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 forensics 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.

In *A Universal Windows Bootkit: An Analysis of the MBR Bootkit "HDRoot"*, William Showalter presents an interesting investigation of the 2015 HDRoot bootkit analysis conducted by Kaspersky. While the findings by Kaspersky were dismissive, Showalter's analysis of the report and the bootkit raises some interesting questions about the analysis and conclusions reached by Kaspersky

In *Discovering Malware with Time Series Shapelets,* Om Patri, Michael Wojnowicz, and Matt Wolffof propose a machine-learning approach to malware classification in order to combat some of the disadvantages associated with signature-based approaches. They discuss the viability of their approach as a stand-alone classifier or when used in conjunction with another classifier. This "shapelet" approach overcomes some of the challenges associated with current methods and provides some interesting insight into the future of classifier.

In *Implications of Malicious 3D Printer Firmware,* Samuel Bennett Moore, William Bradley Glisson, Mark Yampolskiy take us into the new realm of 3D printers with a thought-provoking example of 3D printer malware in action. They develop and implement malicious code and activate it though a desktop command. This exciting example provides a foundation for future research in this area as new avenues for attack are continually being discovered.

Our final paper, *Automating the Generation of Enticing Text Content for High-Interaction Honeyfiles*, by Ben Whitham presents four new designs for automating the content of honeyfiles, a mechanism used to detect unauthorized intruders as well as insider threat. The methodology uses word transposition and substitution coupled with advanced techniques to ensure enticing honeyfile creation. This leads to some promising directions in honeyfile creation as it mitigates some of the challenges associated with traditional honeyfile construction.

URI: http://hdl.handle.net/10125/41895
ISBN: 978-0-9981331-0-2