USTELECOM | THE BROADBAND ASSOCIATION

Global Leadership of Broadband Providers in Securing the Internet of Things (IoT)

By Robert Mayer and Paul Eisler

Contents

USTELECOM | THE BROADBAND ASSOCIATION

Global Leadership of Broadband Providers in Securing the Internet of Things (IoT)

By Robert Mayer and Paul Eisler

USTelecom is the trade association that represents a diverse membership that ranges from large publicly traded global communications providers to small companies and cooperatives all of whom are committed to the security of the digital ecosystem as an essential driver of innovation, economic growth, public safety, our national security and other societal benefits.

I. IoT Security Challenges

The Internet of Things (IoT), a broad term referring to many categories of devices that connect to the internet, holds the promise of great benefits for modern society, both as a consumer-driven economic force that improves quality of life and as powerful sets of tools designed to increase efficiencies in measurable ways across businesses, governments, and non-profits. Today, we already see those benefits in diverse areas such as energy management, manufacturing, health care, and transportation to name a few. Yet, with 30 billion connected devices expected within a few short years and further exponential growth a virtual certainty, securing IoT is among the chief cybersecurity challenges we face today.[1]

By now, we have a significant body of evidence that points to the harmful consequences of poorly-designed and managed connected devices. While some manufacturers take great care to secure their products, the sobering reality is that as IoT has grown and evolved, the security flaws have not been adequately addressed in many parts of the ecosystem, and not enough consideration has been given to the implications for the broader digital economy. Two separate studies – one of which surveyed about 400 technology executives in 19 different countries – found that 46% of companies that deploy IoT products have experienced security incidents, and the costs of handling these incidents exceeds ordinary security breaches.[2]

Like many transformative technologies, IoT has radically increased the attack surfaces that malicious actors can target and exploit. These factors include, among others, sophisticated cybercriminals, ideologically motivated hackers, and well-financed, state-sponsored hacking groups with destructive ambitions.

Now, there is an urgent need for industry and governments across the globe to work together to fight back against these threats through collaborative engagement across multiple venues and jurisdictions to drive real-world, ecosystem-wide operational solutions.

A. The Evolving Problem of IoT Botnets

The sustained level of insecurity in IoT devices has facilitated the growth and evolution of botnets. Botnets are large networks of compromised devices that malicious actors can use to conduct a wide range of nefarious activities, such as infecting systems with malware, launching denial of service attacks, and spreading disinformation on social platforms. While botnets are not a problem exclusive to IoT, the sheer ubiquity of these devices and attendant insecurities have greatly exacerbated the problem.

One cannot discuss IoT security incidents without acknowledging the infamous Mirai Botnet, which at its peak ensnared more than 600,000 IoT devices – including devices such as surveillance cameras and wireless routers, and more.[3] On October 21, 2016, Mirai weaponized an army of infected devices against Dyn, a major DNS provider.[4]

Without owners of the compromised devices noticing any disruption, the devices began stealthily wreaking havoc along the U.S. East Coast, causing millions of people to suddenly lose access to major websites.[5] The consequences were tangible. Businesses could not reach their customers; citizens lost access to news, financial platforms, social media, and many other online services.[6] The economic damage approximated $100 million dollars in just a few hours.[7]

Since then, IoT botnets based on Mirai's code have become part of many hackers' arsenals. Because Mirai's code has been publicly released,[8] criminals in different parts of the world can experiment and create their own variants of IoT botnets. Strategies that would have worked against Mirai will not necessarily work against the newer botnets.[9]

In January 2018, one of Mirai's descendants attacked global financial institutions.[10] Whereas Mirai needed default passwords to gain control of devices, newer botnets like Satori – which generated about 280,000 bots within 12 hours – Wicked, and Reaper have found ways around this weakness.[11] Because of the evolution of IoT botnets, many devices that would have been impervious to Mirai may end up becoming part of a botnet today.

To make matters worse, some of the new botnets can be rented for a low fee by cyber-criminals who lack the technical skills to make a botnet of their own. This arrangement, called malware-as-a-service (MaaS), expands the threat landscape to a broader set of bad actors.[12]

The breathtaking scope and severity of Mirai and subsequent IoT botnet attacks has sent shockwaves throughout the global cyber policy community. These incidents have become a rallying call to action, not just in the United States but across the world. Securing connected devices is essential to mitigate the botnet threat.

B. IoT Vulnerabilities Undermine Trust in the Digital Economy

Besides economic damage, IoT vulnerabilities undermine essential trust in the platforms that constitute the digital economy. Security cameras can be used to invade their owners' privacy.[13] Confidential personal or business information can be stolen through seemingly innocuous IoT devices, such as thermometers.[14] Deeply personal objects, from children's toys[15] to baby heart monitors[16] are vulnerable to hackers. Vehicles can potentially be manipulated to cause deadly traffic accidents.[17] Hackers can manipulate temperature in smart homes,[18] and whole buildings have lost heat in the middle of winter.[19] Even *surgically implantable* healthcare devices, such as pacemakers and defibrillators, have been discovered to be hackable.[20]

Concerns of this kind can have a massive influence on public perception of technologies, and if not addressed in meaningful ways, trust in the digital ecosystem will erode, causing unpredictable levels of disruption and economic harm.

C. Market Incentives Need Improved Alignment

Beyond the technical and operation challenges of securing IoT against malicious actors, there is the problem of incentives. Due in large part to the first-to-market mentality that has characterized highly prevalent business models, the current state of IoT device security can be attributed to what is commonly referred to as a "tragedy of the commons" situation.[21]

Everyone wants better security in theory, but many companies pursuing what can be deemed as rational business interests will often fail to produce sufficiently secure devices. Central to this problem is the fact or widespread perception that consumers will not pay more for better security.

One possibility is that consumers are uninformed about IoT security risks. USTelecom and many of our members engage in cybersecurity educational programs and initiatives, including webinars, publications, and in-person events. We participate in Cybersecurity Awareness month and develop an annual Cybersecurity Toolkit that addresses the topic of IoT security.

Many consumers, however, seem not to care about IoT security risks for low-end devices that will soon be disposed – even when they are educated about the nature of the risks – since they do not perceive any personal benefit for the additional cost.

Because consumers do not demand better security, many manufacturers, especially for the low-end products, are not providing it. Secure products are costlier to produce. If consumers are unwilling to pay the higher costs associated with securing products, it is generally believed that those manufacturers who do the right thing will either absorb costs directly and thus forego revenues or their products will be costlier and less competitive, causing them to lose market share.

These harmful incentives are compounded by the first-to-market mentality. It is conventional wisdom expressed by many market analysts that products that appear on the market first will

have competitive advantages. Manufacturers are therefore incentivized to get their devices on the shelf first which in some instances compromises security.

There are of course exceptions to this generalization. Just about everyone will want a secure pacemaker, for example, considering it will be surgically implanted and one's life literally depends on it. But it is unclear that consumers care about ordinary devices they expect to soon dispose of. And these devices can produce serious consequences due to their volume.

Often, the apparent harm of an insecure IoT device will befall third parties rather than the consumer. This further diminishes market demand signals for improved security. What is clearly needed is a common set of baselines so that all manufacturers in the ecosystem play by the same rules and responsible manufacturers do not lose market share or suffer competitive disadvantages for doing the right thing.

D. Conflicting Security Standards Impede Progress

Given the significance of IoT security to governments across the world, it is understandable that both U.S. and foreign policymakers are eagerly searching for solutions. Alongside industry and civil society recommendations, many governments have established or are in the process of establishing recommendations or standards for IoT security.

Government has a vital role in supporting industry initiatives and the evolving standards and practices that are necessary to combat this growing threat. It is our view that voluntary, prioritized, flexible and cost-effective solutions embodied in the NIST Cybersecurity Framework can be effectively applied in the IoT space. We are also mindful that many states are pursuing legislation in this area and we are concerned that a patchwork quilt of state compliance requirements will add complexity, confusion and costs to an already challenging global landscape. In the digital ecosystem, no jurisdiction exists totally independent of others. Therefore, recommendations aimed at setting standards in one part of the ecosystem, while ignoring the others, are misjudging the scope and nature of the IoT security challenge.

The U.S. government should speak with one unified voice on the world stage, as a collaborator in the global industry-facilitated standards creation process. We believe the best way forward is through global policy harmonization – not fragmentation. Inconsistent and overlapping IoT security recommendations, whether by different U.S. states or different countries, significantly increases the risk of confusing consumers, retailers, enterprises, and other stakeholders, especially when it comes to the actual implementation of cybersecurity capabilities. Fragmentation also limits the growth of IoT and the digital economy by reducing efficiencies of scale – hindering efforts to create better and more secure products.

II. Industry Leadership

In the fight against cyber threats, industry is often on the front lines. It is therefore essential to minimize barriers to the adoption of cybersecurity practices, so that more stakeholders are able to combat the threat effectively. Governments are in widespread agreement that mitigating the most serious IoT-related threats will require multi-jurisdictional collaboration. Although important conversations can take place on a government-to-government basis, effective collaboration across borders will require global input from industry and in many cases industry leadership.

The major IoT manufacturers and providers of IoT-related services, such as cloud services that increase security, are global in nature. These companies have experience combating cyber threats in many contexts and environments. Governments should take steps to protect their own connected devices and systems from cyber threats, while leveraging the private sector's expertise to effectively implement IoT solutions ecosystem-wide.

A. Broadband Providers' Cost-Effective Solutions

Broadband providers own and operate the networks that connected devices connect to. As such, they are an important part of the ecosystem-wide solution to IoT security. For example, AT&T and Ericsson recently joined forces to make IoT security testing and certifications available to businesses.[22] The testing process identifies device vulnerabilities that could compromise data transmitted across communications networks.

In addition, USTelecom members use a variety of botnet detection and filtering techniques; provide IoT managed security services; and collaborate with security researchers and law enforcement to limit the destructive potential of IoT botnets.

Networks at every level are evolving to accommodate exponential growth in traffic associated with billions of new end-point devices. The introduction of 5G and the associated architecture will allow industry to incorporate security measures into more layers than in previous generations.

ISPs, security vendors and other infrastructure providers are developing improved security offerings, such as firewalls that more intelligently identify authorized users and attackers. While these solutions are generally effective where deployed, economic barriers and technological challenges impede their ability to scale on an ecosystem-wide basis.

Consequently, a holistic ecosystem-wide approach to IoT security must include baselines for devices and device systems. That is why we have partnered with a broad variety of stakeholders in the digital ecosystem who are committed to addressing the root causes of IoT vulnerabilities.

B. Council to Secure the Digital Economy (CSDE) Formed to Advance Coordinated, Industry-led Activities

Commitment to ecosystem-wide solutions led to establishment by USTelecom in 2018 of the Council to Secure the Digital Economy (CSDE). Created in partnership with ITI, CSDE is led by 12 global ICT companies whose mission is to identify sophisticated and evolving cyber threats and the security practices that, if widely adopted, would materially contribute to the resiliency and sustainability of the global digital economy.

In November 2018, the CSDE, in strategic partnership with the Consumer Technology Association (CTA), published the *International Anti-Botnet Guide*.[23] This Guide discusses the problems inherent of IoT security and contains sets of baseline practices and advanced capabilities that are directly relevant to securing connected devices and the enabling infrastructure.

In recognition that sophisticated malicious actors are constantly maturing their capabilities, we have committed to updating the guide on an annual basis. As a result of our leadership in this space, the CSDE was mentioned no less than nine times in the U.S. government's Botnet Roadmap, developed jointly by the Departments of Commerce and Homeland Security.[24]

In 2019, we at USTelecom, through the CSDE, continue to demonstrate our commitment to a secure digital economy by focusing squarely on IoT security – one of the greatest challenges facing the ecosystem. After surveying the work and recommendations of dozens of industry alliances and organizations in the United States abroad, the CSDE, in partnership with CTA, convened a subset of fifteen organizations to produce a consensus set of IoT baseline capabilities.

Through this collaborative industry-led process, we found significant agreement on core baseline capabilities that – if adopted throughout the IoT ecosystem – would significantly reduce the cyber threat. These core baselines would be applicable to all types of IoT devices.

C. Next Steps Toward Global Policy Harmonization

Significant work remains to be done. The CSDE's work in the IoT arena will be used to inform industry and governments in many parts of the world as they work to develop common IoT capabilities for the global market.

Both the U.S. government and private industry are engaged in a variety of global initiatives aimed at improving IoT security, in cooperation with our foreign jurisdiction counterparts. We are strongly supportive of U.S. government and industry collaboration on IoT security at the federal level, through the highly successful public-private partnership model. The very nature of this challenge requires a highly adaptive and evolving response in as close to real-time as possible. That level of innovation and operational implementation can only be realized when policies are carefully aligned with market dynamics.

We are paying close attention to the European Union's Cybersecurity Act, which is set to give the EU Agency for Network and Information Security (ENISA) powers to establish a certification regime for ICT products and services, including those directly related to IoT. The need to secure connected devices is among the principal drivers of this sweeping European legislation, which can have significant consequences for U.S. industry.

In Japan, the Ministry of Economy, Trade and Industry (METI) has released a draft Cyber/Physical Security Framework pertaining to IoT and related systems; this framework could have implications for U.S. companies that want to do business with our major trading partner.

Many other initiatives are underway in countries throughout the world, and as time goes on the risk of fragmentation increases. What we need is a global standard that unites diverse countries and jurisdictions under a common set of baseline capabilities for IoT security.

Governments throughout the world have an important role to play, alongside industry, in adopting and promulgating common recommendations that measurably improve IoT security against malicious exploits, thereby protecting their citizens from ecosystem-wide threats that exist simultaneously within and beyond their own borders. Harmonization across these jurisdictional and geographical boundaries that do not exist in cyberspace is critical to the long-term sustainability of a global digital ecosystem.

---

[1] Susan Galler, *How 30 Billion IoT Connections Will Build Future Industries*, FORBES (Mar. 5, 2018), https://www.forbes.com/sites/sap/2018/03/05/how-30b-iot-connections-will-build-future-industries/#76dc16e35126.

[2] Dawn Kawamoto, *IoT Security Incidents Rampant and Costly*, DARK READING (July 18, 2017), https://www.darkreading.com/vulnerabilities---threats/iot-security-incidents-rampant-and-costly/d/d-id/1329367.

[3] Garrett Graff, *How a Dorm Room Minecraft Scam Brought Down the Internet*, WIRED (Dec. 13, 2017), https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet.

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] G Data, *IoT: Mirai-creators Get Mild Sentences After Cooperation* (Sept. 24, 2018), https://www.gdatasoftware.com/blog/2018/09/31124-botnet-no-jailtime-for-mirai-creators.

[8] Brian Krebs, *Source Code for IoT Botnet 'Mirai' Released*, KREBS ON SECURITY (Oct. 1, 2016), https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released.

[9] *See* SentinelOne, *Mirai Botnet Descendants Will Lead to Even Bigger Internet Outages*, CSO (Dec. 22, 2016) https://www.csoonline.com/article/3153031/mirai-botnet-descendants-will-lead-to-even-bigger-internet-outages.html

[10] Zack Whittaker, A New Mirai-Style Botnet Is Targeting the Financial Sector, ZDNET (April 5, 2018), https://www.zdnet.com/article/new-mirai-style-botnet-targets-the-financial-sector.

[11] *See, e.g.*, Grace Johansson, *Satori Botnet Able to Launch Crippling Attacks at Any Time*, SC MAGAZINE UK (Dec. 8, 2017), https://www.scmagazineuk.com/satori-botnet-able-launch-crippling-attacks-time/article/1473666; *see also* John Leyden, *OMG, That's Downright Wicked: Botnet Authors Twist Corpse of Mirai into New Threats*, THE REGISTER (June 1, 2018), https://www.theregister.co.uk/2018/06/01/mirai_respun_in_new_botnets.

[12] Chris Bing, *You can Now Buy a Mirai-Powered Botnet on the Dark Web*, CYBERSECOOP (Oct. 27, 2016), https://www.cyberscoop.com/mirai-botnet-for-sale-ddos-dark-web.

[13] Ms. Smith, *Hijacked Nest Devices Highlight the Insecurity of the IoT,* CSO (Feb. 4, 2019), https://www.csoonline.com/article/3338136/hijacked-nest-devices-highlight-the-insecurity-of-the-iot.html.

[14] Oscar Williams-Grut, *Hackers Once Stole a Casino's High-roller Database Through a Thermometer in the Lobby Fish Tank*, BUSINESS INSIDER (Apr. 15, 2018), https://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4.

[15] Glenn McDonald, *Strange and Scary IoT Hacks: Child's Plays*, NETWORK WORLD (July 3, 2018), https://www.networkworld.com/article/3285968/strange-and-scary-iot-hacks.html#slide3; Glenn McDonald, *Strange and Scary IoT Hacks: Toy Stories*, NETWORK WORLD (July 3, 2018), https://www.networkworld.com/article/3285968/strange-and-scary-iot-hacks.html#slide4.

[16] Iain Thomson, *Wi-Fi Baby Heart Monitor may Have the Worst IoT Security of 2016*, THE REGISTER, (Oct. 13, 2016), https://www.theregister.co.uk/2016/10/13/possibly_worst_iot_security_failure_yet.

[17] Andrew Meola, *Consumers Don't Care if Their Connected Car can Get Hacked – Here's Why That's a Problem*, BUSINESS INSIDER (Mar. 7, 2016), https://www.businessinsider.com/smart-car-hacking-major-problem-for-iot-internet-of-things-2016-3 ("Hackers could potentially crash a compromised car, but they are more likely to exploit IoT devices to gain entry to corporate and government networks and databases.").

[18] Luke Denne et al., *We Hired Ethical Hackers to Hack a Family's Smart Home — Here's How It Turned Out*, CBC NEWS (Sept. 28, 2018),)https://www.cbc.ca/news/technology/smart-home-hack-marketplace-1.4837963.

[19] Lee Mathews, *Hackers Use DDoS Attack To Cut Heat To Apartment*, FORBES (Nov. 7, 2016), https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/#2b7483fb1a09.

[20] Selena Larson, *FDA Confirms that St. Jude's Cardiac Devices can Be Hacked*, CNN BUSINESS (Jan. 9, 2017), https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack.

[21] Samuel Bieler, *Market Dynamics Encourage Weak Security in Consumer IoT*, NYU SCHOOL OF LAW (Mar. 5, 2019), https://wp.nyu.edu/compliance_enforcement/2019/03/05/market-dynamics-encourage-weak-security-in-consumer-iot.

[22] Ericsson, *AT&T and Ericsson team up on IoT cybersecurity* (Sept. 26, 2018), https://www.ericsson.com/en/news/2018/9/iot-cybersecurity---att-and-ericsson.

[23] Council to Secure the Digital Economy, INTERNATIONAL ANTI-BOTNET GUIDE (2018), https://securingdigitaleconomy.org/wp-content/uploads/2018/11/CSDE-Anti-Botnet-Report-final.pdf.

[24] U.S. Dep't of Commerce & U.S. Dep't of Homeland Sec., A ROAD MAP TOWARD RESILIENCE AGAINST BOTNETS (2018), https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_0.pdf.