CHAPTER

14

Security Printing and Seals

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

— Karen Spärck Jones

You can't make something secure if you don't know how to break it.

— Marc Weber Tobias

14.1 Introduction

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

- Most security products can be defeated if a bad man can get at them — whether to patch them, damage them, or substitute them — before you install them. Seals, and tamper-evident packaging generally, can help with *trusted distribution*, that is, assuring the user that the product hasn't been tampered with since leaving the factory.
- Many software products get some protection against forgery using seals and packaging. They can at least raise the costs of large-scale forgery somewhat.
- We saw how monitoring systems, such as taxi meters, 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.
- I also discussed how contactless systems such as those used in the chips in passports and identity cards can be vulnerable to man-in-the-middle

attacks. If you're scrutinising the ID of an engineer from one of your suppliers before you let him into your hosting centre, it can be a good idea to eyeball the ID as well as reading it electronically. If all you do is the latter, he might be relaying the transaction to somewhere else. So even with electronic ID cards, the security printing can still matter.

- Many security tokens, such as smartcards, are difficult to make truly tamper proof. It may be feasible for the opponent to dismantle the device and probe out the content. A more realistic goal may be *tamper evidence* rather than tamper proofness: if someone dismantles their smartcard and gets the keys out, they should not be able to reassemble it into something that will pass close examination. Security printing can help here. If a bank smartcard really is tamper-evident, then the bank might tell its customers that disputes will only be entertained 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, 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 [178]. These include invisible copyright marks that can enable forgeries to be detected, can help vending machines recognise genuine currency, and set off alarms in image processing software if you try to scan or copy them [562]. Meanwhile, vendors of color copiers and printers embed forensic tracking codes in printout that contain the machine serial number, date and time [425]. So the digital world and the world of 'funny inks' are growing rapidly closer together.

14.2 History

Seals have a long and interesting history. In the chapter on banking systems, I discussed how 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.

Seals were commonly used to authenticate documents in classical times and in ancient China. They were used in medieval Europe as a means of social control before paper came along; a carter would be given a lead seal at one tollbooth and hand it in at the next, while pilgrims would get lead tokens from shrines to prove that they had gone on pilgrimage (indeed,

the young Gutenberg got his first break in business by inventing a way of embedding slivers of mirror in lead seals to prevent forgery and protect church revenues) [559]. Even after handwritten signatures had taken over as the principal authentication mechanism for letters, they 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 the company seals and notaries' seals 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 USA suffered an epidemic of tampering incidents, particularly of soft drinks and medical products, leading to a peak of 235 reported cases in 1993 [699]. This helped push many manufacturers towards making products tamper-evident.

The ease with which software can be copied, and consumer resistance to technical copy-protection mechanisms from the mid 1980s, led 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 poured into seals and other kinds of secure packaging. Unfortunately, most seals are still fairly easy to defeat.

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

14.3 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 were involved on both sides, as when a government's intelligence services try to forge another government's passports — or even its currency, as both sides did in World War Two.

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 that is about 1 mm wide and comes to the paper surface every 8 mm. So 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. Yet 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, and then printed a pattern of solid bars over it using white ink to leave the expected metal pattern visible. They were found at their trial to have forged tens of millions of pounds' worth of notes over a period of several years [477]. (There was also a complacency issue; European bankers believe that forgers would go for the US dollar as it only had three colors at the time.)

14.3.1 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 (whether 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 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. Amateurs used to be thought a minor nuisance, but since about 1997 or 1998 they have accounted for most of the forgeries detected in the USA (it varies from one country to another; most UK forgers use traditional litho printing while in Spain, like the USA, the inkjet printer has taken over [628]). 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 which a forged banknote or document may or may not pass [1279]:

1. a *primary* inspection is one performed by an untrained inexperienced person, such as a member of the public or a new cashier at a store. 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;
2. a *secondary* 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;
3. a *tertiary* 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 state of the security printing art can be summarised as follows. Getting a counterfeit past a primary inspection is usually easy, while getting it past tertiary inspection is usually impossible if the product and the inspection process have been competently designed. So secondary inspection is the battleground — except in a few applications such as banknote printing where attention is now being paid to the primary level. (There, the incentives are wrong, in that if I look closely at a banknote and find it's a forgery I'm legally bound to hand it in and lose the value.) The main limits on what sort of counterfeits can be detected by the secondary inspector in the field have to do with the bulk and the cost of the equipment needed.

14.3.2 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 that 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. The printing on front and back can therefore 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 to be hard on cheap color printing equipment. The Simultan presses also have the special ducting to make ink colors vary along the line (*rainbowing*);
- rubber stamps that are used to endorse documents, or to seal photographs to them;
- embossing and laminates that are also used to seal photographs, and on bank cards to push up the cost of forgery. Embossing can be physical, or use laser engraving techniques to burn a photo into an ID card;
- *watermarks* 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. Many other special materials, such as fluorescent threads, are used for similar purposes. 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, photochromic or thermochromic properties;
- printing features visible only with special equipment, such as the micro-printing on US 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 US bills);
- metal threads and foils, from simple iridescent features to foil color copying through to foils with optically variable effects such as *holograms* and *kinegrams*, as found on the latest issue of British banknotes. 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 with 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 a barcode.

For the design of the new US $100 bill, see [921]; and for a study of counterfeit banknotes, with an analysis of which features provide what evidence, see [1280]. 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 a forged note is standard practice, and skilled banknote forgers mimic watermarks with faint grey printing (though watermarks remain surprisingly effective against amateurs). Holograms and kinegrams can be vulnerable to people using electrochemical techniques to make mechanical copies, and if not then villains may originate their own master copies from scratch.

When a hologram of Shakespeare was introduced on UK bank 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 which 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 UK bank cards if he wished to. By then, a police expert estimated that there were over 100 forgers in China with the skill to produce passable forgeries [969].

So the technology constantly moves on, and inventions that aid the villains come from such unexpected directions that technology controls are of little use. For example, ion beam workstations — machines which can be used to create the masters for kinegrams — used to cost many millions of dollars in

the mid-1990's 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 which rent out machine time for a few hundred dollars an hour. Scanning electron microscopes, which are even more widely available, can be used with home-made add-ons to create new kinegrams using electron beam lithography. 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 the business focus can also change. For many years, banknote designers aimed at preventing forgeries passing secondary or tertiary inspection rather than on the more common primary inspection. Much time was spent handwringing about the difficulty of training people to examine documents properly, and 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. In other words, the technological focus had usurped the business focus. This defect is now receiving serious attention.

The lessons drawn so far are [1279]:

- 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 our trade to have devoted a lot of thought to security usability. (We've seen over and over again that one of the main failings of security products is that usability gets ignored.) When it comes for 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 [874].

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

With banknotes, the theory is that you design a note with perhaps twenty 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 retired from circulation and replaced. This process 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 and accurate 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 round. 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 — perhaps 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 towards 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 and 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 countermeasure is background printing using inks which 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 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), there is very little about check fraud. Yet check fraud is many times greater in value than credit card fraud, and debit cards are almost insignificant by comparison. 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 small 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 chop verification is possible [630]. However, with handwritten signatures, automated verification with acceptable error rates is still beyond the state of the art (I'll discuss it in section 15.2). 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). Such a change means overcoming huge cultural inertia, but the move to the Euro is pushing this along in Europe. Although about two dozen countries now use a common currency, their national banking systems survive, with the result that electronic payments are much quicker and cheaper than check payments in the Euro zone. Presumably the lower costs of online payments will also persuade US businesses 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. Up till the early 1980s, card transactions were recorded mechanically using zip-zap machines; then banks started to save on authorisation costs at their call centres by verifying the card's magnetic strip data using an online terminal. This meant that the authorization was done against the card number on the strip, while the transaction was booked against the card number on the embossing. Villains started to take stolen cards and reencode them with the account details of people with high credit limits — captured, for example, from waste carbons in the bins outside fancy restaurants. 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. Now the hologram really doesn't serve any useful purpose, at least against competent villains.

It's important to pay attention to whether partial alterations like these can be made to documents or tokens in ways that interact unpleasantly with other parts of the system. 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.

14.4 Packaging and Seals

This brings us on to the added problems of packaging and seals. A seal, in the definition of the Los Alamos vulnerability assessment team, is 'a tamper-indicating device designed to leave non-erasable, unambiguous evidence of unauthorized entry or tampering.'

Not all seals work by gluing a substrate with security printing to the object being sealed. I mentioned the lead and wire 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 that are easy to tighten but are supposed to be hard to loosen without cutting. We also mentioned the special chemical coatings, microscopic bar codes 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 to get a tag, and then fixing this tag to the material to be protected. The most important application in financial terms may be the protection of pharmaceutical products against both counterfeiting and tampering, though it's useful to bear in mind others, from nuclear nonproliferation through cargo containers to ballot boxes.

14.4.1 Substrate Properties

Some systems add random variability to the substrate material. We mentioned 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 which can subsequently be read and written using standard low-coercivity equipment without the unique random pattern being disturbed. They are used in bank cards in Sweden, telephone cards in Korea, and entry control cards in some of the buildings in my university.

A similar idea is used in arms control. Many weapons and materials have surfaces that are unique; see for example Figure 14.1 for the surface of paper. Other material surfaces can be made unique; for example, a patch can be eroded on a tank gun barrel using a small explosive charge. The pattern is measured using laser speckle techniques, and either recorded in a log or attached to the device as a machine-readable digital signature [1172]. 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.

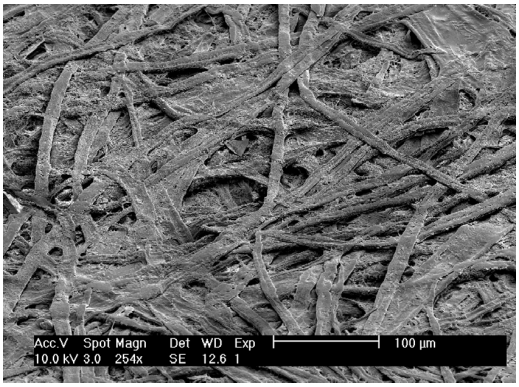

Figure 14.1: Scanning electron micrograph of paper (courtesy Ingenia Technology Ltd)

Recently there have been significant improvements in the technology for reading and recording the microscale randomness of materials. One system is Laser Surface Authentication, developed by Russell Cowburn and his colleagues [236]. They scan the surface of a document or package and use laser speckle to encode its surface roughness into a 256-byte code that is very robust to creasing, drying, scribbling and even scorching. (Declaration of interest: I worked with Russell on the security of this technique.) A typical application is to register all the cartons of a fast-moving consumer good as they come off the production line. Inspectors with hand-held laser scanners and a link to an online database of LSA codes can then not just verify whether a package is genuine, but also identify it uniquely. This is cheaper than RFID, and is also more controllable in that you can restrict access to the database. It thus may be particularly attractive to companies who are worried about internal control, or who want to crack down on grey market trading. In the long term, I'd not be surprised to see this technique used on banknotes.

14.4.2 The Problems of Glue

Although a tag's uniqueness can be a side-effect of its manufacture, most seals still work by fixing a security-printed tag 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 very hard to remove.

In the particular case of tamper-evident packaging, the attachment is part of an industrial process; it could be a pressurized container with a pop-up button or a break-off lid. The usual answer is to use a glue which is stronger than the seal substrate itself, so that the seal will tear or at least deform noticeably if pulled away. This is the case with foil seals under drink caps, many blister packs, and of course the seals you find on software packages.

However, in most products, the implementation is rather poor. Many seals are vulnerable to direct removal using only hand tools and a little patience. Take a sharp knife and experiment with 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 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.) Or open the envelope at the other end, where the glue is not designed to be mildly tamper-evident. Either way you'll probably get an envelope that looks slightly crumpled on careful examination. If it's noticeable, iron out the crumples. 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 tricks. For example, there is a colored adhesive tape that when ripped off leaves behind a warning such as 'Danger' or 'Do not use'. The warning is printed between two layers of glue, the bottom of which is stronger, and is supposed to remain behind if the seal is tampered with. But the tape only behaves in this way if it is pulled from above. By cutting from the side, one can remove it intact and re-use it [749].

14.4.3 PIN Mailers

An interesting recent development is the appearance of special print stocks on which banks laser-print customer PINs. In the old days, PIN mailers used multipart stationery and impact printers; you got the PIN by ripping the envelope open and pulling out a slip on which the PIN had been impressed. The move from impact to laser technology led to a number of companies inventing letter stationery from which you pull a tab to read the PIN. The idea is that just as a seal can't be moved without leaving visible evidence, with this stationery the secret can't be extracted without leaving visible evidence. A typical mechanism is to have a patch on the paper that's printed with an obscuring pattern and that also has an adhesive film over it, on which the PIN is printed. behind the film is a die-cut tab in the paper that can be pulled away, thus removing the obscuring background and making the PIN visible.

My students Mike Bond, Steven Murdoch and Jolyon Clulow had some fun finding vulnerabilities with successive versions of these products. The early products could be read by holding them up to the light, so that the light glanced off the surface at about 10 degrees; the opaque toner showed up clearly against the shiny adhesive film. The next attack was to scan the

printing into Photoshop and filter out the dense black of the toner from the grey of the underlying printing. Another was thermal transfer; put a blank sheet of paper on top of the mailer and run an iron over it. Yet another was chemical transfer using blotting paper and organic solvents. This work was reported to the banking industry in 2004, and finally published in 2005 [205]. The banks have now issued test standards for mailers. Yet to this day we keep getting mailers on which the PIN is easy to read: the latest ones have inks that change color when you pull the tab, and come in an envelope with a leaflet saying 'if the dots are blue, reject this PIN mailer and call us'; but an attacker would just swap this for a leaflet saying 'if the dots aren't blue, reject this PIN mailer and call us'.

This is an example of a system that doesn't work, and yet no-one cares. Come to think of it, if a bad man knows I'm getting a new bank card, and can steal from my mail, he'll just take both the card and the PIN. It's hard to think of any real attacks that the 'tamper-evident' PIN mailer prevents. It might occasionally prevent a family member learning a PIN by accident; equally, there might be an occasional customer who reads the PIN without tearing the tab, withdraws a lot of money, then claims he didn't do it, in which case the bank has to disown its own mailer. But the threats are vestigial compared with the amount that's being spent on all this fancy stationery. Perhaps the banks treat it as 'security theater'; or perhaps the managers involved just don't want to abandon the system and send out PINs printed on plain paper as they're embarrassed at having wasted all this money.

14.5 Systemic Vulnerabilities

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

A possibly useful example is in Figure 14.2. 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 one end it has a printed pattern and serial number on one side and glue on the other; the paper is cross-cut with the result that it completely 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 in fact have been caused by careless application. The point is that the damage done

Figure 14.2: A wristband seal from our local swimming pool

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.)

Despite this, the wristband seal is perfectly fit for purpose. There is little incentive to cheat: the Olympic hopefuls who 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.)

14.5.1 Peculiarities of the Threat Model

We've seen systems where your customer is your enemy, as in banking. In military systems the enemy is the 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. Again, it's often 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 grey markets provide natural distribution channels. Even detecting such frauds — let alone proving them to a court — can be hard.

A typical solution for high-value goods such as cosmetics may involve sourcing 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 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 harder than one would think. The distributor who has bought counterfeit goods on the grey market, believing them to be genuine, may set out to deceive the inspectors without any criminal intent. Where grey markets are an issue, the products bought from 'Fred' will be pushed out rapidly to the customers, ensuring that the inspectors see only authorized products in his stockroom. Also, the distributor may be completely in the dark; it could be his staff who are peddling the counterfeits. A well-known scam is for airline staff to buy counterfeit perfumes, watches and the like in the Far East, sell them in-flight to customers, and trouser the proceeds [783]. The stocks in the airline's warehouses (and in the duty-free carts after the planes land) will all be completely genuine. So it is usually essential to have agents go out and make sample purchases, and the sealing mechanisms must support this.

14.5.2 Anti-Gundecking Measures

Whether the seal adheres properly to the object being sealed may also depend on the honesty and diligence of low-level staff. I mentioned in section 12.3.2.2 how in truck speed limiter systems, the gearbox sensor is secured using a

piece of wire that the calibrating garage seals with a lead disc that is crimped in place with special tongs. The defeat is to bribe the garage mechanic to wrap the wire the wrong way, so that when the sensor is unscrewed from the gearbox the wire will loosen, instead of tightening and breaking the seal. There is absolutely no need to go to amateur sculptor classes so that you can take a cast of the seal and forge a pair of sealing tongs out of bronze (unless you want to save on bribes, or frame the garage).

The people who apply seals can 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 the check-in queue. On about half of the occasions this has been done to my baggage, the tape has been poorly fixed; either 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.

Much of the interesting recent research in seals has focussed on usability. One huge problem is checking whether staff who're supposed to inspect seals have actually done so. *Gundecking* is a naval term used to refer to people who pretend to have done their duty, but were actually down on the gun deck having a smoke. So if your task is to inspect the seals on thousands of shipping containers arriving at a port, how do you ensure that your staff actually look at each one?

The vulnerability assessment team at Los Alamos has come up with a number of anti-gundecking designs for seals. One approach is to include in each container seal a small processor with a cryptographic keystream generator that produces a new number every minute or so, just like the password generators I discussed in Chapter 3. Then the inspector's task is to visit all the inbound containers and record the numbers they display. If a tampering event is detected, the device erases its key, and can generate no more numbers. If your inspector doesn't bring back a valid seal code from one of the containers, you know something's wrong, whether with it or with him. Such seals are also known as 'anti-evidence' seals: the idea is that you store information that a device hasn't been tampered with, and destroy it when tampering occurs, leaving nothing for an adversary to counterfeit.

Carelessness and corruption interact. If enough of the staff applying or verifying a seal are careless, then if I bribe one of them the resulting defect doesn't of itself prove dishonesty.

14.5.3 The Effect of Random Failure

There are similar effects when seals can 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 protection 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.

14.5.4 Materials Control

Another common vulnerability is that supplies of sealing materials are uncontrolled. Corporate seals are a nice example. In the UK, these typically consist of two metal embossing plates that are inserted into special pliers and were used to crimp important documents. Several suppliers 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: all you have to do is write a letter that looks like it came from a law firm.

A more serious example is the reliance of the pharmaceutical industry on blister packs, sometimes supplemented with holograms and color-shifting inks. All these technologies are freely available to anyone who cares to buy them, and they are not particularly expensive either. Or consider the plastic envelopes used by some courier companies, which are designed to stretch and tear when opened. So long as you can walk in off the street and pick up virgin envelopes at the depot, they are unlikely to deter anyone who invests some time and thought in planning an attack; he can substitute the packaging either before, of after, a parcel's trip through the courier's network.

It is also 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 — 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 [676].

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 have 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 a cheap color printer, these assumptions are fairly ambitious. In any case, the arrival of desktop color printers has caused a lot of organizations to stop using preprinted stationery. This makes the forger's job much easier.

14.5.5 Not Protecting the Right Things

I mentioned how credit cards were vulnerable in the late 1980's as 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 use shrink-wrap or blister packaging, which if well designed can be moderately difficult for amateurs to forge well enough to withstand close inspection. However when selecting protective measures you have to be very clear about the threat model — is it counterfeiting, alteration, duplication, simulation, diversion, dilution, substitution or something else? [1025] 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.)

14.5.6 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 but is a much deeper issue of applied psychology and public education. It's a worry for bankers when new notes are being introduced — the few weeks during which everyone is getting familiar with the new notes can be a bonanza for forgers.

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 and 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.

A somewhat shocking experiment was performed by Sonia Trujillo at the 7th Security Seals Symposium in Santa Barbara in March 2006. She tampered with nine out of thirty different food and drug products, using only low-tech attacks, and invited 71 tamper-detection experts to tell them apart. Each subject was asked to pick exactly three out of ten products that they thought had been tampered. The experts did no better than random, even though most of them took significantly longer than the four seconds per product that they were directed to. If even the experts can't detect tampering, even when they're told it has been happening, what chance does the average consumer have?

So the seal that can be checked by the public or by staff with minimal training, and without access to an online database, remains an ideal. The main purpose of tamper-evident packaging is to reassure the customer; secondary purposes include minimising product returns, due diligence and reducing the size of jury awards. Deterring incompetent tamperers might just about be in there somewhere.

Firms that take forgery seriously, like large software companies, have adopted 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 the latest version of Microsoft Office, which they may purchase every five years or so. For this reason, much of the work in protecting software products against forgery has been shifting over the past few years to online registration mechanisms.

One of the possibilities is to enlist the public as inspectors, not so much of the packaging, but of unique serial numbers. Instead of having these numbers hidden from view in RFID chips, vendors can print them on product labels, and people who're concerned about whether they got a genuine product could call in to verify. This may often get the incentives aligned better, but can be harder than it looks. For example, when Microsoft first shipped its antispyware beta, I installed it on a family PC — whose copy of Windows was immediately denounced as evil. Now that PC was bought at a regular store, and I simply did not need the hassle of explaining this to the Empire. I particularly did not like their initial negotiating position, namely that the remedy was for me to send them more money. The remedy eventually agreed on was that they

gave me another copy of Windows XP. But how many people are able to negotiate that?

14.6 Evaluation Methodology

This discussion suggests 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:

- If a seal is forged, who's supposed to spot it? 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? And how well are these inspectors — public or professional — really motivated to find and report defects?
- Has anybody who really knows what they're doing tried hard to defeat the system? And what's a defeat anyway — tampering, forgery, alteration, erosion 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 it been in the field, and how likely is it that 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, and if so, how will you cope with that?
- 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, oil, noise, vibration, cleaning, and manufacturing defects? Will the product have to survive outdoor weather, petrol splashes, being carried next to the skin or being dropped in a glass of beer? Or 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?
- 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 which settled US law on 'phantom withdrawals' from cash machines [674].)

- Once the product is used, how will the seals be disposed of — are you bothered if someone recovers a few old seals from the trash?

Remember that defeating seals is about fooling people, not beating hardware. So think hard whether the people who apply and check the seals will perform their tasks faithfully and effectively; 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 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-life-cycle assurance process should also be applied to computer systems in general. I'll talk about that some more in Part III.

14.7 Summary

Most commercially available sealing products are relatively easy to defeat, and this is particularly true when seal inspection is performed casually by untrained personnel. Sealing has to be evaluated over the whole lifetime of the seal 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 already being spent on research and product development in this area. But much of it isn't spent effectively, and it has all the characteristics of a lemons market which third rate products dominate because of low cost and user ignorance. No doubt lots of fancy new technologies will be touted for product safety and counterfeit detection, from nanoparticles through ferrofluids to DNA; but so long as the markets are broken, and people ignore

the system-level issues, what good will they do? Do any of them have novel properties that enable us to tackle the hard problems of primary inspectability and the prevention of gundecking?

Automatic inspection systems may be one way forward; perhaps in the future a product's RFID tag will deactivate itself if the container is tampered. At present such devices cost dollars; within a few years they might cost cents. But which vendors would deploy them, and for what applications? Where will the incentives be? And, hardest of all, how does this help the consumer? Most of the counterfeits and poisoned products are introduced at the retail level, and protecting the retailer doesn't help here.

Further Reading

The definitive textbook on security printing is van Renesse [1279] 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.

The essential writing on seals can be found in the many publications by Roger Johnston's seal vulnerability assessment team at Los Alamos National Laboratory (e.g., [668]).

The history of counterfeiting is fascinating. From Independence to the Civil War, Americans used banknotes issued by private banks rather than by the government, and counterfeiting was pervasive. Banks could act against local forgers, but by about 1800 there had arisen a network of engravers, papermakers, printers, wholesalers, retailers and passers, with safe havens in the badlands on the border between Vermont and Canada; neither the U.S. nor the Canadian government wanted to take ownership of the problem [887]. It was in many ways reminiscent of the current struggle against phishing.