*THE BLOG*
08/24/2016 07:24 am ET **Updated** Dec 06, 2017

# The Internet Of Things? What Things?

**By Jeb Harrison**

## A Boomer's Guide to IoT and Security

For those of us Boomers who have witnessed first hand the invention, application, proliferation and ultimately the world domination of the Internet, it might all seem like sort of a blur.

Doesn't it feel like just yesterday that the nerdy guy in your office barged into your cubicle, took control of your IBM PC or Compaq or maybe even your Mac SE, and logged onto NetScape?

"This is the future of computing," he might have said as you studied the awkwardly formatted text slowly rendering across your screen. I remember my reaction:

“Bull pucky! Where’s the sound, the music, the voice-over, the animated graphics, the color photos, the video windows?”

It must have been around 1994, and multimedia on CD-ROM, created in a popular authoring tool called MacroMind Director, was all the rage. How could the snail-paced, text-based content delivered on the NetScape browser over the World Wide Web possibly supplant the showbiz content we could deliver on CD-ROM?

Well, we all know what happened next. By the end of the century multimedia CD-ROMs were nothing more than museum pieces and bookmarks, and the Internet had become the sole platform for delivering content on a PC.

Since then, the internet has gone places where no byte has gone before: into “things:“ cars, phones, refrigerators, coffee makers, garage doors, security systems, MRI machines, CAT scanners, car radios, baby monitors, power plugs, toaster ovens, televisions, watches, light bulbs, herb gardens, fish finders, beds, sprinkler systems...

**So, what isn’t connected to the internet?**

Your dog? Not if he/she/it has a chip implanted under its fur. The GPS (Global Positioning System) delivers its location information via IP.

Your vacuum cleaner? Not if you’re using the robotic variety, like Roomba.

Your bird feeders? Maybe, so long as they're not equipped with a remote-controlled seed dispenser.

There you have it. A device for everything and everything for a device.

**You, Online**

Now, pause for a second and cogitate on how many websites, or apps, you use regularly. Each requires some form of identification — usually your email address and a password. Spread that across your most commonly used devices: your PC, your tablet and your phone.

Those various online signatures are what security folks call the "attack surface." The more you have, the more ways hackers have to find a way in. And it's all these "things" that are now on the Internet that have opened up the floodgates.

There are no shortage of alarms being sounded across the security industry (the flip side of which is the hacking business), but if you're not subscribed to the tech news you're not likely to hear the alarms. Here are a few of the loudest:

**The Monster Under the Bed**

One of the most discussed, scary and perverse hacks is on baby monitors. There have been several reported instances of nursery voyeurs commandeering not only the video but the audio feeds and actually speaking to — or with — infants and toddlers while mom and dad are in the other room. We don't need to illustrate the creepy scenarios ... our imaginations can easily fill in the blanks. For those of us with grandchildren and device-savvy kids, we may want to suggest some extra precautions.

Another almost unimaginable breach was demonstrated at last year's Black Hat conference in Las Vegas, where a couple of high-profile hackers demonstrated how totake control of a Jeep Cherokee. This year, researchers at the conference will "explain how a computer worm could spread through a network of smart lightbulbs, how to hack medical systems, and how a new kind of ATM skimming device could steal tens of thousands of dollars in just minutes."

## Insecure Security Systems

It's easy to imagine how the same information thieves that hacked their way into baby monitors could do the same with home video security systems. If there's one surefire way to broadcast your away-from-home schedule to tech-savvy burglars, it's through a smart security system. And, once a cyberburglar knows that your house is empty on Wednesday afternoons, they can just as easily hack the smart padlocks that are supposed to protect your valuables.

Not only can smart systems make the home less secure, they can make the home itself a target for cyber-nappers. Smart HVAC systems, with smart thermostats and vent controllers, along with smart solar panels, can be turned off in the dead of winter, and only turned on again by the hackers. For a price.

These sorts of "denial of service" attacks become more ubiquitous as the number of service-providing devices get connected to the internet. According to Deral Heiland,"Your mobile phone is part of the loop, so is the app, the cloud interface and then you also have the connectivity between all of these devices," he said. "From a security standpoint, any failing in any one of these devices affects the security of the whole thing, the ecosystem."

## Okay, We're Scared. Now What?

While a great many of these "things" that are coming to market in droves have very lax security controls, there are some things an individual can do to mitigate the risk.

First, as sober responsible Boomers, we have the advantage of having lived most of our lives without the Internet, or at least without the Internet of Things. If I remember correctly, we seemed to get along just fine without smart coffee makers, watches, or the other dozens of devices that have the potential to collect our personal data. We didn't have to worry about where our profiles were stored or who had access to them because we kept it all in our little black books. For the most part, we still have the ability to keep it that way.

Alternately, if we preferred the sound of music on magnetic tape, we would have a hard time listening to anything recorded after 1990. But if we love the convenience and variety that an app like Pandora or Spotify affords us, we've got to be online. If our kids want to be able to text us pictures of the babies, we'd probably better have a smart phone, lest we forget what our kids and their babies look like.

Some of us, regardless of the breadth or our attack surface and whether or not we like adjusting the temperature of our refrigerator from the golf course, are donning an extra layer of protection in the form of a Virtual Private Network (VPN). This service allows us to encrypt the data that travels from our devices to our Internet service provider. Corporations have employed them for years, which is what our corporate friends are talking about when they refer to information "behind the firewall." VPNs aren't a guarantee of complete safety, but they make our data more difficult to hack.

The net-net of it all: if we want to keep something private we'd better keep it offline, to the extent that we can. It may be a little more difficult to teach our kids, and especially our grandkids, about things like 35mm film, padlocks with real keys, checkbooks and other rapidly disappearing devices of the analog age.

Who ever would have thought that so much havoc could be wreaked with a bunch of zeros and ones?

**EARLIER ON HUFF/POST50:**

---

**Follow Jeb Harrison on Twitter: www.twitter.com/jebdelimboman**