File 20100528.0307: Weekly activity report 0138:

weekly activity report 138 (loughry)
Joe Loughry
Sent: 28 May 2010 03:07
To: Niki Trigoni; Andrew Martin; Joanna Ashbourn
Cc: otaschner@aol.com; anniecruz13@gmail.com; andrea@hpwtdogmom.org;
chip.w.auten@lmco.com; diane@dldrncs.com; Joe Loughry; mmcauliffesl@comcast.net;
tom.a.marso@lmco.com
Attachments:
Weekly activity report no. 20100527.1649 (GMT-7) sequence no. 0138, week 5 TT

I am working on an idea related to asymmetry of information that was previously identified in accreditor--CDS--accreditor communications during the ST&E phase of an accreditation. The problem in any given ST&E is that there will always be a set of at least two accreditors each representing different data owners, and the accreditors necessarily have different views on the total risk of the system and their residual risk (necessarily different for each accreditor because each accreditor 'owns' information of a different sensitivity level). Each accreditor has (1) a set of risks it is desirable to mitigate, (2) a set of risks it is possible to mitigate, and (3) a set of risks it is acceptable not to mitigate---a.k.a. the residual risk. Some accreditors may be aware of threats that other accreditors are not cleared to know of, and they may be aware of a partially non-overlapping set of risk mitigations that other accreditors are not cleared to know about. This is a an artificial situation, probably more complicated than would normally happen in real life, but it is general enough to cover all situations. It forms my theoretical model.

The majority of interactions in the model are bi-directional between an accreditor and the CDS installer. One of the important questions I need to answer is about inter-accreditor communication. I can use the survey methodology to determine this, something I realised today after my meeting with Dr Martin. More about that below. The insight I had this week is that the accreditor information problem might be solvable as an economics problem. We have asymmetry of knowledge and we want to optimise: to find a solution that satisfies all parties that the residual risk is low enough to meet their acceptability thresholds---which may be different---without requiring everyone to lay their cards on the table. Because of security clearance and classification walls, accreditors cannot share information freely.

A friend of mine last year told me about a system he wanted to invest in called a Prediction Market. The idea behind it is that participants buy and sell futures tied to predictions about certain events; when the price of a prediction is seen to rise (so the theory says) the prediction can be considered as having a higher probability of being accurate. The events he was interested in are trends in the price of magnetic data storage affecting manufacturers like Seagate and IBM.

When I thought about this, it occurred that a market simulation might be applicable also in the case of the accreditors. Markets are also a case of asymmetric knowledge (time and space are also exploited in the practice of arbitrage). It is a weird kind of market, because it involves buying and selling commodities that you don't know the value of. Someone else knows the value---you know only the price you are willing to bid, the price you are willing to ask, and the prices of others' transactions as they occur. In a sense, the commodities in the accreditor market are sealed boxes. The contents of each box is either a risk or a risk mitigation---positive or negative values---affecting the residual risk

'position' of a participant in the market. Risks can add or subtract; mitigations always subtract from residual risk, but the existence of a partial mitigation that implies the existence of an incompletely handled threat might not be desirable to disclose because it increases the level of residual risk. Prices correspond to quantifiable levels of risk in a CDS. Obviously, one of the primary problems is how to quantify risk. The next problem is how to compare risks amongst accreditors representing different data owners, at different security classification levels. Collateral classifications, at least, are already quantified and ranked. SCI is quantifiable but not rank-ordered, because compartments are not always hierarchical and may be incomparable. I believe I can re-use a solution published in DDS-2600-6216-93, 'Compartmented Mode Workstation Labelling: Encodings Format' (Defence Intelligence Agency, September 1993), which uses bit vectors to solve the problems of classifications, compartments, caveats and releasabilities.

Markets are effective for optimising in the presence of incomplete knowledge. They do have problems, notably instability in the presence of uncertainty, positive feedback effects, known behaviour around monopolies, and sometimes unfairness. Other optimisation techniques exist. The accreditor information problem might be solved as a constraint satisfaction problem, or by linear programming. To determine whether a market is a solution, I need to build a model and test it.

I don't know if this will work. I asked my friend for some primary references where I can go learn about it. I think there might be something in Nash equilibrium theory about it. I discussed the idea with Dr Martin in our meeting on Thursday morning. Dr Martin is not sure he believes yet that it will work. When I described the process of allowing accreditors to exchange information whilst keeping their secrets, he said 'You're trying to build a covert channel machine.' That is an interesting way of looking at it, and I might be able to use some of the established techniques of covert channel analysis to characterise the bandwidth of the channels, what information is allowed or disallowed to cross them, and to limit the bandwidth of channels to a defined amount. There exists an ad hoc process today, of course, by which accreditors balance their residual risk tolerance 'around' the CDS; what I would like to do is optimise the process in terms of time, effort, and lowering the threshold of the generally agreed-upon level of residual risk amongst all accreditors of a CDS, through the CDS (or to be more precise, through the CDS installer). The artificial market approach seems like a good fit with the existing method used today, which is serial in nature.

Which brings up an interesting point: the way things work today has never been well established. Several government standards exist that prescribe certain steps that must be followed, but the nature of a CDS necessarily spans boundaries, as a result multiple standards almost always obtain, partly overlapping in their scope of authority but with substantial areas of sole authority on the edges. How do accreditors resolve this now? Do they work serially, or concurrently? I can determine the answer by means of one of the surveys I had already planned. The topic of inter-accreditor communication was not one that I had initially thought would be important, but now I can see that it is. I will immediately begin writing a survey to determine how and how much accreditors talk to other accreditors on the same or different CDS ST&Es. The aim will be to find out what connections exist, how much and what kind of information are exchanged, and whether participants prefer the present arrangement or would be amenable to a new solution. How the market optimisation algorithm would work, if it turns out to be the way to go, is unknown. It could be interactive, or it could work more like a simulated-annealing operation, starting from fixed initial values and

searching for a satisfactory solution. The way to go can be determined from the responses from working accreditors, so I will ask some general questions from which I can gauge the probable acceptance of alternative solutions by practitioners before developing a prototype.

The present delay in getting those surveys out and done, therefore, has had fortunate consequences. I need to get those surveys out, because I need the data to analyse into preliminary results to show to the assessors for confirmation of status. I promise I will get the surveys out this week.

Dr Martin reminded me that I want to define the contribution that I intend to argue at Confirmation of Status, so I can circumscribe it clearly for the assessors. It is definitely focussing, continuing to narrow down on a solid topic, but Dr Martin warned me not to concentrate too much on confirmation yet because that could distract me from focussing on the work. I talked a bit about the question of whether to split my research into two pieces: CT&E and ST&E, since all the work I have been doing lately bears on ST&E. On reflection, I think I will not drop half of it. First of all, the CT&E study was a lot of work, and secondly, the ST&E theory is best understood in light of lessons learnt from the two case studies of CT&E. Looking back at my transfer report, the thesis is not all that different from what was described then, just more definite and less full of maybe and what-if. There is less emphasis on Common Criteria and more on DIACAP, but that reflects policy changes and contributes a useful sanity check that the final result will be relevant.

I reported that VALID 2010 paper camera-ready copy was submitted on time. I spent the last week working on the ACM workshop paper, but to proceed on that I need the survey design (not results, just questions)---which also forms part of the methodology chapter I need to finish writing. Crosstalk article is waiting for time to spend on it.

This week I talked about the paper 'Experimental Security Analysis of a Modern Automobile' by Koscher, et al. (Oakland, California: IEEE Symposium on Security and Privacy, 16--19 May 2010) at Security Reading Group. The interesting points about this paper from my perspective were: (1) here is a cross-domain system that was successfully attacked because of weaknesses in the assumptions underlying its security model; (2) automobiles are cross-domain systems---and by implication so are aircraft, trains, buildings, power and water systems, and other entities. Thinking of them as cross-domain systems may suggest applicability of security analysis techniques not previously applied.

Other status: RM 5.0 CT&E testing is proceeding normally. The schedule has not changed. Beta 2 installation is expected to occur as planned; the developer and programme office are finalising their formal response to the list of Beta 1 findings from SSC Charleston and I733. Plan of Actions and Milestones (POA&M), a required document in the NIST SP 800-53 process, is is being drafted now.

I got a CAS number under the Tier 4 scheme so I can renew my student visa. All department actions are now complete. I will submit my paperwork next week.

I read in an article on dissertation writing that if I want to include anonymised data I had better have an appendix listing all the codes used so that anonymised names can be traced back to the original source. This is apparently standard practice and there are policies and procedures for protection of personal data in the publishing process. Scientific ethics requires that the provenance of the original data be traceable,

and it is usually done by means of a separable appendix.

Current list of tasks in priority order, most urgent priority first:

Immediately:

1. Accreditor survey new questions. List of email addresses for known accreditors. 2. UK student visa. 3. Write up an explanation of the accreditor optimisation strategy. 4. Go through slide packages from RMUG for names, dates, addresses. 5. Register a new abstract for the ACM workshop in October. 6. Finish list of email addresses for other two surveys; develop questions, enter in SurveyMonkey and test. This is very very late. 7. Finish methodology chapter (waiting on survey design). 8. Outline the Crosstalk journal paper.

As soon as possible:

9. Update dissertation Table of Contents. 10. For Chapter 3 or 4, start writing the interpretation of first case study results and second case study preliminary results. (This will be needed for confirmation of status.) 11. Document codes in a new appendix de-anonymisation information for all participants. 12. Begin writing progress report for confirmation of status. 13. Update the schedule. 14. Apply for confirmation of status---I want to submit the forms with written work by end of June for August or September.

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

End of WAR 0138.

References