A Model of Certifier and Accreditor Risk Calculation for Multi-Level Systems

Joe Loughry
Doctoral Student in the Department of Computer Science
University of Oxford
Wolfson Building, Parks Road
Oxford, OX1 3QD, UK
Email: joe.loughry@stx.ox.ac.uk
Tel: +1 303 221 4380

***Abstract*—From direct observation of the certification (post–software-development) and accreditation (pre-deployment) testing of cross domain systems used for the interconnection of classified security domains in U.S. and U.K. defence and intelligence community systems, certain characteristic behavioural patterns have been noted. The savvy developer can use these to exert a measure of control over the duration and cost of certification testing and to predict the likely direction and magnitude of the residual risk calculation performed by security accreditors in multi-lateral, multi-level, collateral, and compartmented site accreditations. DCID 6/3, Common Criteria, DIACAP, and ICD 503 testing efforts across the evolution of a long-lived software development programme were examined using grounded theory methodology. While discovered through investigation of classified cross domain system testing inefficiencies, it is believed that the principles are applicable more widely to privacy-sensitive areas such as electronic health care, financial, and law enforcement record keeping systems. The first thing found was a syndrome of pathological regressive interactions amongst software developers, managers, independent verification and validation contractors, penetration testers, and certification authorities that resulted in schedule slippage during the certification testing phase and, in the accreditation phase, ineffective duplication of testing with no corresponding improvement in residual risk. To understand why these problems occurred, an abstract model of how security accreditors discover and agree upon the true level of residual risk in multi-level cross domain system installations was developed. The model is powerful enough to handle collateral, SCI, and international cross domain systems with any number of endpoints. It works by establishing the visibility of threats, vulnerabilities, and mitigations from each data owner's perspective according to the associated accreditor's clearance over the space of all possible multi-level configurations, then identifying the smallest set of covert-channel–like information flows necessary to reach a concord about residual risk without violating the global security policy. Conventional wisdom holds that security rules should be strictly enforced, but it can be shown that under present regulations, some desirable information flows are inhibited and other undesirable information flows are forced. Paradoxically, it is sometimes the case that relaxing the rules actually improves security.**

***Index Terms*—cross domain systems, certification and accreditation, security test and evaluation, certification test and evaluation.**

I. Author Biography

Joe Loughry received the B.A. degree in mathematics from the University of Colorado, Boulder in 1986 and the M.S.E. degree in software engineering from Seattle University in 1996. He is currently a Ph.D. student in computer science at the University of Oxford [1]. He did some of the first research on compromising optical emanations and holds U.S. patent 6,987,461 on countermeasures. His research interests include cross domain systems, security certification and accreditation testing, penetration testing, side channels, and efficient enumeration of subsets.

References

[1] J. Loughry, "Security test and evaluation of cross domain systems," Ph.D. dissertation, University of Oxford, Michaelmas Term 2012.