Nexa Center for Internet & Society
Politecnico di Torino

Tales from the Hackable Connected World

IoT Hell, and why its gates must be closed — right now

Fabio Chiusi, Fellow Nexa Center

Working paper nr 1/2017

Studying the Internet, exploring its potential & experimenting new ideas

Via Pier Carlo Boggio 65/A, 10129 Torino, Italia

(http://nexa.polito.it/contacts-en)

+39 011 090 7217 (Telephone)

+39 011 090 7216 (Fax)

info@nexa.polito.it

Mailing address:

Nexa Center for Internet & Society

Politecnico di Torino - DAUIN

Corso Duca degli Abruzzi, 24

10129 TORINO

ITALY

The Nexa Center for Internet & Society is a research center affiliated to the Department of Control and Computer Engineering of Politecnico di Torino (http://dauin.polito.it).

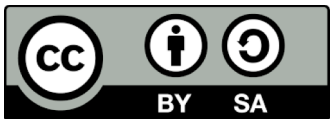

Table of contents

Tales from the Hackable Connected World

IoT Hell, and why its gates must be closed — right now

Fabio Chiusi
fabiochiusi@yahoo.it

1 Introduction

Imagine the forecasts are right. It is 2025, and the world contains some 100 billion[1] "smart", connected devices. The dream of Silicon Valley has become true: the so-called "Internet of Things" is no longer promise, but everyday reality.

Now imagine Jim is an early IoT-adopter, a model user and citizen in this latest technological revolution. What's his life like? Sensors collect, store and analyze his every move through wearable devices and his smartphone, so that calories intake is finely tuned on energy consumption, his heartbeat is under constant check, and of course he can enjoy the best deals from the shops in the surroundings — offers just pop-up as notifications on his fashionable, geolocalized, augmented reality glasses.

Cars self-drive him on "smart" roads, effectively gathering all kinds of data about his commute; thanks to real-time traffic analysis, it is invariably the quickest possible route home, and he can just sit back and relax while chatting with friends and sending heart emojis to his loved one. Once he gets there parking is not a problem, as the car has already learnt from its Big Data-led artificial intelligence which spots are free.

After a quick eye-scan at the front door, Jim is greeted with the exact amount of heating and lighting he desires, while one of his favorite songs starts playing — without him having even asked — thanks to the virtual assistant that crunches his preferences and turns them into personalized comfort. The fridge is not empty — as it never is — because it is capable of recognizing, notifying and even buying missing groceries by itself. Look,

1 http://www.huawei.com/minisite/iot/en/

a drone is just about to deliver fresh fruit, vegetables, milk and all the necessary ingredients for the soup he loves, right on time!

After a properly balanced lunch, the result of the lifestyle personalization suggested by health-tracking connected applications, the smart citizen can finally thank the AI, sit on the sofa and play some smart tv programming, while his kids enjoy the company of their new smart toys, with which they can converse about their interests and hobbies as with a real, caring friend. “You should drink a glass more of me”, says the smart bottle of water on his lap; “you should go to bed now”, adds the virtual assistant in his pocket a few minutes later: it knows tomorrow morning Jim has an early meeting, and if he doesn’t get enough sleep he won’t be performing at his best. “At least I won’t have to be driving the children to school”, he thinks to himself just before closing his eyes, “as my car will, by itself”.

Is this not-so-distant future envisioned by Silicon Valley heaven or hell? At the surface, it undoubtedly looks like the former. Technology understands what you think, and enables you to realize it before you even asked. Everything is efficient. Everything is comparable, and therefore subject to “empowerment”. And everything is easy, “frictionless” — as social media theorists used to say before realizing the sound of it was really, really bad.

But there’s no hiding that this utopian Tech-heaven could easily turn into the latter, with just a few scratches. Leave the socio-anthropological and philosophical objections to Jim being reduced to its “quantified self[2]” aside for a moment. Let’s say there is nothing inherently inhuman or dehumanizing in having every aspects of one’s life tracked, datified and ultimately judged and driven by (opaque) algorithms.

We would still have to grapple with one critical feature of connected devices: their cybersecurity. Are they safe? Can they actually preserve the immense amount of data they generate, and keep them from unwanted scrutiny? Thanks to the age of smart, connected devices Jim’s life has never been easier, his activities more efficiently

2 http://www.economist.com/node/21548493

managed, his body healthier: but does this entail the end of his privacy, together with a form of constant surveillance which is unprecedented even now, in the post-Snowden era? And could a society of Jims be a dream society, a utopia for the XXIst century or is it more aptly described as a fitting, contemporary dystopia?

Answers to such questions crucially depend on how cybersecurity will be implemented into the "Internet of Things" — a convenient catchphrase which can be better defined as the "emerging network of devices (e.g., printers, routers, video cameras, smart TVs) that connect to one another via the Internet, often automatically sending and receiving data[3]".

The aim of this essay is to show that, absent a revolution in the security of IoT devices, the life of Jim - and all of the Jims in the world - will look like hell much more than heaven. Because as things now stand, the IoT is easily hackable, and easily hacked. And when everything is connected, this means that our entire lives are too.

2 The Internet of Hackable Things

Back to reality: in 2017, IoT is still mostly a promise. Numbers are growing, and fast, but there's no Jim around. If estimates are right, though, there will be many soon. According to IHS, "the IoT market will grow from an installed base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025[4]", writes Forbes; 100 billion of them, if you listen to Huawei instead. By then, in Jim's future, it will have a potential economic impact of $3,9-11,1 trillion a year, in McKinsey's forecasts[5].

Dresner Advisory Services claims[6] that biotechnology, consulting and advertising already consider IoT critical for their industries, but manufacturing, asset management, logistics, supply chain management and marketing are quickly catching up. And the revolution is here for every industry, for everything. "While IoT 'smart home' based applications grab

3 https://www.us-cert.gov/ncas/alerts/TA16-288A

4 https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#7a92c169292d

5 http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

6 https://www.forbes.com/sites/louiscolumbus/2016/10/02/2016-internet-of-things-iot-big-data-business-intelligence-update/#79c890054923

media headlines", writes Juniper Research, "it is the industrial and public services sector – such as retail, agriculture, smart buildings and smart grid applications – that will form the majority of the device base.[7]"

Take a look at the current statistics: 200 smart city projects are underway around the world (Markets and Markets); 8 million smartwatches have been shipped in the last quarter of 2015, and 17 million fitness trackers sold last year — together with 9 million smart thermostats, smart smoke and CO2 detectors, Wi-Fi cameras, smart lock and smart home systems, plus 27 million smart TVs (Consumer Technology Association). Wearable cameras will peak at 22 million units in 2020 (CCS Insight)[8], thus making dystopian, 1984-esque surveillance (and *sousveillance*[9]) a permanent feature of Jim's existence.

As things embed more and more knowledge about us and the world, many more subjects do too: not only those who create or exploit them to extract value from the data we produce through them — or they produce in autonomy — but also government and law enforcement agencies, in case Jim becomes a suspect; and, of course, cybercriminals who wish to steal our quantified lives and use them against us.

And that's the problem. The IoT hype fueled by what is depicted as a necessary — look at the numbers! — and necessarily beneficial — look how efficient we are! — revolution hides the fact that we are focussing way too much on stats and utopian scenarios, and not enough on the nefarious implications of connecting billions and billions of everyday devices to the Internet without producers making their cybersecurity a top priority.

Experts in the field are well aware of the risks: "The rush to connect everything to the Internet is leaving millions of everyday products vulnerable and ripe for abuse[10]", wrote Level 3 Communications in August 2016. Later, in November, the Broadband Internet Technical Advisory Group added that "several recent reports have shown that some

7 https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020

8 https://www.mediapost.com/publications/article/279953/the-numbers-in-the-internet-of-things-a-mid-year.html

9 http://www.surveillance-and-society.org/articles1(3)/sousveillance.pdf

10 http://netformation.com/level-3-pov/attack-of-things-2

devices do not abide by rudimentary security and privacy practices[11]". It is not sophistication that's lacking: it's the basics. Which means that anyone, not just high profile attackers, can breach into the IoT devices and, from there, into the most intimate details of our lives.

The issue is so serious that the US Department of Homeland Security explicitly files it under the category of the threats to "national security". Here's what it wrote, again last November, in its 'Strategic Principles for Securing the Internet of Things[12]':

"While the benefits of IoT are undeniable, the reality is that security is not keeping up with the pace of innovation. As we increasingly integrate network connections into our nation's critical infrastructure, important processes that once were performed manually (and thus enjoyed a measure of immunity against malicious cyber activity) are now vulnerable to cyber threats. Our increasing national dependence on network-connected technologies has grown faster than the means to secure it."

3 Opening the gates of IoT Hell

And it's not purely theoretical: the gates of IoT hell have already opened. On October 21st, 2016, a malware known as 'Mirai' infected hundreds of thousands of IoT devices to enroll them in the botnet army that realized the largest Distributed Denial-of-Service, or DDoS, attack in history. What this means is that users in North America and Europe could not connect to websites as diverse as Airbnb, Amazon, the BBC, CNN, Comcast, EA, Etsy, Guardian, GitHub, HBO, Imgur, New York Times, PayPal, PlayStation Network, SoundCloud, Twitter, Yelp and many, many others for hours[13].

The attack aimed at hitting the Domain Name System (DNS) provider Dyn reached 1,2 terabits per second[14], and it did so by exploiting the lack of even basic defenses in

11 https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

12 https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

13 https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

14 https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

thousands of baby monitors, printers, videocameras and routers. ‘Mirai’, which incidentally means “future” in Japanese, managed to spread through 164 to 177 countries, according to estimates by Imperva and MalwareTech[15]. Its source code is even available online, and everyone who knows how to find it — and who is willing to pay for it — can now rent a botnet of at least 400.000 infected IoT devices[16].

It’s no surprise then that variants of the IoT-powered ‘Mirai’ malware have been found in the cyberattacks aimed at the ‘Krebs on Security’ blog — with an alleged army of 1,5 million devices — and at the French cloud computing company OVH — peaking at 1,5 terabits per second[17], even more than the Dyn attack. The same happened to 900.000 Deutsche Telekom broadband routers: infected with the malware, they left 5 million devices insecure in countries all over the world, from Germany, Italy and the United Kingdom to Turkey, Iran, Australia, Argentina and Brazil[18].

‘Mirai’ replicas are so widespread that “the botnets”, writes Motherboard journalist Joshua Kopstein, “have even been observed attacking one another, in some kind of bizarre cyber-dystopian turf war[19]”.

All of this may well inform politically-motivated cyberattacks, and be inserted into a larger geopolitical picture in which cyber-warfare is quickly gaining ground as one of the most urgent issues to be tackled in order to protect national security. IoT-powered botnets can in fact be turned into instruments to shut down the Internet at politically-sensitive timings, therefore preventing speech and dissent, and hindering the democratic process.

A variant of the ‘Mirai’ botnet, called ‘Botnet 14’, has already been used to try and take down the Internet for a whole country, Liberia[20]. The attack peaked at 500 gigabits per second, half of the Dyn blackout. But researchers worry that with more devices infected

15 https://motherboard.vice.com/en_us/article/internet-of-things-mirai-malware-reached-almost-all-countries-on-earth

16 https://www.bleepingcomputer.com/news/security/you-can-now-rent-a-mirai-botnet-of-400-000-bots/

17 https://www.us-cert.gov/ncas/alerts/TA16-288A

18 https://www.flashpoint-intel.com/new-mirai-variant-involved-latest-deutsche-telekom-outage/

19 https://motherboard.vice.com/en_us/article/twitter-account-shows-mirai-botnets-using-your-smart-fridge-in-cyber-turf-war

20 https://medium.com/@networksecurity/shadows-kill-mirai-ddos-botnet-testing-large-scale-attacks-sending-threatening-messages-about-6a61553d1c7

the attack could be powerful enough to disrupt connectivity in all of the 23 countries that rely on the same ACE fiber cable that connects France, Portugal, Canary Islands, Senegal, and the coastal countries of Western Africa, all the way to South Africa. With a total capacity of 5,12 terabits per second, a million of IoT zombies would be enough to severely hinder web and connected services usage for millions of people[21].

It is therefore rather telling that cybersecurity guru Bruce Schneier had been able to foresee such developments even a month before the Dyn catastrophe. This is what Schneier wrote in September 2016:

"Over the past year or two, someone has been probing the defenses of the companies that run critical pieces of the Internet. These probes take the form of precisely calibrated attacks designed to determine exactly how well these companies can defend themselves, and what would be required to take them down. We don't know who is doing this, but it feels like a large nation state. China or Russia would be my first guesses.[22]"

Can you imagine Jim's life with no Internet connection? How "smart" and useful could be his connected appliances, once they are connected no more? Who would drive his self-driving car, once its connection is disrupted? And what if hackers could interfere with it remotely? As Wired journalist Andy Greenberg showed with a live demonstration[23], it is technically possible for a hacker to halt the engine of a car on a highway while comfortably seating on his sofa, miles away. And what if the next Niece- or London-like terror attack is brought about by a hacked driverless car or van? Figures about the ascent of the IoT world would get a much less enthusiastic meaning.

But an IoT connected world in which IoT is insecure is not just an individual nightmare: it is a social nightmare. Imagine a shutdown of the networks that drive life-sustaining activities. Imagine an attack on power grids, like the one happened in Ukraine. "IoT security is now a matter of homeland security", writes the DHS, but it is also a powerful

21 http://thehackernews.com/2016/11/ddos-attack-mirai-botnet.html

22 https://www.lawfareblog.com/someone-learning-how-take-down-internet

23 https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

way of disrupting the social order. When homes, cars, biometric data, health data, and just about everything can be manipulated remotely, the avenues for abuse are larger than imagination. But there's no need to aim at critical infrastructures: a doll, a billboard, a thermostat are enough to turn everyday objects into criminals asking for ransom, or into nazi propagandists, or into spies who never stop listening and watching.

The intelligence community knows it best. Its top officials even admit they will make use of IoT devices for surveillance purposes. "In the future", argued former Director of National Intelligence, James Clapper, "intelligence services might use the [Internet of things, ndr] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials[24]".

Jim might not know it, but there are more reasons for his IoT assistants to listen to him than to barely — and freely — serve him and his preferences. Too bad it's not written on packages and brochures.

4 Goebbels-printers, NSA-Barbies and other smart demons

But what do we know exactly of the Internet of Hackable Things? Enough to say that hell is about to brake loose, and that it's going to be cynically amusing. It is not only that an estimated 70% of IoT devices is hackable, according to an HP study conducted in 2014[25]. It is, again, the lack of even the most fundamental protections: in 8 out of 10 cases, investigated IoT devices did not even require a password strong enough to be useful.

To understand what this means in practice, we don't need to fantasize about the kids of an imaginary Jim living in 2025: our kids are enough. Imagine a dad who bought one of the CloudPets teddy bears produced by California-based company Spiral Toys to his son. The toy has an interesting — and increasingly common — feature: by connecting to the Internet, it enables parents and children to exchange recorded voicemail.

24 https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

25 http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WPYadFOGMWo

Unfortunately, the company did not provide its bears with any requirement for password strength. The result is that the toy has been hacked in January 2017, and consequently an estimated 2 million voice messages ended up online for anyone to listen. Worse: the messages remained available for at least a week, writes Mashable, even after multiple notifications to the company[26].

Even worse is the fact that episodes like this are not unique, but rather quickly becoming a discomforting trend in the industry. Take the connected Fisher Prize teddy bear toy whose controlling smartphone app has been hacked, thus revealing "names, birthdates and gender of the children using the toy". Data that can make a criminal's dream come true: "It makes it a lot easier for me to present myself as somebody who ought to know the kid's name, or the kid's birthday", a cybersecurity researcher told Motherboard[27].

Even Barbie dolls can be hacked[28], and turned into a listening device for criminals who are good enough to grab and enjoy the conversations they recorded. Smart toys may well be a 2,8 billion dollars industry[29], with the prospect of growing to 8,4 in 2020[30], but they sure lack basic security, and this is endangering the lives of thousands of children and their families.

No cynical amusement here. But there sure is in the 14.000 connected printers forced by notorious hacker Weev into printing nazi propaganda. Again, it didn't take a genius: "I did not hack any printers", says Weev, "I sent them messages, because they were configured to receive messages from the public[31]".

26 http://mashable.com/2017/02/27/internet-of-things-cloudpets-hacking/

27 https://motherboard.vice.com/en_us/article/internet-connected-fisher-price-teddy-bear-left-kids-identities-exposed

28 https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children

29 https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-to-hit-$2-8bn-this-year

30 http://www.businesswire.com/news/home/20160127006124/en/Global-Smart-Toys-Market-Worth-USD-8.4

31 https://motherboard.vice.com/en_us/article/hacker-weev-made-thousands-of-internet-connected-printers-spit-out-racist-flyers

And what about a connected dildo, Siime Eye, whose camera has been easily hacked[32] allowing any malicious subject to tap into the livestream of the user's most intimate moments? Too easy, when the default password is "88888888".

Or get this. In August 2016, Motherboard describes the first smart thermostat-dedicated ransomware. Lorenzo Franceschi-Bicchierai puts it best: "One day, your thermostat will get hacked by some cybercriminal hundreds of miles away who will lock it with malware and demand a ransom to get it back to normal, leaving you literally in the cold until you pay up a few hundred dollars[33]". So funny you could wonder why they don't put it in the ads!

A smart city with smart lights? It could be forced into generalized blackout. According to a paper noted again by Franceschi-Bicchierai, "A single infected lamp with a modified firmware which is plugged-in anywhere in the city can start an explosive chain reaction in which each lamp will infect and replace the firmware in all its neighbors within a range of up to a few hundred meters.[34]"

Just smart traffic lights, then? "We could actually make the lights all red. We could change the light to be green in our direction", says Michigan University researcher Branden Ghena. Criminals could create congestions and stuck people in traffic jams "for hours[35]".

Smart parking garage systems are hackable too[36], by first obtaining the login credentials of employees, then using them to take over the whole system, and extract credit card data from parking fee transactions.

Even the thousands of smart billboards on the streets can be turned off all at once just because the API of the dedicated Android app contains several exploitable bugs[37].

32 https://motherboard.vice.com/en_us/article/camera-dildo-svakom-siime-eye-hacked-livestream

33 https://motherboard.vice.com/en_us/article/internet-of-things-ransomware-smart-thermostat

34 https://motherboard.vice.com/en_us/article/this-virus-automatically-kills-smart-light-bulbs

35 http://www.nbcchicago.com/investigations/series/inside-the-new-hacking-threat/New-Hacking-Threat-Could-Impact-Traffic-Systems-282235431.html

36 https://motherboard.vice.com/en_us/article/heres-a-map-of-hackable-smart-parking-garages

And "about 90% of the (smart) TVs sold in the last years[38]" are vulnerable to the attack developed by Oneconsult cybersecurity researcher Rafael Scheel — one that goes even further than the one designed by the CIA, "Weeping Angel": Scheel's does not require physical access to the device. Instead, "the attacker can execute it from a remote location, without user interaction, and runs in the TV's background processes, meaning users won't notice when an attacker compromises their TVs".

There's much to worry about while your fridge is hacked into sending spam messages together with a zombie army of other 100.000 connected devices. When it really happened, back in 2014, the spam emails sent were approximately 750.000, of which 25% through smart TVs, domestic routers, kitchen appliances and other IoT objects[39].

Smart but insecure things can also be the gateway to access our phones, or other more secure devices. Two researchers for example showed that Belkin's WeMo Android app controlling connected coffee machines, pots and light bulbs contained a vulnerability that allowed hackers to violate the smartphones on which it was installed — we're talking 100 to 500 thousand downloads - by stealing pictures and even tracking the whereabouts of their owners. Says Scott Tenaglia, of Invincea Labs: "The insecurity of my [Internet of Things device] now affects the security of another device I own, something that I probably care a lot more about than my IoT[40]".

5 It's easy to avoid the IoT Hell

All of this could be avoided in most cases with just minimal effort. Think of the 'Mirai' disaster: experts agree that hundreds of thousands of infections could have been prevented by just requiring, for each device, a change from the default password to a stronger password.

37 https://motherboard.vice.com/en_us/article/a-flawed-android-app-for-billboards-made-real-life-ad-blocking-possible

38 https://www.bleepingcomputer.com/news/security/about-90-percent-of-smart-tvs-vulnerable-to-remote-hacking-via-rogue-tv-signals/

39 https://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/

40 https://motherboard.vice.com/en_us/article/how-hackers-could-steal-your-cellphone-pictures-from-your-iot-crock-pot

The failure here is of both the industry and its users. “Admin”, “password” or “123456” cannot be even allowed to be considered passwords, in the cyber-scenario of 2017. Imagine what this means when IoT gets applied to medical data and data-based services. Director of Zvi Meitar Institute for Legal Implications of Emerging Technologies, Dov Greenbaum, and Yale professor Mark Gerstein wrote on the New York Times that “with medical IoT, hacking threats are scarier than just a night without Netflix and Twitter; they threaten the privacy of our medical information, or in extremely malicious cases, even lives[41]”.

And yet, 62 “common default” usernames and passwords were enough to hack into over 380.000 IoT devices, in the Mirai attack on Krebs on Security - according to the Computer Emergencies Readiness Team of the DHS. It is the very same blog that uncovered how another offspring of the Mirai code, ‘Bashlite’, managed to infect a million devices just through the use of default passwords.

Until they get changed, expect the worse. Writes the US-CERT report[42]: “With the release of the Mirai source code on the Internet, there are increased risks of more botnets being generated. Both Mirai and Bashlite can exploit the numerous IoT devices that still use default passwords and are easily compromised. Such botnet attacks could severely disrupt an organization’s communications or cause significant financial harm”.

There is a bad and a good aspect to this. While the above mentioned examples seem to justify the claim that insecurity is the norm — rather than the exception — in the industry, and this is bad, it is at the same time true that a banal change of the default password into a stronger one would *actually do good*, at least by forcing IoT criminals into more sophisticated methods, and therefore raising the cost of engaging in malicious hacking.

41 https://www.nytimes.com/2016/11/03/opinion/a-cyberattack-and-medical-devices.html?_r=1

42 https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

Another simple thing that should be collectively done: force-install any software updates. An updated system is usually a safer system, and this applies to IoT objects as well.

What is most important, though, is to realize that escaping the IoT hell is urgent. As its gates are rapidly opening, public opinion seems to remain unaware of the data disaster potentially awaiting each and every user if the industry is not immediately pushed towards better cybersecurity practices. The US Department of Homeland Security seems to know it better than most Silicon Valley enthusiasts: “It is imperative that government and industry work together, quickly, to ensure the IoT ecosystem is built on a foundation that is trustworthy and secure”, reads its report on the ‘Strategic Principles for Securing the Internet of Things’.

“The time to address IoT security is right now”, concludes the report. And there are several ways to do it immediately: enable security by default and coordinate the disclosure of vulnerabilities, as a start.

And then plan “end-of-life” strategies for IoT products — because not even the IoT gods can avoid obsolescence and, ultimately, death. “Developers should consider product sunset issues ahead of time”, writes the DHS, “and communicate to manufacturers and consumers expectations regarding the device and the risks of using a device beyond its usability date”.

A level of care and transparency still unheard and unimaginable to users. Also, the IoT era further widens the scope of Internet usage, forcing users of objects which are traditionally unrelated to the Internet into the realm of data extraction, and therefore involvinvg “non-technical or uninterested consumers”. IoT insecurity is not an “Internet” problem: it’s an issue that concerns a slice of the population that may be even bigger than that of Internet users.

Then there’s the interoperability problem, a Tower of Babel for connected things in which each device speaks its own language, and therefore they collectively fail to

understand and communicate with each other. And “each big company has developed its own standard”, writes Scientific American[43]. Good luck on checking the security of multiple devices in multiple ways every day, keeping all of them constantly updated, remembering all the different (strong) passwords and still having time to *actually use* the connected devices you longed to secure!

Which gives in to a deeper question, from the same article: “Do we really want to connect our kitchens, heating and cooling, and other home systems to the great wide world of hackers? Especially our door locks?”

Not if you think the solution will emerge from the market alone. “The market can't fix this because neither the buyer nor the seller cares”, argues Schneier. “There is no market solution because the insecurity is what economists call an externality: it's an effect of the purchasing decision that affects other people. Think of it kind of like invisible pollution[44]”.

“The IoT will remain insecure unless government steps in and fixes the problem. When we have market failures, government is the only solution”, writes Schneier.

Clearer privacy policies is not enough. Greater transparency in data usage is not enough. Security by default, even if absolutely necessary, is not enough. What we need is the law stepping in, if Schneier is right, and preferably at international level — so that standards can immediately translate into prescriptions for the whole industry, without giving way for the obvious opportunisms allowed by unregulated markets.

In the real world of 2017, however, some IoT devices are too dumb to even get a firewall installed. If the market is indeed trying to step in and self-correct the IoT world, as Silicon Valley producers and pundits would like us to believe, it’s doing it extraordinarily silently. So silently that it is legitimate to suspect that Jim’s world, in 2025, will be as

43 http://www.nature.com/scientificamerican/journal/v315/n1/full/scientificamerican0716-25.html

44 https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html

enthusiastic and insecure as ours — just with many, many more working devices installed, and towards even greater uses.

It's time to understand that this *laissez-faire* attitude in IoT innovation has led us at the gates of Hell, and we're not even close to entering the connected Heaven so gloriously depicted by the evangelists of a "smart" world. It's time for corporate responsibility, norms, standards, minimum requirements — and to educate users of the coming IoT revolution.

And it's time to seriously consider whether this is enough to actually convince St. Peter, and let us in. We might find ourselves wandering in IoT-Purgatory nonetheless. And that would mean that it's already too late. It's discomforting — but it's a possibility we, the digital grown-ups, have to face anyway.