February 2021
Geoff Huston

The Internet of Trash

It's often a clear signal that we're in deep trouble when politicians believe that they need to lend a hand and help out with regulations. A bill has been passed by the US Congress, and now signed into law, that requires the National Institute of Science and Technology to work with other agencies in developing guidelines for the use of devices that manage security vulnerabilities, patching, together with configuration and identity management (https://www.congress.gov/bill/116th-congress/house-bill/1668/text).

Either the actions of the market have failed consumers and some form of public action is necessary to address aspects of this failure, or the situation is so desperately broken and beyond help that the legislature is performing a largely ineffectual action that serves more to disclaim any residual responsibility on the part of the public sector for the mess that we've created than to actually achieve a tangible outcome.

In the case of the Internet of Trash it certainly has the appearance that everyone, including sundry politicians, are taking a big step backwards to stand well clear any form of attribution of blame when we wonder how we managed to stuff it up so thoroughly. And who can blame them. This mess was not of their making.

And without doubt this is a pretty major mess that we find ourselves in!

How did we get here?

The silicon chip industry is truly prodigious. These days a small set of fabrication plants manufacture upward of 30 billion processors each year and the total production of various forms of memory, logic, processing and control systems is worth some half a trillion dollars per year. The market capitalisation of the public semiconductor makers and integrators now exceeds a stunning 4 trillion USD, 4 times their valuation of just five years ago. We are digitising our world at a phenomenal pace and at the same time embarking on the process to bind them together, often using the Internet as the connective substrate. The internet may be populated with some 4.6 billion human users, but the various conservative estimates of a device census for the Internet typically exceeds 30 billion devices of one form or another. Our label for this is the Internet of Things and the term encompasses all kinds of devices, services and functions. These days we can find these devices in cars, televisions, household security systems, weather stations, web cams, thermostats, power strips, lightbulbs and even door chimes. Beyond the consumer market there is are entire worlds of devices in workplaces, in hospitals and diagnostic centres, in factories, in farms, vehicles of all shapes and sizes, and so on. This is not a recent shift, but it's certainly taken off in recent years as chip costs plummet, chip power consumption falls, battery technology improves, and our ability to embed digital capabilities in all kinds of devices just keeps on improving.

Who gets to look after all these computers? What does "look after" even mean?

The 1980's was the last decade of so-called "mainframe" computers. These devices not only required their own carefully conditioned temperature and humidity-controlled environment but were assiduously

tended by a team of specialists who looked after the hardware, kept the software up to date and even maintained the copious paper-based system documentation. While the capital costs of these devices were considerable, the lifetime operating costs of these mainframe systems were probably far higher. As general-purpose processing computers dropped in size and price and became more tolerant of a greater range of environmental conditions, they relocated out of the computer room to the desktop, then into our pockets, and from there to an existence of being embedded in devices where they are all but invisible. We don't have "computer operators" to tend to these devices. We don't even want to look after them ourselves. We paid so little for most of these "clever" devices that neither the retailer nor the manufacturer or anyone else in the supply chain is remotely interested in looking after their products once they are sold. I guess that we just assume that the computers will be able to fend for themselves!

In some cases, and for some devices, that assumption about the lack of care on the part of the vendor as to the fate of the devices that they've pushed out into the consumer market is not warranted. Automatic updates have been incorporated into a number of popular computer platforms, where the vendor has assumed some responsibility for the device for a while, and during this time it exercises some level of remote control to automatically synchronise the device's software version to the to the current level, applying updates and patches as necessary over the Internet. An Android or iOS platform will upgrade its software from time to time, and the apps on these platforms seem to be living in a constant upgrade cycle. In some ways it's reassuring that the platform is being updated and known vulnerabilities are being addressed within this regular framework.

However, that's not always the case. In many other cases it's left to me to look out for software and firmware updates, and then go through the process of applying them to the device. Why should I bother to do this? If I bought a camera and it still takes photos, or a printer that still prints, or a car that still seems to work perfectly well as a car, then why should I bother? Obviously, the issue is not about a better camera, a better printer or a smarter car. The issue that vulnerabilities within the processing functions that are embedded in the device are exposed over time and older systems are at risk from being exploited through these vulnerabilities. The risk is perhaps a little more subtle than this. The printer may be a perfectly fine printer, and it would still function in precisely the same way that it always works. It's just that it may also have been quietly and invisibly co-opted to be a rabid attack zombie in its copious spare time!

In too many other cases there's just no ongoing vendor support at all. No patches. No updates. Nothing. It's not that the devices are just perfect and no maintenance at all is necessary. They're so far from any such ideal, assuming that we have any idea what such an ideal may be in any case. Vulnerabilities are uncovered on an on-going basis. Some are as simple as exploiting usernames and passwords that were loaded into a device at manufacture. (*admin/admin123* and *username/password* are, depressingly, still common, and anyone who did a jail break on iOS device must remember the *root/alpine* credential combination). Other vulnerabilities come from third party software libraries that are packaged into the device, and these days every system is largely built on a disparate collection of third-party libraries. Other vulnerabilities are more insidious, resulting from subtle interactions between code and data that push the device into an unanticipated state. All this means that without ongoing support from the vendor, the task of keeping a system up to date with respect to currently known vulnerabilities is a close to impossible task. If neither the vendor or the consumer is able to upgrade or even manage the device, then this is where we are at our most vulnerable. If these devices are widely deployed, unmanageable and vulnerable to hostile manipulation and control then the results can be truly catastrophic. We need to look no further than the *Mirai* botnet attack of October 2016 that caused a few hours of massive disruption in the United States. You'd probably like to think that maybe we've learned from this and we no longer use devices on the network that are absolutely wide open for hostile exploitation. But, of course, that's just not the case. It's far easier and of course far cheaper to just forget about such risks and press on!

What should we do about it?

Maybe the US Congress is doing the right thing in trying to impose some minimum standards of post-sale vendor support for devices. Maybe we go further and adopt a regulatory framework that bans the sale of devices that are not upgradeable in the field.

Ignoring the obvious issues of national jurisdictions and the ease of global shipping of goods, there are still issues with this regulatory approach. Devices don't get upgraded for a myriad of reasons. One is that silicon does not age so readily. It's not at all unusual to see fully functioning hardware platforms that are more than 30 years old. For how many years should a vendor be required to provide upgrades to devices that they sold? And if the vendor goes out of business for any reason then who takes over the support role for the equipment? What's the economic model that provides sufficient incentive for a vendor to continue provide ongoing software maintenance for legacy systems that were last sold two or three decades ago? Is this a case of legislating a standard of behaviour that is impossible for the industry to achieve?

For example, in the router business Cisco was the dominant vendor for many years. Router hardware was built to last, and it is not surprising to find equipment in the field that is more than 20 years old. If you look at a workhorse like a 7200 router that Cisco introduced in the mid-1990's, and stopped selling in 2012. then there is a considerable legacy issue. Cisco retired the system from maintenance patches a year ago, but of course there is still a sizeable population of devices out there that are now operating in unsupported mode. Equally, there is still a robust market for these devices, even though there is no ongoing vendor support. From the perspective of the vendor, a legacy support timeframe of 7 years after the last sale is probably an anomaly in our industry, and shorter timeframes are more the rule than the exception. Maintaining support for a further 7 years after the product was no longer being manufactured and sold is perhaps as much as could reasonably be asked.

Other vendors retire support at more rapid pace. Apple released iOS 10 in late 2016 and the last software patch was released in July 2019. The situation with Android is perhaps more dire, where the hardware vendors are placed in the position of being responsible for the provision of Android software updates to their platform, and this responsibility is only partially transferred to mobile network operators. The result is that the dominant operating system platform out there on the Internet is supported only in a manner that can best be described as somewhere between piecemeal and none at all!

No doubt many vendors would like to solve this service problem by reducing the useful service lifetime of the product even further and providing almost irresistible incentives to consumers to replace their device every year, and simply avoid the entire field upgrade support issue as a result. However, such short useful product service lifetimes generate their own issues. We sell some 1.5 billion smartphones per year, and which a short service lifetime we are also generating some 1.5 billion items of retired smartphones each year, generating its own issues of copious quantities of e-waste. This is a problem that just get larger each and every year.

All this is getting ugly. We have ongoing issues with maintaining resiliency in these devices in the face of the increasing complexity of service and function that we are cramming into them. The Android operating System has some 12 million lines of code. Windows 10 is reported have 50 million lines of code. And that's just the platform. Apps add to the burden of course. The Facebook app comes in at some 20 million lines of code. Maintaining such vast code bases is challenging in any environment, and it seems like we are operating all this digital infrastructure by just keeping a few millimetres ahead of then next big problem. These common code bases are deployed in billions of devices. And the support arrangements we currently use for the scale of deployment are, on the whole, just not coping.

If we really don't have a good understanding of how to operate a safe and secure digital infrastructure within the current computing environment with its diversity of support and security models, its mix of proprietary and open-source code bases, and the increasing complexity of the roles where we deploy such devices, it feels like sheer madness to then adopt a model of truly massive production and relentless cost shaving to embrace the world of the Internet of Things. At some point along this path this Internet of Trash becomes so irretrievably toxic that we just can't keep it going any longer!

It's impossible to just give up and walk away from the entire mess. While it took many decades for the digital world to permeate into all aspects of our lives, we are now well beyond the point of no return. Mere convenience has turns into complete dependence, and for better or worse we are stuck with this.

So we are back to the a quite conventional view of the role of the public sector in intervening in markets where there is a clear case of market failure. In this case the industry has become trapped in a vicious cycle of producing large volumes of product within a cost-constrained environment where concepts of the quality and robustness of the product are secondary to considerations of time to market and cost of the product. The conventional response to such situations is invariably one of imposing a minimum set of product standards on the industry that ensure the utility and safety of the product. Perhaps the real question is why has it taken so long for us to realise that such regulatory measures are as necessary in the digital world as they are in food safety and the airline industries?

"Move fast and break things" is not a tenable paradigm for this industry today, if it ever was. In the light of our experience with the outcomes of an industry that became fixated on pumping out minimally viable product, it's a paradigm that heads towards what we would conventionally label as criminal negligence. And if the industry is incapable of making the necessary changes to create sustainable and safe products under its own volition, then the intervention through regulatory standards is not only reasonable, its necessary.

Disclaimer

The above views do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.

Author

Geoff Huston AM, B.Sc., M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region.

www.potaroo.net