Internet of Things - A New Security Challenge

Lieutenant General Davinder Kumar, PVSM, VSM and Bar (Retd)@

Introduction

The Internet of Things (IoT) is all about intelligent machines connecting to people or to each other. Such connected machines can be remotely controlled or they can collect and communicate valuable data. The word IoT was coined by British entrepreneur Kevin Ashton in 1999.1 But the concept was discussed as early as 1982 when a coke machine at Carnegie Mellon University became the first internet connected appliance. IoT implies convergence of people, processes, data and things which is bringing about unprecedented disruption.2 The common elements that hold it together are connectivity, sensors and processing.

Definition

The IoT can be defined as a, "network of unique physical things that contain embedded technology to communicate, sense, analyse and/or interact with their internal or external environment".

So what are these "things" or "machines"?3 The answer is just about anything. They could be household appliances, irrigation sensors in a rice field, a cutting machine on a factory floor or an aircraft engine. Right now, companies are in the process of giving machines the intelligence and connectivity they need to participate in this connected world. An industry that has previously been known as the "Embedded Industry" is now referred to as the "Internet of Things Industry" and it is growing at a phenomenal pace. After surpassing the human population in 2011, internet connected devices are expected to number between 26 billion and 50 billion globally by 20204, that is 4 to 8 connected things for each person in the world. These devices, which in the past, could only be thought to be mobile phones, laptop and desktop computers now include almost anything like ATM machines, gas pipelines, street lights, factory automation, mining, energy, transportation vehicles, health monitoring devices and even the soil used for agriculture.

IoT in Defence Industry

In the defence industry, the concept of the IoT has been around for some time. The planes, vehicles, ships and weapons systems found in the connected battlefield were networked and sharing tactical data among themselves well before the IoT gained momentum in commercial markets. with the growth of autonomous vehicles, this connected battlefield is ever-expanding and reaching into more applications and machines. Embedded rugged computers are providing intelligence for military machines large and small. Sensor processors are helping to gather and process large amounts of data such as high definition video. Network solutions — rugged routers and switches provide the connectivity infrastructure and high-performance embedded computers process the big data generated by the connected battlefield.

Now that the defence forces have experienced the benefit of the connected battlefield and beyond, they are aiming to connect even more machines. The concept of connecting every battlefield asset, whether large or small, human or machine has taken hold.5 This has impacted the civil industry which is now giving increased emphasis on Size, Weight and Power (SWaP) and miniaturising for the Commercial Off The Shelf (COTS) products for the military. It has also led to an increased emphasis on security — segregating classified and unclassified data, anti-tamper and information assurance.

Software development for speedy information processing and security are critical areas. There is a wide scope of employing the software developed for industrial internet to be used for defence applications with little modification. For instance, software that is used to analyse and optimise the operation of diesel engines in large mining vehicles could be applied to armoured military vehicles. Or the tools and software that collect data from sensors installed in an aircraft engine and can notify maintenance crews in real time are directly applicable to military aircraft. Even the software that rail transport companies use to optimise the operation of locomotives — saving them millions of dollars in energy costs —could be applied to the operation of unmanned submarines, allowing them to execute longer missions further and further from port.

It is important to note that IoT will work in conjunction with other technologies like analytics, data protection, cyber security and data governance.6 However, IoT should not be viewed only as a technology initiative. It is a tool for increasing efficiency, reducing cost, optimising resource utilisation and increasing customer satisfaction. It helps in establishing real time co-relation of events.

Opportunities and Challenges

IoT presents both a large opportunity and many challenges as we try to integrate it into overall industrial and military capabilities and as it matures and our connected world grows. Some of the challenges are :-7

(a) **Myriad of Technologies, Networks and Protocols.** Starting with sensor equipped things themselves, there are a wide variety of situation specific technologies, networks, protocols and data formats that must be chosen, managed and integrated.

(b) **Distributed Business Data, Analytics and Logic.** Sensors, devices and gateways are often capable of local data filtering and analysis. They can also store business logic to enable quick response to various situations, such as a safety issue. The IoT software platforms would have to manage things and gateways,

analyse and manage sensor data and integrate with enterprise systems. The challenge is that business data, analytics and logic are resident outside of the core enterprise applications and processes.

(c) **New Security Risks**. IoT brings with it new security challenges that span customer premises, the internet and the enterprise. It is critical to ensure that the connected devices and the data they collect are tamper-resistant and tamper-evident. One has to select which identity, authentication and encryption technologies will work for sensors and gateways. It is absolutely imperative that the chain of custody remains secure all the way through cloud services and back to the enterprise applications.

(d) **New Network Demands.** The network administrators and managers have to cater for a surge and variety of devices that would connect to the network nodes. Some devices may stream data continuously, while the others need low latency and high quality of service for quick responses to critical events.

(e) **Vast Quantities of Time-series Data.** Analysis of huge quantity of time-series data would require new generation of analytics technology to decide how best to transmit, capture, store and retrieve data.

While the efficiencies and insights gained through the deployment of this massive interconnected system will bring new benefits, it could also bring new risks. Experience shows us that when everything is connected, everything is vulnerable. As cyber threats become more sophisticated and aggressive in this expanding IoT environment, four areas of concern will rise in importance.8 All organisations should, therefore :-

(a) **Make sure information is reliable and systems are resilient.** With the large amount of data generated by the IoT, a key question will be: “How do I know the data generated by this system is reliable?” Chief information security officers (CISOs) will have to find answers within their information assurance strategies.

(b) **Keep pace with technology.** With each new device that enters the IoT domain, new vulnerabilities and threats are introduced. A cyber adversary will not only have this new target with its vulnerabilities to exploit, but he will also have a new path from which to attack the other entities on your network. Security organisations must have a lab and do their research on new devices to understand, not just how to use a device, but also what is embedded in the device; what data is generated and transmitted; where does the device transmit its data; and what connections will it accept from other devices in an environment, among a host of other concerns.

(c) **Focus on the insider threat.** The IoT is about connections among devices, the masses of data generated by sensors, cloud processing and storage, and automated actuators. Threats to this environment may be slowed by perimeter defences, but the most dangerous threat is the one inside – where the most serious damage can be done. The Target Corporation, WikiLeaks, and Snowden breaches are evidence of this damage. The Target Corporation is a typical example of insider threat in the IoT environment, whereby adversaries were able to penetrate the point-of-sale (POS) devices by first entering through a heating, ventilation, and air conditioning controller! As a result, banks and credit unions lost more than US $200 million, according to the Consumer Bankers Association. In this new environment, it’s critical for agencies to have insider-focused security and continuous monitoring solutions that can detect anomalies, unauthorised privileged user activity, and determine when information has been accessed inappropriately. These must be behavioural analytics, not just simple rules and policies.

(d) **Embrace (big and community) data analytics to minimise cyber threats.** The IoT will generate more data as new devices and systems are added to the ecosystem. Innovations in analytics will drive more than efficient processes but also new ways to detect threats. For example, successful data analytics programmes apply algorithms that automatically identify areas of cyber security interest in large volumes of data. In this new ecosystem, analytics will hold the key to predicting threats before they happen.

The IoT has moved from the military to everyday life, allowing us to create and process more data than ever before on everything from the products we buy, to critical power and water, to how we drive on the highway. Making sure this system of systems is secure will help us ensure the IoT delivers its promise of convenience and efficiency.

Network and Security Architecture

Connectivity is at the heart of IoT capability. It serves dual purpose. First, it allows information to be exchanged between the product and its operating environment, its maker its user and other products and systems. Second, connectivity enables some functions of the product to exist outside the physical device. The opportunity with IoT comes from its ability to link components via an intelligent, secure and programmable network in which physical objects like vehicles, weapons and unmanned vehicles are connected to secure networks to create information dominance.

Connectivity is also the most significant vulnerability both in civil and military applications of IoT. Many nations have developed their warfare doctrines and capabilities to attack and degrade this connectivity provided by networks. Consequently, the architecture of IoT must ensure complete security of networks and the systems connected to them as an integral part of design and implementation. This presents a very serious and a major challenge.

An integrated and secure architecture for IoT creates interconnected physical and virtual environments that combine IoT devices with secure virtualisation, mobility, unified communications and other advanced technologies. Networks and system integration must cater for unification of computing, storage and networks with sensors, devices

and collaborative applications

The proliferation of unstructured imagery and video data from a variety of sensors is creating new capture, storage, computing and exploitation opportunities. To accommodate an influx of new devices without sacrificing security, they must be managed as part of an integrated architecture for IoT. The framework should preferably leverage commercial products which are not only less expensive and technologically current but are easier to field, manage and support.

Security concerns surrounding IoT will be particularly important for military operators connecting to classified networks. Hence, network-aware intelligence and end-to-end physical security for video and all networked sensors must be at the heart of any military IoT solution.

Architecture suited to support IoT will include compute, storage and virtualisation assets in the data centre. It will also include secure network fabric for connectivity, voice and video-enabled secure mobile infrastructure and battlefield sensors. Virtualisation combined with advanced security from the network to application levels are essential to allowing highly secure access to sensitive and classified information on multiple networks while lowering the risk of vulnerabilities. When properly designed and deployed, IoT will help to realise the vision of net-centric warfare while providing technology advantage to our connected soldiers and systems.

IoT in the Indian Context

At the national level, we have been using IoT for some time in manufacturing, health care and in some cases for monitoring and maintenance of power supply and so on. Most of these are connected to private networks and hence can be managed comparatively easily. Digital India and Smart City projects would see large scale deployment of IoT and connectivity with public networks. This presents an unprecedented challenge with regard to technology, products, skills, cyber security and privacy of citizens. IoT adds another dimension to cyber security and demands enhanced capabilities in encryption, software development, networks, and system integration and so on.

The Government of India has released a draft IoT Policy in April 2015.9 The key stakeholders in the Iot initiatives would be the citizens, the government, academia and the industry. Participation and collaboration of each of the stakeholder at an appropriate stage is essential. At this juncture, we require policies for promotion of IoT, selection of the essential domains and emphasis on building answers for ‘What Data will Service the Citizens’. IoT products and solutions should clearly strategise with a simple goal of ‘Value Up’ and ‘Cost Down’.

The Policy framework of the IoT Policy has been proposed to be implemented via a multi-pillar approach. The approach comprises of five vertical pillars (Demonstration Centres, Capacity Building & Incubation, R&D and Innovation, Incentives and Engagements, Human Resource Development) and two horizontal supports (Standards & Governance structure).

The Governance structure would consist of :-10

(a) **A legal framework.** IoT will lead to new systems/products/services where machine will take decisions based on certain available data. Legal frameworks will be created for issues that might arise due to IoT related product/systems/services.

(b) **Advisory Committee.** To set up a High Level Advisory Committee including representatives from the Government, industry and academia for providing ongoing guidance in the emerging area of IoT.

(c) **Governance Committee.** To set up a High Powered Governance Committee for different application domains to be chaired by Secretary of respective Ministry/Department including representatives from Government, industry and academia governing all IoT initiatives, projects and their progress against planned timelines.

(d) **Programme Management Unit.** Provide ongoing support in identification, implementation, monitoring of IoT initiatives and conduct of periodic review of policies.

Based on the above strategies and structure, India will have to invest in capability and capacity building to include technologies for setting up smart cities, Human Resource Development with necessary skills, R&D, innovation and formulation of standards. To ensure security of our assets, these technologies will have to be developed indigenously. Sensors, gateways, analytics, data centres, encryption, networks and connectivity will have to be fully secure with trusted software, products, chips and components.

IoT and the Indian Armed Forces

Employment of IoT in the Indian Armed Forces is very limited at present. With the doctrine stipulating capability build up for Network Centric Warfare, planned large scale induction of unmanned and autonomous platforms, missiles, robotics, smart health and smart logistics, a lot needs to be done for capacity building in IoT. Besides what has been mentioned above, the emphasis would have to be on secure and agile networks supported by highly qualified human resource in big data and analytics. While technology standards for these networks have yet to evolve fully, some experts feel that adoption of Internet Protocols (IP) with its latest version of IPv6 would be a recipe for disaster from security and vulnerabilities points of view.11 We will have to have our own standards and protocols and resist the technology push by the developed nations.

Armed Forces must work closely with the civil industry, R&D establishments and academia and exploit COTS products/technology. “Make in India” drive must concentrate on joint R&D, development of secure software and manufacture of secure products based on trusted chips produced in India. Concurrently, the Armed Forces must examine employment of IoT as part of its doctrine for a digital battlefield and concentrate on establishing necessary infrastructure, organisation, skilled manpower and training. The time is running out and we need to act now.

Endnotes

1 Monika Mitra, Internet of Things for Dummies, ET July 2015/Wikipedia-Internet of Things.
2 VC Gopalaratnam, Making Smart Tech Work for India, ET July 2015.
3 Christopher Lever, The Military Internet of Things, GE Intelligent Platforms.
4 Cisco/Wikipedia-Internet of Things.
5 Internet of Things for Defence—Wind River.(www.windriver.com/.../wind-river_%20IoT-in-Defense_white-paper.pdf).
6 Larry Payne, vice president at Cisco Federal.
7 Five IoT Era Challenges for CIOs by Frank Gillett, Vice President and Principal Analyst at Forrester Research.
8 Four Security Tips from Military: Michael K. Daly, CTO, Cybersecurity and Special Missions of Raytheon Intelligence, Information and Services. www.darkreading.com/mobile/internet-of-things...military/.../1297546
9 Draft Policy on Internet of Things-2015. Ministry of Communications and Information Technology, Government of India.
10 Ibid.
11 Arvind Tiwary, Indus Entrepreneurs quoted by Hari Pulakkat in ET, July 2015.

@Lieutenant General Davinder Kumar, PVSM, VSM and Bar (Retd) was commissioned in the Corps of Signals in December 1965 and retired as Signal Officer-in-Chief in September 2006. Post retirement he has worked in the Corporate Sector, contributed extensively in professional journals and has been a member of National IT Task Force and number of Committees.

Journal of the United Service Institution of India, Vol. CXLV, No. 602, October-December 2015.