The alternative to policing is burglar-proofing: making things harder to crack. In principle, you might think that the gazillion-dollar software industry would be able to produce uncrackable software. In practice, it can't, although it certainly keeps trying.

Take the dongle, for example. It is the summit of copy protection, an explicit melding of software and hardware. Without the right hardware key - the dongle - plugged into the machine's parallel port, the software won't run. And without the right software, the dongle is a mindless doorstop. Calls to the dongle are woven into the code at the lowest level. "The program may call the dongle every 150 mouseclicks, or every time you print, or every time you select flesh tones as your desktop color scheme," says one dongle expert. If the response to the call is false or not forthcoming, the program shuts down. All communications between the two are encrypted by uncrackable algorithms. Internal security fuses ensure that any attempt to hack the dongle mechanically will cause it to self-destruct. "Nothing short of an electron microscope," says the expert, "could extract the algorithm from that mess."

The biggest player in the dongle market is Rainbow Technologies, whose Sentinel hardware keys are used by 55 percent of all protected software. There are 8 million Sentinel keys attached to 8 million printer ports the world over. The company calls it "the world's most effective way to stop piracy" - a clarion call to crackers if ever there was.

The logical approach to cracking a hardware key is to create a "pseudodongle" - a chunk of code that sits in memory, giving the correct answers to any query. To do this, a cracker would have to monitor and trap traffic to-ing and fro-ing across the parallel port, then use this information to build an infallible query/response table. Unfortunately, if the query is, say, six characters long, it can have more than 280 trillion responses (281,474,976,710,700 to be exact). With the speed of modern machines, this would take approximately 44,627 years to collate. With the SentinelSuperPro dongle ("the most secure and flexible protection available") the query length can be 56 characters - requiring a mere 10 125 years (in theory) for a complete table. However, the dongle in SentinelSuperPro for Autodesk 3D Studio MAX was cracked in just under seven days of its retail release - substantially less than the 44 millennia emblazoned on the sales brochures. Other expensive high-end applications that use Sentinel - including NewTek's LightWave 5 and Microsoft's SoftImage - have ended up the same way: cracked, repackaged, and redistributed to every corner of the Internet within weeks of their release. How? Instead of attempting to simulate the dongle, expert crackers simply remove its tendrils from the program code, unraveling the relationship skein by skein, function by function, call by call, until the application ceases to need the dongle to function. Then it's ready for anyone and everyone to use - or, more likely, gawk at.

Nobody says this is easy. There may be only three or four crackers in the world who could manage such an opus. But with the Internet to transmit the result, only one needs to succeed.

With the latest wave of dongles, warez world looked to Russia to get the job done - and a shadowy group called DOD "won" the contract. The self-styled "Warez Bearz of Russia and Beyond," DOD appears to have arms throughout Europe, Asia, and the US. It undid Microsoft SoftImage's dongle protection in two weeks, which wasn't easy. The crew riotously celebrated in their "NFO" file: "Totally awesome work of glorious DOD cracker - Replicator after five other crackers gave up! We decided not a do a crack patch 'coz it will take too much time to code it ... you ask why? 'Coz there are only 72 (!!!) EXEs patched. All options now work 100%!"

NFO files do more than brag or supply installation instructions; they testify that the ware is a bona fide release, guaranteed to work. And this is more than just posturing; a group's reputation is paramount. Each release is painstakingly beta-tested. These are their products now, their labors of love. Nobody wants to find a "bad crack" in his hands after a seven-hour download. Nobody wants to be accused of being "unprofessional." Nobody wants the ignominy of anything like the bad crack for Autodesk's 3D Studio that made the rounds in 1992. For all intents and purposes it ran correctly, all features seemed 100 percent functional. Except that the dedongled program slowly and subtly corrupted any 3-D model built with it. After a few hours of use, a mesh would become a crumpled mass of broken triangles, irrevocably damaged. Cleverly, Autodesk had used the dongle to create a dynamic vector table within the program. Without the table, the program struggled to create mathematically accurate geometry - and eventually failed. Many a dodgy CAD house saw its cost-cutting measures end in ruin. Autodesk support forums and newsgroups were flooded with strangely unregistered users moaning about the "bug in their version of 3D Studio." A rectified "100 percent cracked" version appeared soon after, but the damage was done. The Myth of the Bad Crack was born, and the pirate groups' reputations tarnished.

But the pirates bounced back. They always do. And there's no reason to think that there's any way to stop them. Software security people are at an intrinsic disadvantage. Compare their job to that of securing something in the real world that's valuable and under threat - a bank, say. Typically, only one set of armed robbers will hold up a bank at a time, and they'll get only one crack at it. Imagine an army of robbers, all in different parts of the world, all attacking the same bank at the same time. And in the comfort of their own homes. Not just once, but over and over again. Imagine that each set of robbers is competing against every other, racing to be first in. Imagine, too, that some of the robbers are so technically adept that they could have built the alarms, the safe, and even the jewels themselves. And that they have cracked more than 30 banks with the same protection system. And that they're learning from all their failures, because they're never caught. No security could realistically resist such an onslaught. It may be that the only way to avoid having your software cracked is to put no protection whatsoever on it. No challenge, no crack.

Popularity only feeds the frenzy. Doom is a good example. In 1993, id Software distributed the original shareware version of its nasty-guns-in-nasty-dungeons masterpiece on bulletin boards, CompuServe, and a then-little-known system called the Internet. Downloaded by more than 6 million people worldwide, Doom was a trailblazer in the world of modem marketing. The shareware gave you a third of the game: if you liked it, you had to buy the rest on disks. Millions did.

Doom and its makers became a dream target. Weeks before Doom II's release, the sequel was available on the Internet - not as shareware, but warez. And not just as a teaser, but the whole damn thing. "Yeah, that was leaked," says Mike Wilson, id's then-vice president of marketing, now CEO at Ion Storm. "Can't tell you how much that hurt." The leaked copy was rapidly traced - rumors abounded that the version was a review copy fingerprinted to a British PC games magazine - but too late. It was already on Usenet, doing the rounds on IRC, filling up FTP sites. The pirates were in ecstasy and id was left with recoding the final retail release, to ensure future patches and upgrades would not work on the pirated version. Then they shut the stable door. No more external beta testing; no more prelaunch reviews. "We assured ourselves it would never happen again," says Wilson. "No copy of our games would leave the building."

Nice try. Quake, Doom's much-anticipated follow-up, turned up on an FTP server in Finland three days before the shareware come-on was due to be released. The pirate version was a final beta of the full game - complete with eerily empty unfinished levels and bare, unartworked walls. Within hours, it had been funneled to sites all over the globe. IRC was swamped with traders and couriers desperate to download.

"Somebody actually broke into our then poorly secured network and started to download it right before our eyes," Wilson recalls. "We managed to stop the transfer before he got all of it. We traced the call, got his name and address. He was pretty scared, but, of course, it was some kid. We didn't pursue that one. It hurt, but not enough to put some little kid in jail."

When the legitimate Quake hit the stores last year, it was initially in the form of an encrypted CD, which let you play a shareware version for free but would only unlock the rest on receipt of a password, available for purchase by phone. The encryption scheme, an industry standard called TestDrive, was eventually cracked by a lone European pirate called Agony. And id's crown jewel was now available, courtesy a 29K program. "In order to unlock the full version, you are supposed to call 1-800-IDGAMES," Agony gloated in a posting. "Hahahahahah."

"We knew it was going to be hacked," says Wilson. "We of all people knew. But we thought it was safe enough, certainly safer than Doom II." And, truth to tell, it didn't matter too much. The gap between the game's release and the warez version becoming widespread was enough for id to sell the copies they expected.
"Copy-protection schemes are just speed bumps," laments Wilson.

Nobody really knows how much actual damage cracking does to the software companies. But as the industry rolls apprehensively toward the uncertain future of an ever-more frictionless electronic marketplace, almost everyone thinks piracy will increase. "The level of activity out there is overwhelming. We know that we have to take action to take control of it. We will continue to bring a critical mass of prosecutions," says Novell UK's Smith. He doesn't sound all that convinced.

Somewhere back on the US East Coast, Mad Hatter has a final swig of ginger ale and settles down to bed with his wife, White Rabbit. She thinks his obsession is a wasted resource, but didn't complain when he installed the latest version of Quicken on her computer - a cracked copy, of course. "We are all family men, married with children, day jobs, dedicated accounts, and multiple phone lines," Mad Hatter says. "Our kids have been looking over our shoulders for years. They will be the next couriers, the next warez gods."