DoD Policy Recommendations for The Internet of Things (IoT)

December 2016

Chief Information Officer

U.S. Department of Defense

Contents

Foreword

While the Department of Defense (DoD) has been using automated sensors and controls for over a century, and connecting them to computers for decades, we are now in the midst of enormous technological change. And, there are huge risks and opportunities associated with this change. We now have the opportunity to exploit the potential of extremely low cost sensors and controls with an amazing and exponentially growing variety, availability, and depth of capability. DoD has already deployed these technologies in green buildings, environmental monitoring, health monitoring, and facility security. We are purchasing vehicles with these sensors and controls already embedded.

However, the immense promise of this technology comes with immense risks. While there have always been risks to DoD sensors and controls, their proprietary nature and isolation limited the possibility of attack. Now, with such capabilities being given Internet access, DoD is entering a quickly deepening pool of vulnerability. At risk are all the things that embrace the Internet of Things (IoT): DoD facilities, equipment, employees, and their possessions—any of which could be used to cause harm. We could soon be in a position where a determined adversary could shut down our power and water, turn off our security systems, disrupt our ability to provide medical care, listen to our conversations, and monitor our movements. Gartner estimates that more than 6 billion IoT devices will be deployed in 2016, rising to almost 21 billion by 2020[1]*. If the Department does not take action to get ahead of this problem, it will get exponentially worse, and the rise of IoT could immerse DoD like a tidal wave.*

[1] http://www.gartner.com/newsroom/id/3165317

I. Purpose

This paper provides background and policy recommendations to address vulnerabilities (and take advantage of opportunities) related to the increasingly pervasive and semi-autonomous internet-capable devices that make up what is known as the Internet of Things (IoT). Due to high utility, low cost and ease of deployment, the IoT is proliferating rapidly as both stand-alone devices, and embedded sensors and controls in nearly every type of electronic device, from household appliances to aircraft. At the same time, IoT introduces vulnerabilities and concerns to the operation and security of networks and information, including those of the Department of Defense (DoD). IoT is already upon us, with millions of these devices already installed in our facilities, vehicles, and medical devices. The newest DoD green buildings have tens of thousands of sensors. The growth of internet-connected medical devices has been similarly exploding. IoT devices have the potential to be incorporated in our weapons and intelligence systems (both intentionally and unintentionally). Due to the sheer number of IoT devices and their limited processing power for running firewalls and anti-malware, the issue of their security vulnerabilities is quantitatively and qualitatively different than vulnerabilities previously associated with mobile devices and industrial control systems; as such, we are overdue in implementing associated policy and controls. Given the security and sensitivity of DoD missions, we need to act now to address DoD interests and identify additional steps that must be taken. Insights gained should be shared with the commercial world.

II. Defining the Internet of Things (IoT)

In describing the definition of Internet of Things, we essentially follow the basic definition from the IEEE paper “Toward a Definition of Internet of Things (IoT)”[2] with its full text provided in Appendix A. The IoT consists of two foundational aspects—1) the Internet itself and, 2) semi-autonomous devices (the “things”) that leverage inexpensive compute, networking, sensing, and actuation capabilities to sense the physical world and act on it. Such devices have the capability to connect to the Internet—being Internet Protocol (IP) based—but may also be deployed in stand-alone IP networks not connected to the Internet. These devices are unambiguously identified using the Web and Internet’s existing unique identification standards, such as the many Universal Resource Identifier (URI) schemes. With their sensor and activation capabilities, they establish relationships between the digital and physical worlds that did not previously exist. IoT includes the functions that allow users and organizations to analyze and understand the data gathered and actions taken by the things.

IoT is extending the reach of the Internet to inexpensive, miniature, pervasive computing and control devices.

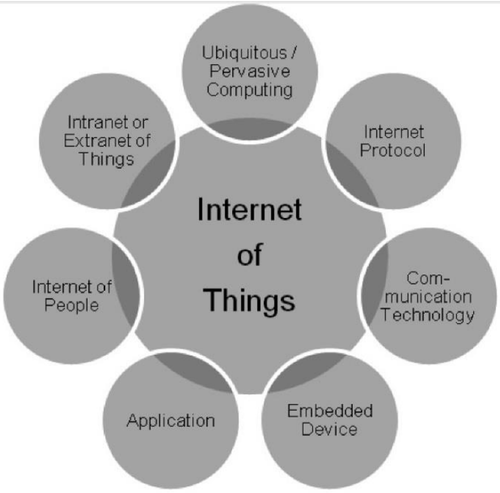
IoT brings together primary characteristics of traditional Internet and mobile capabilities and those of industrial control systems. The major difference between IoT and previous Internet and mobile capabilities is the control and sensing capabilities of *Things*. The major differences between IoT and previous industrial control system capabilities are the connectivity of *Things* to the Internet and their wider scope of application. Still, IoT and industrial control systems do share three quality dimensions of systems: *Integrity*, *Availability,* and *Confidentiality*. While traditional information systems generally prioritize *Confidentiality*, then *Integrity,* and lastly *Availability*, control systems and IoT usually prioritize *Availability* first, then *Integrity* and lastly *Confidentiality*. This does not

[2] “Towards a Definition of the Internet of Things (IoT),” Roberto Minerva, Abyi Biru, Domenico Rotondi; IEEE Internet Initiative, iot.ieee.org; May 27, 2015.

mean that focus should be exclusively on *Availability*. We need to ensure that we maintain sufficient focus on *Integrity* and *Confidentiality* to address DoD's safety, privacy, and mission requirements.

In this paper, we emphasize that IoT includes both core concepts: the notion of (mostly) autonomous things and connectivity to the Internet. Many areas of technology usage and deployment overlap with IoT, as shown in Figure 1, taken from the IEEE paper[3] discussing the definition of IoT. The definition we provide, while expansive, does not include all these overlapping areas. For example, we exclude from its scope the smart devices that have augmented and sometimes replaced personal computers: tablets and smart phones. Like the PC, these devices are essentially user-focused and built to interact with users, no matter the degree of autonomy they may exercise.

Figure 1: Overlaps of the Internet of Things with other fields of Research


Internet of Things
Ubiquitous / Pervasive Computing
Internet Protocol
Com-munication Technology
Embedded Device
Application
Internet of People
Intranet or Extranet of Things

Appendix A provides a more detailed discussion of these concepts, along with additional definitions of IoT from various sources to show both the emerging consensus on what IoT is, as well as the variations in concept.

The basic idea of IoT is quite simple, as was the earlier idea for the World Wide Web. Butler Lampson of Microsoft Research noted as a failure of Systems Research, "We didn't invent the Web. Why not? Too simple."[4] As with the Web, this simple idea has given rise to a vast and rich ecosystem that continues to expand exponentially. We next describe this briefly.

III. The IoT Ecosystem

From its initial introduction, nearly two decades ago, the application of IoT has grown to encompass wide and heterogeneous uses - from the very personal or individual uses in physical fitness or medical devices, to planetary scale mechanisms for monitoring climate change, wild fires, and the impact of development. It includes technology for smart homes and smart buildings; smart communities and cities; government tracking of growth and development; and countries' management of risks, defense, and border control. Figure 2 on the next page is emblematic of this range.

Within our individual smart homes, there are a wide variety of IoT opportunities. Lighting can be dynamically adjusted via the Internet to provide a range of colors without changing bulbs or lamps based on the owner's choosing. The lighting system can communicate with other IoT devices to learn the state of the weather, outdoor light, and occupancy of various rooms to automatically adjust lighting to suit activities. Following circadian rhythms, light can be set brighter and whiter to increase energy and alertness, or to a warmer light as bedtime approaches to help our bodies prepare for sleep. IoT power controls can adjust the timing and use of certain appliances to make best use of off-peak lower rate charges for energy. Tied into a smart power grid, the power controls

[3] Ibid.

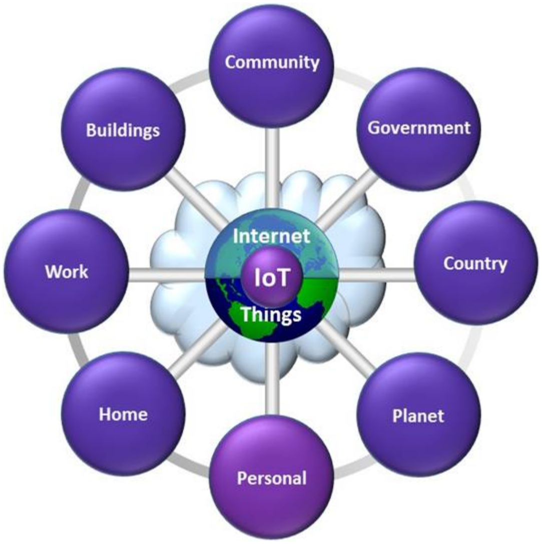
[4] "Gold and Fool's Gold: Successes, Failures, and Futures in Computer Systems Research," Butler Lampson; Microsoft presentation at USENIX Annual Meeting; June 2, 2006.

will also respond to the power utility's request to lower energy usage during peak demand, lessening strain on the grid. The smart fridge can notify us of the expiring milk, and the need for more eggs. Shades can raise and lower with the time of day and the level of exterior light. Doors can lock and unlock automatically, unlocking as we approach in response to the proximity ID we carry.

The house is just one specific example. Capabilities are available across the broad range of application space noted above - bringing automation and machine intelligence into our lives as far as the Web brings information to us now. This has vast potential to significantly change the way we live.

In addition to vertical applications (things to use via the internet), there is also a rich set of applications that take in and aggregate data produced by the things—often many, many things—to produce insight and intelligence. These horizontal applications are often cloud-based, provided by an IoT vendor in addition to the basic capability provided for such things as home control. Additional services can enrich the functionality of the IoT devices and enable updates and needed augmentations. These cloud and vendor-based augmentations are part of an increasing ecosystem of capabilities and services built for deployment on top of the IoT. This new ecosystem brings great benefits, but also new risks and threats, as noted in the following section.

Figure 2: The Range of IoT Applications



IV. Risks and Benefits of IoT

The benefits of IoT are numerous and compelling. However, significant threats and risks must be addressed to fully realize the benefits without compromising DoD missions. Risks and benefits are summarized below and detailed in Appendix B.

Threats and Associated Risks

Many IoT issues arise specifically from the ability to access and control various things from the Internet, potentially by anyone anywhere on the planet. Others arise from provenance issues of the devices themselves.

IoT presents grave challenges for privacy, confidentiality, security, and information

Expanded Attack Surface: The number and relative simplicity of IoT devices greatly expands the attack surface exposed to the Internet.

Attack Deployment – BotNets: The IoT provides many more potential BotNet participants and directions from which attacks can originate. These BotNets may use DoD platforms to mount attacks elsewhere, or to directly attack DoD networks and computers.

Expanded Aggregation of Information: The ability to obtain many dimensions of information about the same assets through various IoT capabilities whose information is aggregated for big data analytics greatly increases the potential benefit of the information. However, it also renders it a far bigger target for attackers looking for high value information.

Vulnerability of Manufacturing Supply Base: With much of industry using IoT and related industrial control devices, the potential for devices to be compromised greatly increases, which in turn can compromise critical manufacturing capability.

Provenance - Subversion of the Things Themselves: It is not just that IoT devices can be compromised; they may also be counterfeited or subverted during their manufacture and distribution with the introduction of "back doors" at various points in the supply chain. Therefore, it is not necessary for an attacker to find and exploit a vulnerability when they can just unlock the back door they have installed.

Ownership: While business models for using things without ownership (renting, leasing, licensing) exist, the increasing prevalence of software and networking embedded in purchased devices has increased restrictions on what owners can do with their devices. These restrictions may inhibit realization of full benefits of devices after purchase. While we have become accustomed to this with our computers and phones, we now face the possibility that this will extend to things like our lighting and air conditioning. For example:

- Users may not receive needed security patches if their device goes past a certain age or release.
- Licensing restrictions may restrict a user's ability to properly monitor software components installed on their device.
- Devices may depend on a cloud capability provided by the vendor for normal operation, and cease operating if the vendor goes out of business or drops support.
- Users may be restricted from opening or repairing their owned device when needed.

Benefits

IoT also promises to bring many benefits to DoD:

Better Management of DoD Assets: Assets can be tracked and monitored in real-time. Information—both item specific and in aggregate—can be readily available to those who need it anywhere in the DoD.

IoT promises greatly improved situational awareness and ability to do more with less.

IoT Unique Identification of Things: The ability to uniquely identify things in the Internet of Things through adoption of the Web and Internet's URI schemes can help DoD achieve long-sought unique identification goals, leveraging a proven approach without re-inventing another UID mechanism.

Improved Readiness: Knowing the real-time status of materiel and weapons systems enables the DoD more rapid and agile response to emergent threats.

Ability to do More with Less: The low cost and pervasive nature of IoT allows tracking, inventory, control, and data gathering activities to be accomplished with significantly less personnel labor, and greatly reduced intermediate processing and handling of information.

An Example of IoT Risks and Benefits to the Supply Chain

Imagine the supply-chain management benefits of an extensive IoT implementation that improves visibility, physical security, and even automates portions of the logistics process.

For example, at a DoD fuel depot, IoT devices could:

- Inexpensively and precisely monitor tank levels, temperatures, and flow rates
- Easily integrate back-end business systems with inventory, usage, and payments
- Enhance perimeter security with more inexpensive cameras and motion sensors
- Continuously measure soil, water, and air quality for leaks or emissions
- Monitor tank and pipe corrosion, and pump vibration, allowing repairs to be made in advance of impending failure
- Remotely operate transfer pumps and valves from a variety of locations using applications on government smartphones

However, imagine the havoc that a hack into this IoT tank farm could cause if threats are not addressed and risks mitigated. Tank levels could be misreported; monitoring could be disabled; and malicious operators could dump fuel - perhaps creating fires and explosions. An appropriate level of IoT security must be attained before the highest risk portions of such implementation would be warranted. DoD policy should both promote the benefits and ensure the mitigation of risks inherent in IoT.

Additional scenarios can be found in Appendix C.

V. Recommended Approach and Policy Actions

The DoD must properly govern and manage deploying IoT. This must begin with identifying characteristics of the problem to help shape resultant actions. Appendix D provides examples of some questions that can help DoD frame the problem.

It is key to have set policy tenets to help DoD improve policies that minimize the risk and maximize the benefit of IoT. Implementing revised policies based on these tenets will enable better and wider situational awareness of the use of IoT across the Department. At a basic level, policies must prepare the Department to react to security incidents, and ensure appropriate diligence with regard to security, integrity, confidentiality, and safety of IoT devices and solutions during procurement and deployment processes. A summary of key tenets is listed here:

IoT must be proactively managed and governed for DoD to meet threats and realize benefits.

- Each IoT acquisition must be supported by a business case
- Each IoT implementation and associated data streams must be supported by a security and privacy risk analysis
- IoT data must be encrypted at every point, where costs are commensurate with risk and value
- IoT networks must be monitored to identify anomalous traffic and emergent threats
- IoT data will be fed to analytics capabilities and cross-correlated to get the maximum utility from the information
- IoT devices and Logical Processing Area Networks (LPANS) must be connected to as small a controlled network segment as feasible, rather than having unfettered access to the full IP network
- IoT devices must only be acquired through approved contract vehicles
- IoT device supply chains from factory to installation must be actively managed

- Network operations must be able to verify the network identity of IoT devices, and track the provenance of the information they provide
- Network operations must be able to detect, isolate and remove unauthorized IoT devices
- USCYBERCOM must oversee the policy and processes related to acquiring, testing, and operating IoT networks, and for monitoring the implementation of these policies and processes to ensure a safe, security provision of the associated capabilities (whether connected to the NIPRNet, SIPRNet, or another network - such as facility control or building security or medical.)

Based on these tenets, recommendations for policy updates should reflect actions needed to exploit the opportunities and address the threats and vulnerabilities. These recommendations should incorporate the following guidances:

- Changes to DoD 5000 series and Defense Acquisition Guidebook
- Changes to DoD 8500 series Cybersecurity and Risk Management
- New DFARS contract clauses
- JIE Technical Guidance and Reference Architectures
- An IoT overlay for NIST guidance

VI. Conclusion

IoT vulnerabilities present a growing threat to the Department's mission, and to the safety and security of our personnel. At the same time, these technologies present significant opportunities to improve the efficiency and effectiveness of DoD's capabilities. The Department should take proactive action in developing and implementing policy to both manage the risks and reap the potential of these technologies.

VII. Next Steps

- Issue policy and guidance that establish responsibilities and controls
- Monitor the execution of responsibilities
- Monitor the effectiveness of controls

Appendices

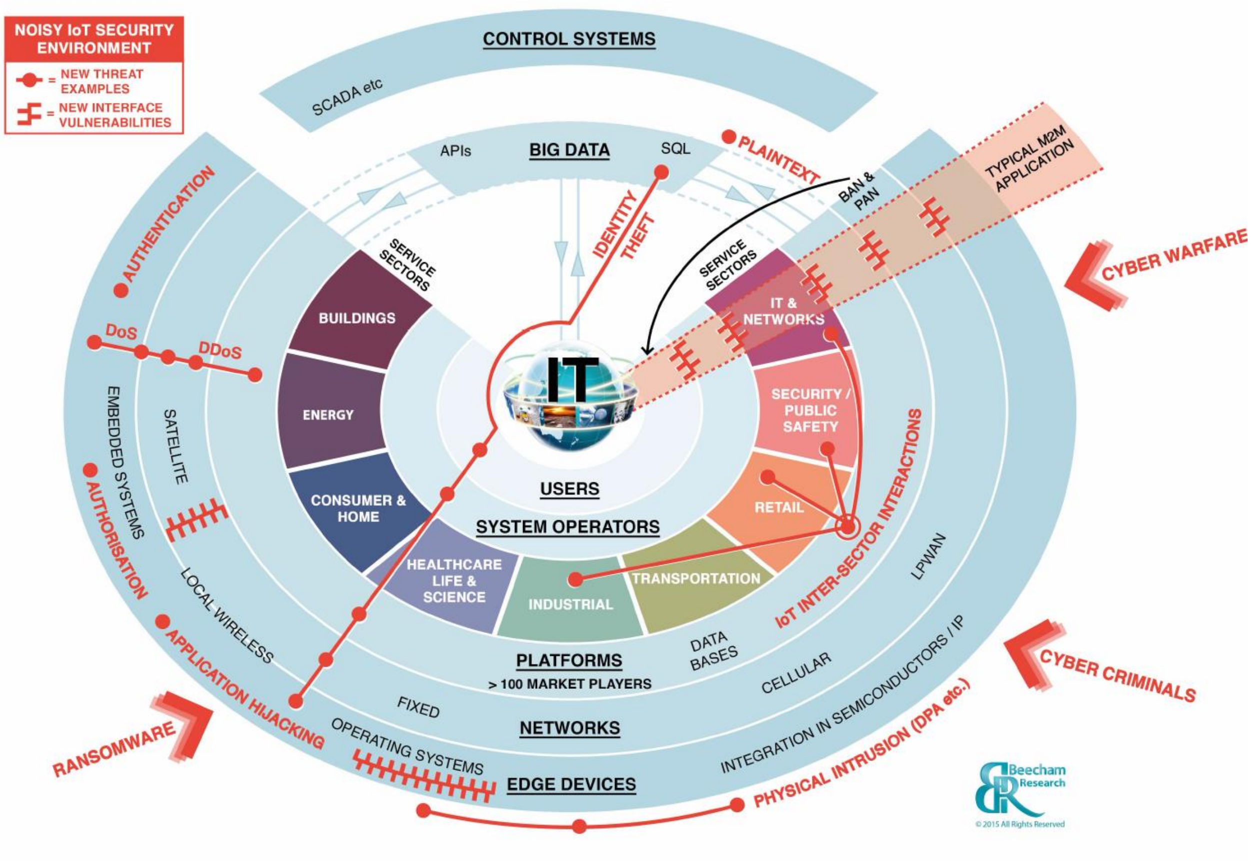
Appendix A. Internet of Things (IoT) As Variously Defined

This paper leverages the basic Internet of Things definition provided in the IEEE paper "Toward a Definition of Internet of Things (IoT)"[5] provided below. The Internet of Things consists of two foundational things:

1. The Internet itself
2. Semi-autonomous devices (the "things") that leverage inexpensive compute, networking, sensing and actuation capabilities in uniquely identified implementations to sense the physical world and act on it.

Such devices have the capability to connect to the Internet, being IP based, but may also be deployed in stand-alone IP networks that are not connected to the Internet. In addition, IoT includes the facilities that allow users and organizations to analyze and understand the data gathered and actions taken by the things.

Figure 4: Beecham Research[6] IoT Security Threat Map



Inexpensive, pervasive, highly capable edge devices create a new attack surface

[5] Ibid., footnote 2

[6] http://www.beechamresearch.com/download.aspx?id=43

As Figure 4 shows, the Internet of Things spans nearly every organization and function. Associated edge devices now expose a series of vulnerabilities exploited by all traditional threat vectors. These edge devices can be as simple (a smart light switch) or complex (industrial control system). They can be fixed in place (security camera), or mobile (smart watch or drone). They can have a focused purpose (thermostat), or be an embedded part of a general-purpose device (a car). Edge devices can support low-risk tasks like monitoring pollution, or high-risk tasks like controlling the delivery of medication to a patient. Ways in which these devices can be exploited is constantly evolving. The smart thermostat senses when you are not home and makes that information available to an intruder. A smart TV accepts voice commands and connects to the Internet, but also listens to a room and sends overheard conversations to the cloud. All can be controlled remotely and send their valuable data through the Internet.

The sections below highlight IoT characteristics and issues.

Things

The "things" in IoT may be looked at from a couple of perspectives. Kevin Ashton, the person who coined the term, said:

> "If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best."[7]

More recently and commonly, IoT "things" are viewed as devices that have internet access along with sensor and/or actuation or control mechanisms. These two views represent much the same point - "Things" are at the boundary of interaction between cyberspace and the real world—the cyber-physical interface.

A Deloitte paper, "Inside the Internet of Things," noted the following.

> "In 1991 Mark Weiser … described 'ubiquitous computing,' a world in which objects of all kinds could sense, communicate, analyze, and act or react to people and other machines autonomously, in a manner no more intrusive or noteworthy than how we currently turn on a light or open a tap."[8]

These functions can be distributed among the network of devices, or within a single device, and provide the basis for "things". The idea of connecting such things to the Internet provides the full concept of IoT.

IoT things have roots in both the mobile phone and embedded industrial control devices of the past. As smartphone makers dramatically drove down the cost of computational chips, sensors, and small radios, there was a move to standardize the architecture and networking of such control devices to allow more rapid, extensive, and inexpensive deployment of these sensing and control capabilities. Specialized radios and networking standards and approaches such as Zigbee and ZWave were developed and aimed at remote monitoring and control applications. Devices implementing one of these standards could be connected together, easily allowing information to

[7] "That 'Internet of Things' Thing," Kevin Ashton; RFID Journal; June 22, 2009

[8] "Inside the Internet of Things (IoT)," Jonathan Holdowsky, Monika Mahto, Michael E. Raynor, and Mark Cotteleer; Deloitte University Press; pulled July 2016 from: https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/technology/Inside%20The%20Internet%20Of%20Things.pdf

be gathered and control to be effected over aspects of the real, non-digital, world. Connecting them to the Internet has created both the greatest benefits and the greatest risks.

Internet

The internet provides a standardized means for end-to-end networking across multiple networks, often of disparate organizations and physical characterization. With common upper levels of networking stacks standardized on IP, overall Internet behavior is not determined by the technology of specific networks, but by the connected endpoints. An endpoint device that is connected by IP to a ZigBee thing can be connected to a web browser on a WiFi network that is many hops and thousands of miles away—delivering real-time information to the browser and real-time control over the thing. This Internet connectivity brings with it the same threats and vulnerabilities as are posed to traditional Internet usages and users.

Other Example Definitions

Below are a representative set of Internet of Things definitions.

IEEE definition in the IEEE paper "Toward a Definition of Internet of Things (IoT)"[9]:

1. IEEE provides *Small* and *Large* environment scenario definitions of IoT where the "actual distinguishing element between the Small environment scenario and the Large environment scenario is complexity".

Small Environment Scenario

"An IoT is a network that connects uniquely identifiable 'Things' to the Internet. The 'Things' have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the 'Thing' can be collected and the state of the 'Thing' can be changed from anywhere, anytime, by anything".

Large Environment Scenario

"Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration."

US Government definition taken from GSA's recent Alliant 2 RFP[10], seeking Leading Edge Technology experience from offerors:

1. The Internet of Things (IoT) is a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS) and the Internet.

[9] Ibid., footnote 2.

[10] *ALLIANT 2 GWAC UNRESTRICTED PROCUREMENT: Official Request for Proposal # QTA0016JCA0003*; John Cavadias, Procuring Contracting Officer; U.S. General Services Administration, Federal Acquisition Service 24 June 2016

A “thing”, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low—or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network. So far, the Internet of Things has been most closely associated with machine-to-machine (M2M) communication in manufacturing and power, oil and gas utilities. Often, products built with M2M communication capabilities are referred to as being smart (smart label, smart meter, smart grid sensor).

Definitions gleaned from various sources:

1. “The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data. "If one thing can prevent the Internet of things from transforming the way we live and work, it will be a breakdown in security."“
   - Oxford Dictionaries · © Oxford University Press

2. “The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data.”
   - Wikipedia

3. “The term “Internet of Things” isn’t new. Almost 20 years ago, MIT professors described a world where “things” (devices or sensors) are connected and able to share data. Data coming from these devices and sensors provides business insights that were previously out of reach. The invaluable insights enabled by harnessing and analyzing the data from these connected devices are what the Internet of Things is all about.”
   - Microsoft

4. “The Internet of Things connects devices such as everyday consumer objects and industrial equipment onto the network, enabling information gathering and management of these devices via software to increase efficiency, enable new services, or achieve other health, safety, or environmental benefits.”
   - Goldman Sachs

5. “The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.”
   - WhatIs.com

6. “The Internet of Things (IoT) is a computing concept that describes a future where everyday physical objects will be connected to the Internet and be able to identify themselves to other devices. The term is closely identified with RFID as the method of communication, although it also may include other sensor technologies, wireless technologies or QR codes.”
   - Techopedia

7. “The Internet of Things (IoT) refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.”
   - Webopedia

8. “In simplest terms- the ability to turn any THING (a good/ object/ machine/ appliance/ building/ animal/ plant...) into a smart object. This smart object will in turn be able to connect, monitor, manage, control, search and more without the necessity for human intervention. This basic definition can then be implemented in endless applications where imagination is the only limit. Whether it be a refrigerator that tells your smartphone that you're out of milk/a hearing aid device that alerts you 2 hours before your battery is about to run out/a home thermostat that detects your car is 10 minutes away and turns on/a plant that lights up when it's time to be watered...”
   - Mor Rahimi, Quora.com

9. “A network comprised of physical objects capable of gathering and sharing electronic information. The Internet of Things includes a wide variety of “smart” devices, from industrial machines that transmit data about the production process to sensors that track information about the human body. Often, these devices use Internet Protocol (IP), the same protocol that identifies computers over the world wide web and allows them to communicate with one another.”
   - Investopedia

10. “Sensors and actuators embedded in physical objects are linked through wired and wireless networks”
   - iot-analytics

11. “The Internet of Things represents the idea that ordinary objects—from thermostats and shoes to cars and lamp posts—will be embedded with sensors and connected to the Internet.”
   - Center for Data Innovation

12. “The Internet of Things, commonly abbreviated "IoT," is an umbrella term that refers to anything connected to the Internet. It includes traditional computing devices, such as laptops, tablets, and smartphones, but also includes a growing list of other devices that have recently become Internet enabled.”
   - TechTerms.com

IEEE paper “Toward a Definition of Internet of Things (IoT)[11]:

International Telecommunication Union (ITU) endorses the definition of IoT as a network that is: “Available anywhere, anytime, by anything and anyone.”

CASAGRAS’ definition of IoT (CASAGRAS, “Final Report,” 2009):
“A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability.”

Cluster of European Research Projects-IoT (CERP-IoT) project states:
“Internet of Things (IoT) is an integrated part of Future Internet and could be defined as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and

[11] Ibid., footnote 2

virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.”

The Internet of Things European Research Cluster (IERC) definition states that IoT is (IERC, “Internet of Things,” 2014):
"A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual ‘things’ have identities, physical attributes and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network."

Internet Connected Objects for Reconfigurable Ecosystems (iCore):
“Our world is getting more and more connected. In the near future not only people will be connected through the Internet, but Internet connectivity will also be brought to billions of tangible objects, creating the Internet of Things (IoT).”

Appendix B. Risks and Benefits of IoT

Threats and Associated Risks

Many IoT issues arise specifically from the ability to access and control the various things from the Internet, potentially by anyone anywhere on the planet. As with more typical cyber warfare situations involving our personal and organizational computing, when connected to the Internet, the enemy can be anywhere.

> "Many types of attacks have been around for a very long time. What's new is the scale and relative simplicity of possible IoT attacks. There are millions of devices that are a potential victim to traditional style cyber attacks, but on a much larger scale and often with limited, if any protection."[12]

This may include things not expected to be part of the IoT, as there is no identification of Internet-connected features or capabilities. In other words, malicious Internet capabilities can be embedded in mass-market "dumb" products. The BBC published this report:

> *Cyber criminals are planting chips in electric irons and kettles to launch spam attacks, reports in Russia suggest. State-owned channel Rossiya 24 even showed footage of a technician opening up an iron included in a batch of Chinese imports to find a "spy chip" with what he called "a little microphone". Its correspondent said the hidden devices were mostly being used to spread viruses, by connecting to any computer within a 200m (656ft) radius using unprotected WiFi networks. Other products found to have rogue components reportedly included mobile phones and car dashboard cameras. The report quoted one customs brokerage professional as saying the hidden chips had been used to infiltrate company networks, sending out spam without administrators' knowledge. News agency Rosbalt reports that while the latest delivery of appliances was rejected by officials, more than 30 devices had already been sent to retailers in St Petersburg.*[13]

While some IoT threats are described below, a more extensive list and discussion can be found in the Cloud Security Alliance's paper on security for IoT.[14] Many IoT areas overlap with other security, information assurance, and supply chain protection work in industry and DoD.

Expanded Attack Surface: The number and relative simplicity of IoT devices greatly expands the attack surface of the Internet. Attackers often reverse engineer embedded software in a device to create counterfeit products, or locate software vulnerabilities that they then can exploit to steal sensitive data, or to tamper with the device for sabotage and espionage purposes. An attacker only needs one compromised device among thousands to gain network access—and they may not even need to do that. Compromised devices can provide a false picture of the world to decision makers and war fighters. Attackers may also directly subvert control of a device. Recent attacks on embedded networks in cars have shown that control can be removed from the driver. While work is being done to build in security to the lower level network protocols, such as ZigBee, the more limited compute capability of IoT devices means that they cannot implement the more powerful and sophisticated defense mechanisms that have become widely deployed on traditional servers and end-user computers.

[12] GlobalSign Blog; April 29, 2016

[13] "Russia: Hidden Chips 'Launch Spam Attacks from Irons,'" BBC News, *News from Elsewhere*; October 28, 2013; http://www.bbc.com/news/blogs-news-from-elsewhere-24707337

[14] "Security Guidance for Early Adopters of the Internet of Things," Cloud Security Alliance Mobile Working Group; April 2015; https://cloudsecurityalliance.org/research/surveys/

Attack Deployment – BotNets: BotNets are large collections of compromised computers that are controlled by malicious actors over the network. With potentially billions of IoT devices deployed - many sharing the same design and implementation, BotNets constructed from compromised IoT devices and used to mount distributed denial of service (DDOS) or massive spam campaigns become possible. BotNets consist of a wide variety of devices, including compromised home wireless routers, smart TVs, or even smart refrigerators. The IoT provides many more potential participants in such botnets, and many more directions from which attacks can originate.

Expanded Aggregation of Information: Aggregation of information from different sources creates the possibility that, while the individual pieces and sources of the information may be unclassified, the combination or aggregation may synergistically create information that we would not want an adversary to have. Aggregated information could allow adversaries to make inferences about capabilities and deployments that we are otherwise protecting. The ability to obtain many dimensions of information about the same assets through different IoT capabilities— each feeding large amounts of information into advanced big data analytics—greatly increases the potential benefit of the combined information. This makes the resulting dataset a bigger and more valuable target for attackers looking for high value information to exfiltrate while making it easier to find what they want in a single place. They are much more likely to get a full picture if they can compromise a single high-value source, rather than having to strike many sources and perform the aggregation themselves.

Vulnerability of Manufacturing Supply Base: With much of industry using IoT and related industrial control devices, there is a significant potential for such devices to be compromised, and in turn compromise critical manufacturing capability. As Stuxnet compromised Iran's industrial control equipment, which in turn ruined their centrifuges, manufacturing controls that have been compromised can in turn affect the manufacturing of weapons systems and related items. This can have significant impact on national security. This also provides another vector for loss of intellectual property, as compromised devices forward collected information, or highjacked cameras transmit images of unknowing owners and the like.

Provenance - Subversion of the Things Themselves: It is not just that IoT devices can be compromised; they may also be counterfeited or subverted during their manufacture. In this way, it is not necessary for an attacker to find and exploit a vulnerability. The door is unlocked in advance. The firmware installed on the device may include malware that lets the attacker in, or may mount the attack itself. Further, counterfeit versions of chips such as the CPU providing the IoT device's compute power may include backdoors that allow an attacker to defeat encryption and other controls that the real device is designed to use for protection. Uncertainty of provenance, or loss in chain of custody of critical devices, allow malicious actors to insert such counterfeit devices into the supply chain. With them come all the threats of hacked devices noted in the previous paragraph, but much easier for the attacker to realize.

Ownership: One emerging trend - from Zipcars to mobile phones, and now to IoT devices - is the shift from device ownership to device licensing (and back again with market cycles), sometimes called "Product as a Service". This is discussed at length in the article, "Possessing Mobile Devices,"[15] which discusses the security risks when users are locked out of administrative capabilities on their own devices. There are several risks associated with this shift. First, users may be dropped from getting needed security patches if their device goes past a certain age or release. (While this may happen in any case, as with Windows XP, unlocked control at least provides the possibility of "do it yourself" fixes, as with open source software.) Second, users may not have the ability to properly monitor software components installed on their device due to such restrictions.

[15] "Possessing Mobile Devices," *Computing Edge*; A.A. Adams; February 2016, pp. 17-23; IEEE Computer Society.

Third, such devices now often have a dependency on a cloud capability provided by the vendor, not just for updates and security patches, but for normal operation, as is the case with Nest home automation devices such as their thermostat. It should be noted that this is becoming true for more traditional computing devices such as servers and PCs, where traditional network services such as directories and I&A are now provided in the cloud by third parties, as with Azure AD or Facebook and Google single sign-on services. Should the cloud capability go away, the device can no longer function. How this movement may affect enterprise IoT and traditional devices is not yet clear.

Benefits

While presenting significant risks, as do all networked technologies, IoT also promises to bring many benefits to DoD, including better management of DoD assets, improved readiness, and generally the ability to do more with less.

Better Management of DoD Assets: Assets can be tracked and monitored in real time. Information, both item specific and in aggregate can be readily available to those who need it anywhere in the DoD.

IoT Unique Identification of Things: The IoT's ability to uniquely identify the things in Internet of Things can help DoD achieve the unique identification goals the Department has long sought.

Improved Readiness: Knowing the status of materiel and weapons systems in real time allows DoD to be ready to respond to emergent threats in a more rapid and agile fashion.

Ability to do More with Less: The low cost and pervasive nature of IoT allows many tracking, inventory, control, and data gathering activities to be accomplished with much less personnel labor involved, and with significantly reduced intermediate processing and handling of information.

IoT:

Promises greatly improved situational awareness and ability to do more with less.

Appendix C. IoT Case Studies

Case Study: DoD Fuel Depot

IoT Uses and Potential Benefits

Imagine the supply chain management benefits of an extensive IoT implementation to improve visibility, physical security, and even automate portions of the logistics process. For example, at a DoD fuel depot, tank levels, temperatures, and flow rates could be inexpensively and precisely monitored. Inventory, usage, and payments could be easily integrated with the back-end business systems. Perimeter security could be enhanced with more inexpensive cameras and motion sensors. Soil, water, and air quality could be continuously measured for leaks or emissions. Tank and pipe corrosion and pump vibration could be monitored to enable fixes before impending failure. Transfer pumps and valves could be remotely operated from a variety of locations using apps on government smartphones, keeping operators far away from the dangers of climbing tanks and potential fuel-related hazards.

Threats and Vulnerabilities

Imagine the havoc that could be caused by a malicious actor hacking into this IoT tank farm. If the typical IoT vulnerabilities are not addressed, tank levels could be misreported, monitoring could be disabled, and malicious operators could dump fuel (perhaps even causing fires and explosions).

Recommendation

Clearly a high level of IoT security must be attained before the highest risk portions of such an IoT implementation would be warranted. Policy and processes should be implemented to ensure that the IoT devices are purchases from trustworthy sources meeting defined standards, the data streams are encrypted, and that only authorized personnel can access the IoT network.

Case Study: DoD Smart Building

IoT Uses and Potential Benefits

To meet our green building goals and to reduce costs, we have instrumented our buildings with thousands of network-connected sensors, from lighting to heating and air conditioning. These devices reduce energy and water use, monitor and control access, and enable HVAC (heating, ventilation, and air conditioning) systems to work with fire and smoke detection devices to shut off and fans furnaces during emergencies. Sensors can make building systems (from HVAC to elevators) more reliable, by predicting maintenance needs. Synthesizing the data between IoT sensing systems could enable safety improvements, such locating people in an emergency, and pinpointing hazards such as smoke or an active shooter. IoT data can also enable further efficiencies in the dynamic allocation of conference rooms and office space, location of open parking slots, vending of office supplies, delivery of packages, and even ordering lunch from the cafeteria.

Threats and Vulnerabilities

A malicious actor hacking into building could turn off the power, flush all the toilets at once, or trigger the fire alarms. More significantly, they could gather OPSEC related to which people were present or organizations were working overtime. Each sensor represents a potential vulnerability into the attack surface of the associated network, and if that network is not sufficiently isolated from other functions broader vulnerabilities would be created. Counterfeit could potentially look and listen into sensitive discussions, and even change their characteristics as these devices communicate over the Internet.

Recommendation

Prioritize addressing the highest risk vulnerabilities already installed in DoD buildings, such as ensuring that the building networks are segmented and have the required security accreditations. Implement policies and processes (and communicate these changes broadly) to ensure that the installations community follows the same cybersecurity rules as the IT community.

Case Study: Executive Vehicle

IoT Uses and Potential Benefits

We are increasingly familiar with the advantages of mobile internet connected cars, with onboard intelligence—software that increasingly controls more aspects of the vehicle behavior, from the traditional engine controls, braking and steering, to the value-added capabilities to make one's phone hands-free when in the car and take voice commands to control navigation, the radio, and music playlists. With the addition of cellular internet connectivity, one can ask the monitoring company to do anything from provide directions when you ask, opening your doors when you have locked your keys in the car, to disabling your vehicle when stolen. To assure safety and rapid response in case of an accident, the car is continuously monitored via the Internet.

Threats and Vulnerabilities

Consider the security implications of a malicious actor accessing these features in the car of one of our senior executives: listening to conversations, disabling the car during an attack, and unlocking the doors to abduct the passengers. Demonstrations have been made of hacking a car's software controls to take over the steering and braking of the car from the driver, showing that such concerns are far from theoretical.

Recommendation

Prioritize addressing the highest risk vulnerabilities already installed in DoD vehicles, such as ensuring that the executive vehicles do not have security flaws that endanger our leadership. Implement policies and processes (and communicate these changes broadly) to ensure that the vehicle fleet management community follows the same cybersecurity rules as the IT community.

Case Study: Battlefield Situational Awareness

IoT Uses and Potential Benefits

The very small size and low cost of sensing and communications devices makes them ideal for deploying in low power networks in forward situations to provide warfighters with enhanced situational awareness, giving them real power to see around corners and across hostile terrain. Connected into communications capabilities built into their uniforms and armor, these capabilities greatly augment their ability to execute their missions and effectively engage and dominate the enemy in difficult environments. With the addition of internet capability, real time situational information can be relayed to command and support facilities remote from the battlefield, allowing advice and additional big picture information to be sent back to the warfighters, again increasing their effectiveness.

Threats and Vulnerabilities

Imagine that the enemy takes advantage of vulnerabilities in the devices or networking, hacking into or compromising these devices and the information they supply. This may allow the enemy to provide false information to the warfighter and the supporting remote organizations, making decisions and actions and actions they take either unreliable or dangerous. At the same time, they can also see the information that should have gone to the warfighter, giving them the advantage of the situational awareness and further allowing them to take advantage of the confusion they have created through the injection of false information into the warfighter decision making.

Recommendation

Prioritize addressing the highest risk vulnerabilities already installed in mission systems, such as ensuring that the information is encrypted where needed. Implement policies and processes (and communicate these changes broadly) to ensure supply chain risk management of a broader array of potential devices that could be deployed with our troops.

Appendix D. Questions to Ask in Preparation for IoT

The first thing organizations should do is be prepared both to deploy IoT, and to properly govern and manage it. As industry working groups begin to apply security standards to IoT devices, DoD can work to drive some of these standards, by requiring protective features during acquisition of the devices. The advisory company EY (formerly Ernst & Young) prepared a list of questions in an information paper on IoT security[16] that organizations should ask when preparing to take action on IoT. Many of these are worth repeating here, to be shaped with a DoD context:

- What IoT capabilities does your organization have today?
- Can you harness the complementary insights of both service and IT leaders?
- Have you identified major IoT opportunity areas that link with your vision and strategy?
- Can you build an "IoT culture" around the possibilities of connecting the unconnected?
- How will IoT change the basis of competition? *(the conduct of warfare)*
- How will you delight customers as everything gets connected? *(satisfy relevant stakeholders)*
- Do your business plans reflect the full potential of IoT?
- Are your technology investments aligned with opportunities and threats?
- How will IoT improve your agility?
- Do you have the capabilities to deliver value from IoT?
- What is your accountability and governance structure/ model for IoT execution?
- How are the risks associated with IoT being addressed?
- How will you communicate about IoT to stakeholders?

[16] "Cybersecurity and the Internet of Things," *Insights on Governance, Risk and Compliance* Series; EYG no. AU2979; March 2015