File 20100918.0003: This is the abstract I submitted to the 2010 Comlab DPhil Student Conference:

Title: An Artificial Risk Market Solution to the Problem of Information Asymmetry in Cross Domain Systems Security Test and Evaluation [Extended Abstract]

Sometimes you find it necessary to violate your own security policy. The most concrete example of the necessity for this principle lies in the existence of Cross Domain Systems (CDS), whose *raison d'être* is to violate system security policy in a controlled manner [2, 3]. CDS security accreditations are interesting because—by definition—they always span at least one security boundary, thereby virtually guaranteeing an adversarial environment during site security validation testing [4]. Data owners of classified end-systems rarely trust outsiders—among whom they number their users, their own software developers, owners of other classified systems, and vendors or installers of CDS solutions. In the crossfire of all this mistrust is the Designated Accrediting Authority (DAA), a government employee whose unenviable task it is to try to determine the true level of risk in a system, reduce it to acceptable levels, and formally accept personal responsibility on behalf of the data owner for the correct operation of the system [6, 7, 11, 12]. Approved CDS solutions regularly encounter security testing criteria that represent the duplicated responsibility for residual risk of multiple security accreditors. Each DAA perceives a site-specific set of risks A that would be desirable to mitigate, a technology-dependent set of risks B it is possible to mitigate, and their relative complement $A - B$, being the residual risk it is felt acceptable by that DAA not to mitigate. In this paper we show that time and cost inefficiency in CDS accreditation arise directly from asymmetry of knowledge; Spence's (1973) criteria for market signalling are shown to hold by analogy for inter-DAA communication in the presence of unequal or non-hierarchical security clearances [8, 9, 10]. Akerlof's (1970) requirement that signals must be costly enough to preclude spoofing [1] is shown to be satisfied by the negative incentive for cheating that exists when the result of dishonesty in communicating a false reading of the residual risk R as perceived by DAA k would either raise the value of R, thereby increasing the amount of risk that DAA k must accept formal responsibility for, or conversely, artificially depress the apparent level of risk below what DAA k knows the true value to be, again raising the level of personal risk to DAA k. Following from this result, a solution is proposed to reduce costs in a generalisable scenario in which some data owners are aware of risks or risk mitigations that not all DAAs are cleared for. Based on a metric we define for total residual risk, an artificial market comprising risk assessments and risk mitigations is constructed with the aim of enabling semantically limited and covert-channel–free *ad hoc* communication amongst DAAs participating in a single CDS accreditation [5]. The tool we are developing, called *nihil obstat*, presently implements bid/ask functionality together with a Black–Scholes-like options pricing model in which the cost of a risk is set by the data owner affected by that risk, and the price of a risk mitigation is proportional to an amount of work (e.g., test procedures completed and witnessed) that must be done by someone—not necessarily the bidder—for the accreditation to proceed. By formalising signals, an efficient route to agreement about the true level of residual risk in a CDS accreditation will avoid repeated re-testing and redundant risk mitigations. If successful, the unnecessary cost of duplicated security test and evaluation effort could be greatly reduced.

I need to update the Information Asymmetry paper to include the new material.

References

[1] George A. Akerlof. The market for 'lemons': Quality uncertainty and the market mechanism. *Quarterly Journal of Economics*, 84(3):488–500, August 1970.

[2] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, Inc., second edition, 2008.

[3] Director of Central Intelligence. *DCID 6/3 Industry Annex: Protecting Sensitive Compartmented Information Within Information Systems*, 24 May 2000. For Official Use Only.

[4] Joe Loughry. Unsteady ground: Certification to unstable criteria. In *Proceedings of the Second International Conference on Advances in System Testing and Validation Lifecycle*, Nice, France, 22–27 August 2010.

[5] National Computer Security Center. *A Guide to Understanding Covert Channel Analysis of Trusted Systems*, November 1993. NCSC-TG-030 Version 1.

[6] National Institute of Standards and Technology. *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010. NIST Special Publication 800-37 Revision 1.

[7] Ron Ross, Arnold Johnson, Stu Katzke, Patricia Toth, Gary Stoneburner, and George Rogers. *Guide for Assessing the Security Controls in Federal Information Systems*, July 2008. NIST Special Publication 800-53A.

[8] Michael Spence. Job market signaling. *The Quarterly Journal of Economics*, 87(3):355–374, August 1973.

[9] George J. Stigler. The economics of information. *Journal of Political Economy*, 69(3):213–225, June 1961.

[10] Sun Microsystems, Inc. *Compartmented Mode Workstation Labeling: Encodings Format DDS-2600-6216-93*. Trusted Solaris 2.5, 2550 Garcia Avenue, Mountain View, California 94043-1100 USA, July 1997. Revision A.

[11] United States Department of Defense. DoD information assurance certification and accreditation process (DIACAP). ASD(NII)/DoD CIO, November 28, 2007. DoD Instruction 8510.01.

[12] U.S. Department of Commerce, National Institute of Standards and Technology. *NIST Special Publication 800-53, Revision 3: Recommended Security Controls for Federal Information Systems and Organizations*, June 2009. Final Public Draft.