File 20100709.0823: Weekly activity report 0144:

```
weekly activity report 144 (loughry)
Joe Loughry
Sent: 09 July 2010 08:23
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. 20100708.2243 (GMT-7) sequence no. 0144, week 8+3 TT

I finished the paper for the ACM CCS workshop in time for the deadline
tomorrow.  After much work I was able finally to prove the contribution I
wanted to claim in this paper: that the market for residual risk amongst
accreditors having different security clearances meets the criteria for
'signalling' that were first established by Spence in 1973, and for which
Spence, Akerlof, and Stiglitz received the Nobel prize in economics.
For signalling to work as a means for resolving the asymmetry and thereby
preventing the collapse of a market, the signal must be costly.  I still
haven't determined what the signal is exactly, nor have I got a simulation
going yet of the market for residual risk, but I was able to show that
the signal (in the specific case where at least two accreditors have
different, possibly non-hierarchical security clearances) is costly,
and that it works in both directions: high-to-low and low-to-high.
As a corollary, I was able to show that dishonesty has a strong negative
incentive, again in both directions, because a dishonest signal will
unavoidably come back to hurt the sender.  Either it will elevate the
apparent level of residual risk above the true level, or it will depress
the apparent value below the level that the accreditor knows is true,
thereby increasing the personal risk to the accreditor since he or
she is signing on the dotted line to formally accept responsibility.
The preceding argument is no guarantee that the rest of my scheme to solve
the local minima problem by means of an artificial market will work,
but it is a good sign, and a real contribution, and I hope the paper
will be accepted.  It is right at the page limit for this conference;
if the conference does not accept, I will extend it with more material
in an appendix and re-submit to another conference right away.

I am looking forward to the ACM workshop helping to develop the concept
further.  I have run the idea past a few US government accreditors,
and they all think it's an interesting idea, but they want to minimise
the amount of extra work they have to do.  They all agree that if my tool
can force the other guy to do all their work, it will be a great success.
I have not had a chance yet to show the most recent result to Mr Ozura;
on Monday I will be able to get his opinion.  For now, I am just happy
that the proof worked; I have been stressing over this problem for weeks
trying to solve it, reading economics journals and having to learn yet
another new language.

It is late, and I want to get this report out.

The RM 5.0 certification status telecon met Thursday after a hiatus
of two weeks.  In attendance were Kevin Miller, Larry Brown, myself,
Larry Sampson (moderating), Jonathan Scott from the western region,
UCDMO, Emily, Dan Griffin (representing the PMO), Corinne (DNI CAT),
and Paul Ozura (IV&V).

Mr Sampson sent out an agenda before the telecon along with a template
for the RM 5.0 fact sheet to be distributed by the UCDMO baseline.
Emily started off by reporting that they are still doing regression
```

testing, nowhere near done. Results so far: they have found previous findings not fixed, and some new ones. The new problem is reproducible by two different means. Testing is not finished yet.

Corinne remarked that one of the problems, as it stands now, is a DoS. Kevin Miller, for the developer, replied with a detailed technical explanation justifying why the problem that was found is limited to the testing lab configuration and would not result in a DoS under normal field conditions. The explanation was accepted and agreed with by Emily and Corinne.

Plan of Actions and Milestones (POA&M): the developer plans to fix the underlying technical problem with a post-5.0 patch. At this point, Mr Griffin asked for a review of all open CRs. There are three. The developer understands why the first two CR failures occur (they are in fact the same problem, the one that is to be addressed by a software patch after certification); for the third CR, there is a workaround that requires no code changes. That covers all the open CRs so far found by regression testing in this round.

Mr Griffin stated that the PMO's recommendation, based on funding levels and schedule, is to come out with a POA&M and not to burden Corinne with another round of regression testing. PMO recommends issuing a patch for these three CRs post-certification.

Corinne asked how I173 testing is going in Charleston. I173 reported that they have not received a status report from SPAWAR, but Dennis Bowden called yesterday to relate that Rob Drake is in agreement that none of these items are show-stoppers, that they can be handled in a POA&M.

Emily: the pen testers feel that they are finding old things that have not been fixed, and new things besides. She wants to talk it over with Phyllis, who is more experienced and will be back in the office tomorrow. Recommends not making a decision yet.

I173 concurs with waiting (USN SPAWAR SSC Charleston).

Western region STRATCOM concurs with waiting.

Corinne: on the DoS issue, the availability parameter of this certification is moderate, so there should be no problem with handling it via POA&M. NSA I733 recommends waiting, and to get Rob Drake to chime in as well.

The consensus was to wait for people to get back from holiday, then revisit the question next Thursday. On 16th July, the next report from the pen testers is expected. Emily asked, 'how are we going to validate the fixes between now and STRATCOM?' She wants to consult with Phyllis about it. This is a new situation, said Emily, one that has never happened before, to have a guard with unfixed findings.

Dan Griffin (PMO) again emphasised the importance of keeping to schedule, for reasons of funding and funds allocation. Emily said that rather than waiting for the 16th, she will send out a quick report to the group immediately. I173 will do the same.

Returning to the agenda, Larry Sampson said that the schedule is going to have to be looked at, but Dennis Bowden is not on the line today. It is noted that Dan Griffin wants to stick to the schedule for funding reasons. Next topic: prioritising the findings in the POA&M. Of the 101 findings resulting from Beta 1 testing, some will be fixed, some will be

put off. This is understood. Corinne wants an updated priority list. Kevin Miller responded that everything that needs to be fixed before the end of regression testing is in the spreadsheet. Some findings are addressed by documentation changes, some are impossible to fix.

Corinne: I173 still have some issues with the developer's response to the list of findings.

Kevin Miller: a few weeks ago when developer representatives were on site during set-up of the labs for regression testing, the developer sat down with all the testers and went through every finding together, in front of the actual machine, to come to a common understanding.

Corinne: still, some of the developer's responses to findings as written in the POA&M are not acceptable.

Dan Griffin then asked the developer to update the POA&M with additional notes on the discussions that took place in Charleston and Ft Meade, to clarify.

Larry Sampson polled for feedback on the ST&E procedures for STRATCOM Beta 2. Corinne noted that Rob Drake really needs to chime in on the ST&E plan. Paul Ozura then said the ST&E plan for Beta 2 will be finished tomorrow, with a copy sent to Rob Drake. It is derived from SP 800-53 security controls. The tick list is a complete description of what will be tested in ST&E Beta 2 at STRATCOM; the tick list is an appendix to the ST&E plan.

The last thing discussed was the template for a one-page fact sheet to be distributed by the UCDMO baseline. The PMO will have the template properly filled out by the time ST&E finishes. They want it accurately to reflect those capabilities that are actually in the baseline. The fact sheet is submitted along with the final certification package.

Next telecon scheduled for Thursday, 15th July at 0800 MDT. The focus will be on findings from regression testing and the POA&M. Call ended 0849 MDT.

Security Reading Group this week enjoyed some assembly language. John Lyle started off the discussion of this very interesting paper: 'The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86)' (Shacham, 2007) and a follow-on paper, 'When Good Instructions Go Bad: Generalizing Return-Oriented Programming to RISC' (Buchanan, et al., 2008). [The title of the first paper comes from a Bob Dylan song about Galileo.]

A number of ideas for defending against or preventing this attack were floated by the members of Reading Group, among them libc randomisation (Shamal), minimisation of libc, elimination of shared libraries combined with minimisation (John), fixed-size stacks, stackless programming, a new processor instruction that would allow a programme to declare how much stack it would use (or the same idea at the function level) with backwards compatibility, 'introspective attestation', and generalised methods for preventing buffer overflows (the common attack vector) or stack smashing (the root cause). Non-executable stacks will not help; the only things required to be on the stack are pointers and data.

I wondered how robust this technique is, given that it depends on side effects of instruction sequences and unspecified behaviour to leave certain registers in certain states. I speculated that a context switch at just the wrong time might break it. To defend against this,

keep your exploit code small, to minimise the time probability of a context switch happening whilst exploit code is executing. With luck, and a deeper search (not just 0xc3 'ret' op codes can be used!) it might be feasible to make the attack completely robust. It is a nice result.

I recalled that some high-assurance processor designs eliminate in-memory stacks entirely as being too much of a security vulnerability. Perhaps in future, stacks that can be allowed to grow to arbitrary size in memory will be looked upon as poor engineering practice. Other CPU architecture changes that might be considered include separate stacks, elimination of register window protocols (such as made the SPARC architecture vulnerable in the follow-on paper from 2008), and a reference monitor devoted to stack discipline.

I wonder if the IBM mainframe architecture is as vulnerable. I would like to see the authors try to implement the attack there. The stack discipline on 390 architecture processors is tighter than it is on either x86 or SPARC.

Android, said John, is based on the ARM processor.

I wondered aloud whether any biological viruses have been observed to use analogous techniques against existing sequences of codons in the DNA of a host organism. There are things simpler than a virus, called prions, that seem to work this way. Prions carry so little RNA information themselves that they have to patch into existing DNA code on the host. What other of the techniques for both attack and defence that we invented here in the last hour will biological systems eventually be discovered to have been using all along, or might evolve themselves in future, or be tailored to use in future with a little human help?

I observed that the snippets of x86 code exhibited in the example gadgets are very old-style and backwards compatible at least to the 80386 architecture, indicating that the exploitable parts of libc are old code. Updating the compiler back-end that generated the libc code observed here to use more modern instruction sequences might possible result in a libc that was less easily exploited. Assembly language programming on the x86 architecture got weird after post-Pentium CPUs introduced aggressive superscalar pipelining and speculative execution---needed to get efficiency gains on the more complex processors. From the look of the instruction sequences, this libc was compiled without those extensions. The static analysis done on libc might not work so well on one of my FreeBSD systems at home, because I always recompile the system with compiler flags set to one single architecture (currently 686).

In response to libc randomisation (Dr Martin observed that Microsoft probably do not want customers recompiling Windows every time), I speculated that a response to that defence might be to do the static analysis on the fly in your attack code. There is no reason why the static analysis has to be done off-line. John observed that gadgets are sufficiently general to be able to implement static analysis, and the author showed that his static analysis only took one second or so, but I speculated that on-the-fly static analysis would be more efficiently done by a Trojan horse programme separate from the attack code, which after all might suffer from the fragility problem mentioned earlier, and so needs be kept small.

Dr Martin asked about other papers on similar topics. John related that return-oriented programming attacks are currently in vogue and all the latest presentations of new attacks seem to be using them. This was followed by discussion of giving the Security Reading Group a name so

that we can explicitly acknowledge it in our own papers. Reading Group will continue with a new paper next week and through the summer.

Dr Martin offered afterwards to talk any time I need it. I pleaded a need to finish my paper for the CCS workshop, but promised to give a complete update in my weekly status report (here).

The last thing I want to report are a few more notes from my observations of the CDS developer this week: one of the software developers told me that NSA testers have a whole pocketful of special tricks aimed at testing guards. NSA will not give developers their test procedures, because NSA do not want the developers writing products around it.

It is up in the air what the most recent findings will mean. Certification is critical to this developer; they need 5.0 to be certified; many customers are waiting, many proposals.

The developer feels that the certifiers have been changing the rules in the middle of the game. In the past, doing SABI and TSABI separately, they would have been long done with TSABI by now. Under the new unified process through the UCDMO, there is no SABI and TSABI any more. TSABI was always much less strict than SABI. SABI always took longer. But under the unified process, NSA is in charge, and NSA are extremely strict. Everything is being held up by NSA.

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

To be done immediately:

1. ACM workshop paper is due tomorrow. Paper is finished and only needs to be uploaded. 2. Still waiting on invitation to get into CDTAB; may be combined with DSAWG and UCDMO trip (early August). 3. List of questions for the accreditor survey. Having gone through the economics model, I now understand the accreditor's world-view better. 4. Get the other two surveys done. 5. Finish methodology chapter (waiting on final survey questions). 6. Crosstalk journal paper. 7. Prepare talk for VALID 2010 and submit to PIRA for approval. 8. Compare NIST SP 800-53A to ISO 27002.

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

9. Update dissertation Table of Contents. 10. 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 likely audience questions in France.) 11. Begin writing progress report. 12. Update the schedule. 13. Apply for confirmation of status.

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

End of WAR 0144.

References