CHAPTER 12

Security Printing and Seals

A seal is only as good as the man in whose briefcase it's carried.
—KAREN SPÄRCK JONES

12.1 Introduction

Many computer systems rely to some extent on secure printing, packaging, and seals to guarantee important aspects of their protection.

- Many software products get some protection against forgery, using tricks such as holographic stickers that are supposed to tear when removed from the package. They can raise the costs of large-scale forgery; on the individual scale, a careful implementation can help with *trusted distribution*, that is, assuring the user that the product hasn't been tampered with since leaving the factory.
- We discussed how monitoring systems, such as taximeters, often use seals to make it harder for users to tamper with input. No matter how sophisticated the cryptography, a defeat for the seals can be a defeat for the system.
- Many security tokens, such as smartcards, are difficult to make truly tamperproof. It's often feasible for the opponent to dismantle the device and probe out the content. The realistic goal for such a system may be *tamper evidence*, rather than tamper proofness: if someone dismantles their smartcard and gets the keys out, that person should not be able to reassemble it into something that will pass close examination. Security printing can be the key technology here. If a bank smartcard really is tamper-evident, then the bank might tell its customers that disputes will be entertained only if they can produce the card intact. (Banks might not get away with this, though, because consumer protection lawyers will demand that they deal fairly with honest customers who lose their cards or have them stolen).

Quite apart from these direct applications of printing and sealing technology in computer systems, the ease with which modern color scanners and printers can be used to make passable forgeries has opened up another front. Banknote printers are now promoting digital protection techniques [109]. These include invisible copyright marks that enable forgeries to be detected or even set off alarms in image-processing software [357]. The digital world and the world of "funny inks" are growing rapidly closer together.

12.2 History

Seals have a long and interesting history. In the chapter on banking systems, I explained that bookkeeping systems had their origin in the clay tablets, or bullae, used by neolithic warehouse keepers in Mesopotamia as receipts for produce. Over 5000 years ago, the bulla system was adapted to resolve disputes by having the warehouse keeper bake the bulla in a clay envelope with his mark on it.

In classical times and in ancient China, seals were commonly used to authenticate documents. They were used in Europe until a few hundred years ago for letters. Even after signatures had taken over as the principal authentication mechanism, seals lingered on as a secondary mechanism until the nineteenth century. Letters were not placed in envelopes, but folded over several times and sealed using hot wax and a signet ring.

Seals are still the preferred authentication mechanism for important documents in China, Japan, and Korea. Elsewhere, traces of their former importance survive in company seals and notaries' seals, which are affixed to important documents, and the national seals that some countries' heads of state apply to archival copies of legislation.

However, by the middle of the last century, their use with documents had become less important in the West than their use to authenticate packaging. The move from loose goods to packaged goods, and the growing importance of brands, created not just the potential for greater quality control but also the vulnerability that bad people might tamper with products. The United States suffered an epidemic of tampering incidents, particularly of soft drinks and medical products, leading to a peak of 235 reported cases in 1993 [445]. This helped push many manufacturers towards making products tamper-evident.

The ease with which software can be copied, coupled with consumer resistance to technical copy-protection mechanisms from the mid-1980s, drove software companies to rely increasingly on packaging to deter counterfeiters. That was just part of a much larger market in preventing the forgery of high-value, branded goods, ranging from perfume and cigarettes through aircraft spares to pharmaceuticals.

In short, huge amounts of money have been poured into seals and other kinds of secure packaging. Unfortunately, most seals are still fairly easy to defeat.

The typical seal consists of a substrate with security printing, which is then glued or tied around the object being sealed, so we must look first at security printing. If the whole seal can be forged easily, then no amount of glue or string is going to help.

12.3 Security Printing

The introduction of paper money into Europe by Napoleon in the early 1800s, and of other valuable documents such as bearer securities and passports, kicked off a battle between security printers and counterfeiters that exhibits many of the characteristics of a coevolution of predators and prey. Photography (1839) helped the attackers, then color printing and steel etching (1850s) the defenders. In recent years, the color copier and the cheap scanner have been countered by holograms and other optically variable devices. Sometimes, the same people are involved on both sides, as when a government's intelligence services try to forge another government's passports (and in some cases, even its currency, as both sides did in World War II).

On occasion, the banknote designers succumb to the Titanic effect, of believing too much in the latest technology, and place too much faith in some particular trick. An example comes from the forgery of British banknotes in the 1990s. These notes have a *window thread*—a metal strip through the paper about 1 mm wide that comes to the paper surface every 8 mm. When you look at the note in reflected light, it appears to have a dotted metallic line running across it, but when you hold it up and view it through transmitted light, the metal strip is dark and solid. Duplicating this was thought to be hard, but a criminal gang came up with a beautiful hack. They used a cheap hot-stamping process to lay down a metal strip on the surface of the paper, then printed a pattern of solid bars over it using white ink to leave the expected metal pattern visible. At their trial, they were found to have forged tens of millions of pounds' worth of notes over a period of several years [299]. (There may also have been a complacency issue here, as European banks tend to believe that forgers will go for the U.S. notes, which have only three colors.)

12.3.1 Threat Model

As always, we have to evaluate a protection technology in the context of a model of the threats. Broadly speaking, the threat can be from a properly funded organization (such as a government trying to forge another nation's banknotes), from a medium-sized organization (such as a criminal gang forging several million dollars a month, or a distributor forging labels on vintage wines) to amateurs using equipment they have at home or in the office.

In the banknote business, the big growth area in the last years of the twentieth century was in amateur forgery. Knowledge had spread in the printing trade of how to manufacture high-quality forgeries of many banknotes, which one might have thought would increase the level of professional forgery. But the spread of high-quality color scanners and printers has put temptation in the way of many people who would never have dreamed of getting into forgery in the days when it required messy wet inks. In the past, amateurs were thought a minor nuisance, but since about 1997 or 1998, they have accounted for most of the forgeries detected in the United States (it varies from one country to another; most U.K. forgers use traditional litho printing, while in Spain, as in the United States, the inkjet printer has taken over [393]). Amateur forgers are hard to combat as there are many of them; they mostly work on such a small scale that their product takes a long time to come to the attention of authority, and they are less likely to have criminal records. The notes they produce are often not good enough to pass a bank teller, but are uttered in places such as dark and noisy nightclubs.

The industry distinguishes three different levels of inspection that a forged banknote or document may or may not pass [765].

A *primary* or *first-level* inspection is one performed by an untrained, inexperienced person, such as a member of the public or a new cashier at a store. Very often, the primary inspector has no motivation, or even a negative motivation. If he gets a banknote that feels slightly dodgy, he may try to pass it on without looking at it closely enough to have to decide between becoming an accomplice or going to the hassle of reporting it.

A *secondary* or *second-level* inspection is one performed in the field by a competent and motivated person, such as an experienced bank teller in the case of banknotes or a trained manufacturer's inspector in the case of product labels. This person may have some special equipment such as an ultraviolet lamp, a pen with a chemical reagent, or even a scanner and a PC. However, the equipment will be limited in both cost and bulk, and will be completely understood by serious counterfeiters.

A *tertiary* or *third-level* inspection is one performed at the laboratory of the manufacturer or the note-issuing bank. The experts who designed the security printing (and perhaps even the underlying industrial processes) will be on hand, with substantial equipment and support.

The executive summary of the state of the security printing art is that getting a counterfeit past a primary inspection is usually easy, whereas getting it past tertiary inspection is usually impossible if the product and the inspection process have been competently designed. Thus, secondary inspection is the battleground (except in a few applications such as banknote printing, where attention is now being paid to the primary level); and the main limits on what sort of counterfeits can be detected by the inspector in the field have to do with the bulk and the cost of the equipment needed.

12.3.2 Security Printing Techniques

Traditional security documents utilize a number of printing processes, including:

- *Intaglio*, a process where an engraved pattern is used to press the ink on to the paper with great force, leaving a raised ink impression with high definition. This is often used for scroll work on banknotes and passports.
- *Letterpress* in which the ink is rolled on raised type which is then pressed on to the page, leaving a depression. The numbers on banknotes are usually printed this way, often with numbers of different sizes and using different inks to prevent off-the-shelf numbering equipment being used.
- Special printing presses, called *Simultan presses*, which transfer all the inks, for both front and back, to the paper simultaneously. This means that the printing on front and back can be accurately aligned; patterns can be printed partly on the front and partly on the back so that they match up perfectly when the note is held up to the light (*see-through register*). Reproducing this is believed too hard for cheap color printing equipment. The Simultan presses also have special ducting to make ink colors vary along the line (*rainbowing*).

- Rubber stamps which are used to endorse documents, or to seal photographs to them.
- Embossing and laminates which are also used to seal photographs, and on bank cards to push up the cost of forgery. Embossing can be physical, or require laser engraving techniques to burn a photo into an ID card.
- *Watermarks* which are an example of putting protection features in the paper. They are more translucent areas inserted into the paper by varying its thickness when it is manufactured. There are many other special properties in use, such as fluorescent threads. An extreme example is the Australian $10 note, which is printed on plastic and has a see-through window.

More modern techniques include:

- Optically variable inks, such as the patches on Canadian $20 bills that change color from green to gold depending on the viewing angle.
- Inks with magnetic or photoacoustic properties.
- Printing features visible only with special equipment, such as the microprinting on U.S. bills, which requires a magnifying glass to see, and printing in ultraviolet, infrared, or magnetic inks (the last of these being used in the black printing on U.S. bills).
- Metal threads and foils, from simple iridescent features to foil color copying to foils with optically variable effects such as *holograms* and *kinegrams*, as found on British £20 and £50 notes. Holograms are typically produced optically, and look like a solid object behind the film, while kinegrams are produced by computer and may show a number of startlingly different views from slightly different angles.
- *Screen traps* such as details too faint to scan properly, and *alias band structures* which contain detail at the correct size to form interference effects with the dot separation of common scanners and copiers.
- *Digital copyright marks* which may vary from images hidden by microprinting their Fourier transforms directly, to spread spectrum signals that will be recognized by a color copier, scanner, or printer, and cause it to stop.
- Unique stock, such as paper that has had magnetic fibers randomly spread through it during manufacture so that each sheet has a characteristic pattern that can be digitally signed and printed on the document using some kind of barcode.

For the design of the new U.S. $100 bill, see [566]; and for a study of counterfeit banknotes, with an analysis of which features provide what evidence, see [766]. In general, banknotes' genuineness cannot readily be confirmed by the inspection of a single security feature. Many of the older techniques, and some of the newer, can be mimicked in ways that will pass primary inspection. The tactile effects of intaglio and letterpress printing wear off, so crumpling and dirtying the forged note is standard practice, and skilled banknote forgers mimic watermarks with faint gray printing (though watermarks remain surprisingly effective against amateurs). Holograms and kinegrams can be vulnerable to people using electrochemical techniques to make mechanical copies; or villains may originate their own master copies from scratch.

When a hologram of Shakespeare was introduced on U.K. check guarantee cards in 1988, I visited the factory as the representative of a bank and was told proudly that, as the industry had demanded a second source of supply, they had given a spare set of plates to a large security printing firm—and this competitor of theirs had been quite unable to manufacture acceptable foils. (The Shakespeare foil was the first commercially used diffraction hologram to be in full color and to move as the viewing angle changed). Surely a device that couldn't be forged, even by a major security printing company with access to genuine printing plates, must give total protection? But when I visited Singapore seven years later, I bought a similar (but larger) hologram of Shakespeare in the flea market. This was clearly a boast by the maker that he could forge U.K. bank cards if he wished to. By then, a police expert estimated that there were more than 100 forgers in China with the skill to produce passable holograms [591].

The technology constantly moves on; and the kind of progress that aids the villain can come from such unexpected directions that technology controls have little effect. For example, ion beam workstations—machines that can be used to create the masters for kinegrams—cost many millions of dollars in the mid-1990s, but have turned out to be so useful in metallurgical lab work that sales have shot up, prices have plummeted, and there are now many bureaus that rent out machine time for a few hundred dollars an hour. So it is imprudent to rely on a single protection technology. Even if one defense is completely defeated (such as if it becomes easy to make mechanical copies of metal foils), you have at least one completely different trick to fall back on (such as optically variable ink).

But designing a security document is much harder than this. There are complex trade-offs between protection, aesthetics and robustness, and it is coming to be realized that, for many years, designers had their focus on preventing forgeries passing secondary or tertiary inspection (the technological focus), rather than on the more common primary inspection (the business focus). Much time was spent handwringing about the difficulty of training people to examine documents properly, while not enough attention was paid to studying how the typical user of a product such as a banknote actually decides subconsciously whether it's acceptable. This defect is now receiving serious attention.

The lessons drawn so far are [765]:

- Security features should convey a message relevant to the product. So it's better to use iridescent ink to print the denomination of a banknote than some obscure feature of it.
- They should obviously belong where they are, so that they become embedded in the user's cognitive model of the object.
- Their effects should be obvious, distinct and intelligible.
- They should not have existing competitors that can provide a basis for imitations.
- They should be standardized.

This work deserves much wider attention, as the banknote community is one of the few subdisciplines of the trade to have devoted a lot of thought to security usability. (We'll see later in Chapter 23 that one of the main failings of current evaluation schemes for security products is that usability gets ignored.) When it comes to documents other than banknotes, such as passports, there are also issues relating to political environment of the country and the mores of the society in which they will be used [546].

Usability also matters during second-line inspection, but here the issues are more subtle, focusing on the process that the inspector has to follow to distinguish genuine from fake.

With banknotes, the theory is that you design a note with perhaps 20 features that are not advertised to the public. A number of features are made known to secondary inspectors such as bank staff. In due course, these become known to the forgers. As time goes on, more and more features are revealed. Eventually, when they are all exposed, the note is withdrawn from circulation and replaced. This may become harder as the emphasis switches from manual to automatic verification. A thief who steals a vending machine, dismantles it, and reads out the software, gains a complete description of the checks currently in use. Having once spent several weeks or months doing this, he will find it much easier the second time around. So when the central bank tells manufacturers the secret polynomial for the second-level digital watermark (or whatever), and this gets fielded, he can steal another machine and get the new data within days. So failures can be more sudden and complete than with manual systems, and the cycle of discovery could turn more quickly than in the past.

With product packaging, the typical business model is that samples of forgeries are found and taken to the laboratory, where the scientists find some way in which they are different—such as because the hologram is not quite right. Kits are then produced for field inspectors to go out and track down the source. If these kits are bulky and expensive, fewer of them can be fielded. If there are many different forgery detection devices from different companies, then it is hard to persuade customs officers to use any of them. Ideas such as printing individual microscopic ultraviolet barcodes on plastic product shrinkwrap often fail because of the cost of the microscope, laptop, and online connection needed to do the verification. As with banknotes, you can get a much more robust system with multiple features, but this pushes the cost and bulk of the reading device up still further. There is now a substantial research effort aimed at developing unique marks, such as special chemical coatings containing proteins or even DNA molecules, which encode hidden serial numbers and which might enable one type of verification equipment to check many different products.

With financial instruments, and especially checks, alteration is a much bigger problem than copying or forgery from scratch. In numerous scams, villains got genuine checks from businesses by tricks such as by prepaying deposits or making reservations in cash, then cancelling the order. The victim duly sends out a check, which is altered to a much larger amount, often using readily available domestic solvents. The standard counter-measure is background printing using inks that discolor and run in the presence of solvents. But the protection isn't complete because of tricks for removing laser printer toner (and even simple things like typewriter correction ribbon). One enterprising villain even presented his victims with pens that had been specially selected to have easily removable ink [5].

While the security literature says a lot about debit card fraud (as the encryption systems that ATMs use are interesting to techies), and a little about credit card fraud (as there's a lot of talk about credit card fraud on the Net), very little has been written about check fraud. Yet check fraud is many times greater in value than credit card fraud, and debit cards are almost insignificant by comparison with either. Although check fraud is critically important, the research community considers it to be boring.

The practical problem for the banks is the huge volume of checks processed daily. This makes scrutiny impossible except for very large amounts—and the sums stolen by small-time check fiddlers may be low by the standards of the victim organization (say, in the thousands to tens of thousands of dollars). In the Far East, where people use a personal *chop* or signature stamp to sign checks instead of a manuscript signature, low-cost automatic checking is possible [395]. However, with handwritten signatures, automated verification with acceptable error rates is still beyond the state of the art; I'll discuss this in Section 13.2. In some countries, such as Germany, check frauds have been largely suppressed by businesses making most payments using bank transfers rather than checks (even for small customer refunds). Making such a change involves overcoming huge cultural inertia, but perhaps the lower costs of online payments (cents rather than tens of cents) will persuade business in most countries to make the switch eventually.

Alterations are also a big problem for the typical bank's credit card department. It is much simpler to alter the magnetic strip on a card than to re-originate the hologram. In fact, during the early 1980s, the system was to verify a card's magnetic strip data using an online terminal, then collect the actual transaction using a zip-zap machine. The effect was that the authorization was done against the card number on the strip, while the transaction was booked against the card number on the embossing. So villains would take stolen cards and reencode them with the account details of cardholders with high credit limits—captured, for example, from waste carbons in the bins outside fancy restaurants—and use these to authorize transactions which would then be billed to the stolen card's account. The bank would then repudiate the transaction, as the authorization code didn't match the recorded account number. So banks started fighting with their corporate customers over liability, and the system was changed so that drafts were captured electronically from the magnetic strip.

Of course, alterations aren't just a banking problem. Most fake travel documents are altered rather than counterfeited from scratch: names are changed, photographs are replaced, or pages are added and removed.

Finally, one promising technology is the use of optically readable digital signatures instead of traditional serial numbers. These can bind printed matter either to the underlying substrate or to information about enclosed materials. When I introduced digital signatures in Section 5.3.5, I mentioned that the United States and some other countries were introducing a new postal meter system that prints out stamps, known as *indicia*, with contain 2-D barcodes. These contain the amount of postage, the sender, and recipient post codes, the serial number of the postal meter, and the date. Although, in theory, a stamp could be pulled off one envelope and put on another—or just photocopied—this arrangement is enough to stop the kind of frauds of greatest concern to the U.S. Postal Service, which involve junk mailers bribing postal employees to introduce large sacks of mail into the system [753]. A sample of the indicia being introduced is reproduced in Figure 12.1.

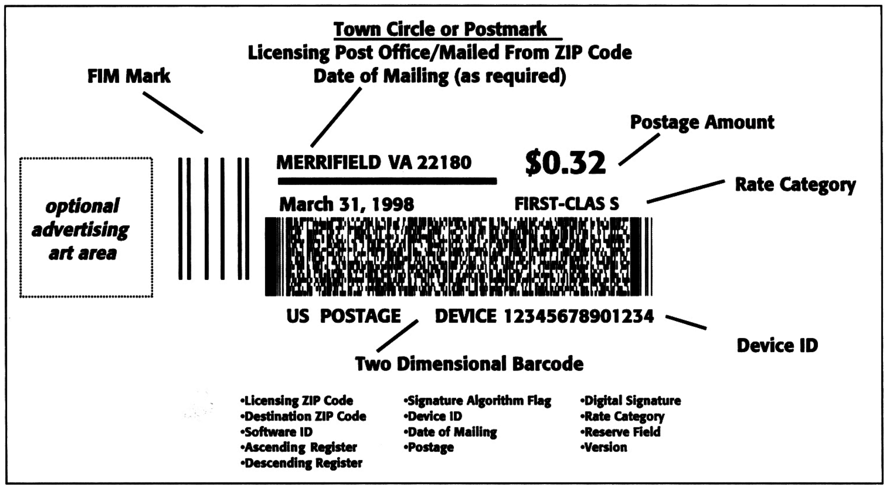

Figure 12.1 The new format for U.S. postal meters (courtesy of Symbol Technologies).

12.4 Packaging and Seals

This brings us to the added problems of packaging and seals.

Not all seals work by gluing a substrate with security printing to the object being sealed. I mentioned the wire and lead seals used to prevent tampering with truck speed sensors, and there are many products following the same general philosophy but using different materials, such as plastic straps, which are supposed to be easy to tighten but hard to loosen without cutting. I also mentioned the special chemical coatings, microscopic barcodes, and other tricks used to make products or product batches traceable. However, most of the seals in use work by applying some kind of security printing to a substrate, then gluing this to the material to be protected.

12.4.1 Substrate Properties

Some systems add random variability to the substrate material. Recall the trick of loading paper with magnetic fibers; there are also *watermark magnetics*, in which a random high-coercivity signal is embedded in a card strip that can subsequently be read and written using standard low-coercivity equipment without the unique random pattern being disturbed. Watermark magnetics are used in bank cards in Sweden, in telephone cards in Korea, and in entry control cards in some of the buildings in my university.

A similar idea is used in arms control. Many materials have surfaces that are unique, or that can be made so by eroding them with a small explosive charge. This makes it easy to identify capital equipment such as heavy artillery, where identifying each gun barrel is enough to prevent either side from cheating. The surface pattern of the gun barrel is measured using laser speckle techniques, and either recorded in a log or attached to the device as a machine-readable digital signature [703].

Similar techniques are being developed for postal systems. An alignment grid is printed on an envelope, and a small microscope is used to observe the paper fibers there. A paper fibre pattern is extracted and recorded in the postal franking mark, which is digitally signed. This has the potential to enable sheets of ordinary paper to become recognizably unique, like the special fiber-loaded papers just mentioned, only much more cheaply.

12.4.2 The Problems of Glue

However, many seals do work by gluing security-printed matter on to the target object. This raises the question of how the beautiful piece of iridescent printed art can be attached to a crude physical object in a way that is difficult to remove. The usual answer is to use a glue that is stronger than the seal substrate itself, so that the seal will tear or at least deform noticeably if pulled away.

However, in most products, the implementation is rather poor. Many seals are vulnerable to direct removal using only hand tools and a little patience. You can experiment with this by taking a sharp knife to the next few letters that arrive in self-seal envelopes. Many of these envelopes are supposed to tear, rather than peel open; the flap may have a few vertical slots cut into it for this purpose. But this hoped-for tamper evidence usually assumes that people will open them by pulling the envelope flap back carelessly from the body. By raising the flap slightly and working the knife back and forth, it is often possible to cut the glue without damaging the flap, and thus open the envelope without leaving suspicious marks. (Some glues should be softened first using a hairdryer, or made more fragile by freezing.) The result may be an envelope that looks slightly crumpled on careful examination, but crumples can be ironed out. This attack usually works against a primary inspection, probably fails a tertiary inspection, and may well pass secondary inspection: crumples happen in the post anyway.

Many of the seals on the market can be defeated using similarly simple techniques. For example, there is a colored adhesive tape that, when ripped off, leaves behind a warning such as “Danger” or “Do not use.” The colored layer is sandwiched between two layers of glue, and the bottom of these is stronger where the color is supposed to remain behind if the seal is tampered with. But the tape behaves in this way only if it is pulled from above. By cutting from the side, one can remove it intact and reuse it [479].

12.5 Systemic Vulnerabilities

We turn now from the specific threats against particular printing tricks, glues, and markets to the system-level threats, of which there are many.

A possibly useful example is in Figure 12.2. At our local swimming pool, congestion is managed by issuing swimmers with wristbands during busy periods. A different color is issued every twenty minutes or so, and from time to time all people with bands of a certain color are asked to leave. The band is made of waxed paper. At the end it has a printed pattern and serial number on one side and glue on the other; the paper is crosscut with the result that it is destroyed if you tear it off carelessly. (It’s very similar to the luggage seals used at some airports.)

The simplest attack is to phone up the supplier; boxes of 100 wristbands cost about $8. If you don't want to spend money, you can use each band once, then ease it off gently by pulling it alternately from different directions, giving the result shown in the photo. The printing is crumpled, though intact; the damage isn't such as to be visible by a poolside attendant, and could have been caused by careless application. The point is that the damage done to the seal by fixing it twice, carefully, is not easily distinguishable from the effects of a naive user fixing it once. (An even more powerful attack is to not remove the backing tape from the seal at all, but use some other means—a safety pin, or your own glue—to fix it.)

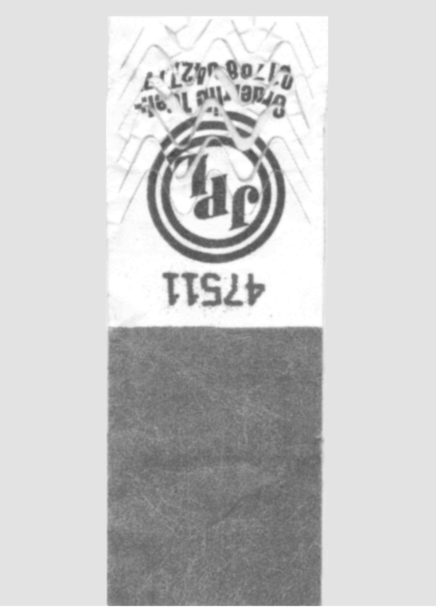

Figure 12.2 A wristband seal from our local swimming pool.

Despite this, the wristband seal is perfectly fit for purpose. There is little incentive to cheat: people in such intensive training that they swim for two hours at a stretch use the pool when it's not congested. They also buy a season ticket, so they can go out at any time to get a band of the current color. But it illustrates many of the things that can go wrong. The customer is the enemy; it's the customer who applies the seal; the effects of seal re-use are indistinguishable from those of random failure; unused seals can be bought in the marketplace; counterfeit seals could also be manufactured at little cost; and effective inspection is infeasible. (And yet this swimming pool seal is still harder to defeat than many sealing products sold for high-value industrial applications.)

12.5.1 Peculiarities of the Threat Model

We've seen systems where your customer is your enemy, as in banking. In military systems, the enemy could be a single disloyal soldier, or the other side's special forces trying to sabotage your equipment. In nuclear monitoring systems it can be the host government trying to divert fissile materials from a licensed civilian reactor.

But some of the most difficult sealing tasks arise in commerce. Their difficulty arises from the fact that it is the enemy who will apply the seal. A typical application is where a company subcontracts the manufacture of some of its products, and is afraid that the contractor will produce more of the goods than agreed. Overproduction is the main source by value of counterfeit goods worldwide; the perpetrators have access to the authorized manufacturing process and raw materials, and gray markets provide natural distribution channels. Even detecting such frauds—let alone proving them in court—can be hard.

A typical solution for high-value goods, such as cosmetics, may involve buying packaging materials from a number of different companies, whose identities are kept secret from the firm operating the final assembly plant. Some of these materials may have serial numbers embedded in various ways (such as by laser engraving in bottle glass or by printing on cellophane using inks visible only under UV light). There may be an online service whereby the manufacturer's field agents can verify the serial numbers of samples purchased randomly in shops; or there might be a digital signature on the packaging that links all the various serial numbers together for offline checking.

There are limits on what seals can achieve in isolation. Sometimes the brand owner himself is the villain, as when a vineyard falsely labels as vintage an extra thousand cases of wine that were actually made from bought-in blended grapes. So bottles of South African wine all carry a government-regulated seal with a unique serial number; here, the seal doesn't prove the fraud, but makes it harder for a dishonest vintner to evade the other controls such as inspection and audit. So sealing mechanisms usually must be designed with the audit, testing, and inspection process in mind.

Inspection can be trickier than one would think. The distributor who has bought counterfeit goods on the gray market, believing them to be genuine, may set out to deceive the inspectors without any criminal intent. Where gray markets are an issue, inspectors should expect to see only authorized products in distributors' stockrooms, while products bought from "Fred" will be pushed out rapidly to the customers. Also, the distributor may be completely in the dark; it could be his staff who are peddling the counterfeits. In a recent high-profile case, staff at a major airline bought counterfeit perfumes, watches, and the like in the Far East, sold them in-flight to customers, and trousered the proceeds. The stocks in the airline's warehouses (and in the duty-free carts after the planes had landed) were all completely genuine. So it is usually essential to have agents go out and make sample purchases, and the sealing mechanisms must support this.

12.5.2 Staff Diligence

Whether the seal adheres properly to the object being sealed may also depend on the honesty of low-level staff. I mentioned in Section 10.4.1.2 how in truck speed limiter systems, the gearbox sensor is secured in place using a piece of wire on which the calibrating garage crimps a lead disc in place with sealing tongs. The defeat is to bribe the garage mechanic to wrap the wire the wrong way, so that when the sensor is unscrewed the wire will loosen, instead of tightening and breaking the seal. There is absolutely no need to go to amateur sculptor classes to learn to take a cast of the seal and forge a pair of sealing tongs out of bronze (unless you want to save on bribes, or to frame the garage).

The people who apply seals may be careless as well as corrupt. In the last few years, some airports have taken to applying tape seals to passengers' checked bags after X-raying them using a machine near check-in queue. On about half of the occasions this has been done to my baggage, the tape has been poorly fixed: it didn't cross the fastener between the suitcase and the lid, or it came off at one end, or the case had several compartments big enough to hold a bomb but only one of their fasteners was sealed. Carelessness and corruption interact. If enough of the staff applying a seal are careless, then if I bribe one of them the defect doesn't of itself prove dishonesty.

12.5.3 The Effect of Random Failure

There are similar effects when seals break for completely innocent reasons. For example, speed limiter seals often break when a truck engine is steam-cleaned, so a driver will not be prosecuted for tampering if a broken seal is all the evidence the traffic policeman can find. (Truck drivers know this.)

There are other consequences, too. For example, after opening a too-well-sealed envelope, a villain can close it again with a sticker saying 'Opened by customs' or 'Burst in transit—sealed by the Post Office'. He could even just tape it shut and scrawl 'delivered to wrong address try again' on the front.

The consequences of such failures and attacks have to be thought through carefully. If the goal is to prevent large-scale forgery of a product, occasional breakages may not matter, but if it is to support prosecutions, spontaneous seal failure can be a serious problem. In extreme cases, placing too much trust in the robustness of a seal might lead to a miscarriage of justice, and completely undermine the sealing product's evidential (and thus commercial) value.

12.5.4 Materials Control

Another common vulnerability is that supplies of sealing materials are uncontrolled. Corporate seals are a nice example. In Britain, these typically consist of two metal embossing plates that are inserted into special pliers. There are several suppliers who manufacture the plates, and a lawyer who has ordered hundreds of them tells me that no check was ever made. Although it might be slightly risky to order a seal for "Microsoft Corporation," it should be easy to have a seal made for almost any less-well-known target—just write a letter that looks like it came from a law firm.

Or consider the plastic envelopes used by some courier companies, which are designed to stretch and tear when opened. This is a promising technology, but as long as the company's regular customers have supplies of envelopes lying around (and they can also be obtained at the depot) it may not deter an attacker from tampering with a package either before, or after, its trip through the courier's network.

It has for some time been an "urban myth" that the police and security services cannot open envelopes tracelessly if the flaps have been reinforced with sticky tape that has been burnished down by rubbing it with a thumbnail (I recently received some paperwork from a bank that had been sealed in just this way). This is not entirely believable [814] —even if no police lab has invented a magic solvent for sellotape glue, the nineteenth century Tsarist police already used forked sticks to wind up letters inside a sealed envelope so that they could be pulled out, read, and then put back [428].

Even if sellotape were guaranteed to leave a visible mark on an envelope, one would have to assume that the police's envelope-steaming department has no stock of comparable envelopes, and that the recipient would be observant enough to spot a forged envelope. Given the ease with which an envelope with a company logo can be scanned and then duplicated using desktop publishing equipment, these assumptions are fairly ambitious. In any case, the arrival of high-quality desktop color printers has caused a lot of organizations to stop using preprinted stationery for all their letters. This makes the forger's job much easier.

12.5.5 Not Protecting the Right Things

I mentioned how credit cards were vulnerable in the late 1980s: the authorization terminals read the magnetic strip, while the payment draft capture equipment used the embossing; Crooks who changed the mag strip but not the embossing defeated the system.

There are also attacks involving partial alterations. For example, as the hologram on a credit card covers only the last four digits, the attacker could always change the other twelve. When the algorithm the bank used to generate credit card numbers was known, this involved only flattening, reprinting, and re-embossing the rest of the card, which could be done with cheap equipment.

Such attacks are now rare, because villains now realize that very few shop staff check that the account number printed on the slip is the same as that embossed on the card. So the account number on the strip need bear no resemblance at all to the numbers embossed on the face. In effect, all the hologram says is, "This was once a valid card."

Finally, food and drug producers often protect products against tampering by using shrinkwrap or blister packaging, which (if well designed) can be moderately difficult to forge well enough to withstand close inspection. However when selecting protective measures one has to be very clear about the threat model—is it counterfeiting, alteration, duplication, simulation, diversion, dilution, substitution, or something else [615]? If the threat model is a psychotic with a syringe full of poison, then simple blister or shrink-wrap packaging is not quite enough. What's really needed is a tamper-sensing membrane, which will react visibly and irreversibly to even a tiny penetration. (Such membranes exist but are still too expensive for consumer products. I'll discuss one of them in the chapter on tamper resistance.)

12.5.6 The Cost and Nature of Inspection

There are many stories in the industry of villains replacing the hologram on a bank card with something else—say a rabbit instead of a dove—whereupon the response of shopkeepers is just to say: "Oh, look, they changed the hologram!" This isn't a criticism of holograms; the issue is much deeper, involving applied psychology and public education. Bankers worry when new notes are being introduced—the few weeks before everyone is familiar with the new notes can be a bonanza for forgers. (This is one of the big worries with the planned introduction of the new Euro currency notes.)

A related problem is the huge variety of passports, driver's licenses, letterheads, corporate seals, and variations in packaging. Without samples of genuine articles for comparison, inspection is more or less limited to the primary level, so forgery is easy. Even though bank clerks have books with pictures of foreign banknotes, and immigration officers similarly have pictures of foreign passports, there is often only a small amount of information on security features; and in any case the absence of real physical samples means that the tactile aspects of the product go unexamined.

As already mentioned, the limiting factor with many technologies is the cost of second-line inspection in the field. If detecting a forged bottle of perfume requires equipment costing $5,000 (e.g., a laptop with a scanner, a UV lamp, and a special microscope), then this may be viable for an exclusive perfume sold only through a few upmarket stores, but is less likely to be viable for medium-value products and is very unlikely to be distributed to all customs posts and market inspectors worldwide.

The ideal remains a seal that can be checked by the public or by staff with minimal training. Firms that take forgery seriously, such as large software companies, are starting to adopt many of the techniques pioneered by banknote printers. But high-value product packages are harder to protect than banknotes. Familiarity is important: people get a "feel" for things they handle frequently, such as local money, but are much less likely to notice something wrong with a package they see only rarely, such as a car part or a medicine bottle. Humans are very vulnerable when they see something for the first or only time—such as the packaging on the latest version of a computer operating system.

12.6 Evaluation Methodology

This section offers a systematic way to evaluate a seal product for a given application. Rather than just asking, "Can you remove the seal in ways other than the obvious one?" we need to follow it from design and field test through manufacture, application, use, checking, destruction, and finally retirement from service. Here are some of the questions that should be asked:

- Has anybody who really knows what they're doing tried hard to defeat the system? And what's a defeat anyway—tampering, forgery, alteration, destruction of evidential value, or a "PR" attack on your commercial credibility?
- What is the reputation of the team that designed it—did they have a history of successfully defeating opponents' products?
- How long has the system been in the field, and how likely is it that technological progress will make a defeat significantly easier?
- How widely available are the sealing materials—who else can buy, forge, or steal supplies?
- Will the person who applies the seal be careless or corrupt?

- Does the way the seal will be used protect the right part (or enough) of the product?
- What are the quality issues? What about the effects of dirt, noise, vibration, cleaning, and manufacturing defects? Will the product have to survive weather, fuel splashes, being carried next to the skin, or being dropped in a glass of beer? Is it supposed to respond visibly if such a thing happens? How often will there be random seal failures, and what effect will they have?
- If a seal is forged, who's supposed to spot this? If it's the public, then how often will they see genuine seals? Has the vendor done experiments, that pass muster by the standards of applied psychology, to establish the likely false accept and false reject rates? If it's your inspectors in the field, how much will their equipment and training cost?
- Are there any evidential issues? If you're going to end up in court, are there experts other than your own (or the vendor's) on whom the other side can rely? If the answer is no, then is this a good thing or a bad thing? Why should the jury believe you, the system's inventor, rather than the sweet little old lady in the dock? Will the judge let her off on fair trial grounds—because rebutting your technical claims would be an impossible burden of proof for her to discharge? (This is exactly what happened in *Judd vs. Citibank*, the case that settled U.S. law on phantom withdrawals from cash machines [427].)
- Once the product is used, how will the seals be disposed of? Are you worried that someone might recover a few old seals from the trash?

When considering whether the people who apply and check the seals will perform their tasks faithfully and effectively, it is important to analyze motive, opportunity, skills, audit, and accountability. Be particularly cautious where the seal is applied by the enemy (as in the case of contract manufacture) or by someone open to corruption (such as the garage mechanic eager to win the truck company's business). Finally, think through the likely consequences of seal failure and inspection error rates, not just from the point of view of the client company and its opponents, but also from the points of view of innocent system users and of legal evidence.

Of course, this whole-lifecycle assurance process should also be applied to computer systems in general. I'll talk about that some more in Part 3.

12.7 Summary

Most commercially available sealing products are relatively easy to defeat, particularly where seal inspection is performed casually by untrained personnel. Sealing has to be evaluated over the lifetime of the product, from manufacture through materials control, application, verification, and eventual destruction; hostile testing is highly advisable in critical applications. Seals often depend on security printing, about which broadly similar comments may be made.

Research Problems

A lot of money is currently being spent on research and product development in this area. The problem appears to be that much of it isn't being spent effectively, or that third-rate products continue to dominate the market because of low cost and user ignorance. An important contribution could be a better evaluation methodology for seals, and for security printing in general. More results on how specific techniques and products can be defeated might also be useful in undermining suppliers' complacency.

Further Reading

The definitive textbook on security printing is van Renesse [765], which goes into not just the technical tricks, such as holograms and kinegrams, but how they work in a variety of applications from banknote printing through passports to packaging. This is very important background reading.

I don't know of a definitive textbook on seals. Most products are proprietary, and depend for their success on criminals' ignorance—which is one of the shakiest foundations I know of. One of the most systematic efforts to overcome this ignorance can be found in a series of publications by the seal vulnerability assessment team at Los Alamos National Laboratory (e.g., [422]).