Deception, Digital Forensics, and Malware Minitrack
(Introduction)

Kara Nance
Hume Center
Virginia Tech
Arlington, VA, USA
knance@vt.edu

Matt Bishop
Department of Computer Science
University of California at Davis
Davis, CA, USA
mabishop@ucdavis.edu

Within the fields of computer science and software engineering greater attention is being given today to the broad topic of information assurance. This has been demonstrated at HICSS over the past 50 years by the increased attention paid to computer security topics and the addition of several minitracks within the Software Technology Track with a security focus and the presentation of security papers within other minitracks (actually a crosscutting theme). The Deception, Digital Forensics, and Malware Minitrack evolved from the Digital Forensics – Education, Research, and Practice minitrack to focus on topics that analyze software technologies to determine what they actually do.

• Digital forensics involves the use of software, computer science, software engineering, and criminal justice procedures to explore and/or investigate digital media with the objective of finding evidence to support a criminal or administrative case.

• Malware is software intended to damage a computer, mobile device, computer system, or computer network, or to take partial control over its operation.

• Deception includes technologies that hide their true identity or mission.

These three topics are closely related as Digital Forensics techniques can be used to identify deception in technologies; malware can use deception to disguise what it is doing; digital forensics techniques can be used to identify the “real story” about what has occurred or will occur; digital forensic tools can use deception to “hide” what they are really doing; and attackers can use deception to hide from digital forensic tools.

The papers this year are diverse in topic and represent a well-rounded coverage of some of the major areas of interest in the new direction for this minitrack.