File 20100820.0407: Weekly activity report 0150:

weekly activity report 150 (loughry)
Joe Loughry
Sent: 20 August 2010 04:07
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

Weekly activity report no. 20100819.1908 (GMT-7) sequence no. 0150, week 8+9 TT

I am getting ready to leave for Europe for the VALID 2010 conference which starts on Sunday. I have a meeting with Dr Martin scheduled for tomorrow morning right before I go to the airport.

RM 5.0 received its Approval to Operate (ATO) from the accreditor at STRATCOM on Wednesday morning. That represents a successful completion of ST&E under DIACAP, and the first successful DIACAP accreditation of a CDS under the new NIST 800-53 rules instituted across the IC in September--November 2009. Penetration testing, which was still going on as of yesterday, was proceeding well---from the developer's perspective. They reported that the pen test team are frustrated in their attempts to compromise the box. Three new CRs were generated during ST&E. The ATO indicates that this CDS is in production now; certification, which means it appears on the UCDMO baseline list of approved cross domain solutions, will likely slip a few days past the 20th August date in the plan. I induce this from the fact that the organisers chose not to have a classified telecon this week following closely on the heels of the UCDMOC and ST&E at STRATCOM. The developer, as mentioned previously, has reviewed the draft of NSA I173's final report, but had not received the penetration test team's final report yet. With pen testing at STRATCOM due to wrap up yesterday, I expect to see the NSA I733 final report in a week or so. It is unknown whether the developer was successful at getting a revised final report out of I173 that showed successful mitigation of all findings. The evidence package that will go before the DSAWG and CDTAB will comprise that report amongst others. I would really like to attend that meeting of the CDTAB. I will send another request up through the Programme Office asking about it tomorrow.

The developer considers the UCDMO conference to have been very useful. There was one session entirely about the RM 5.0 CT&E, which is being watched closely by all the CDS vendors. The session was well-attended and positive in tone; the presenters did not go into any great detail about problems encountered, just the overall plan and outline of the RM 5.0 CT&E. RM is considered to have six competitors in the CDS arena this year: ISSE, BAE's DataSync Guard, the Raytheon High Speed Guard, HardwareWall, the General Dynamics Tactical Cross Domain Solution (TCDS) and TMAN (I wonder what happened to TCS?). Another report I received from UCDMOC was that small CDS vendors there are jealous of the attention that large CDS vendors got at the conference, and---speculating here---from the UCDMO in general. RM is the oldest CDS and the de facto standard that others are compared to. It is based on comparatively older technology, though.

TMAN recently achieved a place on the UCDMO baseline list which means they have both SABI and TSABI approvals now. SABI, despite the implication in the name of a lower assurance level, has always been a tougher approval to demonstrate than TSABI. SABI certifiers consider their threat environment to include the entire internet, so certification to SABI level has always taken about a year and a half for a CDS, compared a third of that for

TSABI. Under the new combined process for the IC, every approval takes a year and a half. TMAN boasted during the UCDMO conference of having a six-month release cycle for new features, leading the RM developer to conclude that TMAN wants to get off the UCDMO baseline list. By focussing on TSABI to the exclusion of SABI approval, they can easily pick off a few customers on JWICS who never come anywhere near the internet. They have a different threat model, a subset of what RM counters.

Virtualisation of guards was the biggest new topic at the UCDMO conference this year. NSA was pushing it, surprisingly; Boyd Fletcher is currently 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 space, weight and power (SWAP) perspective; more importantly, perhaps, hardware virtualisation stabilises the hardware environment that CDS software needs to run in and be certified on; awfully short hardware manufacturer product cycles have always been a problem for certified systems.

A couple of Phyllis Lee's assistants gave a presentation on all the different attacks they perform on CDS test articles. It was widely considered to be the best presentation of the conference, or at least the most entertaining. NSA I733 are sending out a long white paper as a follow-on to the presentation; I have a request in to obtain a copy of it. In their presentation, they named no names but it was clear that a lot of the vulnerabilities they find during penetration testing---in every system they test---are straight out of the CVE. They described their test methodology as being based on the CVE, which the developer is choosing to interpret as a great indication of how to test internally in future. By giving out this sort of clue to CDS vendors, pen testers are making their own job more difficult, they observed. The impression I received from the developer was that CDS vendors at the UCDMO conference thought of this a wonderful piece of competitive intelligence. But personally I wonder if it was intended as a pointed complaint against all the CDS developers, who---it seems apparent---are not paying attention to the CVE. If that is so, I think NSA's message was only partly understood.

I am really feeling the deadline pressure. I spent a lot of time getting an old laptop ready to take on this trip with a totally clean disk, but after I had gotten the OS distribution installed, got X11 working, got wireless working, and determined that power management wasn't ever going to work, the machine began overheating and finally died. At least it did it here and not in France. I will bring my regular laptop on the trip instead and take my chances with border control.

My UK visa is due for renewal. ATAS emailed me back this week to complain that the description of my research I gave them in the application was not the official one on file with the University. It turns out there isn't any on file yet (ATAS is a new requirement), so I needed to write one. I modelled the following paragraph on examples of good and bad descriptions provided by ATAS. Here is what I came up with:

'Cross Domain Systems (CDS) for handling classified information complicate the security test and evaluation problem because, by definition, they span security boundaries; in the present scheme, this leads to multiplication of cost with no concomitant improvement in security. This research will examine project records from a pair of related CDS certification efforts in the US and UK with the aim of developing a tool based on a generalisable model of inter-accreditor communication in which not all accreditors are cleared to the same or comparable levels. (The model is therefore useful for both intra- and international security accreditations.) Other data will come from interviews with certifiers and

accrediting authorities in the intelligence communities of the US and UK governments; MATLAB will be used to develop an equilibrium model based on microeconomic theory and to perform experiments on the equilibrium in silico. The eventual goal of this research is to reduce the time and cost of certification test and evaluation as applied to CDS systems by eliminating unnecessary re-testing of the same or similar security requirements during accreditation by mutually distrustful data owners whose interests align in minimising the residual risk of the CDS.'

If Dr Martin approves, this will be made official by the University.

I gave a talk Friday to an audience of eighty-nine information assurance engineers across Lockheed on the subject of Gentry's fully homomorphic encryption. Extrapolating from the development of RSA, I predicted for them that FHE will become commercially viable in 2014 after efficient-enough implementations are developed and the security of the algorithm has been vetted by cryptographers. The most immediate application is to cloud computing, where FHE permits users to upload large amounts of sensitive information to the cloud without risk of disclosure either to the cloud provider or third parties. A cloud provider could securely perform computational fluid dynamics, molecular modelling, seismic data analysis, or handling of credit card data and PII on extremely large data sets with less risk of misplacing sensitive information. Instead of cloud computing being relegated to non-sensitive information or being used only for remote storage, it could finally be used for sensitive information. One question that came up in discussion afterwards was integrity of information under FHE. I suggested that remote attestation would dovetail with FHE to guarantee trustworthiness at a lower level, with distributed tool kits like Hadoop serving to complete the availability triad.

I filed the required security paperwork for foreign travel with Lockheed, the U.S. Navy, and NSA. My itinerary for the week is: on 20th August: United Airlines fl. 908 from Denver, Colorado to Chicago, Illinois; United fl. 940 from Chicago to Frankfurt, Germany; then on 21st August: Lufthansa 9202 from Frankfurt to Nice, France. Hotel is the Novotel Nice Aeroport Cap 3000, 40 avenue du Verdun, 06700 Saint Laurent du Var, tel. (+33)4/93195555. On 28th August: Lufthansa 9055 from Nice to Frankfurt; Lufthansa 8811 from Frankfurt to London Heathrow; followed by United 939 from LHR to DEN. I will have email at the conference. They have not told me yet how much time I will have available to talk, so I am preparing short, medium and long talks with some general-purpose slides that I can talk to. This is the first time I have ever presented at a foreign conference; I want to make a good impression. I am quite nervous about it. When I get back, I want to talk about confirmation of status.

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

To be done immediately:

1. Finish preparing presentation and talk for Nice.
2. Weekly activity report (finished)
3. Travel (2 days)
4. Update paper for ACSAC submission during down times.
5. Ping Dan Nichols and Frank Sinkular again. Paul Ozura is tied up in ST&E this week but Dave Wallick should be free now that UCDMOC is over. Try to get dates agreed for late October or early November.
6. Keep going on MATLAB tutorial. Code the numerical model for risk--effort pricing equation. Code acid tests. Find an equilibrium and fill in the blanks remaining in the draft paper.

```
7. Talk to Julie about forms for confirmation of status.  Schedule a
meeting with Dr Martin to look at written work.
8. Crosstalk article: interpret the first case study in terms of
accreditor behaviour incentives.  Write a preliminary overview of
second case study now that it is nearly over.
9. Send out second group of US government accreditor surveys.  Look for
UK government accreditor names in old project records.
10. Get the other two planned surveys done for background on the case
studies.
11. Make a fault-tree diagram for R-prime and S-star.
12. Draw up an org chart for R, R-prime, S-star, R-double-prime, N, L
and G.
13. Update anonymisation code chart.
14. Finish methodology chapter (waiting on final survey questions).
15. Write first draft of confirmation report and send to Dr Martin.

To be done as soon as possible:

16. Update dissertation Table of Contents.
17. Collect examples of written work for confirmation evidence.
18. Compare NIST SP 800-53A to ISO 27001/2.
19. Update the schedule.
20. Submit forms and written work for confirmation of status during
Michaelmas term.

Joe Loughry
Doctoral student in the Computing Laboratory,
St Cross College, Oxford
```

End of WAR 0150.

References