File 20101126.0847: Weekly activity report 0164:

weekly activity report 164 (loughry)
Joe Loughry
Sent: 26 November 2010 08:47
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. 20101125.2320 (GMT-7) sequence no. 0164, week 7 MT

I decided to buy the Simscape licence from MathWorks out of own funds.
The student licence for MATLAB through OUCS includes Simulink, but
Simscape can only be activated on an individual or department licence,
and the student licence is a different type. After talking with the
sales support department at MathWorks, it appears to be the only way to
do it. The user guide for Simscape consists of video tutorials showing
how to model a variety of machines and systems; I am going through the
set looking for likely bits that I can re-purpose. It is new enough that
no books on the topic have been published yet.

The RM developer is continuing to work on the 5.01 patch during the wait
for CDTAB and DSAWG to finish deliberating on three remaining TORAs that
lie on the critical path to the first SABI accreditation and an extended
UCDMO baseline configuration. I met with the developer to talk about
version 6.0, particularly the OS migration plans. The roadmap has 6.0 on
a COTS distribution like RH Linux (away from Oracle), but the developer
wanted to talk to me yesterday about hosting it on a specialised kernel
called ESXi. ESXi is a highly stripped down Linux kernel (the disk
image size was reduced from 2 gigabytes to 100 megabytes) for hosting
virtual machines atop a very small attack surface. It underlies the
latest version of the VMware hypervisor. The RM developer is considering
adapting the idea rather than either using a straight (with SE Linux)
COTS distribution or a bespoke kernel. The developer wants an OS that is
supported, which is why they did not like my first suggestion to define
a distribution of their own with a customised kernel the way I do all
the time with FreeBSD installations. As an alternative I offered the
suggestion that they attempt to licence ESXi itself rather than searching
for a standard distribution, e.g., DSL, that is almost but not quite what
they want. The developer asked me to investigate whether ESXi can be
licensed for use. At the least, I suggested, VMware would have to publish
their changes to the kernel in accordance with the GPL. In combination
with a userland like BusyBox, the attack surface should be minimal.

VMware are closely working with NSA on ESXi. NSA are enamoured of the
small attack surface of the minimised kernel, and seem to be sharing
some very interesting technical information with VMware, judging from
the evolution of the content of white papers on VMware's web site in
recent months: some formerly obscure topics are well represented there.
Boyd Fletcher confirmed that NSA IAD are extremely excited about the new
development, more so than their previous champion, NetTop. I agreed
to research the ESXi kernel and find out whether (1) it contains the
necessary functionality to host version 6 successfully, and (2) if it
can be obtained from VMware for cross-use.

On a more closely related side-track to my research topic, I thought
of a possible new solution to an upcoming problem that has not hit
the developer yet but is expected to soon. DoD Instruction 8570,
published 2005 (revised 2010) imposes a deadline for compliance with
certain training requirements and evidence requirements for government,

military and contractor personnel having privileged access to systems or networks handling sensitive information. The deadline is coming up but compliance rates are still low. The government has issued guidance to its departments that commands are not to pay the cost of contractor compliance with 8570.01-M, or with required maintenance fees. The contracting companies, however, have not also stepped up to pay for the training of their own personnel. The expected result is a situation shortly after 1st January, i.e., six weeks from now, when some government auditor is going to figure it out and issue a stop-work order pending compliance.

The problem lies in the cost of incentives. Paying for the training directly is one option, but the estimated cost of the needed mix of training for a single department is over $125 thousand (non-recurring), plus another $10 000 annual recurring expense (not counting training) and the necessary money was never budgeted. This week I thought of a new way to fund it: indirect capitalisation of the expense through use of contingent stock options. It has the advantage of shifting a large expense to the equity side of the balance sheet, at the same time being highly controllable by manipulation of the strike price of the options. Essentially, it can be adjusted to have any desired net present value and at the same time having zero effect on earnings. I proposed the idea to the IA community of practice and asked the corporate counsel whether it seemed allowable. I have a nagging fear that the quid pro quo might be illegal under some obscure tax or securities trading regulation, but it seems like a logical use of resources. I described the scheme to a number of software developers and asked whether they would accept the proposed incentive; they all said yes. It's a solution to the 8570 compliance problem, if I could just get upper management at Lockheed to listen. They seem to be ignoring the requirement, hoping it will go away or be waived. It will be interesting to see what happens if they don't solve the problem.

GSS report has been submitted. It was a short week due to a national holiday in the U.S., so I took a Secure Software Engineering Awareness course at Lockheed, which was pretty good. It covered cross-site scripting and SQL injection, but also---surprisingly---it covered return-to-libc attacks. There was a short but good article on risk assessment in The Register this week; it talked about civil engineering around Heathrow's Terminal 5 but the parallels to software engineering were clear. Security Reading Group did not meet this week because several people were away and a talk by Google on 'Warehouse Scale Computing' was scheduled at the same time. Discussion of the paper by Collberg and Kobourov (2005) is postponed until next week when I will introduce it on Wednesday.

My current task list (in priority order, most urgent first; work on tasks in this order):

1. Go through more tutorial videos for Simscape.

2. I am preparing an introductory talk for the assessors in three weeks. Travel arrangements have been made. The time of the viva is either 9am or 3pm, not yet set. The date is fixed.

3. Rework the Crosstalk article according to latest thoughts. In the outline, I have that R-prime was evaluated under CC v3.0, but I recalled recently that there was an earlier version of the system (call it R_0) for the E project that was supposed to be 'evaluatable' under CCv2.3. R-double-prime was certified under DIACAP as the first test case to replace DCID 6/3, but it looks now like DoD and IC will be put together under the tent by UCDMO soon, as soon as they obtain full control

of DSAWG.

4. Thinking about what the definition of ‘succeed’ and ‘fail’ are in the context of CC evaluation; ‘did not complete validation’, ‘abandoned before the end of validation’, ‘failed to receive certification’, ‘abandoned before the end of evaluation’ and ‘not submitted for evaluation’ are all different and significant events.

5. Use Simscape to modify the MATLAB simulation to do 4 systems in parallel with the same set of fixed points. Implement Prof. Polak’s equilibrium acid test and the double alarm clock option model (should be easy to do in Simscape).

6. Background reading: Pennock and Wellman (2004) on uncertainty markets, Levitt and Dubner (2009) on asymmetric information, Bernstein (1996) on risk assessment (on hold), Karp (2009) on research methods.

7. Ping the following people: Paul Ozura [BAH], Dennis Bowden [San Diego], [Patti Spicer, Charles Nightingale, Hal Forsberg] at CSC.

8. Small tasks (I can do these this week; nobody is home at Lockheed due to the holiday): update first case study chart with changes from last conference; draw fault-tree diagrams for R-prime, R-double-prime and S-star; draw up organisation charts for R, R-prime, S-star, R-double-prime, N, L and G; update documentation of the current set of anonymisation codes.

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

End of WAR 0164.

References