The Difference Engine: Chattering objects

WHATEVER happened to that “internet of things” promised a decade or so ago? Everyday objects—from food, clothing, pills and pets to personal electronics, appliances and cars—were to be tagged with tiny radio-frequency identification (RFID) chips and linked together in an open network of objects that would communicate with one another as well as with their users. Running out of milk, losing the car keys or forgetting to take your medicine would be things of the past. The ability to locate anything, anywhere, at anytime, would cause crime to decrease, stores to remain stocked, healthcare to be improved, road accidents to be reduced, energy to be saved and waste to be eliminated. The internet of things (IoT) was going to be transformative.

It has not happened. Well, not in any significant way. The original idea of having all sorts of things reporting their status and location using simple RFID tags and readers promised opportunities galore. Passive versions of the the tags, costing no more than five cents apiece, need no power supply because they harvest the energy required to transmit their data from the radio signals used to interrogate them. They have a range of around 30cm (a foot) or so, and do not need to be in line-of-sight to be read. High-frequency versions can be read from over three metres away, and active ones containing a battery from up to 100 metres.

Back in the late 1990s, the IoT’s pioneers at the Massachussets Institute of Technology talked about lining the edges of the interactive world with RFID readers capable of collecting information and sending it via the internet to servers that would make various transactions happen. Drive through a toll booth and the electronic pass on the windscreen would tell the transit authority whose credit card to charge. Pay for goods at a convenience store by swiping a mobile phone over a reader at the checkout and the cost would be on your monthly phone bill.

Such things have come to pass—in a limited sort of way. By and large, however, the technology has not kept pace with the vision. One problem, says Laurie Lambeth in a recent study* for GigaOM, a technology consultancy in San Francisco, is that the version of the internet protocol currently in use, IPv4, supports only 4.3 billion unique addresses—a fraction of the number needed to assign a name and location to everyone and everything. Some two billion people—almost a third of the world’s population—are already connected to the internet, leaving precious little address space for the trillions of objects on the planet. That, though, should change. The latest iteration of the internet protocol, IPv6, will provide some 340 trillion trillion trillion addresses—more than enough for everything on the planet and the rest of the solar system as well.

A second problem has been human rather than technical. Firms that make consumer goods have been unwilling to add RFID tags to their products until enough RFID readers had been deployed. The reader-makers, meanwhile, refused to ramp up production until there was a critical mass of RFID-enabled products around for those readers to read. The result has been a perpetual impasse.

There have been other stumbling blocks as well. For instance, there are still too many places where the wired internet does not reach. Nor has it managed to connect as seamlessly as might be desirable with people on the move. Only lately have the wired and wireless networks begun to converge in a meaningful manner.

There have been privacy and security issues, too. Because hackers with the appropriate equipment can interrogate and decode RFID tags, there is always the danger of identity theft—especially now that RFID-enabled passports, smart cards, enhanced driving licences and identity (PASS) cards have become the norm. A year ago, your correspondent worried in print about the lack of security when such forms of identification are used (“Have chip, will travel”, July 17th, 2009). Since the encryption keys they rely on depend on familiar groupings—passport number, driving-licence number, social-security number as well as place and date of birth—they tend to be structured sequences with a fair degree of guessability. Hacking tools can decode such keys in minutes rather than hours.

Also, because RFIDs broadcast their contents over the air, eavesdropping is a cinch. And because they were originally designed for retail use, they can be “locked” or “killed” remotely by wireless commands. As such, the scope for mischief, theft, chaos or worse has frightened off many a potential user.

Belatedly, such problems are being addressed. That is because mobile-phone operators have woken up to the money they can make from offering secure and reliable services to enterprises seeking to network their physical assets. A case in point is the deployment of smart meters by electricity companies. Another is the way internet connectivity is being built into everything from television sets, game consoles and e-readers to health monitors, vending machines and motor cars.

All the big telecoms firms are getting into this new “machine-to-machine” business. Over the past three months, America’s two largest wireless carriers, Verizon and AT&T, have added more connected devices (2.6m between them) than human subscribers (1.2m) to their cellular networks. There are still only 20m connected devices in North America, compared with more than 300m mobile subscribers. But now that everyone who is likely to own a mobile phone has one, connecting things rather than people is where the carriers expect to get their future growth.

By one reckoning, there could be 50 billion connected devices worldwide by 2020. Such a forecast was deemed wildly optimistic a year or two ago. Today, it seems almost pessimistic. Since the free Linux operating system is used widely to manage internet-connected devices, Jim Zemlin, executive director of the Linux Foundation, takes a special interest in the IoT's future. By his reckoning, the coming decade could see two trillion devices being connected to the internet.

All that would require would be for everyone with an internet connection today to have 1,000 of their possessions talking to the internet. People in developed countries are reckoned to have between 1,000 and 5,000 possessions. Your correspondent has close on 1,000 books on his shelves, and many times that number of nuts, bolts, brackets and other bits in his garage. Will such things all be tagged with RFIDs or their NFC (Near-Field Communication) equivalents instead of the bar-codes or ISBN numbers they are labelled with today? Not within the next few years, but probably within a decade. It all depends on how quickly IPv6 is adopted.

Even so, while still a believer, your correspondent is nevertheless left with more questions than answers. For instance, things become connected to the internet by being assigned a unique identifier (ie, a name and an address) as well as the means to talk to other objects. Though the amount of information stored in an object’s electronic tag is typically only 128 bits long,

that is more than enough for the chip to tell an interrogation device where to find a backup database with megabits more.

The questions then become: Who assigns the identifier? Where and how is the information in the database made accessible? How are the details, in both the chip and the database, secured? What is the legal framework holding those in charge accountable? Glossing over such matters could seriously compromise any personal or corporate information associated with devices connected to the internet. Should that happen through ignorance or carelessness, the internet of things could be hobbled before it gets out of the gate.

* “The Internet of Things: What It Is, Why It Matters” by Laurie Lambeth, published by GigaOM of San Francisco.

Fonte: The Economist, Aug. 13th 2010. Disponível em: <www.economist.com>. Acesso em: 17 ago. 2010.