THE STRATEGIC NEWS SERVICE©

GLOBAL REPORT ON TECHNOLOGY AND THE ECONOMY™

SPECIAL LETTER:

AT THE EDGE: THE IOT SECURITY IMPERATIVE

SNS Special Letter:
At the Edge: The IoT Security Imperative

In This Issue

Week of 9/23/2019 Vol. 24 Issue 30

FiRe 2019 Speaker Spotlight

One could be forgiven for referring to Harvard geneticist and Wyss Institute founder George Church as a godfather of modern genomics. He was the first to publish a direct genomic sequencing method and encouraged the creation of the Human Genome Project all the way back in 1984. In the nearly four decades since, Church has continually contributed key technical and infrastructural advancements to the field, including publishing the first study to use CRISPR-Cas9 to edit genes in human stem cells, creating the world's only open-access human genome data set, cloning a woolly mammoth, and co-founding 22 genomics companies, including Nebula Genomics, a blockchain-based solution for making human genome data available to medical researchers.

At FiRe 2019, as our Opening Night keynote, he lays out his plan for ameliorating mass extinction and climate disaster.

Learn more about FiRe 2019 and register here.

Publisher's Note: A few weeks ago, I had a chance to catch up with Paul Clayson over a casual lunch at a seaside restaurant. I've known Paul for years, and it seems as though, even as each of our projects change, our orbits must be changing with them. Last time we were together, we were working to create a new graphene center of excellence at the University of Utah. This time, I'm working on Pattern

Discoveries (including how they can help with security), and he's working on IoT (and how to help with security).

Not long ago, I was being interviewed at Techonomy by my friend David Kirkpatrick, in the conference's last panel. Among my fellow panelists was the head of security for BAE Systems. A consultant friend in the audience asked about the coming era of IoT and what the state of security will be.

"Horrible," I replied. "Unbelievably bad," my British colleague added.

"It can't be that bad, can it?" the consultant asked. We just started laughing, and that ended the interview.

Yes, it's that bad.

In this week's issue, members will benefit from a detailed explanation of what is wrong, why it's wrong, and how we can begin fixing it. I will add that Paul and his team will be at FiRe, as a FiReStarter Company, for those who would like to talk with him personally.

We are also going to set the CTO Design Challenge at FiRe to address a related problem in net security, and we'll have perhaps the world's expert in cybersecurity, Dmitri Alperovitch, CEO of CrowdStrike, with us as well. So, if you want to be secure, read on, and then join us all at FiRe 2019. – *mra*

SPECIAL LETTER:

AT THE EDGE: THE IOT SECURITY IMPERATIVE

by Paul Clayson

This year marks the 50th anniversary of the internet and the 30th anniversary of the World Wide Web. It's been 50 years since the first packet-switching technology was used on a computer network in 1969. The changes wrought by the internet and the web over the past half-century have been nothing short of astonishing.

As we reflect on these milestones, the potential for a great deal more economic transformation is glaringly apparent as these technologies continue to evolve. Highlighted in this Special Letter is one of the biggest internet-driven transformations unfolding today: the trend toward billions of connected devices, or what's generally referred to as the Internet of Things (IoT), which will ultimately

evolve into the Internet of Everything (IoE). The vast majority of these IoT devices interact machine-to-machine (M2M), with no human input.

We need only look around us to appreciate how the internet has profoundly affected the manner in which we live, work, and play. As transformative as the internet has been in connecting people, the proliferation of billions of connected devices promises an equally, if not more profound, shift in the coming years. The extent and scope of the changes wrought by IoT in the future will depend on many factors, some of which we can see today and others which we cannot. One of the biggest factors relates to the security of our connected devices.

In this era of quantum computing, blockchain, 5G communications, and artificial intelligence, securing these billions of devices is imperative. One published study asserts that this very second – and the next second, and the next – over 600 new IoT devices will be deployed, equaling over 20 billion device deployments in 2019 alone. Other published studies show that well over 90% of these devices and all other previously deployed IoT devices have either no security or frighteningly inadequate security.

This lackadaisical attitude toward securing devices for consumers, commercial business, government, and civic entities borders on lunacy. The financial impact of breached devices is well-documented; and hackers are now attacking computers and networks at a rate of once every 39 seconds. You read that right. IoT devices are the fastest-hacked devices in the history of the internet.

As we study the impact of cybercrime, we can emphatically state that without security, IoT will lead to disaster for consumers, businesses, and governments. And security on small IoT devices cannot be implemented using existing security protocols.

To better understand the security imperative related to IoT, it's helpful to look at the current IoT landscape and the present state of IoT security. After presenting this overview, we'll look at some of the challenges related to IoT security and highlight a solution.

An Internet Inflection Point

In 2008, the number of connected devices for the first time exceeded the number of people connected to the internet. Since then, we've seen a massive increase in the number of connected devices in the US and overseas. In 2018, the number of small, M2M connected devices surpassed the number of all other form factors of computing combined.

It took over four decades for 3 billion people to become connected to the internet. Today, it takes less than two months to connect the same number of devices! Analysts at Gartner project that by next year the number of connected devices will

exceed 20 billion worldwide. With more than 617 connected devices deployed per second each day, you can do the math to see where things are heading in the foreseeable the future.

The trend toward billions of connected devices encompasses the consumer, business, civic, and government sectors. It spans all major economic segments and includes things as diverse as ordinary home appliances (e.g., refrigerators, ranges, draperies, door locks, and ovens) to machines and robots on the factory floor, to myriad other devices found on farms, in cities, in commercial buildings, on automobiles, in medical equipment, and in many more fields of work.

As Vodafone recently noted in its IoT Barometer 2019 report, there has been a surge in adoption. Over one-third (34%) of companies are now using IoT. Regionally, the American market saw the biggest increase, rising to 40% from 27% last year. With respect to industries, we are seeing rising IoT penetration in transport, logistics, manufacturing, and industrials. Early adopters are seeing measurable benefits from their IoT projects; and these benefits increase as adoption and sophistication grow.

There are several prominent IoT growth enablers, not least of which is facilitating greater network intelligence. Connected devices enable new data streams and business models that can be harvested to supply an array of useful information and services. We are seeing growing demand for connected devices that foster energy management, safety, and security, as well as chore automation. Wearable devices are proliferating, connecting patients with healthcare practitioners for monitoring and management of health and improving wellness.

In retail establishments, "connected things" are being used in conjunction with automated checkout, layout optimization, supply chain and restocking, smart CRM, in-store personalized promotions, and inventory shrinkage prevention. In the office, we're seeing applications used for organizational redesign and worker monitoring, and augmented reality for training, energy monitoring, and building security. Factories are using various IoT applications for operations optimization, predictive maintenance, inventory optimization, and health and safety.

Connected things are also integral to the development of smart cities, which encompass autonomous cars and trucks, navigation, logistics routing, public safety and health, traffic control, resource management, and many other activities and things. As reported by researchers at McKinsey & Co., cities are home to more than one-half of the world's population, and they're anticipated to add another 2.5 billion new residents over the next three decades.

Additionally, cities face increasing environmental pressures and infrastructure needs – and growing demands from residents to deliver a better quality of life and to do so at a sustainable cost. Urban planners and administrators are increasingly considering IoT-based solutions to tackle some of the vital issues facing cities and to meet these challenges.

All of these applications produce data – data transferred from the smallest of devices to a server in the cloud where it can be analyzed to develop new products, reduce waste, move autonomous vehicles safely and accurately, cut costs, increase services, increase speed and velocity of delivery, and better serve humankind. International Data Corp. (IDC) estimates that this year around 5 zettabytes of data will be collected from computing devices. By 2026, more than 45 zettabytes will be collected annually, with more than 90% of the data being collected from IoT devices. Among the IoT devices collecting data, 90% will be collected from the smallest of devices.

IoT opens the doors to innovation in ways that extend beyond what we saw with the dot-com phenomenon. This is the most exciting aspect of the trend toward connected devices. What's more, IoT is converging with other emerging technologies, such as 5G, blockchain, and AI, mentioned above. The convergence of these transformative technologies promises to unleash a wave of innovation that will extend into the next decade and beyond.

IoT Security Challenges

As exciting as some of the emerging IoT applications are, there are challenges associated with this new world of connected devices, many of which are constrained (e.g., they're battery powered, have limited memory or highly limited processing power, etc.). These constrained devices are not compatible with conventional security protocols – i.e., AES/TLS (Advanced Encryption Standard / Transport Layer Security), collectively known as IPSec. Without sufficient IoT security, bad actors have extremely easy access to data – the crown jewels of the IoT digital age. If we thought security breaches in the pre-IoT age were costly and problematic, just wait: they're likely to grow much larger and much more costly in coming years absent sufficient security.

Over the past couple of years, every day there seems to have been another media headline about this company or that government office or institution being hacked. McKinsey estimates that the cost associated with cybercrime around the world is approaching a whopping $600 billion – almost 1% of global GDP.

The internet and the web have been a boon to business and society at large over the past two decades, but there's no avoiding the dark side of these transformative technologies: it's littered with cyber hackings, in various forms and varieties. No consumer, business, or government is immune to their threat.

The lion's share of reported cyber hackings has been related to people and entities, and information about and generated by them – not about "things." A world of connected things opens up a new frontier for hackers who make a living disrupting internet users. We caught a glimpse of this threat with the Mirai-botnet DynDNS cyberattack on October 21, 2016. The Mirai event was the first large-scale IoT

cybersecurity attack that occurred through millions of unsecured connected devices. Recent illicit cyber activities now make the Mirai attack look small and insignificant.

Another example of the magnitude of IoT security threat was the attack on a petrochemical plant in Saudi Arabia in August 2017. Experts determined that the attack was likely intended to cause a cascading explosion; the only reason it didn't was because there was an error in the hacker's code. This particular hack required a level of sophistication that implied government backing. Some who studied the incident concluded that the malicious code was meant to do far more than just take down one plant; it may have been intended as an act of war against the nation of Saudi Arabia.

In late August of this year, Microsoft announced that an unknown but very significant number of servers around the United States have been infiltrated and compromised with clandestine code which gained access through the IoT devices delivering data to the servers. This attack was perpetrated by an aggressive nation-state effort.

These IoT-related cyberattacks are a wake-up call. Attacks over the past year have increasingly shown that IoT devices with no or weak defenses make for easy targets. Hackers are prone to target the weakest link of any security chain, and there's no weaker link than the increasing number of severely constrained and connected Class 0 and Class 1 devices (see definitions below) that have no security at the present time. A recent research study published by Microsoft concluded that fully 97% of CTO / CIO / CISO executives are very concerned about IoT security because they have not found solutions. There are solutions detailed below that address these very concerns.

The New Edge

A new computing paradigm is emerging with IoT. The computing "edge" has dramatically and rapidly shifted over the last decade. Years ago, the edge was the desktop computer. With the proliferation of wired / wireless network elements and the miniaturization of computer platforms, the edge has migrated from desktops to laptops to smartphones to edge gateways and, ultimately, to IoT devices.

These new, severely constrained IoT endpoint devices are smaller than the tip of a finger, with correspondingly limited memory and compute power. The Internet Engineering Task Force classifies these smallest of devices as Class 0, 1, or 2:

CONSTRAINED IoT DEVICE CHARACTERISTICS		
NAME	DATA SIZE (e.g., RAM)	CODE SIZE (e.g., FLASH)
Class 0	< 10 KB	< 100 KB
Class 1	~ 10 KB	~ 100 KB
Class 2	~ 50 KB	~ 250 KB

Source: Internet Engineering Task Force (IETF)

This vast and rapid integration of connected M2M devices is limited only by two things: 1) the extent that we can imagine what can be done by connecting an inanimate object to the internet through a small processor (e.g., a connected soft-drink bottle cap); and 2) the limited processing power and memory on board the device. To accomplish the seemingly impossible, the new paradigm uses memory which today is cheap and trades use of CPU cycles for RAM using more memory for algorithmic instruction.

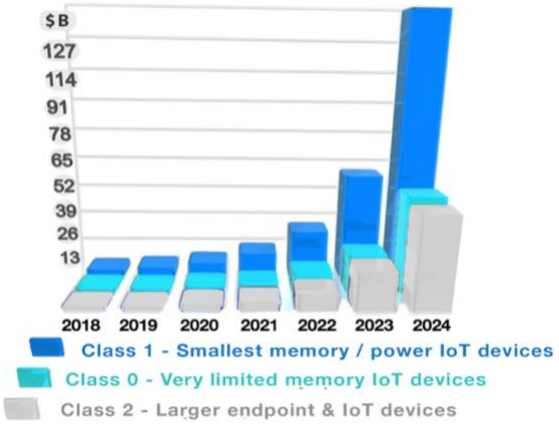
However, while the computing platform has pushed the edge to the smallest of Class 0-2 devices, especially in the last five years, methods of securing the data in transit have not fundamentally changed in over 20 years. Current security systems with classical encryption methods, influenced by Alan Turing, Claude Shannon, and other cryptographers through the decades, require large amounts of storage and compute power – on the order of 1 MB or above – to process the heavy encryption standards. These systems were designed for standard computing devices, not the smallest of devices deployed to IoT.

Think about that. The typical new "edge" device often has a total of only +/-100 KB for all functions on the device! We now have an entire class of computing devices that outnumber all other computing form factors combined, that do not have enough resources to run standard encryption. This creates a major problem and necessitates the deployment of a new, purpose-built encryption platform.

Among the billions of devices currently deployed, and projected to be deployed, in the next few years, the vast majority will be the smallest – Class 0 and Class 1 – of IoT devices. The evolving IoT edge presents a host of new cybersecurity challenges that require new technology solutions beyond the current IPSec paradigm.

AES / TLS has served us well. But the current encryption standard is not compatible with constrained Class 0 and 1 devices, which are projected to grow exponentially as IoT evolves in the years ahead.

Constrained IoT Device Growth



Source: Maximize Market Research

Quantum Concerns

The large and growing number of unsecured IoT devices represents one of our most important security challenges today. This challenge will only become more pronounced as quantum computers come onto the market and become more powerful in coming years.

Cryptographers tell us that current classical encryption is highly vulnerable to the quantum computers of the future. Unlike conventional digital computers, quantum computers are able to factor large numbers easily and quickly. There are mounting concerns in government circles globally – including in Washington, DC – that quantum computing poses a serious threat to cybersecurity in the future.

Our company, AgilePQ, recently joined forces with the Quantum Industry Coalition and the Quantum Industry Alliance to help address the cybersecurity issues related to quantum computers. Last December, the US Congress passed, and the president signed into law, the National Quantum Initiative Act (H.R. 6227). The act directs the president to create a 10-year National Quantum Initiative (NQI) program to accelerate and coordinate federal quantum research and development.

US Rep. Will Hurd (R-TX) has spoken publicly about this threat. Congressman Hurd published an article in *WIRED* in December 2017 highlighting the quantum-computing risk to security. Hurd, who chaired the Information Technology Subcommittee of the Committee on Oversight and Government Reform and serves on the Committee on Homeland Security and the Permanent Select Committee on Intelligence, stated in the article:

> From academics to the National Security Agency, there is widespread agreement that quantum computers will rock current security protocols that protect global financial markets and the inner workings of government…. In short, quantum computing presents both an unprecedented opportunity and a serious threat.

Congressman Hurd's message was echoed in a report titled Quantum Computing: Progress and Prospects, published last year by the National Academies of Sciences, Engineering, and Medicine. As noted in the report, all encrypted data that is recorded today and stored for future use will be cracked once a large-scale quantum computer is developed. The authors of the report stated:

> There is strong commercial interest in deploying post-quantum cryptography even before such a quantum computer has been built. Companies and governments cannot afford to have their private communications decrypted in the future, even if that future is 30 years away. For this reason, there is a

> need to begin the transition to post-quantum cryptography as soon as possible.

We wholeheartedly share Congressman Hurd's view and the position taken in the National Academies' report. With millions of new devices connecting to the internet daily, the key question we have to ask is: Can digital communication on these small, constrained devices and sensors be secured in the age of quantum computing?

The answer is a resounding "Yes!" However, it will require a new generation of post-quantum cybersecurity solutions and a great deal of collaboration with policy makers, regulators, and standards organizations, globally and with private industry, to deploy the solutions.

The AgilePQ team is currently working diligently with these groups on post-quantum cybersecurity solutions. It has developed a new de-facto standard in post-quantum security for connected IoT devices. The team's cybersecurity solution possesses multiple new innovations using encryption technology that renders its solution to be secure in a quantum computer world.

Building Post-Quantum Security from Class 0 Level On Up

To meet the demands of rapid miniaturization of computing platforms, a new security protocol must begin with the size of the device in mind, not just a derivation of the legacy security technology. Among the critical specifications of any new edge security, the following must be inherent in the system:

- Full encrypted data in transit with less than 10 KB processing requirement, leaving the lion's share of available resources for the native function of the device – i.e., "CPU Lite."
- The system must be exceedingly faster than current encryption to accommodate exponentially increasing data transmissions.
- Because over 80% of all IoT devices are battery-powered, the system must use much less energy than current encryption methods.
- The new system must eliminate standard packet sizes to reduce the amount of "overhead" transmitted in current data-in-transit security systems – thus increasing speed of transmission and decreasing the energy required to transmit.
- The system cannot be less secure than current internet protocol security standard technology.
- To prepare for the future, the system should be able to survive attack by quantum computers, thus creating post-quantum security for IoT and all other devices upstream in the network system.

This was the premise of the strategy deployed by AgilePQ. Beginning with a Class 0 device as the benchmark, the team built a security system from the ground up for data in transit which exceeds all critical criteria. The system deploys:

- A total operating code footprint of <2.4 KB that can fit on any Class 0 device and leave 95%+ of the processing power available for the operating code of the device.
- Agile data packets of any size – not just standardized packet sizes, as required by AES – which completely eliminates all transmission of overhead data.
- A system that is up to 10X faster and uses up to 80% less battery power.
- A system that saves so much space in the operating code that it can deploy much larger keys than AES – in fact, they calculate to a total key space that is 429 orders of magnitude larger than AES.
- A proprietary transport layer that connects with one-tenth the data required in a standard TLS system.
- Encryption that deploys much smaller, non-standard–sized data packets than the uniform data packets required in AES and deploys unique keys at the beginning and end of each data packet, rendering even brute force attacks by quantum computers ineffective.

For the first time in the more than 20 years since the adoption of AES, a new post-quantum security technology has been commercially deployed to protect the smallest of IoT devices and scale data in transit all the way through the server and back.

The IoT Security Imperative

The internet has inarguably been a major force of transformation in the global economy since its inception 50 years ago. Today, the reality of billions of connected devices is transforming its use in even greater ways.

We are at an important juncture. There is a growing awareness, in corporate boardrooms both in the US and globally, of the need for solutions to secure vital IoT infrastructure. This awareness must be accelerated and become an imperative.

Policymakers around the world are growing increasingly concerned about the potential threat from the lack of IoT security. Last year, the State of California passed legislation (SB 327), which will take effect in January 2020. The new law requires all connected devices to have what's specified in the legislation as a "reasonable security feature."

Meanwhile, in the US, several initiatives are underway at the Congressional level that seek to address security threats related to connected devices. Sens. Ron Johnson (R-WI) and Mike Rounds (R-SD) have expressed concern that government

security efforts may be hampered by not having a single agency in charge of cybersecurity. There are over 250 departments within federal government agencies with "cybersecurity" in the title, but there's no coordinating entity or person. To fill any gaps, the senators are considering a centralized agency that would oversee national cybersecurity efforts, including connected devices.

Most recently, a bipartisan, bicameral bill – the Internet of Things (IoT) Cybersecurity Improvement Act of 2019 – was introduced in the Senate by Sens. Mark Warner (D-VA) and Cory Gardner (R-CO), co-chairs of the Senate Cybersecurity Caucus, and in the House by Reps. Robin Kelly (D-IL) and Will Hurd (R-TX). The bill would require the government to make sure that any devices it purchases meet minimum security requirements.

In Japan, the government announced earlier this year that it will run penetration tests against all IoT devices in an effort to figure out what is insecure and help consumers secure them. That was a bold move, and it will be interesting to see the results of those tests and related changes in IoT security. There is also movement in Europe and the UK to develop IoT standards. The European Union has already enacted the General Data Protection Regulation (GDPR), requiring security on all future digital connected devices. The European Telecommunications Standards Institute (ETSI) recently developed the first globally applicable standard (TS 103 645) for consumer IoT security.

We expect to see much more in the future on the standards and regulatory front, globally, with respect to IoT security. However, government legislation and initiatives are largely required because industry has been far too slow in deploying security measures. When industry acts first, government regulation becomes less necessary. Immediate industry response can still circumvent some mandatory government-initiated regulations.

To sum up, the opportunities associated with IoT are enormous, but so too are the challenges with respect to securing connected IoT devices. Initiatives within the private and public sectors today to ensure the security of the billions of connected IoT devices are paramount to creating a secure, connected future. AES / TLS have served us well in the past, but they have not evolved at anywhere near the speed of computing platforms and are not compatible with constrained endpoints, nor are they quantum-computing–resistant. We need to employ new solutions now.

This need will only grow as quantum computers move from development to deployment. The upcoming FiRe 2019 conference at Torrey Pines will be a superb place to discuss securing our future.

Paul wishes to thank his colleagues at AgilePQ for their helpful input in preparing this SNS Special Letter.

About Paul Clayson

Paul Clayson joined AgilePQ in 2017, bringing extensive experience in launching and growing early-stage companies. Paul has launched four disruptive technology companies and served as CEO to five early-stage companies in nanotechnology, automotive, graphene, carbon nanotube, PCB, microprocessor, and other advanced technologies. He has deep experience with company governance and boards, and a broad global network of venture and PE firms. Paul currently serves in advisory and mentor roles with the Stanford University TomKat Center for Sustainable Energy, the North Carolina Joint School of Nano-Science and Nano-Engineering (JSNN).

About AgilePQ

AgilePQ provides quantum-safe enterprise Internet of Things security solutions. Headquartered in Salt Lake City with offices in Seattle, San Diego, and Boulder, the company has developed a complete IoT endpoint security solution for the evolving edge that is quantum-computing–resistant. The AgilePQ SLiM IoT solution fits in 2.4 KB and can confidently Provision, Deploy, Identify, Authenticate, and Authorize all IoT devices, no matter how small. SLiM integrates seamlessly with an organization's existing network and cloud infrastructure, including endpoint devices incapable of using TLS. For more information, please visit agilepq.com.

I would like to thank Paul for taking the time to share a fresh technical and legal view of a problem most of us have considered not solvable, and Steve Waite for his technical assistance and role as connector.

And last, but never least, our gratitude to Editor-in-Chief Sally Anderson, for putting all of these thoughts into perfect shape.

Your comments are always welcome.

Sincerely,

Mark R. Anderson

CEO
Strategic News Service LLC Tel.: 360-378-3431
PO Box 1969 Fax: 360-378-7041
Friday Harbor, WA 98250 USA Email: mark@stratnews.com

CLICK HERE TO SHARE THIS SNS ISSUE

To arrange for a speech or consultation by Mark Anderson on subjects in technology and economics, or to schedule *a strategic review* of your company, email mark@stratnews.com.

For inquiries about **Partnership or Sponsorship Opportunities** and/or SNS Events, please contact Berit Anderson, SNS Programs Director, at berit@stratnews.com.

INSIDE SNS

Visit "Inside SNS" for:

- Photo galleries of FiRe and other SNS events
- FiRe videos
- SNS iNews®
- The SNS blog, "A Bright Fire"
- The SNS Media page
- SNS FiReFilms
- Subscription rates and permissions
- About SNS and About the Publisher

UPCOMING SNS EVENTS

FiRe2019™

We look forward to returning to our FiRe roots on the beautiful California coast, **October 8-11, 2019, at The Lodge at Torrey Pines in La Jolla**.

Join us for four days of industry-changing conversations, problem-solving with global leaders, lively debates, and social events, including an exclusive tour of UCSD's Calit2 Lab. And you'll connect with the world's most strategic thinkers and doers on tech, business, climate, and the global economy.

Registration is $5,900 and includes all meals, social activities, program sessions, and networking events.

Our growing roster of 2019 speakers and moderators includes:

- **Ilshat H. Kokbore,** President, Uighur American Assoc.
- **John Mattison,** Emeritus Asst. Medical Director and CMIO, Kaiser Permanente
- **Chris Hegedus,** Documentary Filmmaker, Pennebaker Hegedus Films
- **Jim Louderback,** GM, VidCon
- **Susan C. Schnabel,** Co-Founder and Co-Managing Director, aPriori Capital Partners
- **Derek Harp, CEO,** Control System Cyber Security Assoc. International (CS2AI)
- **Stephen Honikman,** Co-Founder and CEO, Emergent Microgrid
- **Kimberly Prather,** Distinguished Chair in Atmospheric Chemistry, UCSD
- **Elizabeth Unger,** National Geographic Explorer and Filmmaker
- **Anand Rao,** Partner, Advisory Services, and Global AI Lead, PwC
- **J. Augusto de Oliveira,** EVP & CTO, Cypress Semiconductor
- **H.E. Ambassador Abraham Wen-Shang Chu,** Director General, Taipei Economic and Cultural Office in Los Angeles
- **Bob Flores,** CEO, Applicology Inc., and former CTO, CIA
- **Paul Maher,** General Manager, Microsoft
- **Harri Hursti,** Founding Partner and Hacker, Nordic Innovation Labs
- **Susi Snyder,** Nobelist and President, ICAN
- **Jeff Loucks,** Executive Director, Technology, Media, and Telecommunications Center, Deloitte
- **George Church**, Professor of Genetics, Harvard Medical School; Director, PersonalGenomes.org
- **Paul Jacobs,** CEO, XCOM
- **Ali Douraghy,** Chief Strategy Officer, Earth & Environmental Sciences, Berkeley Lab
- **Anne Hardy,** CSO, Join Digital Inc.
- **Jody R. Westby,** CEO, Global Cyber Risk
- **Kim Stanley Robinson**, Hugo-Winning Author of Science Fiction
- **Judy Korin** (Producer) and **Pedro Kors** (Writer / Producer), *The Great Hack*
- **Maryanne Morrow,** CEO, 9th Gear Technologies Inc.
- **Jack Gilbert,** Professor, UCSD School of Medicine and Scripps Institution of Oceanography; Group Leader for Microbial Ecology, Argonne National Laboratory
- **Steve Fey,** CEO, Totem Building Cybersecurity
- **David Gruber,** Presidential Professor of Biology, City University of New York / National Geographic Society

- **Pam Taub,** Founder and Director, Step Family Foundation Cardiovascular Rehabilitation and Wellness Center, Jacobs Medical Center, UCSD
- **Georg Kopetz,** CEO, TTTech Auto AG
- **Vanessa Pegueros,** Board Member, Carbon Black and BECU; former VP and CISO, DocuSign
- **Jason Schwartz,** CEO, Ecellix Inc.
- **Dmitri Alperovitch**, Co-Founder and CTO, CrowdStrike
- **Satchin Panda,** Professor, Regulatory Biology Laboratory, Salk Institute
- **David Brin,** Founder, Futures Unlimited; Sci-Fi Author & Physicist
- **Lyndsay Keys,** Documentary Filmmaker, The Lyme Trials LLC
- **Rob Knight,** Founding Director, Center for Microbiome Innovation; Professor, Pediatrics and Computer Science and Engineering, UCSD
- **David Ewing Duncan,** Author and Independent Correspondent; CEO, Arc Programs
- **John Wells,** Producer and Co-Host, "Cool Science Radio," KPCW (NPR Affiliate)
- **Larry Smarr,** Director, California Institute for Telecommunications and Information Technology (Calit2); Harry Gruber Professor of Engineering, UCSD
- **Kimberly Dozier**, Global Affairs Analyst, CNN; Contributor, The Daily Beast
- **The Pattern Computer Team** (www.patterncomputer.com)

And more to come ---

Register Now!

WITH GREAT APPRECIATION TO:

Our Global Platinum and FiReFilms Partner:

ORACLE

Global Silver Partners:

accenture
High performance. Delivered.

Crown Sterling

Deloitte.

PATTERN COMPUTER®

Silver Academic Partner:

UC San Diego

Exhibitor:

OtoNexus MEDICAL TECHNOLOGIES

And Focus Channel Partners:

VENAFI Viasat

… for their Partnership and Support of SNS events.

ADDITIONAL SUPPORTING ORGANIZATIONS

FiRe Academic Partner:

SCI www.sci.utah.edu

FiRe Event Sponsor:

HAND OF GOD *creating memorable moments*

And a warm welcome to our FiReStarter 2019 companies:

AGILEPQ BioLogiQ Smart Solutions For A Sustainable World

cloudeo ECELLIX BATTERY INNOVATIONS joule

Where's Mark?

• On October 2 and 3, Mark will be a panelist at the Department of Energy "AI XLab" conference, hosted by Argonne National Laboratory and Oak Ridge National Laboratory, on "AI and Precision Medicine," at the Drake Hotel in Chicago. • On October 8-11, he will be hosting the 17th annual Future in Review Conference, at The Lodge at Torrey Pines in La Jolla, California. Seats are limited, so register now, at: http://www.futureinreview.com/. • On November 19-20, he will be speaking at the Info-Tech LIVE conference in Las Vegas, at the Cosmopolitan Hotel.

ISSN 1093-8494