DE GRUYTER
OPEN

Defining the IoT

Dan-Radu BERTE
Santa Clara, California, USA
danberte@gmail.com

Abstract. *IoT, or the Internet of Things, has been in use since circa 1999. It defines a next chapter in the evolution of the Internet where computing devices embedded in everyday objects are able to send and receive data themselves. In recent years miniaturization and economies of scale brought a boon of new devices to the consumer and enterprise market, prompting Gartner to predict over 20bln live IoT devices by 2020. However, the definition of IoT is loose and, for the purpose of predicting trends or discussing security, formulating a clear understanding of the term is crucial. In fact, Internet of Things is a term only mostly used by the media, academia and the industry. Customers in the consumer space refer to the technologies by their benefit describing term of "Smart Home". A quick analysis of this gap shows how it's entirely possible no knowledge permeates the business and market worlds because of the incompatible terms used. As more devices, OSes and heterogeneous platforms entrench the concept of a new digital lifestyle, the new "Digital Kingdom" opens its doors to radical disruption, such as the latest massive Mirai and Reaper attacks. Our ability to correctly define the IoT, it's platforms and components, should lead to better market dynamics and better preparedness, as one can't secure something that can't be defined. This paper proposes to further understand the IoT by exploring available definitions, reiterating misuse and equivocal perception, concluding with a more suiting, contemporary definition.*

Keywords: Internet of Things, IoT, Cybersecurity, Smart Home, AI, Machine Learning.

Introduction

Almost 20 years after its first use as a solution looking for a problem, The Internet of Things (abbreviated IoT) descends into the lives of many as a real, tangible infrastructure of hundreds of millions of new devices that collaborate and distribute data among them or over the internet. But it means different things to many.

To consumers the IoT takes the form of novel smart thermostats, connected security cameras, smart TVs and baby monitors, but also laptops, printers or routers. The industries see connected frameworks of sensors and pumps in smart manufacturing plants.

Though revisited down about 20% (or 5bln devices), there will be 8.4 billion connected things in 2017, setting the stage for 20.4 billion devices to be deployed by 2020, according to analyst firm Gartner. "The 2020 total of IoT devices installed across the world will be more than twice this year's figure". Tung. L, (2017, February 7), IoT devices will outnumber the world's population this year for the first time, retrieved from www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/

New IoT products enrich and simplify life through targeted and context aware, connected, smart devices. They bring cost down and improve efficiency in transportation, energy generation, manufacturing and education. This accelerates growth of new industries and startups in manufacturing, cloud computing, energy, automation, machine learning, AI and cybersecurity. Its largest obstacle to adoption: concerns about privacy and security. But what can't be accurately defined, can't be, consequently, secured.

DOI: 10.2478/picbe-2018-0013

For one of the buzzwords with the fastest growth in relevance in history, scientific study has focused little on structure, beyond observation. There's abundant literature, as this study enumerates in the following, that somewhat wrongly assumes a previous mutual understanding of the concept.

In fact, even the Wikipedia page on the Internet of Things notes, on May 2017, that the article has "multiple issues", needing "additional citations for verification" and "attention from an expert on the subject". The note is still actual as of February 2018.

Definitions of the Internet of Things

The Internet of Things term is coined by Kevin Ashton, co-founder of the Auto-ID Center at the Massachusetts Institute of Technology (MIT):

"I could be wrong, but I'm fairly sure the phrase "Internet of Things" started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999. Linking the new idea of RFID in P&G's supply chain to the then-red-hot topic of the Internet was more than just a good way to get executive attention. It summed up an important insight which is still often misunderstood." Ashton (2009).

Popular knowledge crowdsource website Quora has members try to answer what the IoT is under multiple entries. The accented "What exactly is Internet of Things (IoT)?" has over 106,000 views, over 300 responses and 30, similar, merged questions.

Oxford Dictionary (where IoT was added in August 2013) defines it as: A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data.

Wikipedia files IoT as "uniquely identifiable objects and their virtual representations in an Internet-like structure".

Webopedia, "the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems".

Whatitis.com defines IoT as "a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction".

Forbes defines IoT as "the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig". Morgan (2014)

Postscapes.com proposes a compendium of definitions collected from research publications and conference titles under the aptly named "What is the meaning of IoT exactly?" page.

According to the website, "the term was added to the 2011 annual Gartner Hype Cycle that tracks technology life-cycles from "technology trigger" to "plateau of productivity" and has hit the Hype Cycle's "Peak of Inflated Expectations" in 2014".

Internet of Things versus the Smart Home

In 1998 Apple presented the new Bondi Blue iMac, and with it, the concept of an internet connected PC at the heart of everything digital.

Having the PC as the hub of the digital life had multiple reasons anchored in economics. Peripherals relied on PCs for their processing power and storage. One other limiting factor to the growth of the internet, personal computers and independent, connected, peripherals was the finite and rather low number of assignable IP addresses under the deprecated IPv4 system.

According to Wikipedia, Internet Protocol version 4 provides just 2^{32} (4,294,967,296) addresses. However, large blocks of IPv4 addresses are reserved for special uses and are unavailable for public allocation. On 15 April 2011, APNIC was the first regional Internet Registry to run out of freely allocated IPv4 addresses. The IPv4 provides an insufficient number of publicly routable addresses to provide a unique address to every Internet device or service.

In a typical household, the ISP would allocate an IPv4 address that was translated using a method called NAT (Network Address Translation), essentially cascading all connected devices in the home under a private subnet. Devices under NAT were not directly addressable from the internet.

IPV6 launched publicly in 2011. The new protocol allows for 2128 (approximately 340 undecillion or 340,282,366,920,938,463,463,374,607,431,768,211,456) addresses or as Steven Leibson, a senior Silicon Valley marketing director put it, “we could assign an IPV6 address to every atom on the surface of the earth, and still have enough addresses left to do another 100+ earths.” Leibson, S,. (2008, March 28), IPV6: How Many IP Addresses Can Dance on the Head of a Pin?, retrieved from https://www.edn.com/electronics-blogs/other/4306822/IPV6-How-Many-IP-Addresses-Can-Dance-on-the-Head-of-a-Pin-

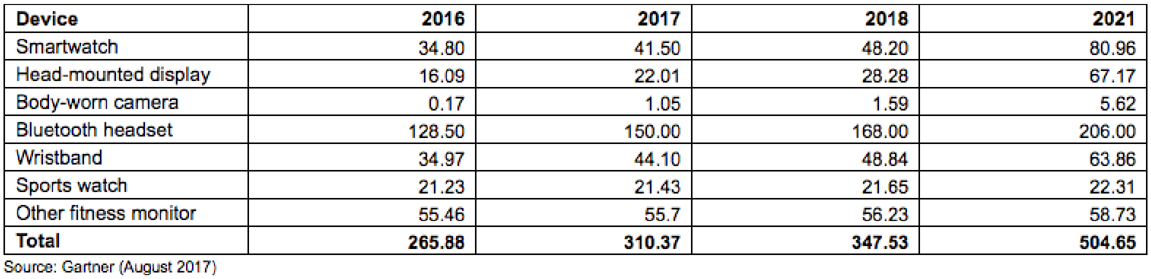
Now, with IPv6 all future connected devices may have their own unique IP address and could connect directly to the internet. LACNIC released a study on the use of Network Address Translation (NAT) in its region. They report that the vast majority of clients (94%) are behind NATs in IPv4 networks. Expectedly, that is unusual in IPv6 networks; only 0.6% are behind IPv6/IPv6 NATs, and NPTv6 appears not to be in use.

In support of research firm’s Gartner claim that over 20.4bn IoT devices will be connected to the internet by 2020 (compared to Cisco’s more aggressive 50bn devices forecast), Computerworld publishes an opinion piece called “No IoT without IPv6” (Sun, 2016).

Recently Apple changed the rules to require that all apps submitted to its App Store support IPv6-only networking. According to Google, as of December 2017, only about 20% of their visitors have already transitioned to IPv6, with over 30% adoption in North America and Europe each.

Verizon Wireless reports that about 90% of its traffic uses IPv6. T-Mobile is another leading provider in the process of turning IPv4 off. Other major cellular IPv6 providers include AT&T Wireless, Sprint, Telus, Tele2, EE, KDDI, Softbank, OTE, Rogers and many more.

In conjunction, SoCs (system on a chip) started including WiFi, Bluetooth and even cellular in one power efficient package cheap enough to make their way into everyday objects. New protocols such as WeMo, Thread, ZigBee and Z-Wave, built around the 2.4GHz spectrum, were added. These new chips broke the PC’s peripheral domination which soon started to claim their independence. Printers and HDDs became network devices, at first wired, then wirelessly. Mice and headphones dropped the cables. The iPhone stopped syncing over cable and would use WiFi.



Device	2016	2017	2018	2021
Smartwatch	34.80	41.50	48.20	80.96
Head-mounted display	16.09	22.01	28.28	67.17
Body-worn camera	0.17	1.05	1.59	5.62
Bluetooth headset	128.50	150.00	168.00	206.00
Wristband	34.97	44.10	48.84	63.86
Sports watch	21.23	21.43	21.65	22.31
Other fitness monitor	55.46	55.7	56.23	58.73
Total	**265.88**	**310.37**	**347.53**	**504.65**

Source: Gartner (August 2017)

Figure 1. Forecast for Wearable Devices Worldwide (Millions of units)

Source: http://gartner.com.

A market of $30.5bn, according to Gartner, was created just by new wearable devices developed around the now more popular smartphones (Figure 1). They would typically use Bluetooth, a low energy wireless transmission protocol, to connect directly to the smartphone.

But today, smart watches, luggage, cars, Kindles, iPads and more, come with their own LTE connectivity to the Internet, providing them with virtually limitless range and always online behavior. The platform fragmentation is so severe that retailers like Home Depot only sell connected products that play well with the top ecosystems such as Phillips's Hue, Amazon's Alexa, Apple's HomeKit and Google Home.

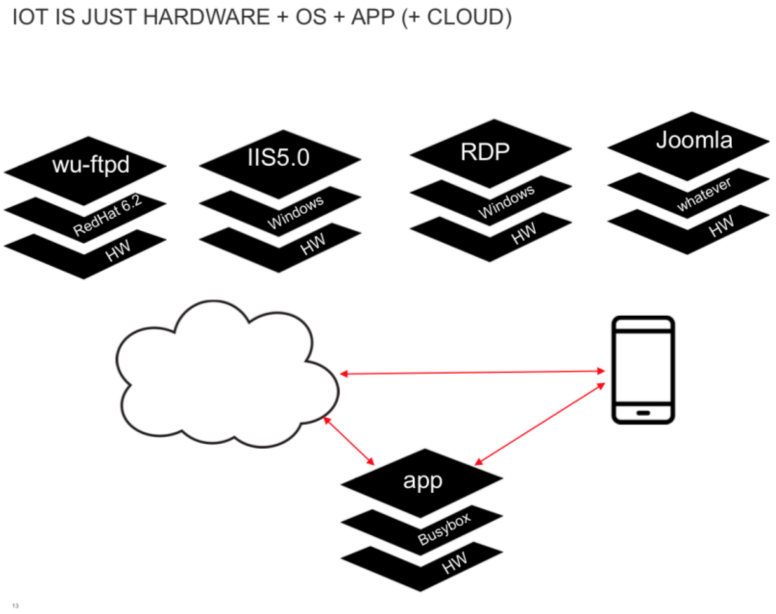


Figure 2. IoT architecture

Source: Balan (2017).

A technical representation, according to Bitdefender Chief Security Researcher, Balan (2017), the IoT is a collaboration between a hardware platform, an OS, an application (usually mobile) and the cloud (Figure 2).

An incumbent industry to reinvent itself alongside the IoT is the cybersecurity industry, which has long departed the use of “antivirus” to describe their products. With the advent of Internet-based threats, rootkits, spyware, ransomware, adware, network attacks, phishing attempts and more, a departure from the “classic” removable media infections of the past, security companies invested significantly in marketing their now even more advanced products as antimalware suites. The core product would be the same, but functionality and features would be greatly expanded. They would be called Internet Security, 360 Security, Total Security and more.

However, to consumers, the *antivirus* designation still dominates as top of mind, almost in spite of the marketing money invested in the rebranding by a determined $120bln industry. It’s been declared dead many times over, first in a historic plateau of irrelevance around the mid 2000s, second on the arrival of the “next-gen” security invasion of the mid 2010s, only to resurface again and again as the handle for all-cybersecurity scares antidote.

The format would remain intact for at least a decade, unperturbed as households added more devices. Bucharest-based cybersecurity company Bitdefender reports an average of 14 connected devices per household in 2017. With advanced routers, smart TVs, connected game consoles and more, most consumers already live in smart homes today. *“Smart” used to be mostly applied to devices in the entertainment console, but now you can kit out essentially every part of your home, from the lights in your entryway to your bed. To build the smart home of your dreams, you have to think through your priorities.* Tsukayama (2017).

The smartphone was the first to decouple the security industry from the PC focus, as vendors diversified laterally to protect Android, the popular but more vulnerable mobile OS.

Additionally, with the growth of IoT, bringing more devices online exponentially raised the attack surface by the same order.

Between 2013-2017, research from Gartner, Forrester, Parks Associates, Infonetics, BI Intelligence and more, single out security and privacy as dominant hurdles to IoT adoption, with a constant support of 30-50% of respondents. Due to the platform fragmentation in the consumer space and the more financially appealing enterprise, most research focuses around the B2B.

US consumer reports from research firm Parks Associates on barriers preventing smart home device adoption in United States broadband homes in 2015 and 2016 shows no customer preoccupation towards security or privacy. As most research and vendors would later learn, the lack of standardization would be the largest roadblock to consumer adoption of the IoT. That can be explained by vendor choices in wireless protocols, different user experience and ecosystems.

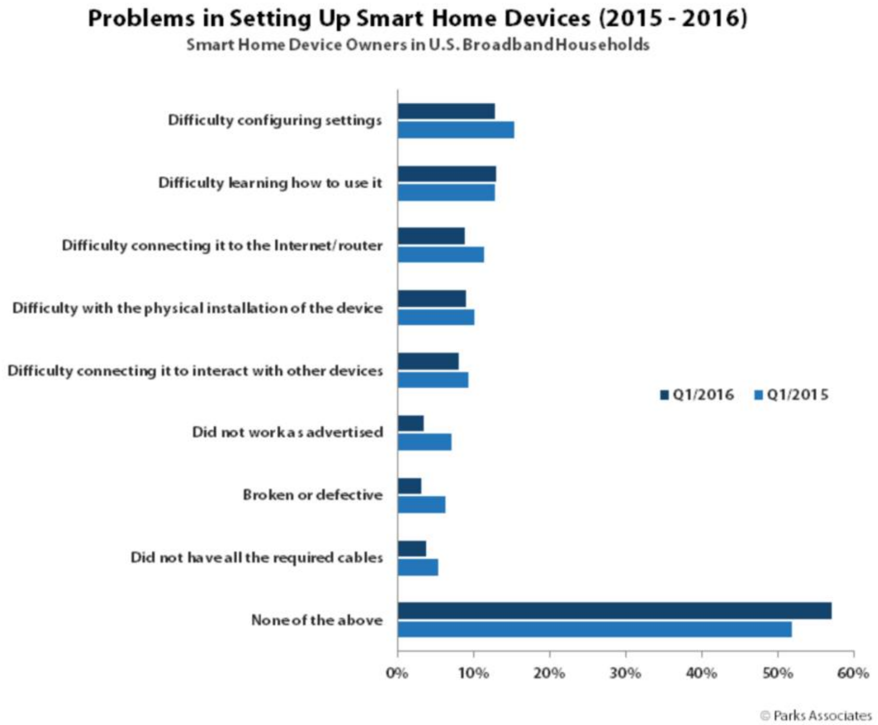


Figure 3. Concerns in setting up smart home devices according to Parks Associates

Source: http://parksassociates.com.

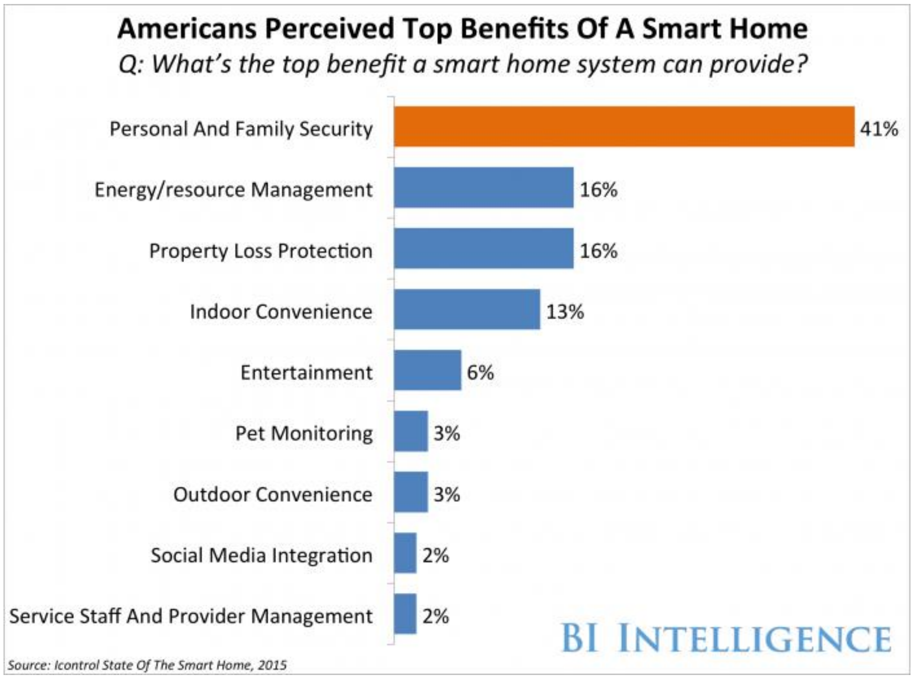


Figure 4. Benefits of a smart home according to BI Intelligence

Source: https://businessinsider.com/research/.

In fact, when BI Intelligence asked American consumers in 2015 what the perceived benefits of the smart home were, 41% surprisingly answered "Personal and family security", (Figure 4).

Public visibility for security risks presented by the IoT came with the first large scale attack that moved outside the research papers and into the real world. According to TechRepublic citing F5 labs, IoT attacks exploded 280% in the first half of 2017 (Reese, 2017).

Mirai, (Japanese for "the future", 未来), according to Wikipedia, is a "malware that turns networked devices running Linux into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks". Unexpectedly, it primarily targets online unsuspecting consumer devices such as internet surveillance cameras and home routers. The Mirai botnet was first found in August 2016 and has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks.

According to theregister.co.uk, on 21 October 2016 multiple major DDoS attacks to the DNS services of service provider Dyn occurred using Mirai malware installed on a large number of IoT devices, which took large websites such as GitHub, Twitter, Reddit, Netflix, Airbnb and many others down (Williams, 2016).

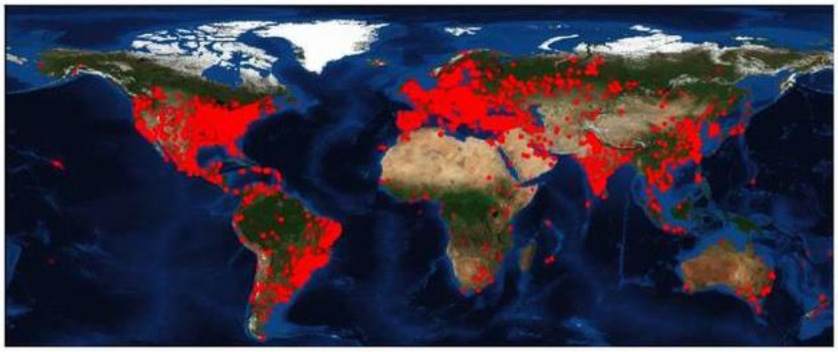


Figure 5. Geographical map of spread of the Mirai botnet

Source: https://www.theregister.co.uk/2017/11/07/mirai_botnet_sitrep/

Not much unlike Mirai, BASHLITE (also known as Gafgyt, Lizkebab, Qbot, Torlus and LizardStresser) is malware which infects IoT devices in order to launch distributed denial-of-service attacks (see Figure 5 for spread).

So are Linux.Darlloz, Remaiten and Hajime IoT worms and malware, to name a few, that demonstrated in 2017 that the threat is real.

To counter the new threats, anticipating distributing attacks leveraging consumer IoT devices, Bucharest-based security vendor Bitdefender, developed Bitdefender BOX in 2013, a hardware security solution for the modern, connected home.

The nascent industry of "security appliances" that monitor the network for anomalies in IP traffic, led by Bitdefender, includes other related products such as the BitCircle, Bullguard Dojo, Luma, Daplie, Norton Core, Disney Circle, PFP Keezel, Cujo and F-Secure Sense and DIY networking devices like Eero. These consumer-oriented devices "probably aren't ready for clients today," but these types of solutions are "something you can actually sell", notes Ihiji's Michael Maniscalco (Jacobson, 2017).

These consumer products usually install in homes alongside ISP-provided gateways or routers and monitor traffic to and from devices to the internet, block malicious websites, look for anomalous device patterns and behaviors, offer VPN lines, parental controls and much more.

Because of platform fragmentation, Bitdefender BOX-like products employ different technologies and methods to protect connected devices, from AI-driven anomaly detection engines for baby monitors to more conventional Total Security endpoint packages for PCs and Macs.

The products were a radical approach, a complete departure from the classic software applications that protected one computer at a time. It created a new category of products in a market anticipating far more connected devices that were not PCs, in the Internet of Things. Bitdefender were, at first, tempted to appeal to the IoT space with its new product, but due to the ambiguity on what exactly an IoT device meant, they relented.

Revealing trends and misuse

Let's take a look at customer trends and the language used in relation to smart home products in marketing communication.

The first, and most striking finding, is that all content can be sorted by two keyword groups, either “Internet of Things” or “Smart Home”. The terms are loosely interchangeable, but are never be used together. In fact, the media, industry events, research and specialized literature, only used the term IoT to describe new, smart devices. But when they talked about and to consumers, they always use the term “smart home”.

For cybersecurity and security consumers likely still searched for “antivirus”.

Google Trends show surprising patterns in searches for the “Internet of Things”, “IoT”, “Smart home” and “Antivirus”. Let's compare IoT and Smart Home in conjunction to antivirus and discover eventual correlations.

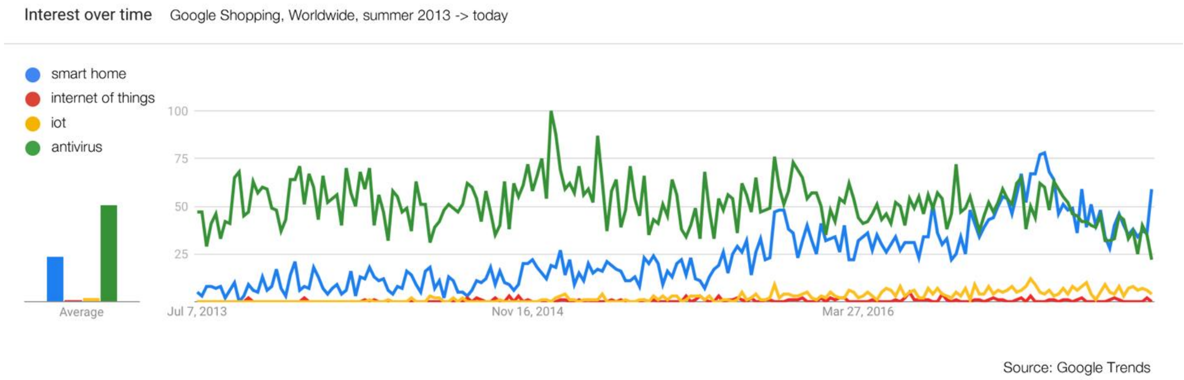


Figure 6. Shopping interest in “Smart Home”, “Internet of Things”, “IoT” and “Antivirus”

Source: https://trends.google.com.

Let's take 2013 as reference start year and look at two sets of data, one describing keyword interest over time in the Google Shopping platforms. Next, the worldwide news search data over the same 2013 to mid-2017 timeframe.

2013 sees the rise of Smart Home shopping interest, significantly up from the baseline. This is the year when Bitdefender moved Bitdefender BOX into development from R&D (Figure 6).

The complete picture becomes clear using both “Internet of Things” and “IoT” for keywords.

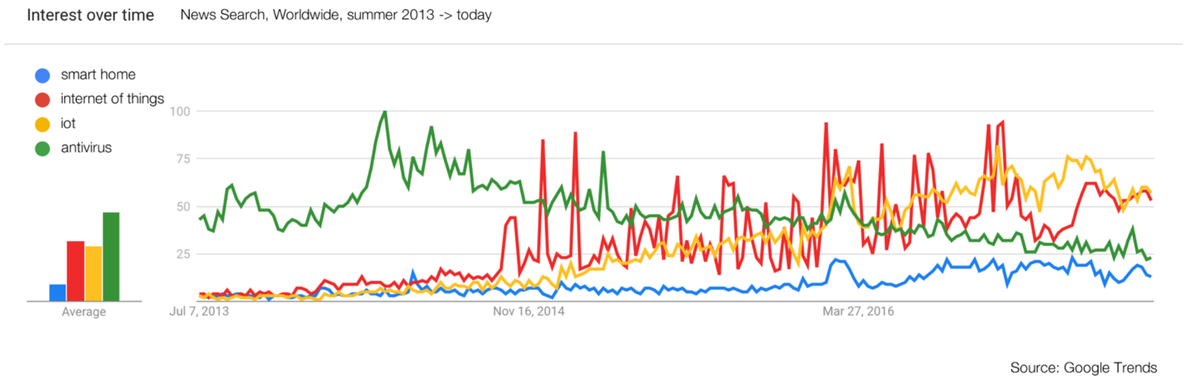


Figure 7. News Search for "Smart Home", "Internet of Things", "IoT" and "Antivirus"

Source: https://trends.google.com.

To a major surprise, customers in consumer markets do not appear to search for information about connected products using either IoT or the Internet of Things as keywords. "Smart Home" is used instead. Also, interestingly, by late 2014 "antivirus" & "smart home" begin show correlation. By 2016 they weigh equally (Figure 7).

This is a significant finding and the trend suggests consumers increasingly ponder on security concerns when expanding their network with new, unproven connected devices.

Now that we know what customers are looking for, let's turn back to the media, news outlets and the professional space.

The picture here is entirely different. IoT & Internet of Things are the most used keywords. There's aberrations generated by hype from news cycles at industry events and product launches (see spikes around Jan for CES and mid-year launches. *IoT* and *Internet of Things* are often used interchangeably, with corresponding spikes that sync "antivirus" to security scares and new product concerns.

Therefore, chances are, you'd be missing content about the Internet of Things if you were looking for smart home cybersecurity scares.

None of the large North American retailers have an IoT section. BestBuy, Amazon, Home Depot and Target have a Smart Home department. Retailer Fry's has a "connected home" section. ADT, the largest perimeter security vendor in the USA, sells smart home security. When TNW picked the best smart home gadgets in 2017 the article had not one mention of the words Internet of Things. Neither did the Washington Post in a November 2017 in the article titled "How to make a smart home", by Tsukayama.

Conclusions

It's unclear why "Internet of Things" terminology suffered a split from the "Smart Home". It's evident that the Smart home makes for better headlines in consumer literature, while IoT is more aligned to other buzzwords, like Machine Learning or AI, in the business world. None of the definitions of the IoT presented in this research even include references to the smart home, although for the consumer market they are a total overlap.

This author believes the split was unintentional, an error, the result of lack of industry leadership.

When vendors like Bitdefender begun communicating their novel hardware security products to a new market, they found out that customers didn't want an Internet of Things security hub, but a Smart Home security solution. Bitdefender wanted to communicate Bitdefender BOX as a product for the IoT, but refrained because it noted the market didn't agree on a clear understanding of what that meant.

Such a mistake would be significant and could cost multiple hundreds of thousands to millions of dollars in miss-aimed marketing around the wrong keywords for SEO and awareness campaigns. Eventual financial losses from this incongruence are hard to calculate.

Fragmentation, found in the multitude of platforms and OSs, means Bitdefender would employ not alike technologies to defend the former, but the consumer demands simplicity and a seamless management process. Similarly, the IoT definition must be inclusive, explicit and simple.

Preserving the naming split is further confusing. The IoT has matured enough to provide mass market products and real experiences to consumers. And the conversation is no longer solely academic.

For practical use, a preferable definition for the Internet of Things is the totality of devices that are connected to a smart home network that assigns them an IP address and communicate to each other directly or through the cloud.

That's anything from conventional and unexpected devices such as PCs, printers, NAS, to baby monitors, game consoles and Dash buttons. All these make up the IoT. And for the consumer, that's the smart home.

Conversely, the enterprise would continue to deal with the more specialized hardware branch of the IoT, the Industrial Internet of Things.

References

Ashton, K., (2009, June 22), That 'Internet of Things' Thing, retrieved at http://www.rfidjournal.com/article/view/4986

Balan, A,. (2017, August), The Gift That Keeps on Giving, DEFCON, Las Vegas.

Morgan, J., (2014), A Simple Explanation Of 'The Internet Of Things, retrieved at https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#7b4ff6321d09

Morgan, S., (2017), Cybersecurity Ventures predicts global cybersecurity spending will exceed $1 trillion from 2017 to 2021, retrieved at https://cybersecurityventures.com/cybersecurity-market-report/

Quora, (2018), retrieved from https://www.quora.com/What-exactly-is-Internet-of-Things-IoT

Reese, H., (2017), Report: IoT attacks exploded by 280% in the first half of 2017, retrieved at https://www.techrepublic.com/article/report-iot-attacks-exploded-by-280-in-the-first-half-of-2017/

Sun, C., (2016), No IoT without IPv6, retrieved at https://www.computerworld.com/article/3071625/internet-of-things/no-iot-without-ipv6.html

Tsukayama, H. (2017, Nov 22). No place like a (smart) home, retrieved from www.washingtonpost.com/sf/business/2017/11/22/no-place-like-a-smart-home/

Tung, L., (2017), IoT devices will outnumber the world's population this year for the first time, retrieved at http://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/

Wikipedia, (2018), retrieved from https://en.wikipedia.org/wiki/Internet_of_things

Williams, C., (2016, October 21), Today the web was broken by countless hacked devices – your 60-second summary, as retrieved from https://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained/

https://businessinsider.com/research/.

http://gartner.com.

https://trends.google.com.

https://www.theregister.co.uk/2017/11/07/mirai_botnet_sitrep/.