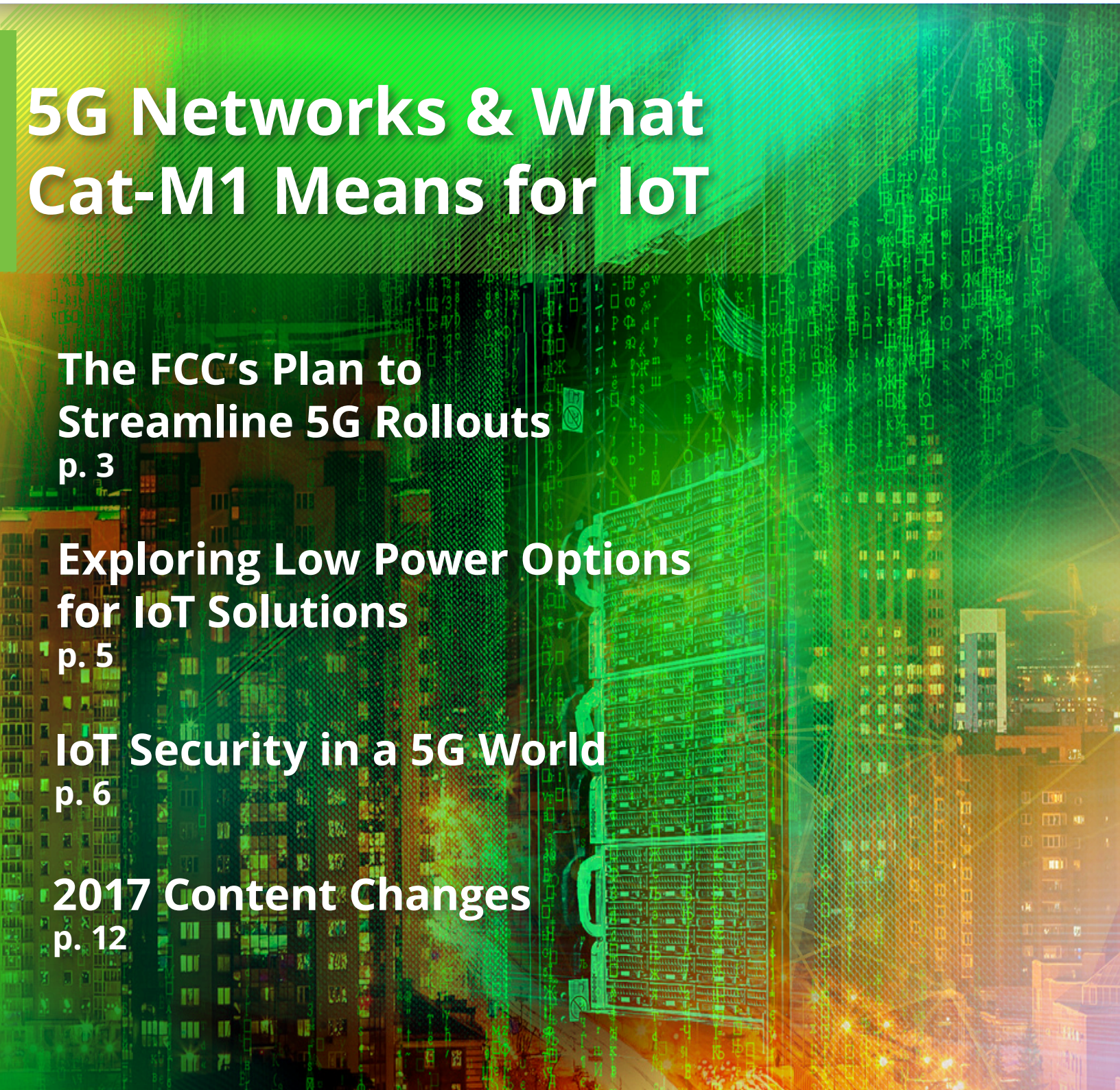
JAMES BREHM & ASSOCIATES

The Connected Conversation

Volume 2 / Issue 10 / December 2016

5G Networks & What Cat-M1 Means for IoT



The FCC's Plan to Streamline 5G Rollouts
p. 3

Exploring Low Power Options for IoT Solutions
p. 5

IoT Security in a 5G World
p. 6

2017 Content Changes
p. 12

News Flash:
Gartner Scoops Up Machina & Beldon Tries to Grab Digi

Beldon Attempts to Strong-arm Digi into Acquisition

On November 10th, Beldon Inc. made an offer to acquire Digi International for an all-cash deal totaling $380 million. This would come in at a 37% premium for Digi's six-month VWAP, and about 25% premium over its current share price, bringing in about $14 per share to shareholders. Digi's Board of Directors, however, adamantly refused the offer, making it clear that Digi isn't for sale. While Beldon claims to be educating shareholders with the press release, at the same time, it doesn't seem like strong-arming Digi into negotiations is really going to work. We'll just have to watch how this one unfolds.

Source: *Businesswire*

Sigfox Nabs $150 Million Euro in Funding

November 18th, Sigfox a world-leader in IoT connectivity, secured $150 million euro in Series E funding. Valuated somewhere around $600 milllion euro, the IoT network giant is hell-bent on providing global IoT coverage. With this round, Sigfox added Alto Invest, Salesforce Ventures, Henry Seydoux, Swen CP, Tamer Group, and Total to their list of investors. Franck Tuil, Sr. Portfolio Manager for Elliot (original investor) stated, "We strongly believe that Sigfox has unlocked the IoT connectivity bottleneck and will bring billions of objects online in the near future."

Source: *Tech.eu*

Gartner Acquires Machina Research

Last month, Garnter acquired industry analyst firm, Machina Research. For the past six years, Machina had been dililigently working on providng top-notch analysis on current trends and challenges in IoT. To quote, Machina founder, Matt Hatton, "We're immensely proud of what we achieved at Machina Research, building the world's leading advisors on IoT, M2M and big data. Gartner has recognised the great work that we've done, and has identified us as an important part of their increasing investment in the IoT space."

Source: *IoT Business News*

The FCC's Plan to Streamline 5G Rollouts

One of the first keynotes of this year's CTIA Super Mobility Conference was delivered by the Federal Communications Commission (FCC) Chairman, Tom Wheeler.

By Joyce Deuley, Founder & CEO *Smart Texas Alliance*

In his keynote, Wheeler discussed the benefits of 5G networks, particularly in terms of benefits of IoT (with an emphasis on smart cities and healthcare), but also shared the FCC's three strategies for rolling out 5G. Wheeler approached these strategies the way a well weathered general would amidst a period of confusion and uncertainty: in firm, absolute terms. The FCC has a clear path laid out for how 5G spectrum and networks will be allocated and operated, and knows that it will only come to fruition if we work as a team.

Ensuring Ample Availability of Spectrum

According to Wheeler, the FCC has retained a light touch to political involvement in terms of spectrum allocation, citing back to the 1996 Telecommunications Act that serves as the model for the "open Internet," and is one that has been proven to be good roadmap for innovation and growth.

Continuing in this vein, the Chairman claimed that the organization has created a market that would have made a 125 MHz of "beach-front" spectrum, but was halted due to involvement from the major carriers. Despite these barriers, however, the FCC is confident that its reverse auction will be a successful one, particularly within the 115 MHz bands, stating that it is within these "mid bands where Europe sees its 5G development," and that there needs to be the creation of new services to use as sharing tools in an attempt to open up more spectrum. There is some debate about whether or not the $86 billion target will extend the auction well into early 2017 because the FCC won't be able to source enough spectrum in larger markets at an attractive price.

Additionally, the FCC is determined to continue to "encourage, provide, and stay out of the [industry's] way." Not only that, but the FCC will also facilitate innovation and experimentation by providing experimentation licenses, greater flexibility for researchers, universities, and companies to field test 5G technologies.

Cost Provisioning in Infrastructure

But making spectrum widely available isn't enough. In order to truly leverage the powerful benefits of a fully-loaded 5G network, we will need to complete serious network upgrades via updated infrastructure, as well as increased numbers of towers, particularly throughout rural areas to ensure even coverage. In an effort to assist carriers in rolling out these

vast networks, Wheeler has talked about the FCC incentivizing carriers and developers to better streamline deployments, however he admitted that with the deployment of cells and cell sites, and limited back haul, end customers may experience higher costs.

How can the government assist in funding new tower and antenna construction? Wheeler says that companies will need to be able to share the story of what 5G is, in "real terms," rather than discussing it from a technical stand point. Additionally, it is important to not talk about IoT benefits or use cases too broadly, but speak about them in terms of opportunities in smart cities and health care. "Let's paint the picture of how it will launch immersive education, create new jobs and services. 5G isn't a technology; it's a revolution."

Removing Hurdles to Prevent Silos

In order to overcome the challenges that lay before us, including local authority approval and high costs, Wheeler emphasized that the IoT industry at large needs to think creatively about smart solutions. Wheeler stated that the industry should "learn from experience and get in front of [these challenges]" and work towards solutions together. The FCC, however, isn't recommending that we "open doors to consolidation," just that when 5G rolls out, the industry will be trying to manage and work around "millions of towers, 4 major carriers," and that "the Commission is committed to cutting that red tape," in order to do lead the market for 5G just as we did for 4G.

Final Thoughts

Wheeler, and the rest of the industry, is confident that the 5G tide will lift all boats, and that it is imperative for us to commit ourselves to "maximizing this for rural America, not just as sole profits for urban America." With the majority of the U.S. population (roughly 60%) living in just a mere 5% of available land, urban areas tend to get the lion's share of focus, but when discussing the advantages of 5G networks, unprecedented data speeds with zero latency, there is too much opportunity to not extend that beyond large city centers.

Additionally, whichever country manages to pave the road for 5G will be leading the pack, which is a position that the U.S. is eager to achieve. But, part of this home-front advantage will reside in which country can resolve cyber security and data exploitation concerns, as Wheeler stressed that "cyber security is addressed during the design phase for all 5G devices and solutions." It can be difficult to see the forest for the trees, and similarly, the FCC was at CTIA to remind all of us of the John Gartner quote, that "history doesn't look like history when you're living it," and that this industry isn't just "living" history, it's in fact writing it.

Exploring Low Power Options for IoT Solutions

Though mostly inaudible to us, the world is filled with the constant chatter of internet-connected machines.

By Consuelo Azuaje

Whether they communicate directly one-to-one ("point-to-point") or as a part of a larger conversation in a vast network, their methods of communications have evolved with market demands and provide different industries with aggregated and contextualized data to run more efficiently and effectively. Point-to-point communications which occur exclusively between machines are "machine-to-machine" communications" (M2M) and the "vast network" referenced above is the "Internet of Things" (IoT). More accurately, the IoT is the internetworking of devices that use sensors and software to collect/share data. The real rewards of IoT, however, are the data analyses and highly valuable, actionable information it yields to users. (For the sake of simplicity, however, because the two are so closely intertwined, we will refer to the two collectively as "M2M/IoT".)

The Institute of Electrical & Electronics Engineers (IEEE) Communications Society (IEEE ComSoc) has forcasted that M2M/IoT communications will be the "dominant communications paradigm for a wide range of emerging smart services," in industries such as fleet telematics, smart cities, smart metering, agriculture, Industrial Internet of Things (IIoT), and more.

M2M/IoT Device Requirements and Potential Solutions

Due to the 2000's exploding market demand for mobile broadband (MBB) service via mobile devices, telecommunications standards bodies' (i.e. the 3rd Generation Partnership Program, 3GPP) predominant focus for years had been on boosting data capacity, speed, and coverage for endusers. The advances that the 3GPP made in that direction were impressive, but they didn't fit the majority of M2M/IoT applications which had begun to emerge. M2M/IoT devices typically collect and send small amounts of data at infrequent intervals and are sometimes located in signal-challenged locations and/or locations with poor coverage (e.g. remote rural areas, underground places like basements) where they must be able to operate for very long periods of time without human intervention. The vast M2M/IoT applications would benefit more from having a long battery life and extended coverage than they would from having high speed capabilities and having large data capacity. The interval of time that passes between battery changes and the sheer number of M2M/IoT devices that have already deployed and/or soon to be deployed are both very important

cost factors. Companies throughout the stack are going to have to design M2M/IoT devices that are cost-efficient as well as power-efficient. Ultimately, M2M/IoT's key requirements are: extended coverage, low device cost, low deployment cost, long battery life, and the ability to support a massive number (billions) of devices.

Low-power wide-area networking (LPWAN) is an ideal fit for many of these use cases, but there's an incredible amount of variety in terms of vendors and LPWAN-solutions out there, making it difficult to keep track of the latest technologies. What options are on the table, then? What vehicle can M2M/IoT use for its communications? Current solutions use either unlicensed or licensed radio frequency (RF) spectrum.

The benefits of 3GPP Long Term Evolution (LTE) networks are that they are all built on the existing LTE infrastructure, making software upgrades simple and drastically reducing network deployment costs. The focus of this article will be on solutions that operate in the licensed spectrum, but LPWAN-solutions using the unlicensed spectrum will be touched on as well.

LPWAN

Unlike LTE, unlicensed LPWAN solutions can operate on non-mobile network operators.Their development and deployment are not dependent on spectrum reallocation because they can operate over unlicensed spectrum. Furthermore, unlicensed LPWAN solutions can save businesses money because they run on unregulated networks which are less costly to operate on. Also, unlicensed LPWAN solutions are less susceptible to interference. Where unlicensed LPWAN solutions fall behind, however, is in latency. While low-data and low-speed are the norm for most M2M/IoT applications, there are events, such as an exploding gas main detected by smart

metering, for instance, where low-latency would need to be an available option. LPWAN simply wouldn't be able to offer the low-latency needed by such an emergency situation—which ultimately means, that like other connectivity types, there is no one-size-fits-all solution, so it is important for end users to be aware of the limitations of each connectivity type.

First introduced via 3GPP's release 8 (R8) in 2008, LTE was created to make affordable mobile broadband feasible via the Cat-1 technology. LTE has since been (and continues to be) developed and improved upon in each subsequent 3GPP release.

3GPP LTE Release 8's Cat-1 & Release 12's Cat-0

While the Cat-1 had been touted as a viable MBB solution, things have shifted. Performing below even 3G standards, however, Cat-1 has lost relevance and has instead gained attention as a good match for IoT. Cat-1 offers two RF receiver chains, operates in full duplex mode, and uses 5Mbps for uplink and 10Mbps for downlink communications. ("Duplex mode" refers to the style of point-to-point organization that two connected devices use when communicating with each other; in full duplex mode the two connected parties can communicate simultaneously, but in half duplex mode, only one connected device

can "talk" at a time.) Many have turned to the Cat-1 module in the interest of energy and cost efficiency. It's a desirable option because it extends battery life via conservative use—also because its module size is small and economical. Plus, Cat-1 is already fully commercial, meaning that it's already being used by numerous M2M/IoT applications.

Cat-1's compatibility with M2M/IoT applications, however, is incidental, not deliberate. Until R12 in 2015, the 3GPP's focus had been on increasing complexity to optimize performance for MBB—an energy-expensive goal. R12 ushered in Cat-0 which was specifically designed for M2M/IoT.

In order to boost power-efficiency, Cat-0's modem complexity is half that of Cat-1's. Cat-0 also defines narrower bandwidths, decreases peak rates for uplink and downlink to1Mbps and decreases signal complexity to reduce cost and power consumption. Additionally, Cat-0 modules offer half-duplex mode as well as full duplex mode, making it easier to support. Cat-0 introduces coverage improvements needed to support M2M/IoT applications and is easy to install because it only requires one receiver antenna, where as Cat-1 requires two.

LTE Release 13's Cat-M

3GPP's R13, completed this summer, introduced Cat-M, narrow-band IoT (NB-IoT), and extended coverage-EC-GSM-IoT. The 3GPP's main design objective for Cat-0 had been to reduce its complexity, improve battery life, and extend its coverage by 12-20 db. Cat-0's modem complexity is half that of Cat-1's. Cat-0 defines narrower bandwidths and decreases signal complexity to reduce cost and power consumption.

In step with R12, 3GPP sought to reduce modem complexity with their R13 offerings. Thus, Cat-M's modem complexity is half of Cat-0's, making it a quarter of Cat-1's. Cat-M's power amplifier (PA) option is an interesting feature that can boost coverage by 20db and allow Cat-M to transmit to and from thick walls, underground, etc. It's important to be able to transmit to/from thick walls and/or underground because that's where smart electricity meters and other simliar IoT devices are located.

According to a recent GSMA report, however, the most important cost reduction achieved in Cat-M is a bandwidth reduction—more specifically the reduction in the number of subcarriers (in a predeterimined amount of time) which the network may use to multiplex multiple streams of traffic in the same spectrum. The bandwidth reduction resulted in a significant decrease in signaling overhead, which, in turn, reduced complexity and cost of the module overall. Because of this, Cat-M is able to sustain a 10 year-plus battery life through use of its power saving mode (PSM) and extended idle-mode Discontinuous Reception (eDRX) capabilities.

PSM is accomplished by using a timer that let's the device know when it should start "paging" (checking in) with the network to send/receive data. eDRX refers to a process that extends the sleeping cycle in idle mode to allow the device to turn off and save power. Neither are exclusive to Cat-M.

LTE Release 13's Narrow Band-IoT (NB-IoT)

Market research firm, MarketsandMarkets, recently released a report that forecasted the NB-IoT chipset market to grow from $16.7 million in 2017 to $181 million by 2022. The 3GPP had several design objectives for NB-IoT, including: battery life of at least 10 years, device-price less than $5, a capacity density of at least 40 devices per hold, and 10x's greater coverage area than current/past 3GPP technologies.

NB-IoT could be a cost-effective source of connectivity to billions of IoT devices—while at the same time, doing so in a way that consumes less power, provides seamless coverage, and supports low-cost devices. Rolled out as software on top of existing LTE infrastructure, NB-IoT's design mimics LTE's in that it takes advantage of radio network evolution and reduces time to market. Because its carrier bandwidth is a scant 200 kHz, NB-IoT can be deployed within an LTE carrier network or in an LTE or WCDMA guard band. In order to boost spectral efficiency, NB-IoT was designed for deployment through a number of different options, including GSM, WCDMA, and the LTE spectrum.

Spectrum being the scarce resource that it is, carriers regularly phase out old networks and refarm (reuse) the spectra they operated on. Part of the beauty in NB-IoT's design is that it would operate unaffected if its spectrum were refarmed for use by other LTE networks. In-band deployment is the most spectrum- and cost-efficient option for NB-IoT. Via in-band deployment, NB-IoT and LTE are able to share a fully integrated infrastructure and spectrum. Also, NB-IoT's operating on a single PRB reduces throughput as well as complexity and, ultimately, conserves power. Under normal use case conditions (i.e. activity level, etc.), a single NB-IoT carrier can support 200 thousand NB-IoT devices. NB-IoT could also be deployed in a guard band without interference. Additionally, the narrowness of NB-IoT's bandwidth ultimately helps it conserve power. One factor driving the NB-IoT chipset to market is a surge in the demand for network-enabled devices, long-range connectivity, and low-power, low-cost connectivity/ network technology.

Final Thoughts

Each succeeding release the 3GPP rolls out provides increasingly cost- and energy efficient solutions that have been optimized for LPWAN connectivity and M2M/IoT applications. However, it is important for M2M/IoT end users to fully understand what the capabilities—and the limitations—are of different licensed LPWAN connectivity optoins. While it is still too early to tell which technology is going to be the go-to M2M/IoT chipset, the market has already begun offering a variety of solutions to suit a variety of scenarios, from health monitoring devices to smart gas and water metering. Cat-M and NB-IoT are two of the latest licensed LPWAN options of a wide range of solutions that have already been presented (and are being developed) to meet the demands of a variety of different use cases.

Fun Facts: Survey Results

James Brehm & Associates conduct industry surveys to get a pulse for what is really happening in IoT. According to a recent survey, the James Brehm & Associates team were able to gather some interesting figures conerning IoT endpoints, what the main barrier is to IoT adoption is, as well as how many companies are utilizing data analysis.

—There are 67.5 million cellular IoT endpoints in the United States at the end of Q3 2016.

—49% of companies surveyed by JBA have deployed an IoT solution…16% of companies have no plans to deploy an IoT solution.

—Of the companies who are working on IoT solutions, half are still in trials or at the proto-type stage.

—Security is the number one barrier to deploying IoT, followed by the Cost to Deploy and Interoperability.

—87% of companies link data analytics to increased ROI.

—Shockingly, 22% of companies surveyed are not doing any data analysis.

For additional information about this survey and others, please contact James Brehm & Associates here: info@jbrehm.com

IoT Security in a 5G World: Leveraging Complexity at Scale

There was a predictably large turn out at this year's CTIA to discuss the impressive impact of 5G and the capabilities it will provide.

By Joyce Deuley

(For more information on how the race to 5G is shaping up, please read Consuelo Azuaje's article in *The Connected Conversation*). Not only will 5G dramatically increase network speeds, but it opens numerous doors for IoT deployment as well as innumerable vulnerabilities.

In light of October's *"Miria" distributed-denial-of-service (DDoS) attacks on IoT devices*—as well as the large-scale attacks waged against companies such as Twitter, Tumblr, Spotify, Amazon and Netflix, the idea of having a zero-latency network that hosts a myriad of unprotected devices is especially terrifying. Even more so now because the how-to documentation has become open sourced. However, there are ways to prevent those kind of attacks that Jay Srinivasan, Sr. Director of Engineering at Infiswift, discussed in his IoT Evolution article, *"Stopping Mirai DDOS: What Consumers & Developers Can Do."* But more than that, DDoS attacks are not the only security threat to be concerned with; Akamai Technologies just released new research, wherein its Threat Research team has identified *recent attacks on IoT devices* via a decade-plus old OpenSHH vulnerability. Meaning that IoT devices must become resilient to both new and old methods of attack.

And when we consider the scale of IoT connections as well as traditional issues with security, (e.g. lack of customer knowledge or awareness), things can look even more tenuous. Thankfully, there were several leading security specialists at the "Securing the Foundation of a 5G World" panel discussion that were able to shed some light on the lack of IoT security and what that means for us going forward. With Rita Marty, Executive Director, Cloud & Security, AT&T Chief Security Officer as the panel moderator, the panel consisted of: Angela McKay, Director, Government Security Policy & Strategy, Microsoft; Gary Davis, VP & Chief Consumer Security Evangelist, Intel; Drew Morin, Director, Federal Cyber Security Technology & Engineering Programs, T-Mobile USA; and Jim Hunter, Chief Scientist & Technology Evangelist, GreenWave Systems.

The security panel recognized that 5G possesses an overwhelming amount of potential to essentially create a whole new architecture, a "clean slate," if you will. But it also acknowledged that 5G also possessed equal or proportional susceptibility to exploitation. That said, security is going to be…difficult at best. Ironically, the root of 5G's security issues, Davis explained, stemmed from the very characteristics that make 5G desirable (i.e. zero latency and the ability to connect to a large number

of devices). According to Davis, if we were to "fast forward to 2020," where we had "billions of connected devices and... a tech that has zero latency, which can send data at unprecedented speeds," then one inevitable consequence would be a huge security challenge—and that is putting it mildly.

As 5G is an emerging technology, there are a lot of things to be considered—like the fact that 5G networks aren't just about connectivity, but also the mission-critical applications and markets they support, and who is ultimately at risk and how best to mitigate that risk. Ultimately, the panelists did an excellent job of addressing these conncerns, as well as identifying the positive opportunities that seem to run parallel to the inherent vulnerabilities of 5G networks.

When asked about the advantages and challenges, GreenWave's Jim Hunter was quick to respond, saying it was the "first time we're seeing the evolution of computer involved with communication. Now we see baked-in technology." However, according to Hunter that doesn't mean that we need to create a "one-size-fits-all" security standard for 5G networks. Instead, he posited that security standards would continue to be siloed [to some degree within markets], but that "these measures" would need to be taken and exchanged back and forth. "The value is in the data and the insights, and you won't get that across one vertical, you need that cross section," he concluded.

In addition to that, Angela McKay stressed that the industry must take an agile approach to solving security issues and improving overall resiliency: "The place we are in now, big tech providers, is a service-managed network. When you move into 5G, you'll have non-IT traditional companies building code, and you'll have the number of vendors involved in delivering those services." In order to achieve sufficient agility and collaboration, McKay maintained that the industry would have to "be responsive to the dynamic nature of the risk environment," evaluate "this-service-requires-this-kind-of-service V.S. another" and how that could change. Additionally, McKay urged the industry to "Be more agile, do risk-based deployment of apps and services based on attributes and machine learning you can get out of the cloud environment."

Fog computing, intelligence at the edge, artificial intelligence, and machine learning are all about putting more advanced computational powers in-field hardware and the network, itself, in order to improve data analysis, security via remote updates, and self-healing capabilities. For Hunter, "Fog… is absolutely right. It works better when it scales from the ground up… The network is computing, and then computing is happening in the network. It's more network than ever. It's not just us changing, it's the entire globe that needs to shift at the same time...there's about 360 IoT shows around the globe."

Drew Morin, however, focused more on edge devices than networks: "It has always been, 'Let me protect the edge device, and I'll let the firewalls protect you with the center being gooey and delicate.' [But now,] we're going to have intelligence at the edge that the network will have to adjust for. All of these things will enable the core components... [that are] handling the switching processing and translating [of] what's going on in the network...[to] cut off whatever slice and kill it, and then do forensics on it." Other aspects to consider are the regulatory environments, who organizations will need

to turn to, who the authorities are, and what additional requirements will need to be met while moving further up the stack. According to Morin, "We, as an ecosystem, need to look at the rule book and start off with a new plan and a new vision. It's a fun, radical time."

Despite Davis' warning that securing 5G networks and IoT deployments would be a "cat-and-mouse game", it isn't all doom and gloom. From McKay's perspective the risks implied with 5G networks also possessed a great amount of opportunity. What the industry would need to do, she advised, is identify what inhibitors challenged them and allowed them to actualize "those opportunities," as well as really embrace the notion that they were "not fully realizing the security opportunities that are on the horizon."

If the industry thought that wide-scale IoT development and adoption looked like the Wild West in terms of aggressive pioneering and an inherent "make-it-work" mentality, then their approach to 5G network security would have to be very similar. It's not so much, the "every-man-for-himself" aspect, but the collaboration that is born out of adversity and perseverance that is natural to exploration. To agree with McKay, "Complexity is the challenge," but, the opportunity is in "managing that complexity" together.

2017 Changes

For 2017, we're adding a couple of new items to our content plan.

First is a premium version of our subscription, "The Connected Conversation". We'll be digging deeper and providing 4x the amount of content in 2017. If you'd like to contribute ideas on what we cover, please email info@jbrehm.com.

Next, we're adding a new section, aptly named "Change Agents," that will include interviews with companies making significant strides in IoT. Those interviewed are the catalysts, the difference-makers, the dreamers-of-dreams, and doers-of-stuff. As Apple said in its revolutionary 1997 television commercial, "Here's to the crazy ones, the rebels, the trouble makers, the ones who see things differently." We hope you enjoy this ongoing service. If you know of anyone who fits in this category, please feel free to submit a name here: info@jbrehm.com.

James Brehm & Associates is a consulting and marketing intelligence firm that provides project-based and retained strategic advisory services to technology companies worldwide. With a firm focus on the Internet of Things (IoT), Machine-to-Machine (M2M) Communications, and Big Data Analytics, Jame Brehm & Associates provides actionable insight and direction to a wide range of organizations including Communications Service Providers, Hardware Maunufacturers, Software Vendors, OEMs, Private Equity, and venture Capital Firms. Through projects on market size and share, competitive intelligence, product development, go-to-market strategy, and client-specific consulting services, we help companies reach their maximum potential. http://www.jbrehm.com

If you'd like to continue to receive *The Connected Conversation*, please email info@jbrehm.com or call (210) 401-0051.