research and a photograph of uncertain origin.) John noted that the Chromium OS does measurement on its own, but does not use a TPM, at least not publicly.

Next week's Reading Group will look at my economics paper. I hope they savage it, because I want the feedback. I need to test the thesis for reasonableness; so far only a few people have looked at it, and the idea is a bit out of the mainstream.

I am back on the approved list for travel to the UCDMO conference in Boston, second week of August. The problem is how to pay for the trip. It would be an opportunity to meet with five accreditors: Paul Ozura, Frank Sinkular, Dan Nichols, Dave Wallick, and Rob Drake in a single trip, but I have to pay for the travel myself. I will check with the airlines tomorrow to figure out the cost. I will try to negotiate payment of hotel costs, given that I would pay for my own transportation, with Lockheed and the government programme office.

My current task list (in priority order, most urgent first):

To be done immediately:

1. I have an invitation to the UCDMO conference; need to arrange meetings with Paul Ozura, Frank Sinkular, Dan Nichols, and Dave Wallick that week. Need to figure out how to pay for the trip. 2. Working on Crosstalk article again. 3. Accreditor surveys. I understand the problem so much better now. I need to be able to describe these in the Crosstalk article. 4. Get the other two surveys done. 5. Finish methodology chapter (waiting on final survey questions). 6. Prepare talk for VALID 2010 and submit to PIRA for approval. 7. Compare NIST SP 800-53A to ISO 27002.

To be done as soon as possible (unchanged from last week):

8. Update dissertation Table of Contents. 9. For Chapter 3 or 4, start writing the interpretation of the first case study results and second case study preliminary results. (This will be needed for both confirmation of status and for answering questions in France.) 10. Begin writing progress report. 11. Update the schedule. 12. Apply for confirmation of status.

Joe Loughry

Doctoral student in the Computing Laboratory,
St Cross College, Oxford

End of WAR 0145.

References