Bogus!

By **Michael Pecht** and **Sanjay Tiku**

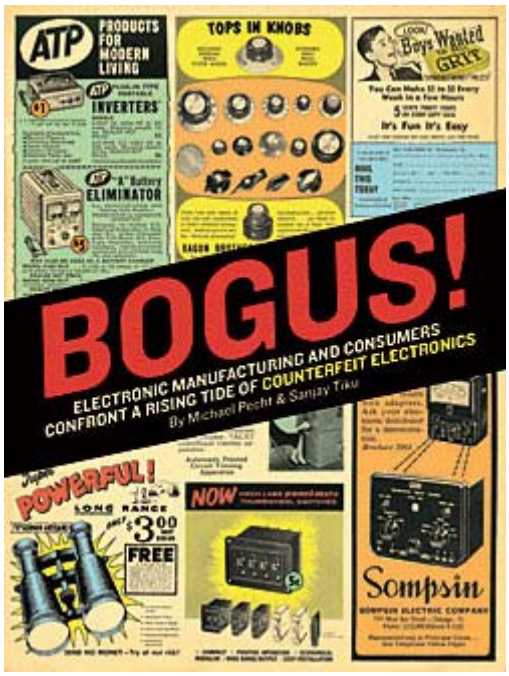


PHOTO COLLAGE: LAURA AZRAN

• A police raid on a suspected counterfeiter in China's Guangdong province turns up US $1.2 million in fake computer parts and documents—enough to produce not only complete servers and personal computers but also the packaging material, labels, and even the warranty cards to go with them. All the parts are neatly labeled with the logo of Compaq Computer Corp.

• A capacitor electrolyte made from a stolen and defective formula finds its way into thousands of PC motherboards, causing the components to burst and leak and the computers to fail and eventually costing more than $100 million to rectify.

• 8 Local authorities in Suffolk County, N.Y., seize counterfeit electrical safety outlets—used in bathrooms, kitchens, and garages to guard against electrical shock—bearing phony Underwriters Laboratories logos. The bogus parts had no ground-fault-interrupt circuitry, and had they been installed anywhere near water, the results could have been fatal.

• Dozens of consumers worldwide are injured, or merely surprised, when their cellphones explode, the result of counterfeit batteries that short-circuit and suddenly overheat.

That the world is awash in fake goods comes as no surprise to anyone who's ever strolled the streets of a major city and seen a gauntlet of sidewalk hawkers selling knockoff clothes and pirated motion pictures. But in recent years a less visible but no less insidious component of the illicit global trade has taken off: the counterfeiting of electronics components and systems, from tiny resistors to entire routers.

High-tech products—including consumer electronics, batteries, computer hardware, and electronic games—accounted for four of the top 10 products seized by U.S. Customs and Border Protection in

2004, the most recent year for which figures are available. And according to the Alliance for Gray Market and Counterfeit Abatement, a trade group founded by Cisco, HP, Nortel, and 3Com to combat illicit trafficking in their products, perhaps 10 percent of the technology products sold worldwide are counterfeit. The group estimates that legitimate electronics companies miss out on about $100 billion of global revenue every year because of counterfeiting. That figure takes into account only the profits that counterfeiters siphon off from manufacturers; it ignores the added repair and maintenance costs necessitated by defective bogus parts and the expenses of trying to identify and intercept suspected counterfeiters.

No company is immune. Counterfeit electronics have turned up in every industrial sector, including computers, telecommunications, automotive electronics, avionics, and even military systems. What's more, nearly every kind of component has been pirated, from low-level capacitors and resistors to pricey DRAMs and microprocessors. Whole servers, switches, and PCs have been faked, but more commonly, only one part in hundreds or perhaps thousands in an end product is bogus.

And that one bad component can cause lots of headaches. For example, a component that may be worth only $2 can cost $20 to replace if it is found to be counterfeit after it is mounted onto a circuit board. Even if a manufacturer catches a counterfeit item on the production line, it will still lose money from having to halt production and swap out the bogus part. And if the product finds its way onto the market and out to customers, there likely will be even bigger problems with field service calls, warranty issues, product recalls, and the like.

For the consumer, the failures of systems that use counterfeits can lead to safety and security problems. Even if the fake part works, at least initially, it still poses reliability risks, because it hasn't undergone the legitimate manufacturer's rigorous quality assurance processes.

For the manufacturer whose product line has been compromised, a less tangible but still significant problem is the tarnishing of the company's image and brand. Counterfeiters also cheat legitimate manufacturers by bypassing the research, development, and marketing that went into the original product.

Unfortunately, most companies are doing little to keep counterfeit parts out of their supply chains. Companies big and small say they can't afford to track the history of every part that goes into every board in every product they make. Indeed, many of the world's biggest manufacturers have been duped, in some cases putting fake or marginal parts into circuit boards that later failed and caused public relations nightmares. As the electronics supply chain grows more complex, with parts coming from many different suppliers all over the globe, it becomes even more difficult to police the problem. Meanwhile, the competitive pressure to slash manufacturing costs makes the trade in cheaper, less-than-legit parts ever more attractive.

Three key factors are feeding the rise in bogus electronics: the shift of manufacturing to China, with its looser enforcement of intellectual property laws and convoluted supply chains; the growing sophistication of technology that enables cheaper and more convincing fakes; and the rise of the Internet as a marketplace, allowing buyers and sellers to make fast trades without ever meeting

face to face.

As many companies are learning the hard way, preventing counterfeiting requires a constant, deliberate, and multifaceted effort, vigorous monitoring of potential trouble spots, and judicious use of anticounterfeiting technologies.

Even the problem isn't simple. "Counterfeiting" can refer to a variety of activities. It could be as simple as re?marking scrapped or stolen and possibly nonworking parts—or as complex as illegally manufacturing complete parts from original molds or designs. A bogus part may be relabeled to appear to come from a different manufacturer or to appear to be a newer or even an older but more sought-after component than it actually is.

Visually, it's usually hard to tell the bogus part from the real thing. In the fall of 2004, for instance, the military contractor L-3 Communications, based in New York City, reported numerous failures with an IC chip bearing the Philips Semiconductors logo. Failure analysis revealed a thicket of anomalies, including missing, broken, or separated wire bonds, and in some cases no silicon IC (die) inside the package. Other customers who bought the Philips chips also complained about their shoddy quality. The chips, it turns out, had all been purchased from an unauthorized reseller. They were indeed Philips ICs, but ones that Philips claimed had been scrapped as defective. Somehow, though, they had made their way onto the electronics gray market.

Sometimes, a look-alike product is sold on the open market under a slightly altered brand name. While that type of counterfeit is easier to spot and trace back to its source, the more insidious and far more prevalent kinds are either sold as legitimate brand-name goods or become components in otherwise legitimate products. Counterfeiters often go to great lengths to duplicate materials, part numbers, and serial numbers so that their wares match those of authentic products. With CPUs, for example, counterfeiters have been known to re-mark components so that they appear to be of higher quality and speed than they actually are. Back in 1998, 266-megahertz Intel Pentium II chips that had been relabeled as 300-MHz Pentium IIs began showing up in PCs; at the time the latter cost $375 apiece, while 266-MHz chips cost $246. But operating the lower-speed chip at higher speeds—known as overclocking—led to reliability problems, because the chip ran hotter and was more likely to process instructions incorrectly. (Extreme computer enthusiasts intentionally overclock their chips to eke out additional performance, but at least they know they're doing it and can provide additional cooling.)

Such fakes are hard to spot and are all too often slipped into the supply chain by either unknowing or corrupt distributors. Among the most popular counterfeit products right now are cellphone batteries [see photo, "

BATTERY DISCHARGE: Workers destroy counterfeit batteries in an event staged by local authorities in Panyu City, in southern China.

PHOTO: CHINA PHOTOS/REUTERS

" In a case recently described in PC World magazine, a woman's cellphone battery suddenly overheated, causing the device to burn a hole through her jacket pocket, fall to the floor, and explode. The woman had bought her Motorola phone, complete with the counterfeit battery, from an authorized Motorola reseller, which in turn had obtained the phone directly from T-Mobile. Although T-Mobile called the episode an isolated incident, ongoing press accounts of self-detonating cellphones suggest otherwise.

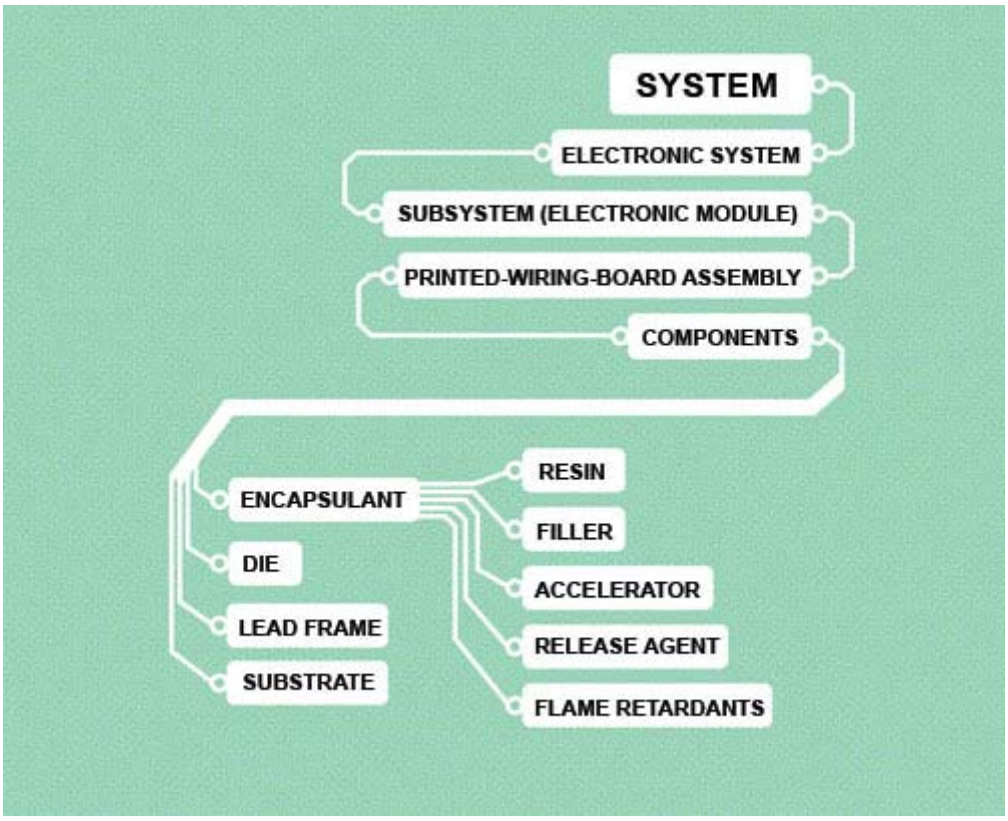
As those cases also demonstrate, most counterfeit products come to light only when a system failure occurs. Even then, the failure isn't always easy to trace, and investigators can be confused about whether the part was defective, was damaged in assembly or use, or was counterfeit.

In our laboratory at the University of Maryland, in College Park, we conduct failure analyses on hundreds of electronic and semiconductor products every year. In recent years we have seen an increasing number of product malfunctions due to counterfeit parts. In many cases, only a thorough analysis reveals the true cause of the failure. One counterfeit semiconductor device we saw used filler in the mold compound that contained mostly silica flakes, rather than more expensive spherical filler. Our analysis revealed that the device failed because the flakes of the cheap filler scratched the die. Such a failure is difficult to detect and quantify, and from a cursory inspection, no one would have known the package was a fake.

Companies that manufacture products in China are especially at risk of having their goods counterfeited or having counterfeit?components enter their end products. China—"the world's Wal-Mart for fake goods," according to a recent article in CSO, a magazine for security executives—does a poor job of enforcing its IP laws. The problem is exacerbated by the complicated manufacturing

relationships that typically exist there. Whereas 20 or 30 years ago, a North American or European manufacturer might have had a vertically integrated operation that dealt directly with only a few trusted suppliers, a manufacturer in China, whether owned by a Western company or not, buys components and materials from many suppliers and through many distributors and other intermediaries. Such a complex supply chain creates abundant openings through which counterfeit items can slip into finished products. That said, counterfeiting can't be traced to just one country or region. Plenty of it goes on in the rest of Asia, Europe, the United States, and elsewhere.

For an electronics equipment manufacturer, identifying counterfeit products from among the thousands of components used to assemble a system like a desktop computer or a commercial jet presents a huge challenge [see diagram, "



CHAIN OF CHANCE: This diagram shows a typical supply chain of parts and materials for an electronics system, whether it be a laptop computer, a digital camera, or a flight management system for a Boeing 777. Each part or material may be manufactured by a different company and sold through a distributor, opening up many potential paths for bogus goods to enter the supply chain.

DIAGRAM: LAURA AZRAN

" A representative of one of the world's largest computer companies recently confirmed for us that bogus components do get into its supply chains and that the company is simply unable to inspect every part and device going into its finished products. Given that the company ships about 10 million computers each quarter and works with hundreds of suppliers, it's easy to see the magnitude of its challenge.

Indeed, most manufacturers these days do not have the resources to trace the origins of every part in their products. Ironically, they once did. Back in the 1970s and early 1980s, companies relied on quality assurance teams to inspect and test new components as they arrived. But as components became more reliable, the need for such rigorous inspections faded away.

The rise of the Internet as a trading tool has greatly expanded counterfeiters' horizons. It can give sellers anonymity, and it allows transactions without buyer and seller ever meeting. Our investigations have determined that many bogus electronic semiconductor devices move through online channels.

Increasingly, though, online markets are the only way to locate what you need. That's especially true when the bona fide product is in short supply. Many avionics systems, for example, remain in service for three or more decades; toward the end of the system's lifetime, the original components may no longer be in production. Carmakers face similar obsolescence. A typical Hyundai car now comes with a 10-year warranty. But by the time that warranty expires, any one of the 20 or so microprocessors it contains will almost certainly be scarce.

Such situations are irresistible to counterfeiters. When the demand for replacement products escalates, the cost of parts also rises, and counterfeiters see their chance. In attempting to replace an obsolete part, an unsuspecting consumer may turn to less reliable sources, including parts brokers. Even among parts brokers there are varying levels of trustworthiness.

All distributors sell parts that they've purchased from the original manufacturer or supplier. But franchise distributors have a formal, ongoing relationship with the manufacturer, while independent distributors generally don't. Parts brokers, by contrast, act as scouting agencies for hard-to-find components; rather than maintaining an inventory, they track down parts only as the need arises.

The Internet has made it possible for virtually anyone to set up shop as a broker or distributor. Those wishing to sell electronics products through Web sites such as NetComponents, IC Source, and Broker Forum need only pay a nominal monthly membership fee. Although the majority of traders on such sites are legitimate, others are not, and there's often no way to tell the difference.

Three years ago, a U.S.-funded agency known as the Government-Industry Data Exchange Program (GIDEP), which tracks instances of counterfeit and defective parts, issued an alert regarding a 20-pin digital memory IC, marked with the lot code TAH9949 and manufactured by Cypress Semiconductor Corp., San Jose, Calif. Cypress had stopped making the part in 1999, but the military electronics firm Telephonics Corp., based in Farmingdale, N.Y., had purchased 100 of them in April 2003 through two parts brokers. When Telephonics engineers tried to enter data into the chips, the ICs wouldn't accept the Cypress algorithm, and a failure analysis revealed they had a smaller die bearing the logo "MMI." Cypress later said that the bogus parts lacked other designators it uses to trace military parts, and that even the parts' country-of-origin code—"TAH" instead of "THA" for Thailand—was wrong.

At our lab, we sometimes see parts that have been relabeled so that they appear older than they actually are, because the old part is the one in short supply. The new part may function nearly identically to

the older part, but it may be faster or lack a bug found in its antecedent. Fixing a bug is good, right? Not always—when you install the newer part into the circuitry, which also fixes the bug, that fix may in turn cause a different problem.

In short, whenever a product can be made more cheaply than the original, counterfeiting can and usually will occur. One area where we expect to see a rise in counterfeits in the coming months is the result of efforts to make electronics more environmentally friendly.

This July the European Union's 2003 Directive on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment—the so-called RoHS directive—takes effect, banning the sale of any new products that contain lead, mercury, cadmium, or several other toxic compounds. (Some military and stationary telecom systems are exempt.) China and the state of California have their own versions of RoHS legislation.

Manufacturers and components makers have been scrambling to meet the EU deadline. Producing lead-free counterparts of existing components is the key issue. The problem is that the processes for producing lead-free parts aren't always compatible with those for making ordinary components. Counterfeiters will almost certainly capitalize on the situation, re-marking leaded components as lead-free.

Another environmentally friendly practice, electronics recycling, is creating a new stream of bogus components. We've seen low-skilled workers in China tearing apart cast-off computers and separating their parts into bins for reuse in other products [see photo, "

BIN THERE, DONE THAT: ICs reclaimed from computers and other electronics at a recycling center in China's Guangdong province will be reused in toys and possibly other products.

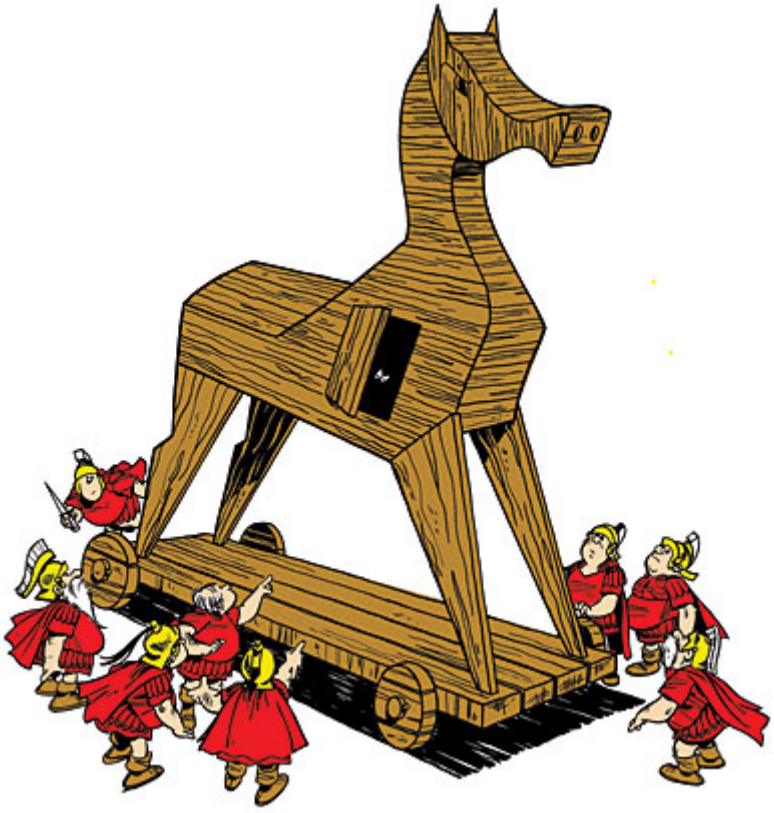
PHOTO: HUANG SHENGCHUN/IMAGINECHINA

" The official line is that the recycled components will be used in toys, but once the parts enter into distribution facilities, there is a real

concern that they will be reused in other products. The parts may not be counterfeit per se, but they are probably being incorporated into subassemblies sold without any indication that some of their parts aren't new.

Attempts to rein in counterfeiters have taken many forms. A number of international agreements such as the Patent Cooperation Treaty of 1978 and the World Intellectual Property Organization Copyright Treaty of 1996 have tried to define and enforce IP rights. Although such pacts might be helpful for companies whose competitors are peddling look-alike products, they haven't done much to stem trafficking in bogus electronics, and they don't address the problem of counterfeit products that enter the supply chain through illicit channels.

The U.S. Congress has considered legislation intended to deter and punish counterfeiters, especially those coming from outside the country. One bill, known as the Keep America Secure Act, would have barred the Defense Department from purchasing equipment that contained electronic products not manufactured in the United States. The bill's goal was to ensure that the Pentagon had secure suppliers, but had it become law, it also would have had the effect of controlling bogus parts [see sidebar, "



COUNTERFEIT ELECTRONICS AS WEAPONS OF MASS DISRUPTION?: Some customers may consider knockoff clothing and watches to be good values, but counterfeit electronics can be devastating. What would happen, then, if some criminal element bent on wreaking havoc and inducing public panic were to intentionally introduce such a bogus product into the electronics supply chain—malfunctioning printed-circuit boards in a critical air-traffic-control system, say, or faulty parts into automobile braking systems? Even the suggestion that such an act had occurred might set off a wave of recalls and might ground suspect

systems.

What form could such weapons of mass disruption take? One possibility is a time-delayed defect, designed to cause a product to fail after some predictable period. Such products might pass an initial qualification test and remain functional for a time, but eventually they would degrade and shut down. A clever counterfeiter might also deploy a Trojan horse, containing embedded software or hardware programmed for disruptive purposes. For example, you could program a cell into a microprocessor to malfunction, with the triggering event being a change in the logic state of some registers. Or the microprocessor could be programmed to release faulty information, such as erroneous Global Positioning System or altimeter readings in an aircraft.

Or imagine products hardwired to fail or otherwise do damage when they receive an external signal; this type of mechanism is used in many of today's roadside bombs in Iraq. A product could also be engineered to allow spying; circuitry inside a personal computer, for example, could surreptitiously collect data and then send the information periodically to a remote receiving station.

If all this seems far-fetched, keep in mind that variants of such disruptive technologies are actually used by legitimate companies now to remotely monitor the health of computers and other electronic systems. That said, just because something can be done doesn't mean it will. So far, at least, those hell-bent on social disruption seem content with more obvious means of instilling terror.

—M.P. & S.T.

IMAGE: LIQUIDLIBRARY/JUPITERIMAGES CORP.; IMAGE MANIPULATION: LAURA AZRAN

" The bill's critics noted, however, that it also would have hamstrung efforts to develop advanced systems, because many of the high-performance technologies already used by the U.S. military originate outside the country.

A number of groups monitor and report on counterfeit products. One of the most active is GIDEP, whose members include government and industry representatives from the United States and Canada. The program's chief resource is a database compiled from reports that members submit describing failed and counterfeit parts. The program has exposed many incidents of counterfeiting, but it's a voluntary service—if members don't submit reports, the information isn't shared. Our experience indicates that many companies are reluctant to go public when they do spot counterfeits, out of fear of being sued by customers and of tarnishing their brands' reputations. And although GIDEP does a service in alerting companies and the public to known counterfeits, it does nothing to actually address the cause of the problem.

Electronic Resellers Association International (ERAI), a group that represents more than 1000 independent distributors, has been working to improve quality control among its members by, for example, setting up an escrow service, which allows buyers to inspect the goods before completing their purchase, and by launching its own

Web-based database, Parthunter.com, for locating parts. Unlike other online trading sites, Parthunter vets its traders and alerts users when they search for a part that is known to have been counterfeited in the past. Such activities are encouraging signs, but the fact remains that most independent distributors don't subject themselves to the kind of scrutiny that ERAI demands of its members.

With no systematic way to defeat counterfeiting, individual companies have been fending for themselves [see photo, "

MOUSETRAP: Thousands of counterfeit computer mice, confiscated in Munich, Germany, by peripheral maker Logitech, get crushed.

PHOTO: MICHAEL DALDER/REUTERS

" One of the chief defenses is to rigorously monitor the supply chain. The large computer company mentioned earlier has a policy of avoiding independent parts brokers; it tries to purchase parts directly from trusted sources—and hopes that its suppliers also purchase directly from trusted sources. Big companies that do all or part of their manufacturing in China and other parts of Asia also make efforts to police their operations there, often maintaining full-time staff or hiring outside services to look out for bogus parts.

Identifying suspected counterfeiters is another approach. Underwriters Laboratories Inc., in Northbrook, Ill., is particularly aggressive in this area. UL is not a manufacturer but is hired by manufacturers to test and certify their products. So when a counterfeiter uses a fake UL logo to lend an air of authenticity to an otherwise bogus product, UL understandably grows concerned. During the last 10 years, the company's dedicated anticounterfeiting team has worked with U.S. Customs and Border Protection, the Federal Bureau of Investigation, and other agencies around the world to identify and seize millions of products bearing counterfeit UL marks. The merchandise seized has included not only computer components and power supplies but also lamps, extension cords, Christmas lights, fans, telephones, and radios.

UL also has introduced holographic labels that it says are virtually impossible to forge. Indeed, the use of sophisticated holograms or

other labeling is another way that companies attempt to thwart counterfeits. For instance, the router and networking company 3Com Corp., Marlborough, Mass., announced in January that it had begun using three-dimensional, tamper-foiling holographic labels on all its switches. But as anyone who has purchased pirated goods in China and elsewhere can attest, genuine-looking hologram labels are cheap and plentiful; even if they only approximate a real logo, the holograms lend that air of authenticity.

Like many companies, 3Com also regularly posts notices on its Web site on how to identify legitimate company products. But with so many manufacturers and suppliers employing their own authenticating schemes, there is simply no way to keep up with the information. Who has time to check that the laser-etched serial number on a particular memory device is exactly as the chip maker says it should be? In one telling example, the outward appearance of a counterfeit lithium-ion battery for a Nikon digital camera differed from the real thing only in the subtly squarer shape of one of hundreds of Japanese characters on its label.

Manufacturers big and small need to be doing more to ensure that the parts and modules contained within their systems are legitimate. This is particularly true for critical systems that have a safety or security function. Among the schemes proposed so far are specially designed tests of individual components and finished products and aggressive identification methods to verify a component's source and type.

Here's another recurring idea: create a licensing procedure for introducing parts into a given industry's supply chain. Anyone lacking the license cannot sell into that supply chain. Unfortunately, the huge number of suppliers that most companies deal with today has deterred them from trying to implement such a scheme. In fact, in 1995, following numerous incidents of substandard components making their way into aircraft, the U.S. Federal Aviation Administration considered licensing avionics parts but rejected the idea. In any case, any company that is willing to risk financial penalties and even jail terms to sell counterfeits is unlikely to be dissuaded by administrative checks or licensing requirements.

Radio-frequency identification (RFID) tags have been highly touted as a means of tracing a product's path as it zigzags through the supply chain. The wirelessly readable RFID labels, which can encode authenticating data such as where and when the part was made and by whom, are more informative and much harder to fake than simple bar codes, and most can be scanned from a distance, saving time and effort. The smallest RFID, Hitachi's micro-chip, measures just 0.3 millimeters on a side, which in theory would be tiny enough to embed in many small components. But use of RFIDs demands that companies agree on a standard encoding scheme; to date that hasn't happened.

A similar approach is to embed in each component software or firmware identifiers, including serial numbers, manufacture date, application code, and country of origin. After a number of fake lithium-ion batteries in digital and video cameras exploded, Nikon experimented with embedding software in two Coolpix digital camera models sold in Japan. Details about the technology are scant, but the software reportedly read an ID number on the lithium-ion battery to confirm its authenticity and to prevent non-Nikon batteries from being used in the camera. Such an approach, while effective, might not be popular with consumers—who probably want the option of using other makes of battery—or with authorities worried about anticompetitive

practices.

Electronics companies also are exploring technologies for identifying the resins, adhesives, and other chemicals used by the industry. Microtrace Inc., based in Minneapolis, markets a technique for tracing explosives after they have detonated. When encoded nanoparticles are mixed into a resin, the data in the "microtaggants" can be read using handheld scanners, enabling the manufacturer to verify the resin's source. Whether such a scheme would work for all kinds of electronics materials, which often need to be extremely pure, isn't yet known.

The other downside to all such safeguards is cost. Incorporating anticounterfeiting technology into a high-value IC or a printed-circuit board could add at least 10 percent to the cost—too high a price for most companies, even if it means preventing the counterfeiting. And for components that sell for mere pennies, embedding even a low-cost RFID tag would be prohibitive.

In short, there is no silver bullet when it comes to defeating counterfeiters. What is really needed is a constant multifaceted approach. Governments everywhere need to beef up their IP laws and, more important, enforce them. Industry representatives need to work together to adopt standard practices for monitoring supply chains. And companies need not only to acknowledge the extent of the problem but to take deliberate steps—some of which are bound to be costly—to root out bogus parts from their manufacturing lines. Whenever a company falls down on the job or authorities fail to police the problem, it simply creates an opening for counterfeiters. If the goal is keep bogus products out of consumers' hands, clearly everyone needs to do more.

About the Author

Michael Pecht, an IEEE Fellow, is the founder and director of the Center for Advanced Life Cycle Engineering (CALCE) Electronic Products and Systems Center at the University of Maryland, College Park, and regularly consults with international electronics companies on strategic planning, design, testing, intellectual property, and risk assessment.

Sanjay Tiku, an IEEE member, has an M.S. and a Ph.D. in mechanical engineering from the University of Maryland and currently works for Microsoft Inc., in Redmond, Wash.

To Probe Further

“Managing the Risks of Counterfeiting in the Information Technology Industry,” a white paper by KPMG and the Alliance for Gray Market and Counterfeit Abatement, describes how counterfeit electronics parts have become a global problem. It’s available at http://www.agmaglobal.org/ICEWhitePaper_V5.pdf.

The Web site of Design Chain Associates, a consulting firm in San Francisco, has an informative section on counterfeit electronics, at http://www.designchainassociates.com/counterfeit.html.