No Gadget Safe From Home-Style Hacks

By DAVID J. WALLACE

MICHAEL ROTHWELL could have bought a bar-code scanner for his computer and an inexpensive software package to catalog his CD-ROM or book collections. He had not considered compiling such a list until he got a CueCat, a free device designed to let users scan bar codes in newspaper and magazine advertisements and navigate quickly to related Web sites..

After a day and a half of experimenting, Mr. Rothwell defeated the CueCat's encryption system, turning it into a simple bar- code reader and laser pointer. From there, he found cataloging software on the Web and set out to make the bar-code reader work with computers running Linux, not just Windows computers.

"Half of it was the hack value — it was fun to do," said Mr. Rothwell, a 29-year-old software developer from Holly Springs, N.C. "It's about the prestige you get from the community."

Every new gadget seems to generate a sort of hobbyist underground, a collection of people who want to disassemble its hardware and decode its software. Some find new uses for the gadgets, while others look for ways to tweak or reprogram operating systems, or soup them up with more power, just as family cars of earlier generations, the gadgets of their day, were turned into hot rods.

Mr. Rothwell said he had turned discarded digital organizers into picture frames that play music. And he knows about people who reprogram Big Mouth Billy Bass, a talking plastic fish, to make it deliver their own joke messages.

Once the tinkerers start dissecting a product, unintended consequences can either undermine or validate a company's entire business strategy. That is what Netpliance learned after it introduced the i-opener in late 1999, a simple device offering home Internet access through Netpliance itself.

It turned out that it took only a cable, software and a hard drive to convert the i-opener into a PC that can work with any Internet service provider. Netpliance had priced the machines at $99 apiece — about a third of what they cost to make — expecting to recoup its investment through monthly subscription revenue. But once the secret of the i-opener spread on the Internet — it came to be known as the i-opened-it — that prospect was doomed. In an effort to preserve the company, Netpliance is now selling the i-opener for $299 and has sold its subscription base to Earthlink.

The Web is replete with sites that will tell the curious how to put new, unintended features or enhancements into devices like cellular phones, digital organizers and laptops. One site tells how to increase the battery life for a Nokia phone by 30 percent, at the expense of call quality — or improve call quality but cut battery life by 5 percent. Another shows a surgical reconstruction of a Furby, a furry talking toy, for those who want to put its speech-recognition and infrared-linking abilities to new uses.

Some hackers view their efforts as a form of research and development, or at least user testing, that benefits manufacturers. Others try to sell their revamped gadgets through personal Web sites, online auctions or word of mouth.

Altering devices will void most warranties, manufacturers warn, and they could make appliances overheat or damage the equipment or its user. But some companies have opened their doors, if only slightly, to those determined to reinvent the company's creations.

Digital Convergence, the maker of the CueCat, is opening its doors to software and hardware enthusiasts, said Douglas Davis, the company's chief technology officer. It is entertaining proposals for new applications for the scanners, including one that lets people scan the bar codes on video-game cartridges to call up on their computers links to Web sites with advice for players.

"We always knew this would be an aspect of our business," Mr. Davis said. "But we were caught more or less off guard — we were expecting dozens and we got thousands."

There has long been tension between the companies who try to keep the inner workings of their systems secret and the enthusiasts who dissect and analyze them, said Chris Wysopal, who directs research and development at @Stake, a security consulting firm in Cambridge, Mass.

As more of their functions have migrated from hardware to software, gadgets have become easier to re-engineer. For example, Mr. Wysopal said, simple reprogramming turns an inexpensive projector used for business presentations into a home theater DVD player that is like one selling for a much higher price.

"It's an arms race," he said. "For every new mechanism that comes out, people will try to reverse-engineer it and see how it works. There may be valuable feedback as long as the devices are used in a legal way, and companies should pay attention to these people."

Pushing the limits is what some enthusiasts have in mind for TiVo, the digital video recorder, when they reprogram the systems to use 80- gigabyte hard drives instead of standard equipment. Scott Moschella, a New Jersey graphic designer who sells upgraded TiVo boxes via online auctions, said that by using software and technical tips shared on the Web, tinkerers can create storage for up to 117 hours of video, nearly twice the maximum offered on standard units.

Altering the machinery voids the manufacturer's warranty, Mr. Moschella said, yet there is strong demand. He bought six refurbished TiVo machines for $400 apiece, and he can sell each for $200 profit after reprogramming them.

"It's not something anyone can do," he said, "but if you have some technical understanding, it isn't that hard. And I test the hard drives for 12 hours to ensure they're properly formatted. Not everybody does that."

Unlike some manufacturers, TiVo has been reasonably friendly to hackers and is well regarded by them, Mr. Rothwell said. TiVo's customer relations director, Richard Bullwinkle, said that he had rewarded some adventurers with free service for telling the company about hacks. About 1 percent of the company's 150,000 customers have altered their machines, he said.

Digital organizers have been a popular target for pranks, aided by the decision of Palm Inc. to open its operating system to the public. The results have included software that can be downloaded to turn a Palm with infrared capability into a remote control for television. And a high school student has turned a Palm into a four-wheeled robot.

Other companies have taken legal action to protect their devices' hardware and software. Manufacturers of digital video discs sued individuals who broke the encryption system used for DVD's so they could use them with Linux systems. That case is before the United States Court of Appeals for the Second Circuit and has grown to include First Amendment issues on whether sharing such data constitutes protected speech.

But in the face of so many reverse- engineers worldwide, Mr. Rothwell said, attempts to stifle such efforts are futile. He is developing software that will let shoppers use any bar- code reader to scan grocery items to check for ingredients that may cause allergic reactions.

"If I own a piece of hardware," he said, "then I should be able to do whatever I want with it. Car makers don't weld the hood shut and prevent you from taking the tires off. And people have shown electronics makers that you can't weld the hood shut. But if I tinker with something, I don't try to have it repaired under warranty — that's not playing fair."