**Chapter 13**

**Locks and Alarms**

**For if a man watch too long, it is odds he will fall asleepe.**

**– FRANCIS BACON**

**The greatest of faults, I should say,**

**is to be conscious of none.**

**– THOMAS CARLYLE**

**13.1** **Introduction**

Most security engineers nowadays focus on electronic systems, but physical pro-  
 tection cannot be neglected. First, if you’re advising on a company’s overall risk  
 management, then walls and locks are a factor. Second, as it’s easier to teach  
 someone with an electrical engineering or computer science background the ba-  
 sics of physical security than the other way round, interactions between physical  
 and logical protection are usually up to the systems person to manage. Third,  
 you will often be asked for your opinion on your client’s installations – which  
 may have been built by contractors with little understanding of system issues.  
 You’ll need to be able to give informed, but diplomatic, advice. Fourth, many  
 information security mechanisms can be defeated if a bad man gets physical  
 access, whether at the factory, or during shipment, or before installation. Fifth,  
 many mechanical locks have recently been completely compromised by ‘bump-  
 ing’, an easy covert-entry technique; their manufacturers often seem unaware of  
 vulnerabilities that enable their products to be quickly bypassed. Finally, many  
 of the electronic locks that are replacing them are easy to compromise, either  
 because they use cryptography that’s been broken (such as Mifare classic) or  
 because of poor integration of the mechanical and digital components.

Much of physical security is just common sense, but there are some non-

obvious twists and there have been signiﬁcant recent advances in technology.  
 There are useful ideas from criminology and architecture on how you can reduce  
 the incidence of crime around your facilities; some of these may go across into  
 system design too. And there’s a very interesting case study in burglar alarms.

For example, in order to defeat a burglar alarm it’s enough to make it stop

working, or even just to persuade the guards that it has become unreliable. This  
 gives a new perspective on *denial of service attacks*. Just as we’ve seen military  
 messaging systems designed to enforce conﬁdentiality and bookkeeping systems  
 whose goal is preserving record authenticity, monitoring gives us the classic  
 example of systems that need to be dependably available. If there is a burglar  
 in my bank vault, then I don’t care very much who else gets to know (so I’m  
 not worried about conﬁdentiality), or who it was who told me (so authenticity  
 isn’t a major concern); but I do care very much that an attempt to tell me is  
 not thwarted. Historically, about 90% of computer security research was about  
 conﬁdentiality, about 9% about authenticity and 1% about availability. But  
 actual attacks – and companies’ infosec expenditures – are often the other way  
 round, with more spent on availability than on authenticity and conﬁdentiality  
 combined. And it’s alarm systems, above all else, that can teach us about

availability.

**13.2** **Threats and Barriers**

Physical security engineering is no different at heart from the digital variety:  
 you perform a threat analysis, then design a system that involves equipment  
 and procedures, then test it. You evaluate it according to criteria agreed with  
 the customer, which in 2019 may mean that a bank headquarters building has a  
 speciﬁcation setting out ﬁve years’ maintenance cost, building software penetra-  
 tion testing and a security policy [350]. The design and testing of entry controls  
 and alarms is driven by a policy based on:

*Deter – detect – alarm – delay – respond*

A facility can deter intruders using hard methods such as concrete walls,

or softer methods such as being inconspicuous. It will then have one or more  
 layers of barriers and sensors whose job is to keep out casual intruders, detect  
 deliberate intruders, and make it difficult for them to get in too quickly. This  
 will be complemented by an alarm system designed to get a response to the  
 scene in time. As the barriers will have doors for authorized staff to go in

and out, there will be entry control that could be anything from metal keys to  
 biometric scanners. Finally, these measures will be supported by operational  
 controls. How do you cope, for example, with your facility manager having his  
 family taken hostage?

As I noted earlier, one of the ways in which you get your staff to accept dual

controls and integrate them into their work culture is that these controls protect  
 them, as well as protecting the assets. You need to embed the operational

aspects of security in the ﬁrm’s culture or they won’t work well, and this applies  
 to physical security just as much as to the computer variety. It’s also vital to  
 get uniﬁed operational security across the physical, business and information  
 domains: there’s little point in spending $10m to protect a vault containing  
 $100m of diamonds if a bad man can sneak a false delivery order into your  
 system, and send a courier to pick up the diamonds from reception. That

is another reason why, as the information security expert, you have to pay

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

attention to the physical side too.

**13.2.1** **Threat model**

An important design consideration is the attacker’s level of skill, equipment and  
 motivation. And as we’ve seen in one context after another, security isn’t a  
 scalar. It doesn’t make sense to ask ‘Is device X secure?’ without a context:  
 ‘secure against whom and in what environment?’

In the absence of an ‘international standard burglar’, the nearest I know to

a working classiﬁcation is one developed by a US Army expert [173].

*• Derek* is a 19-year old addict. He’s looking for a low-risk opportunity to

*• Charlie* is a 40-year old inadequate with seven convictions for burglary.  
 very intelligent he is cunning and experienced; he has picked up a lot of  
 ‘lore’ during his spells inside. He steals from small shops and suburban  
 houses, taking whatever he thinks he can sell to local fences.

*• Bruno* is a ‘gentleman criminal’. His business is mostly stealing art. As a  
 art history on the wall, and one conviction for robbery eighteen years ago.  
 After two years in jail, he changed his name and moved to a different part  
 of the country. He has done occasional ‘black bag’ jobs for intelligence  
 agencies who know his past. He’d like to get into computer crime, but the  
 most he’s done so far is lock hacking and alarm tampering.

*• Abdurrahman* heads a cell of a dozen agents, most with military training.  
 support provided by his home country. Abdurrahman himself came third  
 out of a class of 280 at its military academy. His mission is to deal with the  
 country’s opponents overseas, typically by covert entry into their homes or  
 offices to plant listening devices or to install malware into their computers  
 and phones. One of the possible missions that his agency and government  
 are considering is to steal plutonium. He thinks of himself as a good man  
 rather than a bad man.

So Derek is unskilled, Charlie is skilled, Bruno is highly skilled and may

have the help of an unskilled insider such as a cleaner, while Abdurrahman is  
 not only highly skilled but has substantial resources. He may even have the help  
 of one or more skilled insiders who have been suborned. (It’s true that many  
 terrorists these days are barely at Charlie’s level, but it would not be prudent  
 to design a nuclear power station on the assumption that Charlie would be the  
 highest grade of attacker you have to worry about. And now that your power  
 station’s dozens of contractors are moving their systems to the cloud, you can  
 bet that one of them will be vulnerable to a capable motivated hacker.)

While the sociologists focus on Derek, the criminologists on Charlie and

the military on Abdurrahman, our concern is mainly with Bruno. He isn’t the

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

highest available grade of ‘civilian’ criminal: that distinction probably goes to  
 the bent bankers and lawyers who launder money for drug gangs, or the guys  
 who write malware for online crime gangs. But the physical defenses of banks  
 and computer rooms tend to be designed with Bruno in mind.

**13.2.2** **Deterrence**

The ﬁrst consideration is whether you can prevent bad people ever trying to  
 break in. It’s a good idea to make your asset anonymous and inconspicuous  
 if you can. It might be a nondescript building in the suburbs; in somewhere  
 like Hong Kong, with its sky-high property prices, it might be half a ﬂoor of an  
 nondescript office block.

Location matters; some neighbourhoods have much less crime than others.

Part of this has to do with whether other property nearby is protected, and how  
 easy it is for a crook to tell which properties are protected. If owners just install  
 visible alarms, they may redistribute crime to their neighbours; but invisible  
 alarms that get criminals caught rather than just sent next door can deter crime  
 in a whole neighbourhood. For example, Ian Ayres and Steven Levitt studied  
 the effect on auto thefts of Lojack, a radio tag that’s embedded invisibly in  
 cars and lets the police ﬁnd them if they’re stolen. In towns where a lot of  
 cars have Lojack, car thieves are caught quickly and ‘chop-shops’ that break up  
 stolen cars for parts are closed down. Ayres and Levitt found that although a  
 motorist who installs Lojack pays about $100 a year, the social beneﬁt from his  
 doing this – the reduced car crime suffered by others – is $1500 [148]. The same  
 applies to real estate; a neighbourhood in which lots of houses have high-grade  
 alarms that quietly call the police is a dangerous place for a burglar to work.  
 In fact, physical property crimes have fallen substantially in the USA, the UK  
 and many other countries since the early 1990s.

But that’s not all. Since the 1960s, there has arisen a substantial literature

on using environmental design to deﬂect and deter threats. Much of this evolved  
 in the context of low-income housing, as criminologists and architects learned  
 which designs made crime more or less likely. In 1961, Elizabeth Wood urged  
 architects to improve the visibility of apartment units by residents, and create  
 communal spaces where people would gather and keep apartment entrances in  
 view, thus fostering social surveillance; areas that are out of sight are more  
 vulnerable [2036]. In 1972, Oscar Newman developed this into the concept of  
 ‘Defensible Space’: buildings should ‘release the latent sense of territoriality  
 and community’ of residents [1435]. Small courtyards are better than large

parks, as intruders are more likely to be identiﬁed, and residents are more likely  
 to challenge them. At the same time, Ray Jeffery developed a model that

is based on psychology rather than sociology and thus takes account of the  
 wide differences between individual offenders; it is reﬂected in our four ‘model’  
 villains. Intruders are not all the same, and not all rational [1609].

Jeffery’s ‘Crime Prevention Through Environmental Design’ has been inﬂu-

ential and challenges a number of old-fashioned ideas about deterrence. Old  
 timers liked bright security lights; but they create glare, and pools of shadow in  
 which villains can lurk. It’s better to have a civilised front, with windows over-  
 looking sidewalks and car parks. In the old days, cyclone fences with barbed

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

wire were thought to be a good thing; but they communicate an absence of  
 personal control. A communal area with picnic seating, in which activities hap-  
 pen frequently, has a greater deterrent effect. Trees also help, as they make  
 shared areas feel safer (perhaps a throwback to an ancestral environment where  
 grassland with some trees helped us see predators coming and take refuge from  
 them). Access matters too; defensible spaces should have single egress points,  
 so that potential intruders are afraid of being trapped. It’s been found, for

example, that CCTV cameras only deter crime in facilities such as car parks  
 where there’s a single exit [766]. There are also many tricks developed over  
 the years, from using passing vehicles to enhance site visibility to planting low  
 thorn bushes under windows. Railings can make better barriers than walls, as  
 you can see through them. Advice on these can be found in modern standards  
 such as [324].

Another inﬂuential idea is the broken-windows theory of George Kelling and

Catherine Coles [1029]. They noted that if a building has a broken window  
 that’s not repaired, then soon vandals will break more, and perhaps squatters  
 or drug dealers will move in; if litter is left on a sidewalk then eventually peo-  
 ple will start dumping their trash there. So problems should be ﬁxed when

they’re still small. Kelling was hired as a consultant to help New York clean  
 up its vandalised subways, and inspired the zero-tolerance movement of police  
 chief William Bratton, who cracked down on public drinkers, squeegee men and  
 other nuisances. Both petty crime and serious crime in New York fell sharply.  
 Criminologists still argue about whether the fall was due to zero tolerance, or  
 to other simultaneous changes such as demographics [1151] and right-to-carry  
 laws [1188].

A related set of ideas can be found in the situational crime prevention theory

of Ronald Clarke. This builds on the work of Jeffery and Newman, and is

broader than just property crime; it proposes a number of principles for reducing  
 crime generally by increasing the risks and effort, reducing the rewards and  
 provocations, and removing excuses. Its focus is largely on designing crime out  
 of products and out of the routines of everyday life; it’s pragmatic and driven  
 by applications [440]. It involves detailed study of speciﬁc threats; for example,  
 car theft is considered to be a number of different problems, such as joyriding by  
 juveniles, theft to get home at night and theft by professional gangs of cars for  
 dismantling or sale abroad – these threats are best countered by quite different  
 measures. Such empirical studies may be criticised by criminologists with a

sociology background as lacking ‘theory’, but are gaining inﬂuence and are not  
 far from what security engineers do. Many of the mechanisms discussed in this  
 book ﬁt easily within a framework of application-level opportunity reduction.

This framework naturally accommodates the extension of environmental con-

trols to other topics when needed. So if you’re planning on anonymity of your  
 hosting centres as a defence against targeted attack, you have to think about  
 how you limit the number of people who know where those premises are. At  
 least, that was the traditional approach; but it may not be the last word. Many  
 ﬁrms have moved entirely to third-party cloud services and have no hosting cen-  
 tres any more. This can save physical security costs, as well as sysadmin salaries  
 and electricity.

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

**13.2.3** **Walls and barriers**

Once you’ve decided what environmental features you’ll use to deter Derek or  
 Charlie from trying to break into your site, and how you make it harder for  
 Bruno to ﬁnd out which of your sites he should break into, you then have the  
 problem of designing the physical barriers.

Your ﬁrst task is to ﬁgure out what you’re really trying to protect. In the

old days, banks used to go to great lengths to make life really tough for robbers,  
 but this has its limits: a robber can always threaten to shoot a customer. So  
 by the 1980s, the philosophy had shifted to ‘give him all the cash he can see’.  
 This philosophy has spread to the rest of retail. In 1997, Starbucks reviewed  
 physical security following an incident in which three employees were shot dead  
 in a bungled robbery. They decided to move the safes from the manager’s

office to the front of the store, and made these safes highly visible not just to  
 staff, customers and passers-by, but also to the control room via CCTV. A side-  
 beneﬁt was improved customer service. The new design was tested at a number  
 of US locations, where increased sales and loss reductions gave a good return  
 on investment [505]. I notice that people increasingly leave their car keys just  
 inside the front door at home, rather than keeping them on their bedside table.  
 If someone breaks into your house at night to steal your car, do you really want  
 to engage them in hand-to-hand combat?

Second, having settled your protection goals, you have to decide what perime-

ters or boundaries you’ll have for what purposes, and where. A growth industry  
 recently has been vehicle traps to prevent cars or trucks being brought close to  
 iconic targets, whether to carry bombs or to run down sightseers. But it’s a  
 mistake to focus on rare but ‘exciting’ threats at the expense of mundane ones.  
 Many buildings have stout walls but roofs that are easy to penetrate; perhaps a  
 terrorist would blow himself up at your main gate to no effect, but an environ-  
 mental protester could cripple your fab and cost you hundreds of millions in lost  
 production by climbing on the roof, cutting a hole and dropping some burning  
 newspaper.

For this reason, organisations such as NIST, the Builders’ Hardware Man-

ufacturers’ Association, Underwriters’ Laboratories, and their equivalents in  
 other countries have a plethora of test results and standards for walls, roofs,  
 safes and so on. The basic idea is to assess how long a barrier will resist an  
 attacker who has certain resources – typically hand tools or power tools. Nor-  
 mal building materials don’t offer much delay at all; you get through a cavity  
 brick wall in less than a minute with a sledgehammer, and regardless of how  
 expensive a lock you put on your front door, a SWAT team will just break the  
 door off its hinges with a battering-ram. So could a robber. So the designers  
 of data centres, bank vaults and the like favour reinforced concrete walls, ﬂoors  
 and roofs, with steel doorframes. But if the bad guys can work undisturbed all  
 weekend, even concrete won’t keep them out. In England’s biggest burglary, a  
 gang of elderly criminals drilled through the 20-inch concrete wall of a safe de-  
 posit company in Hatton Garden in 2015 and made off with £14m in diamonds.  
 Four years later, the ringleader was caught and it emerged at trial how he’d  
 posed as a phone company engineer to tamper with the security system, then  
 used a mobile phone jammer to block the alarm signal [1547].

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

Beware that the organisations that certify locks, safes and vaults often make

outdated assumptions about attack tools. The lock on your car steering wheel  
 is certiﬁed to resist a man putting his weight on it; but car thieves have learned  
 to use a scaffolding pole, which gives the leverage to break it. The typical bank  
 vault is certiﬁed to resist attack for ten minutes, yet your local Fire Department  
 can get through in two minutes using a modern angle grinder. And if the bad  
 guys have access to proper explosives, they can get through almost anything  
 in seconds. Another issue is the thermic lance, or burning bar, which will cut  
 through most barrier materials quickly: safe engineers use such things to get  
 into a vault whose combination has been lost. Robbers can get them too. So  
 barriers can’t be seen in isolation. You have to be aware of assumptions about  
 the threats, and about the intrusion detection and response on which you can  
 rely.

**13.2.4** **Mechanical locks**

The locksmithing industry has been seriously upset in recent years by devel-  
 opments that have exposed the vulnerability of many low-cost mechanical and  
 electronic locks.

The ﬁrst of these is *bumping*. This technique enables many mechanical locks

to be opened quickly and without damage by unskilled people using tools that  
 are now readily available. Its main target is the pin-tumbler lock originally

patented by Linus Yale in 1860 (see Figure 13.1). This was actually used in  
 ancient Egypt, but Yale rediscovered it and it’s often known as a ‘Yale lock’,  
 although many other ﬁrms make them too nowadays.

Figure 13.1: – a cutaway pin-tumbler lock (Courtesy of Marc Weber Tobias)

These locks have a cylindrical plug set inside a shell, and prevented from

|  |  |  |
| --- | --- | --- |
| rotating by a number of *pin stacks*. Each stack usually consists of two or three  pins, one on top of the other. The *bottom pin* or *key pin* makes direct contact  with the key; behind it is a spring-loaded *top pin* or *driver pin* that forces the  bottom pin as far down as possible in the keyway. When the correct key is  inserted, the gaps between the top pin and the bottom pin in each stack align  with the edge of the plug, creating a *shear line*; the plug can now be turned. A  106 possible *key di↵ers*. The actual number will be less because of mechanical  typical house or o�ce lock might have ﬁve or six pins each of which could have  the gap in ten di↵erent positions, giving a theoretical key diversity of 105 or | | |
|  |  |  |

tolerances and key-cutting restrictions.

It had been known for years that such locks can be picked, given special tools.

You can ﬁnd details in the MIT Lock Picking Manual [1896] or in treatises such  
 as that by Marc Weber Tobias [1891]: the basic idea is that you twist the plug  
 slightly using a tension wrench, and then manipulate the pins with a lockpick  
 until they all line up along the shear line. Such techniques have been used by  
 specialists such as locksmiths for years; but they take a lot of practice, and it’s  
 unlawful to possess the tools in many jurisdictions (for the laws in the USA,  
 see [1893]). Until recently, lockpicking was generally thought to be a threat only  
 to high-value targets such as investment banks and embassies.

The new discovery was that an attacker can insert a specially made *bump*

*key* each of whose teeth is set at the lowest pin position and whose shoulder is  
 slightly rounded. (Such keys are also known as ‘999’ keys as all the teeth are at  
 the lowest position, or *bitting*, namely number 9.) The intruder can then place  
 the key under slight torsion with their ﬁngertips and tap the key head with  
 a rubber mallet. The shock causes the pins to bounce upwards; the applied  
 torsion causes them to stick as the spring pushes them back down, but with the  
 gap at the cylinder edge. The net effect is that with a few taps of the mallet,  
 the lock can be opened.

This trick had been known for years, but became more effective because of

better tools and techniques. It was publicised by a 2005 white paper written  
 by Barry Wels and Rop Gonggrijp of The Open Organization Of Lockpick-  
 ers (TOOOL), a Dutch ‘lock sports’ group (as amateur locksmithing is now  
 known [2008]). TV coverage spread the message to a wide audience. The view  
 of experts is that bumping deskills lockpicking, with potentially serious conse-  
 quences [1892]. It’s been found, for example, that the locks in US mailboxes  
 can be opened easily, as can the pin-tumbler locks with 70% of the US domestic  
 market. The Dutch paper, and the subsequent publicity, kicked off an arms  
 race, with vendors producing more complex designs and amateur locksmiths  
 reporting bumping attacks on many of them. We now have lockpicking kits at  
 my lab so schoolkids can play with them during open days. They love it!

Just about all metal locks have been broken. When I worked in banking,

locks from Medeco were thought to be unpickable (and even certiﬁed as such),  
 and were used to protect the hardware security modules in which the bank’s  
 most important cryptographic keys were kept. The company had a dominant  
 position in the high-security lock market. Medeco uses secondary keying in the  
 angle at which cuts are made in the key. In this ‘biaxial’ system, angled cuts  
 rotate the pins to engage sliders. In 2005, Medeco introduced the m3 which also  
 has a simple sidebar in the form of a slider cut into the side of the key. Yet  
 in 2007, Tobias reported an attack on the m3 and biaxial locks, using a bent  
 paperclip to set the slider and then a combination of bumping and picking to  
 rotate the plug [1894].

What can a householder do? As an experiment, I replaced my own front

door lock. The only high-security product I could ﬁnd in a store within an

hour’s drive turned out to be a rebranded Mul-T-Lock device from Israel. It  
 took two attempts to install, jamming the ﬁrst time; it then took about a week  
 for family members to learn to use the more complex deadbolt, which can easily

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

fail open if operated carelessly. And the next time we were visited by someone  
 with an intelligence background, he remarked that in the UK only drug dealers  
 ﬁtted such locks; so if the police ever pass by, I might end up on their database  
 as a suspect. The lock did not wear well; after a few years it started sticking  
 open, and when I removed it, I noted that some ball bearings had come out.  
 This dubious improvement to my home security cost me £200 as opposed to  
 £20 for a standard product; and as in practice a burglar could always break a  
 window, our actual protection still depends more on our location and our dogs  
 than on ironmongery. Indeed, Yochanan Shachmurove and colleagues surveyed  
 the residents of Greenwich, Connecticut, and built a model of how domestic  
 burglaries varied as a function of the precautions taken; locks and deadbolts  
 had essentially no effect, as there were always alternative means of entry such  
 as windows. The most effective deterrents were alarms and visible signs of

occupancy such as cars in the drive [1709].

The situation for commercial ﬁrms is slightly better (but not much). The

usual standards for high-security locks in the USA, UL 437 and ANSI 156.30,  
 specify resistance to picking and drilling, but not to bumping; and although  
 pick-resistant locks are generally more difficult to bump, this is no guarantee.  
 Knowledge does exist about which lock designs resist bumping, but you have to  
 look for it. (Tobias’ paper, and www.toool.org, are good starting points.)

Purchasers therefore face a lemons market – as one might suspect anyway

from the glossiness, ﬂuffiness and lack of technical content of most lock vendors’  
 marketing literature. And even expensive pick-resistant locks are often poorly  
 installed by builders or OEMs; when I once had to break into a cryptographic  
 processor with a Medeco lock, I found that it turned a cam made of white metal,  
 which bent easily when we tried to lever it open. Indeed a recent security alert  
 by Tobias disclosed that one of the most popular high security deadbolts could  
 be mechanically bypassed by sliding a narrow screwdriver down the keyway,  
 catching the bolt at the end and turning it, even without defeating the extensive  
 security protections within the lock. This design had existed for more than

twenty years and the vulnerability was unknown to the manufacturer before the  
 disclosure. Many high-security installations employ similar hardware.

The second recent class of problems are *master-key attacks*. These were also

known to locksmiths for some time but were improved and published by Matt  
 Blaze1. Master-key systems are designed so that in addition to the individual  
 key for each door in a building, there can be a top-level master key that opens  
 them all – say, for use by the cleaners. More complex schemes are common;  
 in our building, for example, I can open my students’ doors while the system  
 administrators and cleaners can open mine. In pin-tumbler locks, such schemes  
 are implemented by having extra cuts in some of the pin stacks. Thus instead  
 of having a top pin and a bottom pin with a single cut between them, some of  
 the pin stacks will have a middle pin as well.

The master-key attack is to search for the extra cuts one at a time. Suppose

my key bitting is 557346, and the master key for my corridor is 232346. I make

1There was an interesting response: “For a few days, my e-mail inbox was full of angry

letters from locksmiths, the majority of which made both the point that I’m a moron, because  
 everyone knew about this already, as well as the point that I’m irresponsible, because this  
 method is much too dangerous to publish”. The paper is [259].

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

a key with the bitting 157346, and try it in the lock. It doesn’t work. I then  
 ﬁle the ﬁrst position down to 257346. As 2 is a valid bitting for the ﬁrst pin,  
 this opens the lock, and as it’s different from my user bitting of 5, I know it’s  
 the master key bitting for that pin. I will have to try on average four bittings  
 for each pin, and if three pins are master-keyed then I’ll have a master key after  
 about twelve tests. So master keying allows much greater convenience not just  
 to the building occupants but also to the serious burglar. This matters, as most  
 large commercial premises that still have metal keys use master keying. There  
 are master-keying systems that resist this attack – for example, the Austrian  
 lockmaker Evva has a system involving magnets embedded in metal keys that  
 are much harder to duplicate. But most ﬁelded systems appear vulnerable, and  
 the invention of 3-d printing has made them even more so.

A big headache with mechanical master-keying systems is revocation. Key-

holders leave, and may be dishonest or careless. They may have cut a copy of  
 their key, and sold it to an attacker. Or someone may have taken a photo of their  
 key, and used it to print a copy. Master-key attacks are important here, and  
 many expensive, pick-resistant locks actually make the problem worse. They  
 often depend on a secondary keying mechanism such as a sidebar: the keys  
 look like two normal pin-tumbler keys welded together, as in Figure 11.2. The  
 sidebar is often the same for all the locks in the building (master-keyed systems  
 generally require common sidebars in locks that share master keys). So if a bad  
 man can take a picture of a genuine key belonging to one of my students, he  
 may be able to turn it into a bump key that will open my door, and indeed  
 every door in the building, as in Figure 11.3. This may not be a problem in  
 university premises, where there’s nothing much to steal but books. But it def-  
 initely is for banks, bullion dealers and jewelers where attackers might spend  
 two years planning a raid. If such a facility had a master-keying system using  
 sidebar locks, and a staff member were even suspected of having leaked a key,  
 the prudent thing would be to replace every single lock. So while mechanical  
 locks are easy to change singly, systems that integrate hundreds of locks in one  
 building may end up locking the building owner in to the lock vendor more than  
 they lock the burglar out of the premises.

The combined effect of bumping, bad deadbolts, master-key attacks and 3-d

printing might be summarised as follows. As the tools and knowledge spread, a  
 career criminal like Charlie will be able to open almost any house lock quickly  
 and without leaving any forensic trace, while more professional attackers like  
 Bruno and Abdurrahman will be able to open the locks in most commercial  
 premises too. House locks may not matter all that much, as Charlie will just go  
 through the window anyway; but the vulnerability of most mechanical locks in  
 commercial premises could have much more complex and serious implications.  
 If your responsibilities include the physical protection of server rooms or other  
 assets, it’s time to start thinking about them.

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | |
| **Fig 11.2 – key for a sidebar lock** | | | **Fig 11.3 – sidebar bump key** |
|  |  | |  |

**13.2.5** **Electronic locks**

The difficulty of revocation is just one reason why electronic locks are getting  
 ever more market share. They’ve been around for a long time – hotels have  
 been using card locks since the 1970s. There’s a host of products, using all sorts  
 of mechanisms from contactless smartcards through PIN pads to biometrics.  
 Many of them can be bypassed in various ways, and most of the chapters of this  
 book can be applied in one way or another to their design, evaluation and assur-  
 ance. There are also some electromechanical locks that combine mechanical and  
 electronic (or magnetic) components; but it’s hard to get the locksmithing, the  
 cryptography and the electromagnetic mechanisms to work together seamlessly;  
 and you can never tell until you test them. Such locks not only cost more money  
 than simple metal locks or card locks, but often fail in interesting ways; there’s  
 a whole literature of attacks on them [1839, 1291].

But, from the viewpoint of a big company using locks to protect large and

complex premises, the problem is not so much the locks themselves but how  
 you manage dozens or hundreds of locks in a building, especially when you have  
 dozens or hundreds of buildings worldwide.

Newer buildings are starting to become aware of who is where, using mul-

tiple sensors, and integrating physical with logical access control. In an ideal  
 world, you’d know who went through which door in real time and be able to  
 line this up with security policies on information; for example, if classiﬁed ma-  
 terial is being handled, you can sound an alarm if there’s anyone in the room  
 without the right clearance. Buildings can monitor objects as well as people;  
 in an experiment at our lab, both people and devices carried active badges for  
 location tracking [1982]. Electronic systems can be fully, or almost always, on-  
 line, making revocation much easier. As well as enforcing security policy, smart  
 buildings could provide other beneﬁts, such as saving energy by turning lights  
 off and by tailoring air conditioning to the presence of occupants. But it will be  
 a long haul.

One practical problem, as we found with one organisation I worked with,

is that only a few ﬁrms sell large-scale entry control systems, and they’re hard  
 to customise. In one building project, we found the vendors’ protocols didn’t  
 support the kit we ideally wanted to use and we didn’t have the time or the  
 people to build our own entry control system from scratch. The legacy entry-  
 control vendors operate just as other systems houses do: they make their money  
 from lockin (in the economic, rather than locksmithing sense). You end up

paying $200 for a door lock that cost maybe $10 to manufacture, because of  
 proprietary cabling systems and card designs. The main limit to the lockin

is the cost of ripping and replacing the whole system – hence the proprietary  
 cabling.

We settled for a card system to control access to sections of the building,

and used Mifare contactless smartcards as they were available from multiple  
 entry-control vendors. Other buildings operated by the same organisation used  
 this system, and it allowed more complex access control policies that were a  
 function of the time of day. On the office doors themselves we had metal door  
 keys, which just have a matrix specifying which key opens which lock (this  
 means a master keying system as described above). The organisation hoped to

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

migrate to a more fully electronic system in time, once they could get the sort  
 of components that would make decent systems integration possible – such as  
 reasonably-priced door locks that run off the building’s standard Ethernet.

Then an attack was found on the underlying card system, the Mifare Classic,

sold by NXP Semiconductors. This used a proprietary cipher called Crypto-1  
 whose key had been limited to 48 bits as a result of export controls imposed  
 during the crypto wars of the 1990s, which I discuss in 26.2.7. Mifare Classic  
 had other ﬂaws including a weak random number generator and a protocol  
 that leaked keystream material via error messages. Although mostly used for  
 transport ticketing, it also had an installed base of tens of thousands of buildings  
 and was supported by several major building entry control vendors.

The Mifare Classic was partially reverse engineered by Karsten Nohl and col-

leagues in 2007 [1450]; Flavio Garcia and colleagues at Nijmegen ﬁnished the job  
 the following year, publishing a complete analysis of the chip and showing how  
 a version used in tickets for all Dutch public transport could be subverted [747].  
 NXP tried to get a court to suppress this research, but failed. The effect of these  
 attacks on Mifare was to force transport systems to deploy intrusion-detection  
 systems to detect fare dodgers; the effect on entry control systems was that  
 card keys became easy to clone. Anyone with appropriate equipment who got  
 temporary possession of a key could make a working copy, just as with a tradi-  
 tional metal key. What’s more, an ingenious attacker could deploy a fake lock  
 and copy the key of anyone who went through it. That would include cleaners,  
 whose keys open all the locks in a building, and security patrol staff whose keys  
 open all the locks in all the company’s buildings. You can even put a contact-  
 less reader into a coffee cup which you hold at chest height, to clone the keys of  
 people who keep them on lanyards.

Some lock vendors were badly hit. One vendor sold locks to hotels at near

cost price, reckoning on making its proﬁts by selling replacement card stock  
 for $1 a key. The Mifare break meant that competitors from Taiwan could

sell compatible stock for a few cents, destroying their business model. NXP  
 responded with a product that added a digital signature to the card, so that the  
 lock could tell that although it was a weak key, it was a genuine weak key.

The consequence for organisations with dozens of buildings using Mifare

locks operated by a common staff card was that to move to a more secure lock  
 they had to either replace all the locks and cards at once, or else stick with NXP,  
 who produced two series of successor cards. The ﬁrst were ‘hardened’ classic  
 cards that still used the weak Crypto 1 cipher but ﬁxed the implementation  
 mistakes that made the initial attacks easier; but as the underlying cipher is  
 weak, these were broken too [1316]. The second product line used better algo-  
 rithms, with the DESﬁre card, for example, using two-key triple-DES. However  
 David Oswald and Christof Paar promptly discovered a timing attack on the  
 DESﬁre [1484]. The problem was partly mitigated by entrepreneurial lock ven-  
 dors who started to produce card readers that could cope with multiple product  
 lines; one will cope not only with Mifare but also with NFC (for Android phones)  
 and Bluetooth (for phones made by Apple, which locks down the NFC chip to  
 Apple pay). Others are embracing new technologies such as the new 802.15.4z  
 standard for UWB radio which I mentioned in section 4.3.1.

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

In short, NXP managed to maintain much of its lock-in by migrating its

customers to new products but at some cost in security. Some of the externalities  
 this created were captured by more alert card reader vendors. However the

whole ﬁeld has become way too complex for the traditional lock buyer, who was  
 an architect or building services manager. That’s yet another reason why the  
 CISO’s security engineering team needs to take an interest in physical security  
 too.

**13.3** **Alarms**

Alarms are used to deal with much more than burglary. Their applications

range from monitoring freezer temperatures in supermarkets (so staff don’t ‘ac-  
 cidentally’ switch off freezer cabinets in the hope of being given food to take  
 home), right through to improvised explosive devices in conﬂict zones that are  
 often booby-trapped. However, it’s convenient to discuss them in the context  
 of burglary and of protecting server rooms, bank vaults or art galleries. Alarms  
 also give us a good grounding in the wider problem of service denial attacks,  
 which are an issue everywhere from gaming to electronic warfare.

Standards for building alarms vary between countries and between different

types of risk. As with locks, you’ll normally use a specialist ﬁrm for this kind  
 of work; but you must be aware of the technical issues. My own professional  
 experience has ranged from the alarms built into automatic teller machines,  
 through the security of the communications used by an alarm system for large  
 risks such as wholesale jewelers, to the systems used to protect bank computer  
 rooms.

An alarm in a server room is well protected from tampering (at least by

outsiders). So I’ll take as my case study an art gallery. This has the interesting  
 design problem of safeguarding precious objects and also displaying them. At-  
 tackers can come in during the day as members of the public, and we’ll assume  
 that the attacker is Bruno – the educated professional art thief. The movie  
 scriptwriter’s view of Bruno is that he organizes cunning attacks on alarms,  
 having spent days poring over the building plans in the town hall:

**How to steal a painting (1)**

A Picasso is stolen from a gallery with ‘state-of-the-art’ alarm sys-  
 tems by a thief who removes a dozen rooﬁng tiles and lowers himself  
 down a rope so as not to activate the pressure mats under the carpet.  
 He grabs the painting, climbs back out without touching the ﬂoor,  
 and is paid by a wealthy gangster who commissioned the theft.

The press loves this kind of stuff, and it does happen from time to time.

Reality is both simpler and stranger. Let’s work through the threat scenarios  
 systematically.

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

**13.3.1** **How not to protect a painting**

A common mistake when designing alarm systems is to be captivated by the  
 latest sensor technology. There’s a lot of impressive stuff on the market, such as  
 a ﬁber optic cable which you can loop round protected objects and which will  
 alarm if the cable is stretched or relaxed by less than 100nm – a ten-thousandth  
 of a millimeter. Isn’t modern science marvellous? So the na¨ıve art gallery owner  
 will buy a few feet of this magic cable, glue it to the back of his prize Picasso  
 and connect it to an alarm company. That would detect the chap in the bosun’s  
 chair. So how would you defeat it? Well, that’s easy.

**How to steal a painting (2)**

Bruno comes in as a tourist and hides in a broom cupboard. At one  
 in the morning, he emerges, snatches the painting and heads for the  
 ﬁre exit. Off goes the alarm, but so what! In less than a minute,  
 he’ll be on his motorbike. By the time the cops arrive twelve minutes  
 later he’s gone.

Alarms are rarely integrated well with building entry controls. Many design-

ers don’t realise that unless you can positively account for all the people who’ve  
 entered the premises during the day, you’d better take precautions against the  
 ‘stay-behind’ villain – even if this is only an inspection tour after the gallery  
 has closed. Serious physical security means serious controls on people. In fact,  
 the ﬁrst recorded use of the RSA cryptosystem – in 1978 – was not to encrypt  
 communications but to provide digital signatures on credentials used by staff to  
 get past the entry barrier to a plutonium reactor at Idaho Falls. The creden-  
 tials contained data such as body weight and hand geometry [1747, 1751]. But  
 I’m still amazed by the ease with which building entry controls are defeated at  
 most secure sites I visit – whether by mildly technical means, such as sitting  
 on somebody else’s shoulders to go through an entry booth, or (most often) by  
 helpful people holding the door open.

What’s more, the alarm response process often hasn’t been thought through.

(The *Titanic Effect* of over-reliance on the latest technology often blinds people  
 to common sense.)

So we mustn’t think of the alarm mechanism in isolation. As I mentioned

above, a physical protection system has several steps: *deter – detect – alarm –*  
 *delay – respond*, and the emphasis will vary from one application to another. If  
 our opponent is Derek or Charlie, we’ll mostly be concerned with deterrence.  
 At the sort of targets where Abdurrahman might try to steal ﬁssile materials,  
 an attack will almost certainly be detected; the main problem is to delay him  
 long enough for the Marines to arrive. Bruno is the most interesting case as we  
 won’t have the military budget to spend on keeping him out, and there are many  
 more premises whose defenders worry about Bruno than about Abdurrahman.  
 So you have to look carefully and decide whether the bigger problem is with  
 detection, with delay or with response.

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

**13.3.2** **Sensor defeats**

Burglar alarms use a wide range of *sensors*, including:

*•* vibration detectors, to sense fence disturbance, footsteps, breaking glass

*•* switches on doors and windows;

*•* passive infrared devices to detect body heat;

*•* motion detectors using ultrasonics or microwave;

*•* invisible barriers of microwave or infrared beams;

*•* pressure pads under the carpet, which in extreme cases may extend to

*•* video cameras, nowadays often with movement detectors and even face de-  
 center;

*•* movement sensors on equipment, ranging from simple tie-down cables

Most sensors can be circumvented. Fence disturbance sensors can be defeated

by vaulting the fence; motion sensors by moving very slowly; door and window  
 switches by breaking through a wall. Designing a good combination of sensors  
 comes down to skill and experience (with the latter not always guaranteeing the  
 former). A standard, if slightly dated, reference on sensor installation is [408].

The main problem is limiting the number of false alarms. Ultrasonics don’t

perform well near moving air such as central heating inlets, while vibration  
 detectors can be rendered useless by traffic. Severe weather, such as lightning,  
 will trigger most systems, and a hurricane can swamp a town’s police force  
 not just with rain but with thousands of false alarms. In some places, even  
 normal weather can make protection difficult: how do you defend a site where  
 the intruder might be able to ski over your sensors (and even over your fence)2?

But regardless of whether you’re in Alaska or Arizona, the principal dilemma

is that the closer you get to the object being protected, the more tightly you  
 can control the environment and so the lower the achievable false alarm rate.  
 Conversely, at the perimeter it’s hard to keep the false alarm rate down. But to  
 delay an intruder long enough for the guards to get there, the outer perimeter  
 is exactly where you need reliable sensors.

**How to steal a painting (3)**

So Bruno’s next attack is to wait for a dark and stormy night. He  
 sets off the alarm somehow, taking care not to get caught on CCTV

2For an instructive worked example of intruder detection for a nuclear power station in a

snow zone see [173].

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

or leave any other hard evidence that the alarm was a real one. He  
 retires a few hundred yards and hides in the bushes. The guards  
 come out and ﬁnd nothing. He waits half an hour and sets off the  
 alarm again. This time the guards don’t bother, so in he goes.

False alarms – whether induced deliberately or not – are the bane of the in-

dustry. They are a denial-of-service attack on the alarm response force. Experi-  
 ence from electronic warfare is that a false alarm rate of greater than about 15%  
 degrades the performance of radar operators; and most intruder alarm respon-  
 ders are operating well above this threshold. Deliberately induced false alarms  
 are especially effective against sites that don’t have round-the-clock guards.  
 Many police forces have a policy that after a certain number of false alarms  
 from a given site (typically three to ﬁve per year), they will no longer send a  
 squad car there until the alarm company, or another keyholder, has been there  
 to check.

False alarms degrade systems in other ways. The rate at which they are

caused by environmental stimuli such as weather conditions and traffic noise  
 limits the sensitivity of the sensors that can usefully be deployed. Also, the  
 very success of the alarm industry has greatly increased the total number of  
 alarms and thus decreased police tolerance of false ones. A common strategy is  
 to have remote video surveillance as a second line of defense, so the customer’s  
 premises can be inspected by the alarm company’s dispatcher; many police  
 forces prioritize alarms conﬁrmed in this way [979]. But even video links are  
 not a panacea. The attacker can disable the lighting, start a ﬁre, or set off alarms  
 in other buildings in the same street. The failure of a telephone exchange, as a  
 result of a ﬂood or hurricane, may lead to opportunistic looting.

After traffic and weather, Bruno’s next ally is time. Vegetation grows into

the path of sensor beams, fences get slack so the vibration sensors don’t work  
 so well, the criminal community learns new tricks, and meanwhile the sentries  
 become complacent.

So sites needing serious physical protection often have several perimeters: an

outer fence to keep out the drunks and the wildlife; then level grass with buried  
 sensors, an inner fence with an infrared barrier, and ﬁnally a massive enough  
 building to delay the bad guys until the cavalry gets there. The regulations laid  
 down by the International Atomic Energy Agency for sites that hold more than  
 15g of plutonium are an instructive read [949].

At most sites this kind of protection will be too expensive. And even if you

have loads of money, you may be somewhere like Manhattan or Hong Kong  
 where real estate’s expensive: if you have to be near the exchange to trade  
 quickly enough, your bank computer room may just be a ﬂoor of an office  
 building and you’ll have to protect it as best you can. A good example comes  
 from a gang of jewel thieves in Florida who targeted retail stores that shared  
 a wall with a store such as a nail salon that had no reason to install an alarm.  
 They broke in there, then cut through the wall into the jewelry store [1215].

Anyway, the combination of sensors and physical barriers still makes up less

than half the story.

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

**13.3.3** **Feature interactions**

Intruder alarms and barriers interact in a number of ways with other services.  
 The most obvious of these is electricity. A power cut will leave many sites dark  
 and unprotected, so a serious alarm installation needs backup power. A less  
 obvious interaction is with ﬁre alarms and ﬁreﬁghting.

**How to steal a painting (4)**

Bruno visits the gallery as a tourist and leaves a smoke grenade on  
 a timer. It goes off at one in the morning and sets off the ﬁre alarm,  
 which in turn causes the burglar alarm to ignore signals from its  
 passive infrared sensors. (If it doesn’t, the alarm dispatcher will

ignore them anyway as he concentrates on getting the ﬁre trucks  
 to the scene.) Bruno smashes his way in through a ﬁre exit and  
 grabs the Picasso. He’ll probably manage to escape in the general  
 chaos, but if he doesn’t he can always claim he was a public-spirited  
 bystander who saw the ﬁre and risked his life to save the town’s  
 priceless cultural heritage. The police might not believe him, but  
 they’ll have a hard time convicting him.

The largest ever burglary – the theft in 2019 of about a billion Euros’ worth

of treasures from the Gr¨une Gew¨olbe in Dresden, the home of Augustus the  
 Strong’s treasure chamber and a dozen other rooms of priceless antiquities, used  
 arson [469]. A ﬁre at a nearby building site disabled the local electricity sub-  
 station, turning off local streetlights as well as the power to the museum [1045].  
 Its security guards eventually saw intruders on CCTV and called the police, but  
 they didn’t get there in time.

The interaction between ﬁre and intrusion is always difficult. At nuclear

reactors, there’s typically a rule that if a bomb is discovered, the site is locked  
 down, with no-one allowed in or out; and a ﬁre safety rule that in the event  
 of a blaze, much of the staff have to be evacuated (plus perhaps some of the  
 local population too). This raises the interesting question of which rule prevails  
 should a bomb ever go off. And some ﬁre precautions may only be used if

you can keep out innocent intruders. Many server rooms have automatic ﬁre  
 extinguishers, and this often means ﬂooding with carbon dioxide. A CO2 dump  
 can be lethal to untrained people: you have to get out of the room on the air  
 you have in your lungs as visibility drops to a few inches and you’re disoriented  
 by the terrible shrieking noise of the dump. A nitrogen dump is less spectacular  
 but also lethal; a falling oxygen level doesn’t provoke a panic response the way  
 a rising CO2 level does.

But the most severe feature interactions are between alarms and communi-

cations.

**13.3.4** **Attacks on communications**

A sophisticated attacker is at least as likely to attack the communications as  
 the sensors. Sometimes this will mean the cabling between the sensors and the

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

alarm controller.

**How to steal a painting (5)**

Bruno goes into an art gallery and, while the staff are distracted, he  
 cuts the wire from a window switch. He goes back that evening and  
 helps himself.

It’s also possible that one of your staff, or a cleaner, will be bribed, seduced

or coerced into creating a vulnerability. In Britain’s biggest robbery, in February  
 2006 from the Securitas Cash Management depot in Tonbridge, Kent, robbers  
 took the manager and his family hostage, pretending to be police officers. They  
 then compelled him to let them in, taking £53,116,760; although ﬁve of the  
 robbers were caught and jailed, others escaped and most of the money was  
 never recovered. When I worked in banking back in the 1980s, we took care to  
 brief our cash centre managers that the controls were there to stop their families  
 being taken hostage. It’s great to have knowledgeable and motivated defenders,  
 but the dual-control defence must be carried through in depth. High-value

sites with capable defenders insist that alarm maintenance and testing be done  
 by two people rather than one. Even then, dual control isn’t always enough,  
 especially if your opponent is Abdurrahman rather than Bruno. In Britain’s  
 fourth-largest ever robbery, the Provisional IRA kidnapped two keyholders at  
 the Northern Bank in December 2004 and held their families at gunpoint, to  
 force them to let them into the bank’s Belfast headquarters the next day. The  
 terrorists escaped with £26.4m, and in order to make most of the money useless,  
 the £50 notes they stole were withdrawn from circulation. Another edge case is  
 the prison system, where attacks on sensors, cabling and indeed the very fabric  
 of the building are so frequent that a continuing program of test and inspection  
 is essential. It can be useful to ask yourself, “How would I do this differently if  
 half my staff were convicts on day release?” and “How would I cope if a handful  
 of my staff were working for an organisation that decided to rob me?” I will  
 discuss the implications of dual control in more detail in the chapter on banking  
 and bookkeeping.

The old-fashioned way of protecting the communications between the alarm

sensors and the controller was physical: lay multiple wires to each sensor and  
 bury them in concrete, or use armored gas-pressurized cables. The more modern  
 way is to encrypt the communications [706]. So how do you attack those?

**How to steal a painting (6)**

Bruno phones up a rival gallery claiming to be from the security  
 company that handles their alarms. He says that they’re updating  
 their computers so could they please tell him the serial number on  
 their alarm controller unit? An office junior helpfully does so – not  
 realising that the serial number on the box is also the crypto key that  
 secures the communications. Bruno buys an identical controller for  
 $200 and now has a functionally identical unit which he splices into  
 his rival’s phone line. This continues to report ‘all’s well’ even when  
 it isn’t.

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

Substituting bogus alarm equipment, or a computer that mimics it, is known

as ‘spooﬁng’. There have been reports for many years of black boxes that spoof  
 various alarm controllers. As early as 1981, thieves made off with $1.5 million  
 in jade statues and gold jewelry imported from China, driving the importer  
 into bankruptcy. The alarm system protecting its warehouse in Hackensack,  
 New Jersey, was cut off. Normally that would trigger an alarm at a security  
 company, but the burglars attached a homemade electronic device to an external  
 cable to ensure continuous voltage [861]. And I mentioned in section 13.2.3 how  
 Britain’s biggest burglary involved jamming the alarm signal.

With the better modern systems, either the alarm controller in the vault

sends a cryptographic pseudorandom sequence to the alarm company, which  
 will assume the worst if it’s interrupted, or the alarm company sends periodic  
 random challenges to the controller which are encrypted and returned, just as  
 with IFF. However, the design is often faulty, having been done by engineers  
 with no training in security protocols. The crypto algorithm may be weak, or its  
 key may be too short (whether because of incompetence or export regulations).  
 Even if not, Bruno might be able to record the pseudorandom sequence and  
 replay it slightly more slowly, so that by early Monday morning he might have  
 accumulated ﬁve minutes of ‘slack’ to cover a lightning raid.

An even more frequent cause of failure is the gross design blunder. One is

making the crypto key equal to the device serial number. This often appears  
 in the purchase order, invoice, and other paperwork which lots of people get to  
 see. (It’s a good idea to buy your alarm controller for cash. This also makes  
 it less likely that you’ll get one that’s been ‘spiked’. But big ﬁrms often have  
 difficulty doing this.)

By now you’ve probably decided not to go into the art gallery business. But

I’ve saved the best for last. Here is the most powerful attack on burglar alarm  
 systems. It’s a variant on (3) but rather than targeting the sensors, it goes for  
 the communications.

**How to steal a painting (7)**

Bruno cuts the phone line to his rival’s gallery and hides a few hun-  
 dred yards away in the bushes. He counts the number of men in  
 blue uniforms who arrive, and the number who depart. If the two  
 numbers are equal, then it’s a fair guess the custodian has said, ‘Oh  
 bother, we‘ll ﬁx it in the morning’, or words to that effect. He now  
 knows he has several hours to work.

This is more or less the standard way to attack a bank vault, and it’s also

been used on computer installations. The modus operandi can vary from simply  
 reversing a truck into the phone company’s kerbside junction box, to more so-  
 phisticated attempts to cause multiple simultaneous alarms in different premises  
 and swamp the local police force. (This is why it’s so much more powerful than  
 just rattling the fence.)

In one case, thieves in New Jersey cut three main telephone cables, knocking

out phones and alarm apparatus in three police stations and thousands of homes  
 and businesses in the Hackensack Meadowlands. They used this opportunity to

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

steal Lucien Piccard wristwatches from the American distributor, with a value  
 of $2.1 million wholesale and perhaps $8 million retail [861]. In another, an  
 Oklahoma deputy sheriff cut the phone lines to 50,000 homes in Tulsa before  
 burgling a narcotics warehouse [1923]. In a third, a villain blew up a telephone  
 exchange, interrupting service to dozens of shops in London’s jewelry quarter.  
 Blanket service denial attacks of this kind, which saturate the response force’s  
 capacity, are the burglarious equivalent of a nuclear strike. The move from

phones to broadband has changed nothing; instead of cutting the BT phone  
 line, a British burglar now cuts the BT Openreach DSL line, which is the same  
 piece of copper, but now carrying digital signals. In places where the cable

company carries broadband, you cut that; so an American burglar will learn  
 how to recognise Comcast cables, if they’re the local supplier. What’s more,  
 alarm services often partner with the broadband providers, leaving the ﬁrms  
 that supply the sensors competing in low-cost volume markets where they don’t  
 have the incentive to do anything sophisticated.

Future attacks might not involve snips or explosives, but a distributed denial-

of-service attack on network facilities. Rather than causing all the alarms to go  
 off in the neighborhood of a local telephone exchange (which could be protected  
 to some extent by swamping it with police), it might be possible to set off several  
 thousand alarms all monitored by the same alarm company, or by attacking  
 some other component in the response chain. This might include attacks on  
 police communications, or on 4G networks now that these are used for more  
 alarm communications than wireline. One way of minimising the number of  
 vulnerable components is by making the alarm communications anonymous, so  
 that service-denial attacks can’t be targeted [1423].

For years, the rule in the London insurance market (which does most of the

world’s major reinsurance business) was that alarm controllers in premises in-  
 sured for over £20 million must have two independent means of communication.  
 The traditional approach was one alarm using wireline communications and one  
 using cellular radio; by 2019 we’re seeing offerings that use two different 4g ra-  
 dio services. This opens the prospect of jamming, as used in the 2015 Hatton  
 Garden burglary mentioned in section 13.2.3. In the nuclear world, IAEA reg-  
 ulations stipulate that sites containing more than 500g of plutonium or 2kg of  
 U-235 must have both their alarm control center and an armed response force  
 on the premises [949].

Where the asset you’re protecting isn’t a vault but a hosting center, the

network is also critical to your operations. There’s little point in having eight-  
 inch concrete walls and roofs if the single ﬁbre connecting you to the world  
 runs through a kerbside junction box. You’ll want at least two buried ﬁbres  
 going to at least two different telcos – and you will want them to be using  
 switches and routers from two different vendors. Even so, the simplest way

for a knowledgeable opponent to take out a hosting centre is usually to cut its  
 communications. That’s one reason why small ﬁrms have two centres and the  
 big service ﬁrms have dozens. If you’re not operating at cloud scale, you may  
 want to ask yourself: who wants to dig, who knows where to, and would you  
 detect them in time?

Finally, it’s worth bearing in mind that many physical security incidents

arise from angry people coming into the workplace – whether spouses, former

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

employees or customers. In countries where private ownership of ﬁrearms is  
 widespread, you have to plan for shooters.

**13.3.5** **Lessons learned**

The reader might still ask why a book that’s essentially about security in com-  
 puter systems should spend several pages describing walls, locks and alarm  
 systems. There are more reasons than the obvious ones.

*•* Most locks can be defeated. Metal keys can be photographed and forgeries  
 can often be bumped. Card keys can often be cloned if you can get close.  
 So alarms matter.

*•* Dealing with service denial attacks is the hardest part of many secure  
 us applicable knowledge and experience.

*•* One very general lesson is that one must look at the overall system – from

*•* Another is the observation that the outermost perimeter defenses are the  
 reliance can be placed.

*•* The trade-off between the missed alarm rate and the false alarm rate – the  
 engineering.

*•* It’s hard work to keep guards alert, especially in jobs where almost all  
 US Transportation Security Administration puts test guns into suitcases,  
 whether physically or using software in the X-ray machines. They have  
 found that only about 20% of threats get through if you test screeners  
 several times per checkpoint per shift, but this rises to 60–75% if you only  
 test once [713].

*•* Failure to understand the threat model – designing for Charlie and hoping  
 actually goes wrong, not just what crime writers think goes wrong.

*•* And ﬁnally, you can’t just leave the technical aspects of a security engi-  
 fall down between the cracks.

There are other applications where the experience of the alarm industry is

relevant. In a later chapter, I’ll discuss tamper-resistant processors that are  
 designed to detect attempts to penetrate them and respond by destroying all  
 their cryptographic key material.

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

**13.4** **Summary**

Security engineers have to deal with physical protection as well as with com-  
 puters and cipher systems. Just as the conﬂuence of computers and telecomms  
 saw computer-industry equipment and methods displace the old phone-company  
 ways of doing things, so the automation of physical protection systems is steadily  
 bringing the world of barriers, locks and alarms within our orbit. The move to  
 ‘smart buildings’ means entry controls, alarms and system security integrated  
 with energy management and much else. The design, implementation and man-  
 agement of such complex artefacts will increasingly be the job of systems security  
 people.

In this chapter, I highlighted a few things worth noting. First, environmental

deterrence matters; things like architecture, landscaping and lighting can make  
 a real difference to the likelihood of intrusion.

Second, locks are not as secure as you might think. Recent developments

in covert entry technology have led to wide publication of attacks that com-  
 promise most mechanical locks, and even the expensive ‘high-security’ offerings.  
 Many card key systems are also vulnerable, as the most common products were  
 compromised by US export controls in the 1990s and the process of replacing  
 them with better ones has been held up by industry structures and incentives.  
 Knowing what’s good and what’s not is not possible unless you understand at  
 least the basics of cryptography, protocols and tamper-resistance; it’s a job for  
 security engineers, not for retired cops.

Third, there’s quite a lot to learn from the one aspect of physical security

that’s already fairly well automated, namely alarms. Alarms provide us with  
 a good example of a system whose security policy hinges on availability rather  
 than on conﬁdentiality or integrity. They can give us some useful insights when  
 dealing with service-denial attacks in other contexts.

**Research Problems**

At the strategic level, the conﬂuence of physical security and systems security  
 is bound to throw up all sorts of new problems. I expect that novel research  
 challenges will be found by those who explore the information / physical security  
 boundary; an example that came up as we were going to press in 2020 is the use  
 of acoustic side-channels. Given a decent microphone, you can record the clicks  
 as a Yale key is pushed into a keyway, and use it to deduce the key bitting [1225].  
 No doubt there will be more results of this kind. From the viewpoint of security  
 economics, the problems of the locksmithing industry would make an excellent  
 thesis topic: how the vulnerabilities found in Mifare and other products have  
 been dealt with all along the supply chain is a complex story that nobody, as  
 far as I’m aware, has really analysed systematically. It might be fascinating to  
 compare this with how other complex ecoystems have responded to the security  
 failure of key components.

At the technical level, we will probably need better mechanisms for specifying

and implementing policy engines that can manage both physical and other forms

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

of protection. As for low-level mechanisms, we could do with better tools to  
 manage keys in embedded systems. As one engineer from Philips put it to me,  
 will the smart building mean that I have to perform a security protocol every  
 time I change a lightbulb? And will smart buildings end up being open, in the  
 sense that so many different service ﬁrms will have access to the plans that all  
 capable opponents must be assumed to have a copy? But if you really want the  
 bad guys to not know the precise location of the alarm response centre in your  
 nuclear power station, how do you keep that information conﬁdential? All your  
 contractors will happily claim to be ISO 27001 certiﬁed, but then so is almost  
 every ﬁrm that owns up to a big data breach.

**Further Reading**

The classic reference on alarm systems is [173] while some system issues are  
 discussed in [1423]. Resources for speciﬁc countries are often available through  
 trade societies such as the American Society for Industrial Security [45], and  
 though the local insurance industry; many countries have a not-for-proﬁt body  
 such as Underwriters’ Laboratories [1916] in the USA, and schemes to certify  
 products, installations or both. For progress on lock bumping and related topics,  
 I’d monitor the Toool group, Marc Weber Tobias, and Matt Blaze; Matt has also  
 written on safecracking [261]. Research papers on the latest sensor technologies  
 appear at the IEEE Carnahan conferences [952]. Finally, the systems used to  
 monitor compliance with nuclear arms control treaties are written up in [1748].

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