GUEST EDITORIAL PREFACE

Special Issue on Network Security: Is it Ready for Prime Time?

Michael E. Whitman, Coles College of Business, Kennesaw State University, Kennesaw, GA, USA

Herbert J. Mattord, Coles College of Business, Kennesaw State University, Kennesaw, GA, USA

Information security is maturing as a discipline. From our vantage point, standing on the crossroads of industry, academia, and government, we watch the comings and goings of practitioners who wrestle with great problems of aching complexity. We teach students in various subjects like IT governance, network security, software assurance, or penetration testing and then send them into the workforce with only the bare skills needed to get started on a career. From our perch, we see some trends that may warrant comment. One of these observations is that network technology may be stabilizing and meaningful progress toward secure networks may be possible.

For the last fifty years, networks have been formative. We watched as SNA established an island of stability in commercial networks in the 70s. Then, we saw new networking protocols emerge to make local networks possible. Those protocols, like ARCNET, token-ring, and Ethernet came to the market, often supported only by one or a few companies. They opened up a competitive space for networking to grow. When TCP/IP emerged as a phenomenon, and then an industry standard to supplant everything else--first in Wide-Area Networks and then even inside local networks, the shape of the future began to emerge. When a tidal wave of vendors brought us into the era of ubiquitous wireless by branding themselves as Wi-Fi, the world changed again. But, was Wi-Fi, whatever the 802.11 designation, a fundamental change? Or was it a refinement?

And so, in this new era of relative stability, refinement is happening instead of replacement. Can the network protocols in service now last long enough for academics to study them and practitioners to master them? When we ponder if TCP/IP version 6 will ever reach critical mass, we have to ask if the reason for version 4's longevity is the relative stability it offered after the protocol wars of the 80s and 90s, when token-ring and Ethernet fought it out. Except,

they both lost to TCP/IP. Now we stand on the precipice of "the cloud". Just when organizations seem to be making minute progress toward securing their internal networks, systems, and services, the industry has made a hard left turn and headed into uncharted territory, where security and administration of core infrastructure now depends on an organization's ability to negotiate effective service agreements. Information and network security has now become more critical than ever. But once again we ask, is it really different? Or, is this just a new type of sprinkles on the same flavor of ice-cream?

This edition of IJITN offers an eclectic collection of papers on a variety of network security related topics. Topics range from cryptography for the purist, psychology for the social scientists, privacy policy for the legal and ethical enthusiast, and a number of topics of interest to practitioners and academics alike. The topics presented provide a holistic representation of what is currently being investigated and studied.

Kennesaw State University began offering a bachelor's degree in information security in the Fall of 2005. At the time it was the second such degree at a public university in the country. When this degree was proposed, one of the earliest questions was, "Is security really a discipline inside information systems or is just another specialization like, say, database?" At the time the answer was, we're not sure, but we think it is different. Just as database technology was a hot topic for a number of years and might have become a separate discipline, so too was information security. But, database as a specialization faded back into the woodwork of information systems and computer science, just another skillset for systems builders and implementers. Security may be different. Information security has not yet started to fade, and it may not. Instead, it seems to be headed toward an area of specialization for practitioners rather than just another skill for an IT professional. Since the core tenet of most security is really *informed risk management*, it seems to have merged the respected discipline of risk management with the emergent wonder of information technology to gain an identity of its own. To make this new discipline, start with healthy paranoia from the financial sector where the adversaries really are trying to steal money, layer on a backdrop of information warfare from state-managed capitalism, throw in a little of the market-driven security vendor hype cycle, add a little government sponsored cheerleading, and you might just create a new academic discipline. As this discipline grows and matures, it may well produce offspring disciplines from itself: network security, information risk management, information assurance, or security governance to name a few, each of which may then go on to produce sub-disciplines of their own. As networks evolve, the future is certain in one regard, we will always need network security; and network security will always need academics to develop new and innovative studies to better understand how to educate a future generation of network security professionals, and to enable industry to better respond to as yet unknown threats.

This special edition of IJITN was designed to provide a spectrum of topics and perspectives within Network Security. Each article selected for inclusion was specifically chosen to provide variety of opinion and breadth of subjects. We welcome suggestions and proposals for future special editions focusing on network security. We hold an annual information security conference, typically in October, at Kennesaw State University, and last year invited the authors of the top papers at that conference to submit revised versions for this special edition.

Michael E. Whitman
Herbert J. Mattord
Guest Editors
IJITN