Hackers go home

FROM THE ECONOMIST

Technological tinkering, or hacking, is not limited to computers. Cars, cameras and vacuum-cleaners can be hacked too

The word “hacker” is widely misused. Among hackers themselves, it refers to someone who enjoys tinkering with technology, exploring its boundaries and getting it to do unexpected or unintended tricks, though in general use the word refers to individuals who break into computers for nefarious ends (for whom hackers prefer the terms “malicious hacker” or “cracker”). But a hacker is not necessarily bad and is not necessarily just someone who messes around with computers. Thomas Edison was arguably a hacker, back in the 19th century. Today's technological tinkerers, however, have a far wider range of household gizmos to play with and modify, from cars to cameras. Getting them to do new things, and not merely what the manufacturer had in mind, is an increasingly popular pastime. It even has its own magazine, MAKE, which is filled with projects for the technologically intrepid.

Car enthusiasts have a long tradition of modifying their vehicles to improve on the manufacturer's original specifications. As cars become as dependent on electronics as they are upon mechanics, the business of tweaking their performance has become ever more elaborate. Upgrades for various fuel-injection and ignition computers have been available for well over a decade, providing additional power—often at the expense of warranty cover and fuel efficiency—just by replacing a microchip or two in the engine compartment.

But such modifications are now passé. The latest twist comes from TurboXS of Gaithersburg, Maryland. Its DTEC boost controller uses a standard Nintendo Game Boy Advance SP handheld games console as its display and input device. The software comes on a standard game cartridge, and provides a variety of read-outs and diagnostic options. Wire up a few hardware sensors, and the games console becomes a tuning tool, allowing changes via the boost-controller hardware to the running engine configuration. And all of this was done without any help from Nintendo, notes Nathan Kofahl of TurboXS. It is a new, unintended use of the console—in short, a hack—that is, in turn, used to hack the car's engine.

Hybrid and electric vehicles have also attracted the attentions of hackers. After General Motors introduced the short-lived EV1 electric car in 1996, intrepid owners soon worked out how to connect handheld computers to its built-in diagnostic systems and observe what was going on with their vehicles. Armed with this knowledge, they could then change their driving behaviour to improve the car's range on a single charge. Today, attention is focused on the Toyota Prius, a hybrid-electric vehicle that uses battery power at low speeds (in stop-start traffic, for example) and a petrol engine at high speeds or on long journeys.

The problem, from the point of view of some drivers, is that the control system of the Prius, and the limited capacity of its nickel-metal hydride (NiMH) batteries, prevent it from being used as an all-electric vehicle, even on quite short journeys. So a number of Prius owners have hacked their vehicles, fitting them with larger lithium-ion battery packs that can be recharged from the mains and tweaking the battery-control system to extend the car's electric-only range. EDrive, a firm based in Monrovia, California, is about to launch just such an upgrade package for Prius owners, at a cost of around $12,000.

Closer to home, the ever more complex innards of consumer-electronics devices mean they are also ripe for modification by hackers. The advent of the TiVo personal video recorder was significant in many ways: not only did it precipitate a dramatic shift in viewing habits, it was also one of the first consumer-electronics devices to be based upon Linux, the open-source operating system. Most users, of course, were happily unaware of this fact. But for the more

technically minded, it made possible a wide variety of modifications, letting users make their TiVos work just the way they wanted.

Simple changes—different colours for the on-screen interface, installing a larger hard disk to increase recording capacity—quickly evolved into new software development that, for example, allowed the TiVo to be remotely controlled over the internet, enabling users to add a show to the device's recording schedule from work. This extensibility quickly gained the TiVo a passionate following, but also raised legal concerns. Not content to add features to the device, TiVo users soon worked out how to download programmes to watch them on their laptops, or transfer them to DVD. While TiVo made efforts to prevent this sort of thing, the ingenuity of its users prevailed and instructions have proliferated online.

Even when an electronic device is not based on Linux, it is usually not long before hackers get Linux running on it, which then makes tweaking much easier. The unofficial installation of Linux on Apple's iPod music-player, for instance, led to the discovery of some hardware secrets within it. Some iPods, it turned out, actually had the internal circuitry required to record high-quality audio, though this feature is usually unavailable. Other hacks include the ability to run games and display pictures, even on older iPods. Phillip Torrone of MAKE says this type of modification simply “unlocks the piece of hardware that you paid for.”

But in some cases, such hacks can undermine the manufacturer's business model. Consider games consoles, for example, which operate on a “razor and blades” principle. Consoles are often sold at a loss, but console-makers receive a licence fee of a few dollars for each game sold—so provided each customer buys enough games, the console-maker eventually makes money. When Microsoft launched its Xbox console in 2001, hackers raced to install Linux on it, which transformed it into a low-cost, high performance media-playback system. While this was a minority sport, anyone who did this without buying any games was, in effect, receiving a subsidy from Microsoft. Little wonder, then, that the new Xbox 360 console features significantly beefed-up security measures.

A second example is the low-cost “disposable” digital cameras sold by CVS, an American pharmacy chain. These cameras are designed to be used once and then returned to the shop, where, for a processing fee, the stored pictures or movies are returned to you on CD or DVD. The cameras are then reset and resold. Inevitably, however, hackers have figured out how to access and reuse the cameras themselves. (One even ended up being installed in the nose of a small rocket.) If enough people do this, the business model breaks down. Clever hacking by a few, in other words, could lead to higher prices for the many.

But some companies, at least, have chosen to embrace hackers. iRobot, the company behind the Roomba robot vacuum-cleaner, includes an external data connector in the device and has even documented how to use it. While most customers appreciate their Roombas for their autonomous cleaning skills, there is also a small minority of users who want to reprogram them. iRobot is one of the few firms to acknowledge and appreciate customers who like to tinker. After all, there are few manifestations of feedback as heartfelt as someone who is willing to spend their own time and effort to improve a product.