**Chapter 16**

**Security Printing and Seals**

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

**– KAREN SP¨ARCK JONES**

**You can’t make something secure if you don’t**

**know how to break it.**

**– MARC WEBER TOBIAS**

**16.1** **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 the opponent can get at them be-  
 help with *trusted distribution*, that is, assuring the user that the product  
 hasn’t been tampered with since leaving the factory.

*•* We saw how monitoring systems, such as utility meters and tachographs,  
 how sophisticated the cryptography, a defeat for the seals can be a defeat  
 for the system.

*•* I also discussed how the contactless cards used in most building entry  
 of its successors. If you’re scrutinising the ID of an engineer before you  
 let him into your hosting centre, it can be a good idea to eyeball the ID  
 as well as reading it electronically. Even with electronic ID cards, the  
 security printing can still matter.

*•* In general, it may be a more realistic goal to make credentials *tamper evi-*  
 gets the keys out, they should not be able to reassemble it into something  
 that will pass close examination. Security printing can help here.

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. Since the late 1990s, banknote  
 printers have been promoting digital protection techniques [253]. These include  
 watermarks that stop compliant scanners and printers being used for forgery,  
 and invisible copyright marks that can enable forgeries to be detected in vending  
 machines [830]. Meanwhile, vendors of color copiers and printers embed forensic  
 tracking codes in their printed output that contain the machine serial number,  
 date and time [621]. So the digital world and the world of ‘funny inks’ have  
 been growing closer.

**16.2** **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 used to authenticate documents in the ancient Mediterranean and

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) [825]. Even after handwritten  
 signatures had taken over as the principal authentication mechanism for letters,  
 seals lingered 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 docu-

ments 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, and in the demand in some European countries for electronic sig-  
 natures that comply with the EU’s eIDAS standards.

However, by the middle of the 20th 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 prod-  
 ucts, leading to a peak of 235 reported cases in 1993 [1027]. 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 com-  
 panies 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 pharma-  
 ceuticals. 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. 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.

**16.3** **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 be-

lieving 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 run-  
 ning 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 [697]. British banknotes are now  
 being migrated to plastic, a process pioneered in Australia.

**16.3.1** **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 major organization  
 (such as one country trying to forge another’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 twenti-

eth 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. 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 of a forged

banknote or document [1935]:

1. a *primary* inspection is one performed by an untrained inexperienced per-

son, 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 ban-  
 knotes 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 manufac-

turer 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, where the limitations are skill and, above all,  
 motivation. 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.

**16.3.2** **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

|  |  |  |
| --- | --- | --- |
|  |  |  |

deﬁnition. This is often used for scroll work on paper banknotes and

passports;

*• letterpress* in which the ink is rolled on raised type that is then pressed on  
 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  
 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.  
 Simultan presses also have special ducting to make ink colors vary along  
 the line (*rainbowing*);

*•* rubber stamps that are used to endorse documents, or to seal photographs

*•* embossing and laminates that are also used to seal photographs, and on  
 use laser engraving techniques to burn a photo into an ID card;

*• watermarks* are an example of putting protection features in the paper.  
 thickness when it is manufactured. Many other special materials, such as  
 ﬂuorescent threads, are used for similar purposes.

More modern techniques include:

*•* Modern plastic notes, ﬁrst introduced in Australia, allow a variety of fea-

*•* optically variable inks that change color from green to gold depending on

*•* inks with magnetic, photochromic or thermochromic properties;

*•* printing features visible only with special equipment, such as the micro-  
 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  
 *grams*. 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*  
 effects with the dot separation of common scanners and copiers;

|  |  |  |
| --- | --- | --- |
|  |  |  |

*• digital copyright marks* which may vary from images hidden by micro-  
 signals that will be recognized by a color copier, scanner or printer and  
 cause it to stop. The best-known is the yellow pattern of stars, in the  
 shape of the Southern Cross, that is embedded in the design of many ban-  
 knotes and that stops compliant scanners and printers from processing  
 it;

*•* unique stock, such as the Sandia proposal of paper with optical ﬁbers  
 a characteristic pattern that can be digitally signed and printed on the  
 document using a barcode [1746].

For the design of the US $100 bill, see [1367]; and for a study of counterfeit

banknotes, with an analysis of which features provide what evidence, see [1936].  
 In general, banknotes’ genuineness cannot readily be conﬁrmed by the inspec-  
 tion 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 water-  
 marks 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 [1440].

When polymer notes were introduced into the UK, in 2016 for the £5 note

and 2017 for the £10, we were told they were unforgeable. But by 2018 we were  
 being told how to spot forgeries. One victim reported ‘I looked closer and saw  
 the Big Ben was missing and part of the serial number and the Queen’s face  
 were coming off. When I compared it to a genuine note I already had I also saw  
 the silver strips were green’ [1611]. Later that year, enterprising villains were  
 passing off plastic £20 notes, even though the official £20 note wasn’t due to  
 launch till 2020.

So the technology constantly moves on, and 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 com-

plex trade-offs between protection, aesthetics and robustness, and the business  
 focus can also change. For many years, banknote designers aimed at prevent-  
 ing 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 ban-  
 knote actually decides subconsciously whether it’s acceptable. In other words,  
 the technological focus had usurped the business focus.

The lessons drawn so far are [1935]:

*•* security features should convey a message relevant to the product. So it’s  
 some obscure feature nobody looks at;

*•* security features should obviously belong where they are, so they become

*•* their effects should be obvious, distinct and intelligible;

*•* they should not have existing competitors that can provide a basis for

*•* 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 to documents  
 other than banknotes, such as passports, there are also issues relating to the  
 political environment of the country and the mores of the society in which they  
 will be used [1293].

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 dis-  
 tinguish 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 if 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 feature life, death and rebirth could turn  
 more quickly than in the past. Another possibility, of course, is that developed

|  |  |  |
| --- | --- | --- |
|  |  |  |

countries move entirely to card payments, the path of rich early adopters such  
 as Sweden and Finland.

With product packaging, the typical business model is that samples of forg-

eries 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 be-  
 cause 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.

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 [8].

Check fraud used to be many times greater in value than card fraud, and

also difficult to deal with because of the huge volume of checks processed daily.  
 This makes scrutiny impossible except for very large amounts. In the Far East,  
 where people use a personal *chop* or signature stamp to sign checks, low-cost  
 automatic veriﬁcation is possible [929]. However, with handwritten signatures,  
 automated veriﬁcation with acceptable error rates is still beyond the state of  
 the art (I’ll discuss it in section 17.2). The future for businesses is to move  
 payments to bank transfer; the early adopter here, Germany, largely suppressed  
 check frauds by the early 2000s. SEPA payments are now making electronic  
 payments much quicker and cheaper than check payments in the Euro zone.

Of course, document 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. For this  
 reason, developed countries have largely moved to chip-based passports; visitors  
 from countries that don’t have electronic passports yet may have to get visas  
 that contain chips or that point to an online database storing the traveler’s  
 biometric.

|  |  |  |
| --- | --- | --- |
|  |  |  |

**16.4** **Packaging and Seals**

Supply-chain security involves 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 unau-  
 thorized entry or tampering.’

Most seals 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. Applications  
 range from pharmaceutical products through cargo containers to ballot boxes.  
 Other products follow the same general philosophy but using different materials;  
 at the bottom end we ﬁnd plastic straps that are easy to tighten but hard to  
 loosen without cutting, while at the top there are optical ﬁbres that loop around  
 the protected object and are actively monitored for stretching by an attached  
 laser tag.

**16.4.1** **Substrate properties**

Some systems add random variability to the substrate material. We mentioned  
 the trick of loading paper with optical 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. These were 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 was used in arms control during the Cold War. Many weapons

and materials have surfaces that are unique; see for example Figure 16.1 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 [1749].  
 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. You  
 can even authenticate a piece of paper using laser speckle to encode its surface  
 roughness into a code that is robust to creasing, drying, scribbling and even  
 scorchings [332]. The problem there is ﬁnding an application where you can  
 justify using expensive scanners at each end of the process.

**16.4.2** **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

|  |  |  |
| --- | --- | --- |
|  |  |  |

Figure 16.1: – scanning electron micrograph of paper (courtesy Ingenia Tech-  
 nology Ltd)

pulled away. This is the case with foil seals under drink caps and blister packs  
 of pills.

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 so 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. A notorious example is the *vignette*, or motorway toll sticker, used in  
 Switzerland and Austria. There, you have to pay a road toll for which you get  
 a sticker that goes on your windscreen to certify that you have paid your dues  
 for a year, or a shorter period if you rent a car. If you tear a sticker off your  
 windscreen to use it on another car, some of the ink comes with it while some  
 sticks to the windscreen. So people get dust on the glue before sticking it on,  
 by brushing the sticker back and forth on the dashboard. This has now been  
 made an offence, and you’re ﬁned if you get caught [1468].

**16.4.3** **PIN mailers**

Many banks now print customer PINs on special print stocks. 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 with the obscuring background, 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 [284]. 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.

This is an example of a system that doesn’t work, and yet persists. If a

crook 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 will probably just say “so  
 sue us” and disown its own mailer. But the threats are vestigial compared

with the amount that’s being spent on all this fancy stationery. The driver for  
 such behaviour is probably compliance; it’s too much bother to rethink card  
 scheme rules, audit procedures and insurance inspections that evolved in an age  
 of impact printers.

**16.5** **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.

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 is completely destroyed if you tear it off carelessly;  
 see Figure 16.2. (It’s similar to the luggage seals used at some airports.)

The simplest attack is via the supplier’s website, where boxes of 100 wrist-

bands cost about $8. If you don’t want to spend money, you can use each band

|  |  |  |
| --- | --- | --- |
|  |  |  |

Figure 16.2: – a wristband seal from our local swimming pool

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 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 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 lengths 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 fresh wristband. 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.)

**16.5.1** **Peculiarities of the threat model**

In military systems the opponent is the 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. With voting machines, most attacks come from election officials.

Some of the most difficult sealing tasks arise where it’s the enemy who will

apply the seal. A typical business 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 sourc-

ing 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.  
 Sealing mechanisms usually must be designed with the complementary control  
 processes 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 when they visit countries with  
 unregulated markets, and sell them in-ﬂight to customers [1142]. 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.

**16.5.2** **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 14.3.2.2  
 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. This is simpler than  
 going to amateur sculptor classes so that you can take a cast of the seal and  
 forge a pair of sealing tongs out of bronze.

The people who apply seals can be careless as well as corrupt. Some airports

apply tape seals to 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. But airport security is mostly theatre anyway.

Much of the interesting research in seals has focused 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?

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. 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.

**16.5.3** **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.)

After opening a too-well-sealed envelope, a spy 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, spon-  
 taneous 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  
 undermine the sealing product’s evidential (and thus commercial) value.

My example of this comes from the curfew tags which I described in detail

|  |  |  |
| --- | --- | --- |
|  |  |  |

in section 14.4. There, the tag vendors made grandiose marketing claims about  
 the tamper-resistance of their products, but refused to make samples available  
 for testing by the defence when challenged in court. Terrorism suspects were  
 released when their control orders could no longer be justiﬁed, and eventually  
 the tag ﬁrms lost their contracts for criminal misconduct: they had billed the  
 Ministry of Justice for tagging people who were dead or in jail, and ended up  
 paying multimillion-pound ﬁnes, as did their auditors [193].

**16.5.4** **Materials control**

Another common vulnerability is that supplies of sealing materials are uncon-  
 trolled. 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. The real  
 purpose of sealing is not to prevent forgery but to enable law ﬁrms to charge  
 extra for documents that have to have seals attached.

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, or 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 [1001]; letter writers there and indeed all over Europe  
 used *letterlocking* – complex systems of folds, slits and seals that they hoped  
 would make tampering evident [366].

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.

|  |  |  |
| --- | --- | --- |
|  |  |  |

**16.5.5** **Not protecting the right things**

Where a value token encodes value in two different ways, you may expect crim-  
 inals to exploit any difference, or indeed to create one. Credit cards became  
 vulnerable to forgery in the late 1980s as banks introduced authorization termi-  
 nals that read the magnetic strip, while the imprinting machines used by most  
 merchants to print out vouchers for the customer to sign used the embossing,  
 and most merchants banked the signed vouchers as if they were checks. Crooks  
 who changed the mag strip but not the embossing defeated the system. There  
 are also attacks involving partial alterations. For example, credit cards used to  
 have holograms, but as they covered 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 obsolete, as the old Addressograph draft capture machines  
 are no longer used. In any case, all the hologram said was ‘This was once a valid  
 card’ and most banks have now discontinued it.

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 mea-  
 sures you have to be very clear about the threat model – is it counterfeiting,  
 alteration, duplication, simulation, diversion, dilution, substitution or some-  
 thing else? [1524] 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 them in the chapter on tamper resistance.)

**16.5.6** **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 holo-  
 gram!’ 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, letter-

heads, 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 sketchy information on security features. Crooks  
 frequently get genuine passports and ID cards by corrupt means (and not just  
 from less developed countries.) Oh, and the absence of real physical samples  
 means that the tactile aspects cannot be properly examined.

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 sub-  
 ject 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 rather  
 than a reality. 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 luxury goods makers, 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 a fancy cosmetic or an expensive bottle of wine. For this reason, much of the  
 work in protecting products that contain electronics has shifted to online regis-  
 tration mechanisms. Some products have acquired electronics for this purpose,  
 while others that already have electronics are acquiring wiﬁ chips.

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. I particularly did not like their initial  
 negotiating position, namely that I should send them more money. Eventually  
 they gave us another copy of Windows. But we didn’t buy another Windows  
 machine after that.

**16.6** **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  
 to establish the likely false accept and false reject rates? If it’s your in-  
 spectors in the ﬁeld, how much will their equipment and training cost?

|  |  |  |
| --- | --- | --- |
|  |  |  |

And how well are these inspectors – public or professional – motivated to  
 ﬁnd and report defects?

*•* Has anybody who really knows what they’re doing tried hard to defeat  
 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

*•* How long has it been in the ﬁeld, and how likely is it that progress will

*•* Who else can buy, forge or steal the sealing materials?

*•* Will the person who applies the seal ever be careless or corrupt, and if so,

*•* Will the seal protect the right part (or enough) of the product?

*•* What are the quality issues? What about the effects of dirt, oil, noise,  
 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?

*•* If you’re going to end up in court, are there experts other than your own  
 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? And what happens if you sell your company to someone who  
 sells it to a crook?

*•* Once the product is used, how will the seals be disposed of – are you

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.

This whole-life-cycle assurance process is just a microcosm of the assurance

process you need to apply to systems in general. I’ll discuss that in more detail  
 in Part III.

|  |  |  |
| --- | --- | --- |
|  |  |  |

**16.7** **Summary**

Most commercially available sealing products are relatively easy to defeat, and  
 this is particularly true when seal inspection is performed casually by people  
 who are untrained, unmotivated or both (as is often the case). Sealing has to be  
 evaluated over the whole lifetime of the seal from manufacture through materi-  
 als 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**

This is an area in which a lot of ideas have come and gone without making much  
 impact. 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?

Automatic inspection systems may be one way forward. One example is in

cold chain assurance. Some products such as vaccines need to be kept at less  
 than 40C, and already ship with loggers in the container or pallet that monitor  
 the temperature and allow failures to be identiﬁed. There are also telltale paper  
 strips that display a different barcode, on the basis of a chemical reaction, if the  
 threshold is exceeded. Regulated industries with safety-critical products, such  
 as pharma, might be a good place to try out new ideas.

A much harder problem is how to help the consumer in less regulated in-

dustries. Most of the counterfeits and poisoned products are introduced at the  
 retail level, which used to be highly dispersed. But tech is ﬁxing that, and per-  
 haps the solution doesn’t lie in packaging but in regulatory action against large  
 retailers like Amazon. Its marketplace and fulﬁlment services are reportedly be-  
 coming the most concerning distribution channel for many counterfeit products,  
 as well as products that have been declared unsafe by government agencies, are  
 deceptively labeled or are banned by regulators, including children’s toys con-  
 taining dangerous levels of lead [591]. This is looking like becoming one of the  
 big regulatory battles between governments and Big Tech. Perhaps it’s an in-  
 evitable effect of scale; if everybody’s on Facebook then that includes all the  
 world’s creeps, bullies and extremists, and if all the world’s merchants use Ama-  
 zon to ship their products then something similar can be expected. Eventually,  
 I suspect, Amazon will be compelled to hire tens of thousands of product safety  
 and compliance inspectors, just as Facebook has been compelled to hire tens  
 of thousands of content moderators. But laws usually lag technology by ﬁfteen  
 years or so, and in the meantime secure printing and sealing will continue –  
 albeit with a continuing move to online product registration.

|  |  |  |
| --- | --- | --- |
|  |  |  |

**Further Reading**

The deﬁnitive textbook on security printing is van Renesse [1935] 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 (e.g., [989]).

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 US nor the Canadian  
 government wanted to take ownership of the problem [1311].

More recently there’s been the Supernote controversy. In the late 2000s, a

few million dollars a year worth of counterfeit US currency turned up that was  
 perfect in almost every respect: it was printed with the right presses, on the right  
 paper, and tracked the small changes accurately – except in that it did not use  
 the right magnetic and infrared security features. The US government accused  
 North Korea of forgery and used this to impose sanctions; others suggested that  
 the notes were more likely produced by the CIA in order to trace cash money  
 ﬂows. These notes turned up in only tiny quantities, and only in the hands of  
 people of interest to the CIA such as North Korean diplomats and central Asian  
 warlords. They had been carefully designed to pass all inspections other than  
 the counting machines used by money-centre banks, which would prevent them  
 getting into circulation at scale; and the volumes that turned up were at least  
 one order of magnitude less than a forger would have produced, and would have  
 needed to produce in order to pay for the equipment [622].

|  |  |  |
| --- | --- | --- |
|  |  |  |