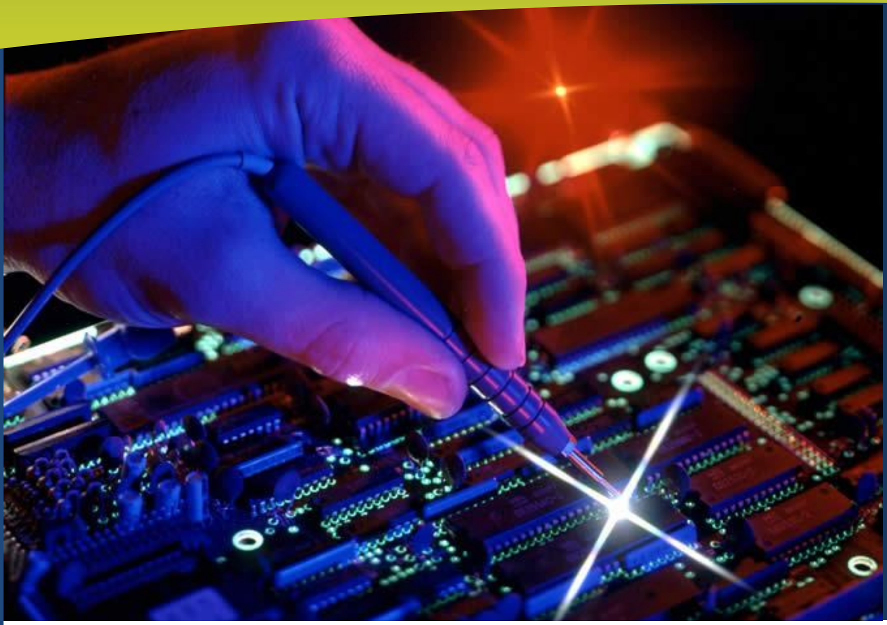
Information Technology Laboratory Newsletter



March—April 2015

Issue 134

INSIDE THIS ISSUE

ITL Focuses on Direct Digital Manufacturing

Information technology has increasingly been incorporated into every aspect of American life. One of those areas is manufacturing. Direct Digital Manufacturing (DDM) involves creating a physical object from a digital design using computer-controlled processes with little to no human intervention. The basic technology has been around for dozens of years, but with the popularization and advancement of Additive Manufacturing (AM) and 3D printing, it is becoming much more common. These technologies have the potential to significantly change traditional manufacturing and supply chain industries, including for information and communication technologies (ICT).

On February 3, 2015, ITL hosted a symposium to explore the cybersecurity aspects of DDM. The event drew about 50 attendees from government, industry, and academia representing a broad array of DDM practitioners, cybersecurity professionals, researchers, and manufacturing innovation organizations. Speakers and attendees discussed cybersecurity risks, challenges, solutions, and implications for ICT supply chain risk management. Mike Molnar, director of the NIST Advanced Manufacturing Program Office, emphasized in his keynote presentation that manufacturing is on the edge of a revolution – a "digital manufacturing renaissance requiring cybersecurity." Cybersecurity has been called out as one of the top five priorities for manufacturing leaders, and cybersecurity solutions are needed.

During discussions and the concluding working session, participants generally agreed that the biggest challenge to building cybersecurity into DDM is culture. Manufacturers see AM devices and 3D printers as machines that happen to have some technological capabilities, while IT professionals see them as computers that happen to have manufacturing capabilities. Especially smaller businesses may not recognize that these devices have any cybersecurity risks and would likely be unwilling to compromise efficiency for security.

With NIST's dual focuses on advanced manufacturing and information technology, the agency is well poised to address these concerns. ITL is already helping manufacturers to address cybersecurity concerns through their work in Cyber-Physical Systems and Industrial Control Systems. Our National Initiative for Cybersecurity Education (NICE) is helping manufacturers be more aware of cybersecurity risks that may go unrecognized. Also, ITL's National Cybersecurity Center of Excellence (NCCoE) is designed to find solutions to hard technical problems.

NIST/UMD Establish Joint Center for Quantum Information in Computer Science

NIST and the University of Maryland (UMD), with the support and participation of the Research Directorate of the National Security Agency/Central Security Service (NSA/CSS), recently inaugurated a new joint venture, The Joint Center for Quantum Information and Computer Science (QuICS). Scientists at the center will conduct basic research to understand how quantum systems can be effectively used to store, transport, and process information.

The new center complements the fundamental quantum research performed at the Joint Quantum Institute (JQI), which was established in 2006 by UMD, NIST, and NSA. Focusing on one of JQI's original objectives, to fully understand quantum information, QuICS will bring together computer scientists—who have expertise in algorithm and computational complexity theory and computer architecture—with quantum information scientists and communications scientists. The center will bring together researchers from the University of Maryland Institute for Advanced Computer Studies (UMIACS); the UMD Departments of Physics and Computer Science; and the UMD Applied Mathematics and Statistics, and Scientific Computation Program with NIST's Information Technology and Physical Measurement Laboratories.

Some of the topics QuICS researchers will initially examine include: 1) understanding how quantum mechanics informs computation and communication theories; 2) determining what insights computer science can shed on quantum computing; 3) investigating the consequences of quantum information theory for fundamental physics; and 4) developing practical applications for theoretical advances in quantum computation and communication.

QuICS is also expected to train scientists for future industrial and academic opportunities and provide U.S. industry with cutting-edge research results. By combining the strengths of UMD and NIST, it is hoped that QuICS will become an international center for excellence in quantum computer and information science.

ITL Advances Public Safety Mobile Application Security

In 2013, the Department of Commerce's Public Safety Communications Research (PSCR) program began cybersecurity research efforts related to public safety communications including public safety mobile application security. The Association of Public-Safety Communications Officials (APCO) International, in cooperation with FirstNet and PSCR, organized the Public Safety Mobile Application Security Requirement Workshop in February 2014. The workshop identified and documented an initial set of mobile application security requirements relevant to the public safety community. Although some of the requirements may be addressed using techniques after the application is deployed, the workshop focused on how the public safety mobile application security requirements might be addressed as part of the application development process. Mobile application developers can consult this list of requirements to reduce the chance of overlooking requirements important to the security of mobile application for public safety personnel. Workshop results are presented in NISTIR 8018, Public Safety Mobile Application Security Requirements Workshop Summary.

ITL Releases New Healthcare Testing Tool

ITL released a new testing tool for Document Sharing Metadata in healthcare. The Cross-Enterprise Document Sharing (XDS) standard facilitates the registration, distribution, and access across the healthcare enterprises of patient electronic health records. These operations are defined and recorded by the metadata associated with each document. In this context, ITL developed the XDS Document Entry Editor, a first step in generating custom document-sharing metadata for health information exchange. Requested by the healthcare industry, the tool will be invaluable in future healthcare interoperability testing.

Staff Accomplishments

Donna Dodson, ITL's Chief Cybersecurity Advisor and Director of the Cybersecurity Center of Excellence, was recently recognized by FedScoop as one of DC's top 50 Women in Technology. The award cites her outstanding leadership of ITL's cybersecurity and privacy programs.

Tim McBride, Director of Operations at ITL's National Cybersecurity Center of Excellence (NCCoE), received a 2015 Federal 100 Award from Federal Computer Week. The award recognizes McBride's leadership of the establishment of the Nation's first Federally Funded Research and Development Center for cybersecurity support to the federal government.

Selected New Publications

The Twenty-Third Text REtrieval Conference Proceedings (TREC 2014)
Ellen Voorhees and Angela Ellis, Editors
NIST Special Publication 500-308
February 2014

This report constitutes the proceedings of the Twenty-Third Text REtrieval Conference (TREC 2014) held in Gaithersburg, Maryland, November 19-21, 2014. The conference was co-sponsored by the National Institute of Standards and Technology (NIST) and the Defense Advanced Research Projects Agency (DARPA).

Recommendation for Key Management Part 3: Application-Specific Key Management Guidance
By Elaine Barker and Quynh Dang
NIST Special Publication 800-57, Part 3, Rev. 1
January 2015

Special Publication 800-57 provides cryptographic key management guidance. It consists of three parts. Part 1 provides general guidance and best practices for the management of cryptographic keying material. Part 2 provides guidance on policy and security planning requirements for U.S. government agencies. Finally, Part 3 provides guidance when using the cryptographic features of current systems.

Vetting the Security of Mobile Applications
By Stephen Quirolgico, Jeff Voas, Tom Karygiannis, Christoph Michael, and Karen Scarfone
NIST Special Publication 800-163
January 2015

This document helps organizations to: (1) understand the process for vetting the security of mobile applications; (2) plan for the implementation of an app vetting process; (3) develop app security requirements; (4) understand the types of app vulnerabilities and the testing methods used to detect those vulnerabilities; and (5) determine if an app is acceptable for deployment on the organization's mobile devices.

Defensive code's impact on software performance
By David Flater
NIST Technical Note 1860
January 2015

Defensive code is instructions added to software for the purpose of hardening it against uncontrolled failures and security problems. It is often assumed that defensive code causes a significant reduction in software performance, which justifies its omission from all but the most security-critical applications. We performed an experiment to measure the application-level performance impact of seven defensive code options on two different workloads in four different environments. Of the seven options, only one yielded clear evidence of a significant reduction in performance; the main effects of the other six were either materially or statistically insignificant.

Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework
By Michaela Iorga and Scott Shorter
NISTIR 7823
March 2015

As electric utilities turn to Advanced Metering Infrastructures (AMIs) to promote the development and deployment of the Smart Grid, one aspect that can benefit from standardization is the upgradeability of Smart Meters. This report describes conformance test requirements that may be used voluntarily by testers and/or test laboratories to determine whether Smart Meters and Upgrade Management Systems conform to the requirements of NEMA SG-AMI 1-2009.

Risk Management of Replication Devices
By Kelley L. Dempsey and Celia Paulsen
NISTIR 8023
February 2015

This publication provides guidance on protecting the confidentiality, integrity, and availability of information processed, stored, or transmitted on replication devices (RDs). It suggests appropriate countermeasures in the context of the System Development Life Cycle. A security risk assessment template in table and flowchart format is also provided to help organizations determine the risk associated with replication devices.

NEURBT: A Program for Computing Neural Networks for Classification using Batch Learning
By Javier Bernal
NISTIR 8037
January 2015

NEURBT, a Fortran 77 program for computing neural networks for classification using batch learning, is discussed. NEURBT is based on Møller's scaled conjugate gradient algorithm which is a variation of the traditional conjugate gradient method, better suited for the non-quadratic nature of neural networks. Different aspects of the implementation are discussed such as the efficient computation of gradients and multiplication of vectors by Hessian matrices that are required by Møller's algorithm, and the stochastic (re)initialization of weights.

Integrating Electronic Health Records into Clinical Workflow: An Application of Human Factors Modeling Methods to Specialty Care in Obstetrics and Gynecology and Ophthalmology
By Svetlana Lowry, Mala Ramaiah, E.S. Patterson, D. Brick, M.C. Gibbons, and L.A. Paul
NISTIR 8042
February 2015

A human factors workflow modeling tool, process mapping, was used to visualize and document insights and the end-user needs to improve EHR workflow for clinicians in two specialty outpatient care settings: 1) Obstetrics and Gynecology (Ob-Gyn); and 2) Ophthalmology. The report proposes targeted recommendations for EHR developers and Ob-Gyn and Ophthalmology centers to improve workflow integration with EHRs to improve quality of care and patient safety, and to reduce medical-legal exposure.

Upcoming Technical Conferences

Hands-on Workshop on Assessing and Reporting Measurement Uncertainty
Dates: March 18-20, 2015
Place: Anaheim, California
Sponsor: NIST
Cost: $895 course only
$995 course bundled with one day of conference

This short course covers many aspects of the propagation of uncertainty using the methods outlined in the JCGM **Guide to the Expression of** Uncertainty in Measurement. Exercises and hands-on applications will use functions for uncertainty analysis from the free software package, metRology, written for the open-source R statistical computing environment.

NIST contact: Will Guthrie

FISSEA Annual Conference
Dates: March 24-25, 2015
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST and FISSEA
Cost: $195 (includes coffee breaks/lunch)
$101 (no coffee breaks/lunch)

The theme of this year's Federal Information Systems Security Educators' Association (FISSEA) conference is Changes, Challenges, and Collaborations: Effective Cybersecurity Training. Attendees will gain a better understanding of current cybersecurity projects, emerging trends and initiatives, and awareness and training ideas.

NIST contact: Peggy Himes

Workshop on Cybersecurity in a Post-Quantum World
Dates: April 2-3, 2015
Place: NIST, Gaithersburg, Maryland
Sponsor: NIST
Cost: $95 (includes coffee breaks/refreshments)
$60 (no coffee breaks/refreshments)

The advent of practical quantum computing will break all commonly used public key cryptographic algorithms. In response, NIST is researching cryptographic algorithms for public key-based key agreement and digital signatures that are not susceptible to cryptanalysis by quantum algorithms. NIST is holding this workshop to discuss issues related to post-quantum cryptography and its potential future standardization.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST). As a world-class measurement and testing laboratory encompassing a wide range of areas of computer science, mathematics, statistics, and systems engineering, our research program supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. ITL cybersecurity experts collaborate to develop cybersecurity standards, guidelines, and associated methods and techniques for federal agencies and industry. Our mathematicians and statisticians collaborate with measurement scientists across NIST to help ensure that NIST maintains and delivers the world's leading measurement capability. ITL computer scientists and other research staff provide technical expertise and development that underpins national priorities such as cloud computing, the Smart Grid, homeland security, information technology for improved healthcare, and electronic voting. We invite you to learn more about how ITL is enabling the future of the nation's measurement and standards infrastructure for information technology by visiting our website at http://www.itl.nist.gov.

ITL Editor: Elizabeth B. Lennon
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900
Phone: (301) 975-2832
Fax: (301) 975-2378
Email: elizabeth.lennon@nist.gov

TO SUBSCRIBE TO THE ELECTRONIC EDITION OF THE ITL NEWSLETTER, GO TO ITL HOMEPAGE

Credit: NIST