Foolproof fingerprints: the counterfeit killers

23 April 2007

Richard Fisher

Do you trust labels? Take a look at the DVD player in your home, for instance. It might be from a famous name, say Sony, NEC or Philips. If so, you probably chose to pay a premium for the promise of a good-quality machine. But what if the player is not all it seems? Perhaps it wasn't manufactured by the company named on its label, but by a counterfeiter exporting fakes from an illegal factory in the Far East.

Most people are familiar with the kind of cheap copies found in, say, east Asian markets, but things have moved on. For example, in 2004 electronics giant NEC heard about some routine-sounding piracy of its computer keyboards and blank CDs in China. Police raided 18 factories and warehouses, but they uncovered more than just a few illegal workshops. The sites were part of a network of seemingly legitimate factories across China, Hong Kong and Taiwan. They were counterfeiting more than 50 NEC electronics products, including home-entertainment centres and MP3, CD and DVD players, and distributing them around the world. The people responsible carried NEC company business cards and licensed out NEC technology in exchange for royalties. They had faked the whole company.

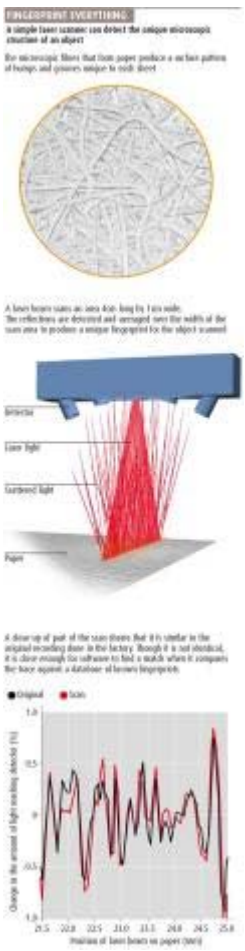
The NEC case shows just how far global counterfeiting has come. "It's not a cottage industry any more, but rather a highly industrialised operation that spans the globe, putting money into the pockets of organised crime," says Peter Lowe, director of the UK's Counterfeiting Intelligence Bureau in London. According to a forthcoming report by the OECD, counterfeit products account for 2.4 per cent of global trade - about $500 billion annually; more than the GDP of Switzerland. And it's not just electronic goods. Everything from condoms and car tyres to medicines and aircraft spares is being faked (see Map).

So what is to be done? Existing methods of detecting counterfeit products are clearly not working, so the hunt is on for new ways to beat the fakers. The solution that most companies favour is radical: log a unique physical fingerprint for every single item that comes off a production line, whether it's a fridge or a packet of cigarettes. The downside for consumers is that everything from a pair of shoes to a packet of biscuits could be traced and linked to its owner. Privacy campaigners are concerned that fingerprinting everything could hand companies and governments a means to track every manufactured item on the planet, and hence us.

The technology could also hand companies an unprecedented degree of control over electronic devices such as DVD and MP3 players. Yet when you realise the lives of consumers are potentially at risk from fake aircraft parts, medicines and electrical safety items, and that the proceeds of counterfeiting fund organised crime, loss of privacy may seem easier to swallow.

Foolproof fingerprints

Today's anti-counterfeiting technology is fundamentally flawed. It is based on the outdated assumption that bona fide manufacturers are better equipped than the fakers. But gone are the days when a product could be protected by simply sticking on a difficult-to-make tag such



Enlarge image
Fingerprint everything

Enlarge image
Faker's world

as a hologram or watermark. Counterfeiters have figured out how to mass-produce such tags, rendering them virtually useless. You need only look at the sophistication of security measures now needed on banknotes - such as the new watermarks recently added to £20 notes in the UK, and plans by the European Central Bank to incorporate radio frequency identification (RFID) tags into high-value euro notes - to see how hard it is to fight the fakers.

Credit card companies suffer particularly badly from counterfeiting, so in the late 1990s Mastercard asked Ravi Pappu at the Massachusetts Institute of Technology to find better ways to prevent its cards being cloned. Pappu realised that the only aspect of a card that is truly irreproducible is its physical structure. What if you could use that to identify an object rather than the digital information stored on it?

In 2002, Pappu published a paper describing how to use light to record the unique physical fingerprint of an object (*Science*, vol 297, p 2026). He suggested that Mastercard create a transparent window in its credit cards in which tiny glass beads would be randomly embedded during manufacture. Shining a laser through the window would create a unique speckled interference pattern that could be used as a fingerprint. In the end, though, Mastercard chose not to adopt the technique, possibly for cost reasons, and the idea fell by the wayside.

Pappu's work nevertheless inspired a fellow MIT researcher, Srini Devadas, who wondered whether the concept of physical fingerprints might work elsewhere. From his work in the electronics industry, Devadas knew that tiny irregularities develop on computer chips when silicon wires are placed on them during manufacture, as a result of minute temperature and pressure variations. He realised that these random differences could be harnessed to check whether a chip was genuine (*New Scientist*, 2 October 2004, p 27). When the chip was made, the manufacturer would measure around 100 different electrical signals - think of them as "questions" - record the values, or "answers", and store them on a protected database. Later, when you wanted to check the chip was genuine, you would interrogate it with one of the questions in your database and see if it answered correctly. Different questions could be asked each time so any eavesdroppers would not be able to copy them, says Devadas.

Now he wants to sell the technology to retailers so they can authenticate RFID tags. These "electronic barcodes" contain a tiny memory circuit and an antenna that allows the contents of the memory to be read remotely. Some retailers, including WalMart, have begun attaching RFID tags to their products to track items through the supply chain without opening every box. The tags' low cost means they could soon be found on everything we buy, down to toothbrushesand chocolate bars (*New Scientist*, 19 October 2002, p 45). The problem with using standard RFID tags for anti-counterfeiting is that a determined pirate can easily duplicate them. Devadas reckons that with just a few extra circuits on tags to include his authentication technology, they could be protected.

Not everyone is convinced Devadas's idea will work, however. One drawback is that it adds to the cost of manufacturing each tag, says Ari Juels, head of research at computer security firm RSA. A basic tag can be produced for less than a cent. Raise production costs too much and companies will lose interest, he says. Juels also has more fundamental doubts. He is sceptical that the imperfections in the silicon wires generate enough random variation to make it a practical technology.

Perhaps the solution, then, is to add more variations at the start. That's what Pim Tuyls, principal scientist at Philips in Eindhoven, the Netherlands, is trying to do. Tuyls sprays a special coating made up of titanium oxide and titanium nitride grains in a matrix of aluminophosphate onto the surface of an electrical circuit or RFID tag. The grains settle randomly, and it is the resulting pattern that gives the device its unique fingerprint. To read it, Tuyls measures the capacitance between aluminium bumps dotted across the layer. A clone of the device would have to have precisely the same properties at a microscopic scale, says Tuyls, which would be close to impossible to achieve.

"The Philips stuff is really cool," says Ross Anderson, a security researcher at the University of Cambridge, though he cautions that it would still be too expensive to use on standard RFID tags. Like

Devadas's technology, it is more suited to high-value electronic goods, smartcard security or protecting chips in mobile phones, he says.

But what if there was a way to measure the unique physical features of a bottle of shampoo or cigarette packet itself, without sticking anything to it? Russell Cowburn, a nanotechnologist at Imperial College London, reckons he can do just that.

Cowburn stumbled on the idea almost by accident. A few years ago his group was trying to find a way to prevent paper documents being faked. Like Pappu, he was looking at how lasers make a unique speckle pattern when they hit an object. His strategy was to shine the laser onto a silicon wafer glued onto a piece of paper and measure the reflection, but he was running into problems. "You couldn't photocopy it without squashing it, for example. Or the glue would fail."

The rough and the smooth

It was poor glue that led to the eventual breakthrough. "One day, during our many failures, the chip fell off," he says. Cowburn noticed that there was still enough laser speckling to measure. At first he thought it was due to ink that happened to be on the paper, but after a few experiments with blank paper he realised it was the paper itself that produced the speckle (*Nature*, vol 436, p 475).

What was happening? On the microscopic scale, paper is made up of tiny fibres in random orientations. As the laser light hits this rough surface, it is reflected back towards the detectors at many different angles (see Diagram). "Looking back, it's not too surprising that you get this effect with paper - it's very rough," says Cowburn. "The real surprise was that it works really well on smooth surfaces like plastic." Plastic has tiny surface crenulations that form randomly as it cools during manufacture. Most materials have an irregular surface, he says. Only glass and mirrored metal won't produce a speckle.

It even works if the surface suffers some damage. You can soak it in water, scorch it or scribble on it with a pen: the unique speckle signature remains readable - and impossible to clone. There's no known way to create two identical signatures, he says. "My day job is making nanostructures, and I don't know how to do it."

Cowburn has now set up a company called Ingenia Technology, and a number of organisations have already adopted his scanners, including Stora Enso, which is one of the world's biggest paper merchants, chemical and pharmaceutical giant Bayer and the International Atomic Energy Agency.

On a mass production line, each product is scanned and its unique laser fingerprint is recorded on a protected database. Each fingerprint takes between 125 and 750 bytes of memory, so a typical 100-gigabyte hard drive could store up to 800 million fingerprints. When you later want to check if a product, say a bottle of shampoo or a banknote, is genuine, you simply scan the fingerprint region again, and the database tells you if you have a match. The scanner measures the average of thousands of points on the surface, so it doesn't need to be held in exactly the same place. Cowburn claims the probability of two naturally occurring matches is 1 in 10^{150}.

Eventually, he wants us to be able to check for ourselves if a product is real, by using a scanner on our PC. This would be linked to the online databases of each manufacturer so we could check whether our shopping was fake the moment we got home. For example, within the past few years fake doses of Pfizer's cholesterol-lowering drug Lipitor somehow appeared on the shelves of pharmacists who thought they had the genuine product. Of course, you'd still need law enforcers to apprehend dealers who sell fakes, but the possibility of identifying fakes would give legitimate retailers a way of checking their wares, would reassure consumers that they were safe, and make it possible for investigators to trace black-market goods.

While these new technologies may be a blow to counterfeiters, there are some downsides for consumers. Seth Schoen of the Electronic Frontier Foundation, an online privacy advocacy group based in San Francisco, says some companies will be equally interested in the ability to monitor in unprecedented detail who has ownership of a particular item. They could use such information to learn about consumer behaviour, for instance.

A company could also use an item's fingerprint to prevent us doing certain things with it, Schoen says. For example, a Californian company called Optikey Security has developed a physical fingerprint technology that could be used to prevent copied CDs or DVDs from working in players fitted with the system. Many discs have digital encryption to protect against piracy but this can be overcome by hackers. Optikey's technology physically stamps a hidden area on an original disc with a microscopic surface pattern, without which it will not play.

The technology will also give companies another means to prevent you using cheaper competitor

products. Many inkjet printer manufacturers already do this by placing chips in their printers and cartridges that prevent you using third-party products. "It is not 'counterfeiting' to make a compatible component, or a generic drug, or similarly styled clothing," Schoen says.

On the positive side, Schoen says that physical fingerprints on RFID tags could actually enhance our privacy. Basic tags broadcast information to anyone, he says. This means eavesdroppers can discover all sorts of information about the objects we own, from marketers knowing the contents of our shopping carts to criminals identifying a Rolex-wearing passer-by to rob. The advantage of using physical fingerprints on an RFID tag is that only the retailer and manufacturer can read them.

Unfortunately, there's another potential flaw: many of these systems rely on a secure database that lists all the legitimate product fingerprints. Hack into it and you can circumvent all the fancy anti-counterfeiting technologies in one fell swoop by inserting the fingerprints of fake products into the database of legitimate ones. "It might be impossible to manufacture two sheets of paper that are exactly the same. But that's not necessarily how counterfeiters work. It might be easier to break into the database," says Ian Brown, an online security researcher at University College London.

Lowe agrees that there is no magic bullet. "Any technology can be beaten," he says. But whatever other advantages companies may gain in introducing these technologies, counterfeit products can be unreliable and even dangerous, so it is in everyone's interests to try to reduce it.

In the case if NEC, there is already evidence of surprising twists to the counterfeiting tale. During its investigation, the company received complaints from customers about products NEC had never seen before. It turned out that the counterfeiters had commissioned their own research and development, and started producing products that NEC itself hadn't thought of. Now what do you call the counterfeiting of products that haven't officially been invented yet?

From issue 2600 of New Scientist magazine, 23 April 2007, page 28-32

Close this window