"Put an Internet on it" and other follies

Security in the Internet of Things

Morgan Gangwere
University of New Mexico, Albuquerque NM

Prepared for Rick Robb, ENG119 Spring 2016

Abstract

The "Internet of Things" has placed many physical objects on the Internet and has been expanded to include any internet-enabled device. From the mid-1990s, internet availability and ease of access have pushed more industrial systems as well as home automation systems to be accessible or rely on the internet; as a result many physical risks as well as privacy concerns must be taken into consideration.

Contents

1 Introduction

The "Internet Of Things" is a highly lucrative business right now; According to Intel, there are currently nearly 15 billion devices connected to the Internet, with a projected 200 billion devices in 2020[1] This rapid increase in internet connectivity has come from a miniaturization of technology needed for embedded network connectivity: Ubiquitous Wi-Fi, cheap system modules and a relentless power-show of manufacturing in China; A perfect storm for a huge wave of small, cheap devices.

The Internet Of Things isn't new. There has been an internet-connected world since the mid 1990's; as network connectivity has become more ubiquitous and as it has become more affordable to put small computers in things, more and more devices and services have been placed online.

There is a downside however: Many consider the Internet of Things a panacea and treat it as such. By doing so, the technology that makes up the fabric of much of our technological backbone becomes the tools by which to set fire to ourselves.

2 In the beginning

In the early days of the Internet of Things, there was the Trojan Room Coffee Pot.[2] A tool of utility, a tiny black-and-white camera was pointed at a coffee pot at the University of Cambridge's Trojan Room's coffee pot so that students and staff working late into the night could know when the coffee needed to be refilled. Serving as the first "Internet of Things... *Thing*," it came during a nascent time in the Internet's development.

Figure 1: Remaining IPv4 allocations[3]

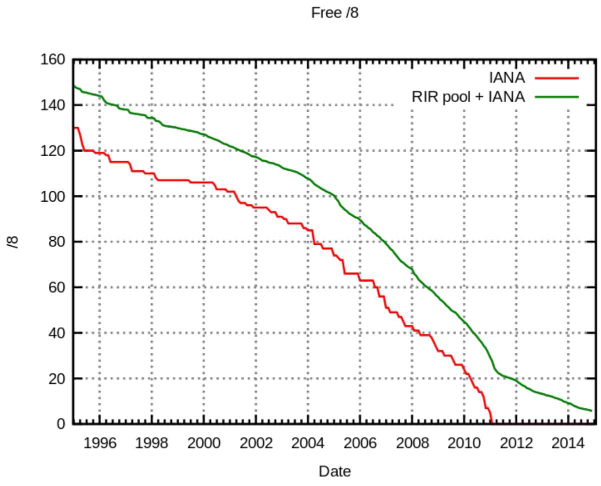

Figure 1 shows availability of "/8 allocations" (apropos to an area code) of the public IPv4 network by IANA (the *Internet Association for Names and Numbers*) and regional registries (which help coordinate usage across physical regions). IPv4 addresses (which typically look like `29.38.57.11`) identify one specific device on the internet with a maximum number of IPv4 addresses is $2^{32} - 1$, or 4294967295 (or, just over four billion.)

Technology such as *Network Address Translation* (NAT) have made it possible for many devices to share one "public" IP address (home networks regularly do this,) to alleviate pressure for addresses; since 1999 efforts have been pressing forward to push for IPv6, a newer addressing scheme which offers $2^{128} - 1$ addresses (enough to, hyperbolically, assign an address range for every human on the planet for the next few centuries.)

Public vs. Private addresses: What's it mean?

Public addresses are addresses which are able to be reached over the internet. *Private addresses* are addresses reachable only through NAT. IPv4 defines three "private" ranges whereas IPv6 encourages all devices to have a public address as well as a private address and that routers are responsible for controlling incoming traffic for devices.

Any device with a publicly routable IP address can be "seen" on the internet; it is often up to a firewall (or consumer router in most home situations) to terminate or control access to devices.

This proliferation of devices, as well as the increasing economy of scale for small consumer devices pushed huge numbers of devices into the market which could consume an IP address and talk to the internet; today, modern cell phones have a public IPv4 address.

3 Attacks on internet-connected devices

An attack on an internet-connected device comes through any of a variety of vectors: Would you consider your light bulbs a security risk? In the case of one vendor, Zengge, an IT administrator's Sword of Damocles may well be the lights above them; Zengge was found to have placed poor trust in the configuration of the network on which their Wi-Fi enabled lights. Discovered[4] in 2015 by Viktor Stanchev, the implications of having control over the lights are rather large:

> The [admin system] allows you to do anything. You can flash the firmware, use it as a proxy, read the WiFi password, make it join a different network, etc. This port is normally exposed only to the internal network.

The typical customer would think "I've never heard of Zengge, I'll stick with reputable brands like Phillips and Belkin." This seems a valid choice at first. A typical customer who would also do some searching around and come to the conclusion that all is hopeless: the major brands are just as vulnerable to attack.

Phillips' Hue lighting was (and to some degree is) vulnerable to a variety of attacks[5] which could result in blackouts, device takeover, and other things which the average consumer wouldn't want.

Turning off lights is one thing; Taking over baby monitors[6] enters the realm of outright dangerous. In 2013, the same security researcher who found flaws in the Phillips Hue lighting system also found that even temporary access to a wireless network placed Beklin WeMo baby monitors at risk. The response from Belkin was a resounding "meh." Belkin made other mistakes in the WeMo system, including actively transmitting plaintext passwords.

4 A search engine for devices

It is, to some degree, a lie to say that there's no search engine for physical things. When it comes to searching out things on the Internet, there are two kinds of search engines. Information search engines like Google, Bing and Yahoo aid researchers in finding data, while one search engine allows for the finding of *things* on the internet.

Shodan (`http://shodan.io`) is a search engine for internet-connected devices. Shodan was named after a hyper-intelligent AI in the System Shock video game series after becoming more than a pet project by its original developer. It scans the internet repeatedly, attempting to gain information about devices which have been publicly exposed.

You can find anything on Shodan: Webcams, DVR systems, even *critical infrastructure* in some cases, at one point finding traffic lights[7] accessible with the text "DEATH MAY OCCUR!!!" across the unauthenticated menu.

5 Effects on the safety of humans

The proliferation of the Internet of Things has driven device makers and maintainers to do two things: Put cars on the internet (via cellular modems) and put critical device infrastructure on the internet.

Cellular modems are cheap and ubiquitous. It has gotten to the point where a hobbyist can cheaply integrate a cellular modem into their projects[8] and control hobby-level devices over the cellular networks; The use of a small computer (such as a Raspberry Pi) brings the game right to the internet.

This presents a whole new level of (in)security: Suddenly, the whole entire internet has access to a device, and a device maker must take precautions to avoid becoming the target of an attack. These attacks are relatively straightforward and are often the result of an attacker stumbling upon them, pressing a few buttons and going "That's interesting!"

Major automaker GM/Daimler was forced to come to terms with this. Security researchers Charlie Miller and Chris Valasek presented at DEFCON 23[9] the talk "Remote Exploitation of an Unaltered Passenger Vehicle"[10] in which Miller and Valasek present an attack against a Jeep Cherokee. The exploits found by Miller and Valasek on the Uconnect system used in Daimler, Jeep and Chevrolet (among others) allowed full and total control of the vehicle, including the disabling of steering, brakes, throttle and other aspects of the vehicle.

Dan Tentler (known in security circles by the handle *Viss*) has been looking at the Internet Of Things from the perspective of a bad person. In his talk[11] "115 batshit stupid things you can put on the internet in as fast as I can go," presented at Devoxx, Tentler asks " If I can put a thing on the internet, should I?"

To Tentler, the short answer is: Well, it *depends.* The long answer is: If you can avoid it, don't. Tentler presents a selection of things that should not have been placed on the internet, including power distribution systems in Italy , hydroelectric dams in France and *a chicken farm in Mexico.* Excerpts from the talk include

> Somebody thought it was a good idea to put chickens on the internet. Why? I have **no idea!**
>
> Grain silos are neat!
>
> You can buy Squid, [because] this is a squid shop!
>
> Never thought I would find car washes on the internet!
>
> This just doesn't sound like a good idea.
>
> I have NO idea what this is, but it's got lots of buttons to press. One of them says "LARM" – Anyone know what "LARM means?"
>
> THIS IS BABY MONITORS... **THIS IS PREGNANT LADIES [...]** ***ON THE INTERNET!***
>
> The interesting point here is... eehhhhh 408 kilowatts.

To anyone who hasn't seen the talk, Tentler sounds like an ADD 12 year old. However Tentler's point is that because he is **not skilled in many of these systems**, he (or someone with the skills to use SHODAN) could **cause serious damage to things** because of how shortsighted the view of the implications were. For instance, who wouldn't want to tip over 24000kg of *liquid steel* for fun?

Back at home, companies have been putting all sorts of things on the internet that fall squarely into the "probably shouldn't be on the internet" category. Rheem for example has EcoNet[12] which lets users put their water heater on the internet. In 2016, the New York Times reported about owners of the Nest internet-connected thermostat who went cold:

> Admittedly, this may strike some as a quintessential first-world problem: a thermostat cant connect to the web. But for some users, it posed genuine issues.

> For those who are elderly or ill, or who have babies, a freezing house can have dire health consequences. Moreover, homeowners who installed a Nest in a weekend home, or who were on vacation, were also concerned that their pipes could freeze and burst, causing major damage.[13]

There is another aspect of human safety to take into consideration; Human safety depends on the privacy of information, which some fear may be a veritable garden of information for an attacker. In MIT's *Design Issues*, Victor Margolin's *Design, The Future and the Human Spirit*[14] questions if we are really heading towards a utopia and presents implications for personal privacy:

> [the] amount of data these objects emit and its potential for public access raises myriad privacy issues that [Bruce Sterling] sidestepped in his glowing vision of [the Internet of Things] as electronic servants, keeping track of our possessions.

The Electronic Frontier Foundation has been taking this into consideration after in 2015, the company Vtech was breached, revealing the information of children across world. Vtech produced a series of hand-held tablets for children; A distinct lack of data privacy allowed for an attacker to gain access to the names, ages, birthdays, addresses and parental contact information of children whose parents had registered the device as prompted. Quoting the EFF, this attack is "remarkable because after a year of other high-profile breaches like Ashley Madison and OPM, VTech was found employing spectacularly outdated security practices and software"[15] as well as making no checks to see content that was being returned should have been returned over the internet.

6 The Panacea

In certain circles, there is little rush to address the real-world implications of the Internet of Things, whereas the security industry has been quick to remind itself of the implications; Microsoft has declared a set of ten "Immutable laws" of security which they follow; #10 is "Technology is not a panacea:"

> Technology can do some amazing things. [...] It's tempting to believe that technology can deliver a risk-free world if we just work hard enough. However, this is simply not realistic.

Academic articles tend to focus on the positive aspects of the Internet of Things. With articles like "Power Shift: Smart Grid Transforms Electric Power for the 21st Century[16]" focusing on the positive benefits of a hyper-connected power grid while taking little to no time to take into considerations the effects of such a system.

In the corporate world, executives "Don't feel responsible," according to researchers who talked to CNBC.[17]. This comes as a side-effect of a lack of understanding, says Dave Damato, chief security researcher at Tanium, who commissioned the study CNBC looked at:

> While the topic is complex, executives need to be educated about cybersecurity and become fluent in the issue [...] Further, the corporate world lacks a standard measure for cybersecurity,

which means companies cannot be assessed by a common metric, and executives have no rubric to determine their performance.

7 In conclusion

The Internet of Things has grown as a side-effect of technology's proliferation into our everyday lives. As a result of the ease of putting a device on the internet, there is an inherent risk of danger in terms of personal safety (baby cameras and home automation being used to track individuals) and danger to people (putting steel smelting plants on the internet: Probably not a good idea).

There are challenges to face with regards to how security is handled in the Internet of Things. Twitter accounts such as `@internetofshit` reveal the hype around just "sticking it on the internet" for what it is, while researchers such as Dan Tentler and Charlie Miller regularly ask the question: "why did they put it on the internet... and how can we break it?" While not inherently bad, the Internet of Things still faces a wide variety of challenges, not only from the perspective of those who are effected by it, but those who effect it. There is real, serious dangerous risk associated with placing industrial equipment on the internet as well as danger in ignorance of the second and third order effects.

Though there have been no documented serious disasters resulting from abuse of a network-enabled industrial system or internet-connected teapot, there are concerns of physical security as well as privacy which must be addressed in the now.

Notes

[1] http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

[2] http://www.cl.cam.ac.uk/coffee/coffee.html

[3] Image from Wikimedia Commons https://en.wikipedia.org/wiki/File:Ipv4-exhaust.svg

[4] https://blog.viktorstanchev.com/2015/12/20/the-many-attacks-on-zengge-wifi-lightbulbs/

[5] http://www.dhanjani.com/blog/2013/08/hacking-lightbulbs.html

[6] http://www.computerworld.com/article/2474439/cybercrime-hacking/hacked-wireless-baby-monitor-lets-pervert-spy-on-and-cuss-at-baby-girl.html

[7] http://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-dangerous-internet-searches/index.html

[8] https://store.open-electronics.org/GSM_GPRS_GPS_SHIELD

[9] DEFCON is one of the largest hacking/security conventions in the United States. It regularly sees 30,000 attendees from across the globe with companies regularly attempting to censor presentations, often to no avail.

[10] https://defcon.org/html/links/dc-archives/dc-23-archive.html

[11] https://www.youtube.com/watch?v=hMtu7vV_HmY

[12] http://www.networkworld.com/article/2602908/internet-of-things/home-automations-next-big-opportunity-controlling-the-water-heater.html

[13] Bilton, Nick for the New York Times, http://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html

[14] Margolin, Victor: "Design, the Future and the Human Spirit ." *Design Issues*, vol 23 no 3 http://www.jstor.org/stable/25224114

[15] https://www.eff.org/deeplinks/2016/03/vtech-we-are-not-liable-if-we-fail-protect-your-data-eff-oh-yes-you-are

[16] Futch, Matthew: "Power Shift: Smart Grid Transforms Electric Power for the 21st Century." *Georgetown Journal of International Affairs* http://www.jstor.org/stable/43134381

[17] Tom DiChristopher for CNBC: "Execs: We're not responsible for cybersecurity." http://www.cnbc.com/2016/04/01/many-executives-say-theyre-not-responsible-for-cybersecurity-survey.html