An Appropriate Design for Trusted Computing and Digital Rights Management

Clark Thomborson

Abstract: Trusted computing and digital rights management systems show great promise in corporate and governmental applications. These technologies are still in their infancy, being used only in a few highly-confidential environments, despite massive development efforts during the dot-com era. In most computing environments, confidentiality is less important than usability, flexibility, cost-effectiveness, availability, integrity, and auditability. With respect to these requirements, current designs for trusted computing and digital rights management systems are inappropriately focused on confidentiality. We sketch a more appropriate design. Our design will make adequate provision for third-party assurance. It will avoid reliance on a single supplier. It will support a full range of interpersonal trusting relationships, not just the hierarchical-confidential relationship of a military or secret-service agency. We close our presentation with an appeal to develop an international standard for the use of trusted computing and digital rights management, based on New Zealand's recently-published principles and policies.

Bio Sketch : Clark Thomborson has served as a Professor of Computer Science at the University of Auckland, New Zealand, since 1996. His prior academic positions were at the University of Minnesota, and at the University of California at Berkeley, with consultancies or temporary positions at MIT, Microsoft Research (Redmond), InterTrust, IBM Yorktown, IBM Almaden, Institute for Technical Cybernetics (Slovakia), and Xerox PARC. He gained several years of commercial experience in the USA as a systems integrator at Digital Biometrics, LaserMaster, and Nicolet Instrument Corporation. Under his birth name Clark Thompson, he was awarded a PhD in Computer Science from Carnegie-Mellon University and a BS (Honors) in Chemistry from Stanford. He has published more than 100 refereed papers on topics in software security, computer systems performance analysis, VLSI algorithms, data compression, and connection networks.