Rediffusion/Edelman

# Coverage report

# The Economic Times Technology (ET Tech)

| | |
|---|---|
| Publication Name | ET Tech |
| Date | 30th November, 2016 |
| Edition | Online |
| Headline | How tech giants & startups tackle IoT security challenge |

# How tech giants & startups tackle IoT security challenge

An in depth look at how legacy tech vendors and new age startups are solving IoT security issues

Imagine a future where attacks on IoT infrastructure could bring down power supplies of entire cities, tamper the manufacturing process in a factory, stop a Tesla in the middle of the highway, overflow tanks in an oil rig, shut down a ventilator in ICU or even tamper cardiac implants.

While this might be the future nobody wants, there are already signs of heavy duty IoT devices based attacks. Take for example when few months ago, 500,000 IoT devices including the likes of video cameras and digital video recorders connected to the internet were compromised by 'Mirai' malware to create a huge network of botnets which hacked the servers of DYN, a web service provider resulting in disruption in services of popular sites like Twitter, Netflix and Amazon alike.

Not only this, a HP labs study of 10 popular IoT devices (thermostat, garage door opener, smart door lock etc) found an average of 25 vulnerabilities on each device. The report even pointed out that 70% of such devices are vulnerable.

Most of the devices are plug-n-play, sell-and-forget. Botnet harvesters identify firmware vulnerability and proceed to locate and exploit all the devices deploying the same firmware and with analysts firms like Gartner predicting the availability of 20.8 billion connected devices by 2020 cyber security becomes extremely critical for IoT devices across consumer and enterprise platforms.

Considering how big the IoT market is going to become, legacy vendors and startups in particular have been bullish in creating secure IoT devices and solutions.

**Legacy Vendor's IoT Push**

Arti Anant Pande, Lead Technologist of Software design and consulting company ThoughtWorks talks about their technology radar which encourages teams to incorporate penetration testing into their continuous delivery pipeline and consider threat modelling to better understand their security needs. The radar also advices teams against anti-patterns that are likely to give them a false sense of security.

They are exploring hybrid, scalable, practical solutions that can handle security requirements of IoT devices throughout their lifetime which will become useful when majority of such devices are owned by end users with none or moderate technical skills.

While Manish Gupta, Director & General Manager, Infrastructure Solutions Group, Dell EMC points out that prior to implementation of an IoT device or solution at a customer's end, they review the end customers security and strengthen their IT security and management practices to prepare them for additional risk exposure following which they establish and defend the functional integrity at the edge with smarter architectural components such as a IoT gateway and firewall to enable protection from risks of less capable connected devices and legacy equipment.

Legacy vendor, Microsoft even has a Windows'10 IoT OS for devices at end points which enable collection and streaming of real time data but in order to avoid IoT based botnet attacks at the software level.

Peter Gartenberg, GM, Enterprise and Partner Group, Microsoft India says, "We secure the IoT device while it is being deployed in the wild by enabling device level provisioning and authentication and at the same time we ensure that all data transmitted between the IoT device and IoT hub is confidential and tamper-proof by facilitating a secure, encrypted channel for the data communication between the device and the cloud."

How tech giants & startups tackle IoT security challengeHow tech giants & startups tackle IoT security challenge - Image

Even enterprise communication technologies player, Tata communications at their security operations centres has a team of skilled engineers who monitor attacks close to the botnet and DDoS heat map. "The attack is broken down in manageable chunks rather than tackled when it has gathered too much momentum particularly when it comes to IoT roll outs and adding more IP-enabled devices to networks, we make security a consideration at a device and application level as well as for the network," says VS Sridhar, senior VP & Head, IoT, Tata Communications.

Moreover, NetApp which helps companies manage and secure information from connected devices across storage platforms. The storage vendor addresses the security issues by securing the data at device end point level. Deepak Visweswaraiah, Vice President & Managing Director, NetApp India explains their usage of Data Fabric strategy to enable companies to process large volumes of data from a variety of IoT sources with the visibility and quick performance .

The NetApp Data Fabric collects, analyses, secures data and help close the time gap between when the data is compromised and when the breach is discovered, so that the data is not stolen or destroyed by attackers.

**Startups IoT game plan**

While age old technology vendors have finally woken up to the game of IoT security issues, the Indian start up community has many IoT vendors who are making a push to cyber security for IoT devices at the device level.

Take for example, Bangalore based healthcare IoT startup Teslon Technologies which works on the tele health platform, Carenation that enables remote healthcare delivery uses the concept of "Fog Computing" to secure IoT platform. "A better way to deploy these resource constrained devices would be to use a "fog computing" layer to enable extra security checks on that layer to mitigate the risks of the attack on an end resource constrained device cascade to the cloud leading to massive Botnet based attacks," says Harsha Muroor, Founder, Teslon technologies.

**K. KRISHNA MOORTHY, CHAIRMAN, INDIA ELECTRONICS AND SEMICONDUCTOR ASSOCIATION (IESA)**

"Internet of Things is at its nascent stage in India from a business standpoint. Entrepreneurs and industrial sectors are trying very hard to adopt the technology across domains. . There are three major groups working on IoT in India – MNCs that have their design centers in India, large and small IT houses that have IoT practice groups now and as well as 400+ IoT startups"

**RR BIPIN, VP, DIGITAL SERVICES, IOT, EMBEDDED PRODUCT DESIGN DIVISION, TATA ELXSI**

"We cater to multiple industry verticals like healthcare, automotive, manufacturing, smart cities and building Automation. We can build solutions around our home-grown IoT cloud platform namely TETHER for the above industry verticals. We also execute end-to-end IoT projects as a system integrator with the help of the strong eco-system we have built through multiple partnerships and alliances"

**SAKET MODI, CO-FOUNDER & CEO, LUCIDEUS**

"Some common concerns that we have seen are in terms of encryption for both data at rest and in motion, application layer challenges while exchanging parameters with the device, data recovery challenges for data present on the device, maintenance of logs for events occurring on the device along with accessibility issues on Bluetooth/wi-fi "

**JITENDER SANDHU, DIRECTOR – INDIA SUB-CONTINENT, MACHINE-TO-MACHINE GEMALTO**

"IoT is already expanding. In absence of standards, there is high risk of data theft – which will eventually make the need for standards more (some word for imp/ highly identified need). So, sooner we have the standards being made mandatory, better for data security and IoT industry"

**JIM MORRISH, FOUNDER, MACHINA RESEARCH AND MEMBER OF THE GLOBAL ADVISORY BODY OF IET IOT**

"All questions on cyber security boils down to the economics of the market and flexibility of products. Sometimes these new age companies just want to push their products and also there is a general lack of awareness amongst the masses about such issues as security costs"

Even Tetherbox Technologies who provide end to end monitoring and automation solutions for treatment plans, biogas plants and desalination uses a secure encrypted communications network and encrypted storage to ensure protection for their customers.

Or take the example of India's first internet connected electric scooter maker, Ather Energy who explains how they collect the data from their bike Ather S340 which helps them gauge vehicle performance and in turn give continuous feedback to improve the product experience.

The S340 does not share any critical personal data which can pose as a security risk and to ensure security on the vehicle, all the connections to and from the vehicle is securely authenticated and are encrypted end to end which includes connections to the charging infrastructure and the cloud.

"Each vehicle has a unique signature used for encryption and addiotnally, safety critical functions such as acceleration, steering and braking are kept inaccessible to add an extra layer of security," Arun Vinayak, Chief Product Officer and Founding Team, Ather Energy.

**IoT in India**

According to the recently launched Norton Cyber security Insights report 2016, 65% of Indian consumers surveyed do not believe that there is enough connected device users for it to be a worthwhile target for hackers and a whopping 80% think that the devices are designed with online security in mind which is far from true.

“While IoT devices are gradually gaining acceptance, the current poor state of security on connected devices will present an increasingly attractive opportunity for cyber criminals in days to come,” says Atul Anchan, Director,systems engineering, India, Symantec.

There is tremendous interest for IoT in India and lots of different groups are coming together to build, adopt and promote IoT solutions but the country’s IoT sector still has a long way to go as more startups need to focus on solving real problems and do it in a commercially viable way.

“Production support is limited as compared to other Asian countries which will change once reduction in customs on electronic component imports will come down and also there is some discomfort around hardware, especially among investors,” says Nihal Kashinath, Founder, IoT Bangalore.