SWCP Portal
September 2016

A dream if it works, a nightmare if it doesn't

Smart Things, Dumb Reasons

The vision behind the "**Internet of Things**" (IoT) of a world where physical objects are connected online is a powerful one. But now that the initial hype has worn off and uncounted thousands of developers are competing to make it real, the difficulties in achieving such marvels and the hazards involved are becoming apparent.

In some ways, IoT is not really that new. **Barcodes** and **RFID chips** which passively allow computers to track physical objects (including pets and people) have been around for decades, quietly tracing and guiding the movements of goods around the globe. What *is* new is giving devices the ability to actively monitor, respond, and maybe even direct the actions of the objects to which they are attached.

Real objects, however, can cause *real* consequences and that's where most of the problems lurk. There are several categories into which these potential disasters fall, all closely interrelated. Unless they are adequately addressed, the Internet of Things might just turn out as badly as any number of sci-fi **dystopian** futures.

Security

This is the biggest concern, and no wonder. In the mad rush to link everything together, **little attention** has been paid to security. Partly this is because manufacturers such as car makers think in terms of mechanical problems, and the challenges of truly securing their hurtling masses of metal and plastic from malicious electronic tampering hasn't even occurred to most of them.

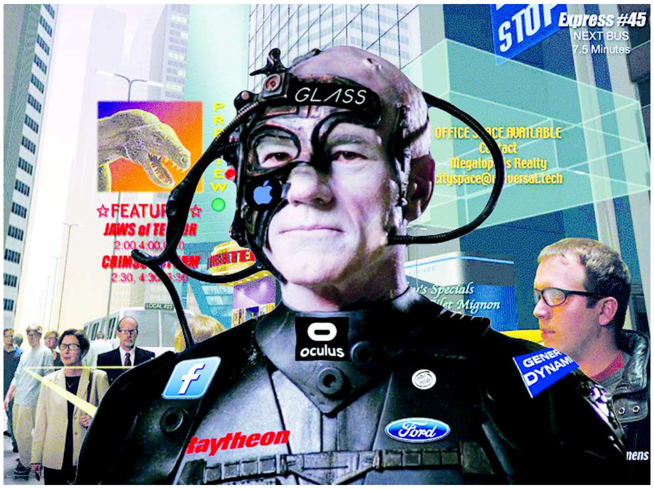
Research shows that many manufacturers and service providers are failing to implement even minimal security procedures. So there have been a number of thefts, including entire fleets of brand-new cars from dealerships, by crooks using laptops to quickly unlock the vehicles.

Even worse, cars can also be remotely **electronically commandeered,** as two DARPA-funded researchers demonstrated last year by taking over a Jeep on a highway. This may be of special concern to users of **GM's OnStar**, **Toyota's Safety Connect**, **Ford's SYNC** and similar hands-free services which are also very vulnerable.

These worries also affect airplanes, traffic systems, power plants (including nuclear reactors), pipelines, and so on which *must* be very well-protected with no room for error. Even medical devices like **pacemakers** in heart patients could be hacked with life-threatening consequences.

Hackers could also exploit these holes to steal data, breach other systems, even send spam. And they are already busy at work. Back in 2014, a hack of 100,000 **smart appliances** such as TVs and refrigerators sent out floods of phishing emails. More recently, a demonstration showed how **smart thermostats** could be struck with ransomware, while a **smart electric socket** was shown to leak email addresses and could be used for more sophisticated attacks, too.

Almost *anything* with a chip can be hacked, but most IoT devices are very simple, with little memory, no encryption capabilities, nor any way to update firmware, and thus may remain not only forever vulnerable but **unpatchable**.



Continued on back

Privacy

Another huge problem with the Internet of Things is **privacy**. All IoT devices produce data, and many are intimately in tune with the environment. So **Amazon Echo**, **Google Home**, and various smart entertainment centers are voice-activated, just like something out of Star Trek.

Which means that they are *always* listening to everything said, patiently waiting for the magic words that awaken them. What else can be done with that data? Who all might access it, and why?

The data could be used to influence your choices, or simply to see who is still up watching TV. But that's just the beginning of creepy uses. Since 2013, for instance, **Shodan**, a website for searching for Internet of Things connected devices, has been posting links to unsecured webcams in parking garages and bars – and also baby monitors and couples' bedrooms.

Big Data Everywhere

Privacy is threatened also because the Internet of Things is intent on gathering lots of data. It's needed to make services work – such as the voice-activated networks – and it is also what marketers seek to pay for their online services.

So what happens when they get together? Windows 10 has just been installed on a **refrigerator door.** Would it someday conspire with your medicine chest to automatically report overindulgences to the your doctor? Much more likely, will the refrigerator, noting that all your yogurt has been used up, be subtly prompted to recommend a more pricey brand the next time you go to the store? If run by Windows, it might just blatantly post ads on the fridge's screen instead.

Cost

Though computing costs continue to fall, making anything smarter and connected also makes it more expensive and complex. But for big ticket items, like cars and houses that require elaborate security systems, even smart doorknobs may cost much more than the dumb kind both to purchase and to use. Mandatory subscriptions could be necessary to maintain service.

This is one of the difficulties of making a smart home. To truly function as an integrated unit, a smart home should really be built that way. Replacing individual systems one at a time will be more costly, time-consuming, and must be integrated. There are hubs and systems that promise to do that, but nothing really smart and versatile enough to make it easy yet.

Technological Change

Some experts think a smart house **will not happen**. One key reason is the rate of technical progress. Devices keep evolving so rapidly these days that a smart house would be obsolete by the time it was designed, much less built.

There's also the question of what happens when a manufacturer goes out of business, merges, abandons the product line, or simply behaves unpredictably. A good example of the latter is the confusion surrounding **Nest**.

Nest made a well-received smart thermostat, and so was snatched up by Google. But there have since been a number of reorganizations. It has been moved into a separate division by Google, who took its engineers for their own smart home products. Nest's future, thought guaranteed when Google got it, is thus very uncertain.

Who's in Control?

Beyond the dangers of having physical objects taken over or used to spy are other practical questions. A home buyer could be in a lot of difficulty, for instance, if the previous owner loses or refuses to surrender passwords. Plus, with smart utilities, there is also the possibility of government regulation or companies throttling service for nonpayment of bills or other reasons.

One basic question that might not be answered for awhile is how much of this are we willing to put up with? Nobody wants to wear a bunch of different net-connected devices, but we may find ourselves in a garish **augmented reality** anyway, full of annoying distractions we may neither need nor want nor can in any way avoid.

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994
505-243-SWCP (7927) ⦿ **SWCP.com** ⦿ **Help@swcp.com**
5021 Indian School NE, Suite 600, Albuquerque, NM 87110

Archived at: http://www.swcp.com/newsletters/.
Click on blue terms in PDF file to open links.