File 20100618.0516: Weekly activity report 0141:

weekly activity report 141 (loughry)
Joe Loughry
Sent: 18 June 2010 05:16
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. 20100617.1517 (GMT-7) sequence no. 0141, week 8 TT

I am working on my paper for the ACM workshop co-located with ACM CCS 2010. Submissions are due 28th June. Lockheed work consumed a large amount of my time this week. I was able to make some progress on my theoretical model despite it, however. I talked with Andy Cooper via email about my thesis, UK government security standards, and confirmation of status. I have requested an invitation from the US government to attend an upcoming meeting of the CDTAB (Cross Domain Technical Architecture Board) and talk with some more CDS accreditors. The Programme Manager will be in town next week; I plan to meet with him to clarify some questions I have about the funding relationship between PMO and developer over the life cycle of the CDS.

I gave two talks on information security this week at Lockheed. The first was on the topic of emanations security and TEMPEST, an overview of discoveries in the last few years including optical, acoustic, RF, thermal, induced, conducted, and exotic emanations. Feedback from the audience of engineers was positive, yielding a number of questions, requests for more information, and requests for a follow-up talk. The second talk I gave this week was about technology for privacy protection. I covered copyright law, historical parallels between book publishers and software makers, and techniques for information hiding that can be used for copyright protection, privacy, or to erode privacy protections. The talk on privacy was well-received by the staff of the Centre for Innovation who maintain the Privacy Protection Framework. The talks were multicast to Lockheed facilities in California and the east coast. I agreed to give one more talk (just one!) later this summer on the mathematics of Gentry's fully homomorphic encryption. A cryptologist who was in the audience for my emanations talk asked me afterwards to do it, and he gave me details of an earlier system (never realised) for homomorphic encryption that I can use to help explain Gentry's scheme over the integers. That talk is scheduled for Friday, 13th August 2010.

Certification testing of Radiant Mercury (RM) version 5.0 is proceeding well. On Thursday I attended a classified telecon with the developer, PMO, IV&V, NSA I173, ODNI, UCDMO, DODIIS, and the Beta 2 site (STRATCOM). Present on the call were Kevin Miller, Ian Mcglothlin, myself, Larry Sampson, at least one person from UCDMO, Orville Brown, Dennis Bowden, Corinne Castanza (representing DNI CAT), Olav Kjono, Lisa Ackerman, Jonathan Scott, Jim Gucken (sp?), Emily Martinez, Dave Aushman (sp?) (representing I173), Phil [last name unknown], Tyler Sipes (NORAD USNORTHCOM HQs), and Dan Griffin (PMO), in addition to several people representing STRATCOM and DODIIS.

The situation last week about some new functionality in the system that caused problems in regression testing has been resolved. There are still a few issues with it, but none are security related and all have workarounds. There were 101 findings during Beta 1 CT&E, 25 of which were fixed with software changes. Of the remaining 76, approximately 20 were fixed with configuration changes, 20 were addressed with documentation

changes, some were assessed as invalid, and a few will not be fixed. There were 22 CRs in 5.0ZC, some of which fixed multiple issues. It is understood by all involved that certain long-standing issues (not named here) will never be changed because the Navy will never come up with the money. Every time a new version of RM undergoes CT&E, these same issues are raised, and the answer is always the same: no money to fix, or they were design decisions made by an earlier sponsor and consequently not the current PMO's fault.

The project manager (from a separate conversation) is satisfied with the progress of RM 5.0 through CT&E. There are more actual customer configurations (ten or twelve this time) in testing than have ever been in previous CT&Es.

The pen test team kicked off Thursday's telecon by commenting on the draft POA&M. The scope of the mitigation effort will be reduced by removing findings related to certain test files that were left on the lab machines by accident. The TOE never mentions these file types, and functionality for processing them is not officially supported yet. To bring the conformance claims back into alignment with the functionality that was fully tested and found to be correct, the developer asked that findings related to these unsupported file types be removed. I173 concurred. DNI CAT also concurred, but requested that the limitations be documented. The developer agreed. File types that are supported in this release---and claimed in the conformance specification---are fully parsed; types that are not supported will be absolutely stopped and will never traverse the guard. The developer intends to bring these additional file formats before the committee at a later date. It is just that they were not ready at the time when testing needed to begin, so functionality and conformance were never claimed for those formats.

Emily Martinez spoke up and said that [a requirement] will be relaxed in [some place] if there are no [some particular file types] in the system. (Details elided.)

Dennis Bowden (representing PMO) then stated that this (5.0ZC still?) is the version of the software that is intended to be installed at STRATCOM, and asked for concurrence from NSA that there were no show-stoppers. Dave and Emily (collectively representing I173) agreed, with Dave further commenting that it is not a particularly high risk. Dennis Bowden said, 'obviously, if you find something in the next four weeks, then all bets are off.' [Editorial note: in general, all of the participants on the call today were mellow and agreed that all findings of risk are being mitigated satisfactorily. Phyllis was not on the call today, however, and has not been the last few times. Emily seems to be trusted more and more by Phyllis as her deputy. I was impressed that Mr Bowden got I173 to agree verbally that the mitigations are sufficient and no show-stoppers are expected. Further, DNI CAT did not contradict that statement. Amazing.]

Next, there was some discussion of anti-virus capability. Orville Brown stated that PMO made a conscious decision years ago that once an RM system is locked down, no data should go in or out of the TOE afterwards, with the exception of archived audit. That has been RM security policy from the beginning, but maybe it is time to revisit. Deferred for possible 5.1 new capability; the PMO will study it. This was followed by a discussion of other new features that may be in the next version.

Following that was a discussion of certain findings and the developer's technical mitigation of them [details elided]. Some classified meetings will take place next week on-site at STRATCOM between the

developer's installers and NSA and DNI CAT. Any remaining questions of the certifiers regarding implementation details of the developer's proposed risk mitigations will be addressed by means of a combination of live demonstration, inspection of the implementation, and consultation between the authors (who will be on site) and the certifiers with equipment at hand. PMO expressed hope that that environment would be the best route to complete understanding.

An overview of the schedule followed next. Some of the dates have been updated. Beginning 28th June, there will be some integration work done at STRATCOM. This will be followed by equipment installation beginning 19th July. Two weeks of government regression testing will be followed by one week of DNI CAT pen testing. Western region will be sending someone. The new equipment will go alongside the existing RM in the space, not replacing it right away. The two systems will run in parallel for a while. No mention of a change to the end date was made.

Regression testing at the Lockheed plant in Colorado is now complete. Results appear in the POA&M. All regression testing was witnessed by IV&V. Yesterday, the developer had a telecon with STRATCOM for the purpose of orientation and coordinating classified visitor requests. Next week, with all the activity going on around the install, there will be no hotwash; next telecon will occur in two weeks. Meeting ended at 0833 hours.

Security Reading group this week met over the topic of infosec certifications. Mingqiu introduced the paper 'The Ten Best Practices for Secure Software Development' by Mano Paul (Vienna, Virginia: International Information Systems Security Certification Consortium (ISC)^2, undated). Cornelius provided the Skype connection so that I could call in. Mingqiu sent me a few emails afterwards asking for more information about how the US government is requiring infosec certifications for its contractors and how it has worked out. I offered to give her any information she needs. Here is what I said afterwards:

From the perspective of US defence contractors, certifications are a big deal.

US Department of Defence directive 8570.1 (2005, revised 2010) requires all personnel having privileged access to DOD systems or any software development responsibilities to be certified in information security by the end of calendar year 2010. More than 100,000 people are affected. So far, the compliance rate extends from 25 to 40 percent amongst defence contractors and parts of DOD, with a few military units at 100 percent. The deadline has already been extended a few times but current information is that no extensions will be given after December 2010.

The only acceptable certifications are A+, Network+, SSCP, CAP, GISF, GSLC, or Security+ for entry-level personnel; GSEC, SCNP, CISM, or CISSP for people with up to five years experience; and CISA, CISM, or CISSP for senior developers. Certain operations personnel will be allowed to substitute the Certified Ethical Hacker (CEH), although it would be an understatement to say that CEH is controversial. The CISSP requires a university degree, although experience can be substituted for a bachelor's degree in some cases.

After 8570.1 goes into effect, the only people allowed to perform security engineering or architecture functions will be those holding one of the advanced certifications beyond CISSP: the ISSEP, ISSAP, or ISSMP. The number of these presently in existence is small. To sit the advanced exams, a person must already have held a CISSP designation for at least

two years.

These certifications have three uses. For individuals, they can get a person hired. For department managers, they are countable tokens useful for demonstrating to upper management that due diligence in hiring and training with respect to security has been done. Finally, for US defence contractors, they are required to satisfy 8570.1 and a necessity for bid and proposal work.

Ivan said that it was surprising to him that 8570.1 pays no attention to university degrees. I confirmed that it does not.

Other activities this week: I met with Larry Brown of Lockheed and Jason Spies of Layer7 Technologies for a demo of their cross domain system product called XML Data Screen. Layer7 say they can filter 30,000 messages per second in the 200 K byte/message range. The user interface they demonstrated for building rules and controlling instances was very impressive. At the present time, all of their installations are with banks; however, the capability they showed would be attractive in the CDS arena, if Layer7 were to go to the trouble of obtaining the necessary approvals.

Next meeting with Dr Martin: I need to schedule a meeting as soon as possible after Dr Martin gets back from travel.

My current list of tasks in priority order, most urgent priority first:

To be done immediately:

1. ACM workshop paper draft due 28th June. 2. Meet with PMO Programme Manager next week to discuss Navy PMO funding of the developer. 3. Waiting for visit request to get into CDTAB. 4. Accreditor survey more new questions. List of email addresses for known accreditors. 5. Transfer list of accreditor meeting attendees and email addresses into a searchable text file. 6. Finalise list of email addresses for the other two surveys. 7. Finish methodology chapter (waiting on final survey questions). 8. Crosstalk journal paper.

To be done as soon as possible:

9. Waiting on UK student visa application. 10. Update dissertation Table of Contents. 11. 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.) 12. Document the codes used in a new appendix for de-anonymisation information for all participants. 13. Begin writing progress report for confirmation of status. 14. Update the schedule. 15. Apply for confirmation of status.

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

End of WAR 0141.

References