INFORMATION TECHNOLOGY LABORATORY

National Institute of Standards and Technology

Information Technology Laboratory

Internet of Things

April 2017

ITL Mission

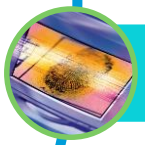
ITL promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and related technology through research and development in information technology, mathematics, and statistics

ITL Technical Capabilities


Advanced Networking


Applied and Computational Mathematics

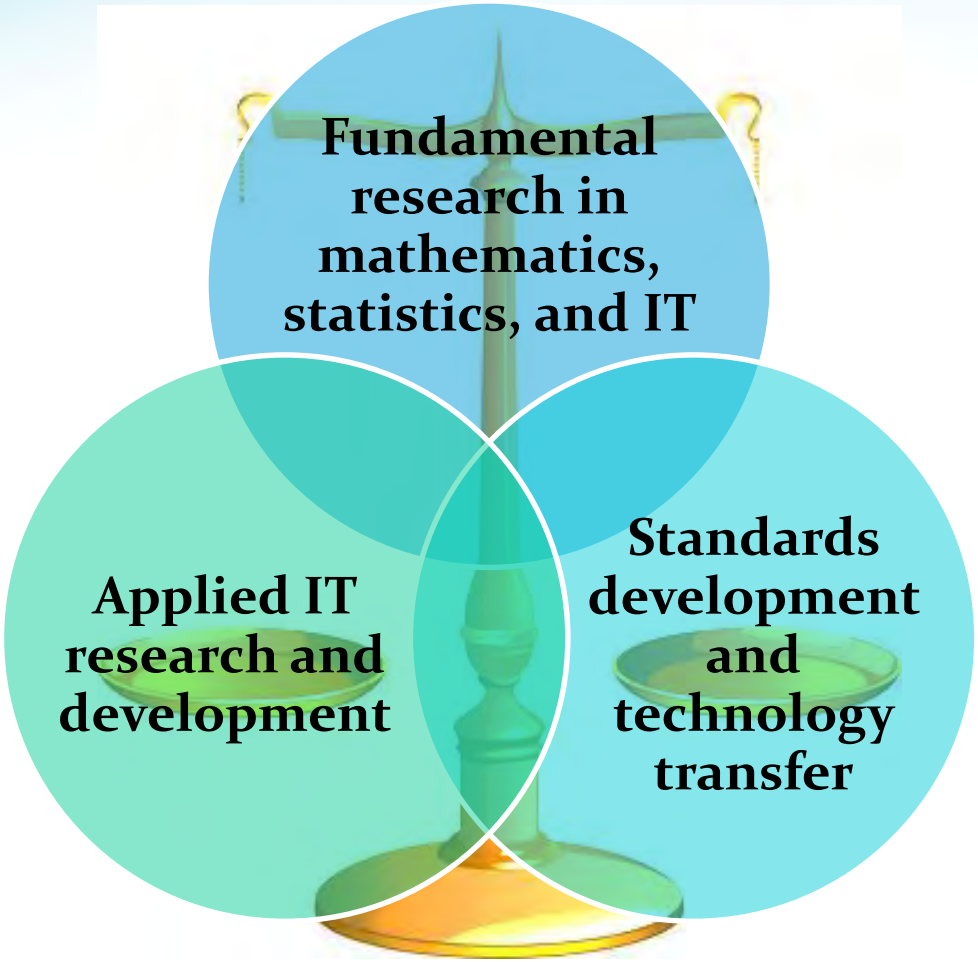

Cybersecurity


Information Access


Software and Systems


Statistics

ITL Approach



ITL Purpose:

"Cultivate Trust in IT and Metrology"

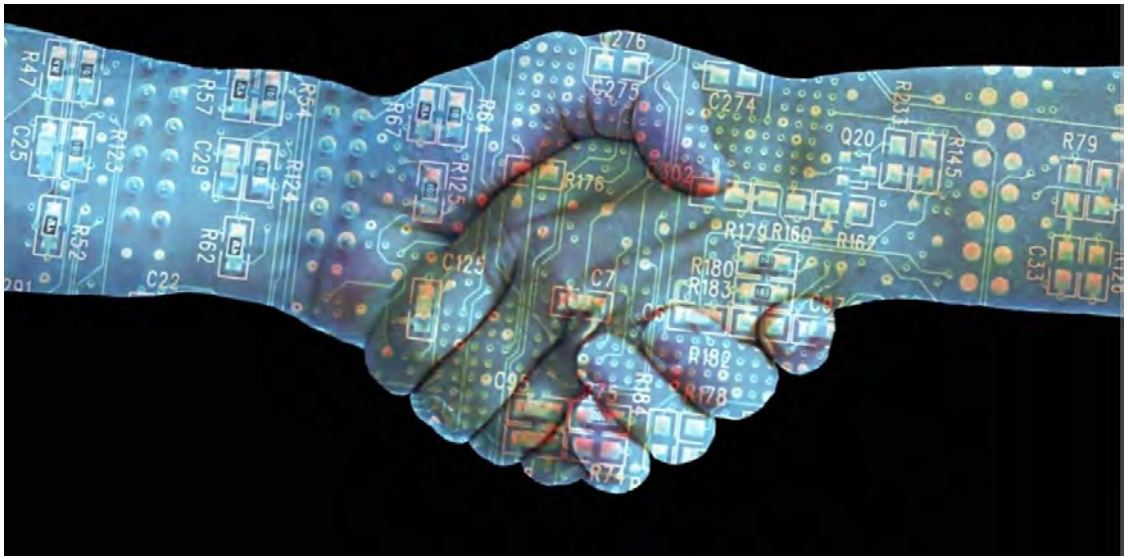


Photo - https://phys.org/news/2016-07-blockchainsfocusing-bitcoin-real-revolution-digital.html - Credit: Robert Bagnall/YouTube

The Internet of Things (IoT)

- There is no widely accepted definition of IoT – one definition states: "*the connection of physical objects to the Internet and to each other through small, embedded sensors and wireless technologies, creating an ecosystem of ubiquitous computing…and embedded intelligence in individual items that can detect changes in their physical state*"[1]
- Potential for enormous societal benefits

  in health, safety, energy, security, productivity, environment …

1 - "Internet of Things, Privacy & Security in a Connected World," Federal Trade Commission, January 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

The Internet of Things

- IoT adoption: early stages - but accelerating
- Standards and guidance needed to enable innovation so that the full benefits can be achieved.
- The NIST Information Technology Laboratory …
  - collaborates with industry, academia, and government to develop measurements and standards to enable IoT innovation
  - has decades of research experience on technological underpinnings of the IoT
  - works with the NIST CPS and manufacturing programs – providing leadership on cybersecurity, privacy, and networking

1 - "Internet of Things, Privacy & Security in a Connected World," Federal Trade Commission, January 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

ITL IoT Research

All ITL Divisions have expertise related to IoT

Examples of ITL research areas include:

- ***Security and Privacy***
- ***Networking***
- ***Data Analytics***
- ***Time, and Space***

Image source: http://techliquids.com/the-importance-of-digital-trust-amidst-decreasing-loyalty/

IoT Security & Privacy Research

- Research, standards and guidance are needed so that the vast quantity of data generated and communicated by the IoT ecosystem can be delivered reliably and securely, while protecting privacy.
- Privacy Engineering and Risk Management: As with any system, when an IoT system is processing information about individuals (PII), privacy risks can arise from this processing. NIST's Privacy Engineering Program has defined a privacy risk model to support the identification of privacy risks in such systems.
- ITL conducts a wide range of research for cybersecurity, focusing on both fundamental and applied research with applicability to the IoT ecosystem some of which are in the following slides. ITL's work ranges from low level security considerations (e.g., BIOS security), to system security guidance (e.g., NIST SP 800-160) *Systems Security Engineering* (Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems)

ITL's "Cybersecurity for IoT" Program builds on the decades of cybersecurity research and experience on the technological underpinnings of the IoT

ITL conducts fundamental cybersecurity research, work in standards and guidance

- Lightweight Encryption Project
  - NIST hosted workshop and has published NISTIR 8114
- Network of Things, NIST Special Publication (SP) 800-183
  - Networks of 'Things' provides a basic model aimed at helping researchers better understand the Internet of Things (IoT) and its security challenges.
  - Its vocabulary and science aims to help researchers understand how IoT components interoperate, and compare the security risks and reliability tradeoffs.
- Guide to Bluetooth Security, NIST Special Publication 800-121·
  - Section that addresses specific needs for Bluetooth Low Energy (BLE) which could support constraints of IoT devices
- Hardware Roots of Trust Project
  - The project is conducting research and develop guidelines (NIST SP 800-147/147B, NIST SP 800-155, NIST SP 800-164) on the use of Roots of Trust to secure information and information systems which could possibly tie into IoT by providing a mechanism for trusted devices

Applied cybersecurity research is ongoing that could support IOT security

- NCCoE - Wireless Medical Infusion Pumps Project
  - The NCCoE is collaborating with the healthcare community to secure their medical devices on an enterprise network, with a specific focus on wireless infusion pumps. The project objectives are to perform a risk assessment, identify mitigating security technologies, and provide an example implementation.
- NIST Guide to Industrial Control Systems (ICS) Security SP 800-82
  - While the guidance broadly focuses on how to secure ICS, it could be applied to IOT security due to its focus on securing the unique devices within industrial control systems and provides specific guidance relating to the unique requirements for these (IOT type) devices.
- Trusted Identities Pilot Project
  - NIST is funding a collaborative smart home pilot in apartment units in Portland, Oregon and San Francisco, CA to test individuals passwordless authentication to their IoT devices, as well as to securely share their IoT generated data through the use of a Personal Data Store
- Connected Vehicles
  - NIST collaborates with a number of organizations (e.g., DOT, NHTSA, SAE…) on the development of smart transportation including considerations for security

Other cybersecurity areas we are exploring as applicable to IoT Security

- Special Publication 800-147 BIOS Protection Guidelines
- Special Publication 800-98 Guidelines for Securing Radio Frequency Identification (RFID) Systems
- Special Publication 800-150 Guide to Cyber Threat Information Sharing
- Special Publication 800-160 Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems
- NISTIR 7966, Security of Interactive and automated Access Management Using Secure Shell (SSH)
  - Contains threat model and recommendations for implementations of SSH which could be applicable to security for IoT NHE-to-NHE, NHE-to-network and NHE-to-cloud communications
- The National Vulnerability Database which has extended its schema to include IoT devices where NIST assesses, scores, standardizes and openly publishes known IoT vulnerabilities .
- Cybersecurity Framework provides organizations with a framework to better understand, manage, and reduce its cybersecurity risks. Organizations should consider IoT devices in the organization's risk management
- Applicability of Blockchain to IoT

"Physical" considerations in cybersecurity

- NIST cybersecurity research considers the physical when anticipating cyber threats as well as leveraging the physical for detection and mitigation techniques. For example:
  - Research into possible tools to adapt the constraints imposed by the dynamics of a physical process expressed in coupled differential equations into common networking specifications so that it can inform cybersecurity performance requirements
  - Investigated the use of signatures derived from physical dynamics of complex systems for authentication and anomaly/intrusion detection
  - Researched and produced an annex to FIPS 140-3 (standard for securing cryptographic modules) that paired non-invasive attacks such as timing attacks (TA), Simple Power Analysis (SPA), Simple Electro-Magnetic Analysis (SEMA), Differential Power Analysis (DPA) and Differential Electro-Magnetic Analysis (DEMA) to various symmetric and asymmetric algorithms and provided requirements based on the threats to those pairings.

IoT Networking Research

The IoT demands scalability, reliability, and interoperability of communications. Networking standards are critical to enable interoperable systems of systems, and support innovation at the application layer.

- Software Defined Networking (SDN) and Information Content Networking (ICN) approaches for improving security, interoperability, and congestion control.
- Analysis of network control systems to identify where wireless infrastructure can reduce wiring costs without impacting performance.
- Controlled mobility algorithm for communication of smart cells in public safety networks.
- Body area networking, and energy harvesting

IoT Data Research

The IoT will generate vast amounts of data for decision making, prediction, and autonomous physical action.

- NIST Big Data Interoperability Framework – Big Data Public Working Group – Phase II - Interfaces
  - Seven volumes: 1 - Definitions; 2 -Taxonomies; 3 - Use Cases and General Requirements; 4 - Security and Privacy; 5 - Architectures White Paper Survey; 6 -Reference Architecture; 7 - Standards Roadmap
- Developing methods and testing infrastructure to measure and compare the performance of data analytic algorithms.

IoT Time & Space Research

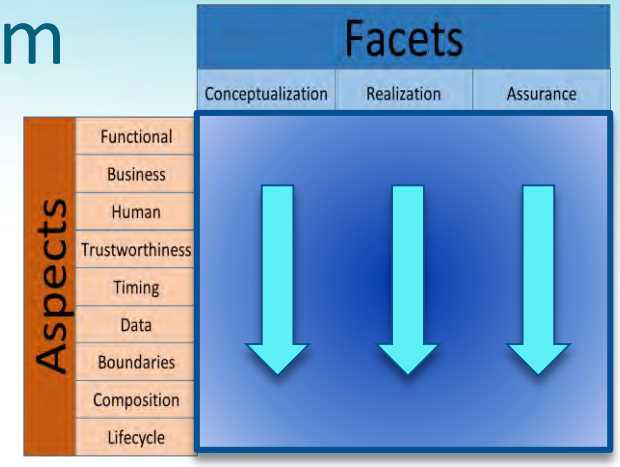
It's estimated that there will be over 30 *billion*[1] devices connected to the IoT by 2020, resulting in *trillions* of interactions presenting localization and interoperability challenges. Some devices will need to be synchronized in real time.

- Research in timing standards including security,
- Interoperability, localization, and real-time data analysis for IoT systems.

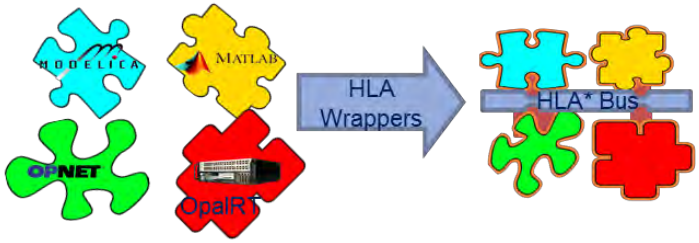
1 http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

NIST Cyber-Physical Systems Program

Promoting the emergence of a globally interoperable Internet of Things



- Measurement science & technology foundations – Cyber-Physical Systems (CPS) Framework
- Powerful research & measurement infrastructure – CPS/IoT Testbed
- CPS/IoT at-scale applications – Smart cities



GLOBAL CITY TEAMS CHALLENGE

Engineering Laboratory:
www.nist.gov/el/cyber-physical-systems

Internet of Things – ITL Research

Future areas

- ***Usability and Human Interface.*** IOT systems won't be adopted unless they are *usable*. We need …
  - Research: how should IoT components best interact with users?
  - Guidance: to aid developers in creating useable designs.
- ***Sensors.*** Sensors are critical components.
  - Research on best practices for sensor data exchange
  - New methods for remote sensor authentication, and quality control, and mitigation of sensor vulnerabilities (e.g., Kevin Fu et.al).