File 20100721.0700: Notes from Security Reading Group this morning:

I presented my paper, 'Information Asymmetry in Cross Domain System Accreditation' to Security Reading Group this week. Cornelius, John, Mingqiu and Shamal were present. I began by explaining the rationale for attempting to apply what appears to be a completely unrelated field to the problem of determining risk from security vulnerabilities to a computer system. I know I am taking a risk with this paper, putting forth a not-completely-developed idea at such an early stage of working out the implications, but I must have feedback from other researchers specifically so that I can validate certain assumptions. Reading Group was a useful sanity check.

What I saw was that the paper does not contain enough background for non-economists unfamiliar with the work of Ackerlof, et al. to read it. I was constrained by the four-page limit imposed by the ACM workshop—good for conciseness but bad for a paper such as this that depends on a background that the audience might not have. It is clear to me that I need an extended intoduction to bring the justification for the central argument into the forefront instead of leaving it implicit in references to three seminal articles. A rapid introduction to Ackerlof's asymmetric information and Spence's market signalling would go a long way towards making the paper easier to understand on its own. I have made notes for extending it.

The paper is under consideration by the 2nd ACM Workshop on Assurable and Usable Security, co-located with ACM CCS in Chicago. Notification is 6th August. I asked if anyone had any ideas where to send it next if SafeConfig 2010 does not accept the paper; the Workshop on Software Engineering Economics (WISE) was mentioned, of course. Shamal suggested NSPW for a longer version of the paper with a more worked-out example. I replied that my model is artificial, but Shamal countered that NSPW dislikes examples from work and would like an artificial example more. They want something that workshop participants can hack on and improve. That is why I submitted the paper to the ACM workshop, hoping for the same kind of interaction. NSPW is more prestigious, but the deadlines worked against me for submitting to NSPW this year.

John suggested looking at who is on the Programme Committee of WISE and to send my paper to other conferences where those same people are on the PC.

Regarding the central idea of the paper, I saw a lot of glazed eyes. I think people generally agreed that the conclusions I drew in the paper are logically valid, but they would like to see more justification. Mingqiu asked, what is the fundamental assumption: is it the satisfaction of all parties? Cornelius asked, what is the signal that an accreditor sends? Is it that he or she wants to optimise the residual risk to as low a value as possible? More to the point, Cornelius asked, do accreditors cooperate, or do they compete as in a traditional market? I proposed that accreditors cooperate. Shamal instantly pounced on that and asked whether a market solution is the right model. I argued that yes it is, because accreditors still use the market mechanism to negotiate a price. Whether that mechanism is driven by competition or cooperation makes no difference: equal but opposite forces can still drive an equilibrium. Shamal agreed that the market interpretation is still valid. He then asked whether a market mechanism was overkill for such a simple result (simply equilibrating residual risk to as low a value as possible within the constraints). I replied that the model I presented in this paper is still very simple, not including some other factors that will make finding an equilibrium level much more interesting. At this point I asked if anyone in the group has experience with systems engineering modelling and simulation tools. Shamal suggested Matlab for systems dynamics modelling. I will look for a book on Matlab and see how well suited it seems for my purpose. I will also ask Greg Shettlesworth at Lockheed. I know he uses an expensive commercial tool for systems dynamics modelling; I will find out what he uses and what its capabilities are.

How does an accreditor make another accreditor want to 'buy' the risk he is 'selling'? The answer is implicit in my straw-man pricing function: risk is inversely related to testing effort. Some tests, for example penetration testing, are very expensive because they require extensively experienced people, sometimes special equipment, and an open-ended amount of time. (Like covert channel analysis, penetration tests are never finished; testers simply run out of time or money and are ordered to stop. Left to their own devices, they would generate findings indefinitely at some baseline rate, fuelled by new discoveries, new tools, and exhaustive enumeration of a finite state machine.) It was pointed out that an accreditor who is not satisfied can always require more and more assumptions to be tested, more requirements. I tried to shore up my argument by showing that arbitrary behaviour like that on the part of an accreditor would work to his or her own detriment:

In response to Cornelius's question, I tried to explain better how the limiting case forces accreditor behaviour from both directions. If an accreditor were to try to falsely manipulate the 'price' by claiming

that the residual risk was lower than the accreditor knew it actually to be, then that accreditor would only be increasing his own personal risk—the risk to his own career by approving an insecure CDS that is more likely to fail. Conversely, if an accreditor were to try to manipulate the price in the opposite direction, the result would automatically be to cause more work for himself, because the other accreditors in the market would demand more time and effort in the guise of additional testing. So the incentives continue to work in the right directions, something that Dr Martin specifically asked about and also the Economics lecturer at Yale that I watched on video emphasised—one of the acid tests for the existence of an equilibrium is to verify that the incentives (he called them 'beliefs') work in the right way. (The other acid test is to assign numerical values and show that the equation balances, which is something I have not done yet. There seems to be an art to picking those numeric values, similar to finding a nice clean integer solution to a system of simultaneous equations.)

There followed some discussion of a possible fallacy. What are the incentives really? In the Common Criteria, the argument goes that Protection Profiles (PPs) are developed by clever and conscientious people who always have the end-user's best interests in mind when they specify the requirements in the PP. And yet we know from experience that PPs are far from perfect. Shamal stated that the fallacy is in assuming a binary outcome, whereas he argued that the real outcome is a continuum because humans are involved in developing it. I need to think about that some more to come up with a good counterargument.

I emailed Mingqiu afterwards to ask if I had answered her question adequately. I do not think I did in Reading Group.

In summary, I am now less sure my paper will be accepted at all; I wish I had had another six pages to expand the introduction, work out the equilibrium numbers formally, and address all the questions that came up in Reading Group. Some of the answers I already knew, just had not had space enough to write them in the paper. Other points were things that I want to put into a new paper, either an extended version of this one (if the present version is not accepted by SafeConfig 2010) or a follow-on article.

References