CHAPTER

1

Insecurity Engineering and the Design of Locks

Today's manufacturing technology, software, and hardware design capabilities mean virtually any company can produce a lock if it has the right capital resources. The challenge facing manufacturers, however, is security and the ability to make a lock sufficiently resistant to different forms of attack.

Through my consulting for most of the world's largest lock manufacturers, I've discovered that locks fail for two fundamental yet interrelated reasons:

1. They fail because everyone involved in the process may lack the imagination to anticipate potential and actual security vulnerabilities.
2. They fail due to a lack of engineering expertise about bypass techniques.

This lack of imagination and expertise can have significant and costly ramifications for manufacturers in terms of security failures, legal damages, an inability to meet state and federal standards, and a loss of credibility from their customers. Ultimately, it often places these unaware consumers at risk.

To imagine a vulnerability, it is a prerequisite that you understand and correlate different attack modes and current or proposed designs. My father, a mechanical engineer, encouraged me from the age of five to take things apart, learn how they worked, and figure out how to break them. Before becoming a lawyer, I began my career by discovering and exploiting security and legal vulnerabilities in lock, safe, and security system design. It was during this time that I realized the ramifications of insecurity engineering.

What Is Insecurity Engineering?

In the simplest of terms, *insecurity engineering* is a lack of expertise and understanding of how locks work and the various ways you can make them fail. It creates insecurity, contrary to a lock's *raison d'etre* (i.e., reason to exist). Insecurity engineering results in a failure to "connect the dots" from simple design errors to compound failures, which finally results in the compromise of components that can potentially defeat security. It's an engineer designer's lack of creativity and imagination to consider a "What if?" scenario. Finally, it's the absence of a complete understanding or knowledge of past mistakes in similar designs. Such insights can only be acquired via experience, by working with seasoned engineers and having a full familiarity with what has been designed and patented to remedy past defects or deficiencies that originally created or allowed the vulnerabilities.

Insecurity engineering is also about legal liability and the failure to understand that defective designs ultimately will invite lawsuits and damage awards. If someone is hurt or a company sustains damage in whatever form, it can cost a manufacturer a monetary loss *and* reputational injury. As the name implies, insecurity engineering highlights the need to forecast, discover, and prevent insecure designs from reaching the end user.

This concept, which is discussed more in Chapter 3, ensures that those responsible for the design of locks, safes, and security systems have the requisite expertise to assess a product from many different perspectives, starting with its inception and continuing through analysis and testing by a vulnerability assessment team. *Competent insecurity engineering*, as the term implies, is an absolute prerequisite to successfully developing any security-related product.

Primary Responsibilities of Lock Manufacturers

Let's begin by discussing the primary missions of lock manufacturers. Lock manufacturers are responsible for making products that securely perform their intended function or purpose. I can identify at least nine critical responsibilities for companies that produce locks and related security systems, all based on a foundation of competent insecurity engineering practices and programs. Here are those nine critical responsibilities:

1. Invent or improve on state-of-the-art technology.
2. Develop and continue to analyze and improve on earlier designs.
3. Understand all vulnerabilities and imagine new ones.
4. Apply design expertise to currently manufactured and new products.

5. Protect intellectual property (IP) from infringement.
6. Ensure that IP produced and sold is secure and will not cause injury or harm.
7. Do not produce defective products.
8. Fully understand product liability and its critical importance.
9. Initiate a disclosure program about serious vulnerabilities.

Let's break down these nine responsibilities further.

NOTE **For more information on security engineering, check out *Security Engineering, Third Edition,* by Ross Anderson. It's a must-read for Internet technology (IT) professionals, risk managers, and computer engineers and covers system design, emerging technologies, and what can go wrong when system developers don't understand security and vulnerability.**

Invent or Improve On State-of-the-Art Technology

Manufacturers should strive to develop, improve, or create new designs to enhance their products, improve overall security, and increase their capability to secure people, facilities, assets, and information. Over the past 200 years, companies have succeeded because they innovated new locking technologies and implemented the latest advancements. The lifeblood of every manufacturer is its creation of IP and the allowance of patents. *Intellectual property* encompasses patents, trademarks, and copyrights and is the foundation of almost every product for every serious lockmaker because patents ensure protection for their work and creativity for 20 years under current patent laws. Customers rely on this protection when they buy *security technology*—a gauge of the state-of-the-art technology in the industry—which is essential for successful product marketing.

Develop and Continue to Analyze and Improve On Earlier Designs

Manufacturers should be vigilant about issues from past and present designs to ensure that they're currently aware of new attacks that could affect the security of their products. Even if a locking system was developed several years ago, if it's currently being sold, any vulnerability can be the basis of a liability. A monitoring system should be set up for every new product, not only for receiving customer feedback but also for discovering or publishing security issues.

Understand All Known Vulnerabilities and Imagine New Ones

A continuous review of products must occur to ensure that a manufacturer's products are secure against current attacks. The Simplex 1000 push-button lock is a perfect example: a mechanical system that was initially patented around 1965 but became the subject of a class action lawsuit in 2010 because it could easily be defeated by a strong magnetic field. Its manufacturer did not review it for or imagine any vulnerabilities, which is critical to securing a lock against attacks.

Apply Expertise to Currently Manufactured and New Products

Manufacturers must maintain and develop an engineering team with the requisite expertise to assess design defects of current and new products in terms of their security. Doing so is imperative to creating locks that can withstand attacks. (You'll find this issue addressed more fully in Chapters 2 and 3).

Protect Intellectual Property (IP) from Infringement

Manufacturers must maintain a corporate policy that stresses the protection of IP in locks and security systems, for the benefit of both the manufacturer and its customers. If patents and trademarks are not constantly monitored for infringement, they will not protect the property's owner or anyone relying on their enforcement. A great example is discussed in Part VI: a large manufacturer held patents for key designs with interactive elements that were reproduced and sold in large quantities in major metropolitan areas by counterfeiters. The manufacturer's inability to protect its IP resulted in economic losses to the manufacturer and many locksmiths and presented security risks to critical customers.

Ensure That IP Produced and Sold Is Secure and Will Not Cause Injury or Harm

From a legal and ethical standpoint, the primary responsibility of a lock manufacturer is to ensure that whatever products it offers for sale are secure and will not harm customers or their facilities due to improper use or the circumvention of security. Any insecurity or harm can potentially damage a manufacturer's credibility, not to mention harming its consumers.

Do Not Produce Defective Products

The term *defective* can be defined in many ways, including design, manufacturing, and warning. In the context of this book, it relates primarily to security vulnerabilities that are present and can or should be predicted. It is imperative

that lock manufacturers ensure their products are not defective, to protect the integrity of their companies and products.

Fully Understand Product Liability and Its Critical Importance

Liability considerations must be built into every project and product from its inception until it's sold to its end users. A lock manufacturer's employees should be trained to be sensitive to legal issues that can result in a company's legal liability, which could even extend to its employees. Protocols should be set in place to document in detail every security-related product's development, modifications, and fixes to minimize the company's exposure to lawsuits and damages. Management, in addition to every employee, must be cognizant of the multiple tenets of product liability law and how to guard against tort liability and contract violations while protecting trade secrets, non-disclosure agreements, and confidentiality.

Initiate a Disclosure Program about Serious Vulnerabilities

Once vulnerabilities are discovered and their seriousness is verified, there must be a process to properly disclose all product defects affecting the security of critical customers or even the general public. It is suggested that this process detail warnings about security issues, including those involved with master key systems, key copying, and capabilities to circumvent key control. (Such a process is discussed in more detail in Chapter 2.)

Several years ago, I introduced and promoted the concept of *unethical non-disclosure,* where lock manufacturers were aware of vulnerabilities but failed to disclose them to customers or did nothing to remedy design problems. As a lawyer, I counseled my manufacturing clients to be up front with their customers and the public about their security-related issues. Customers have a right to rely on a manufacturer's expertise in lock design and an expectation to be forewarned about potential or known defects that could place them at risk. It is unethical for a company to fail to disclose or warn its customers about a significant flaw.

Examples of Insecurity Engineering Failures

Throughout this book, I cite insecurity engineering failures that have led to extensive product delays, product recalls, redesign, and significant legal damages. Such failures are more fully described in Part VI, but I summarize a few in this section as a sobering reminder of what can happen when there's a lack of hardware and software design expertise as it applies to lock security.

Locks can be circumvented in several ways. Here are a few examples:

- *Bumping*: A technique based on the application of force to pin tumblers by a special key, which has caused many security issues for the world's lock manufacturers (see Figure 1-1).

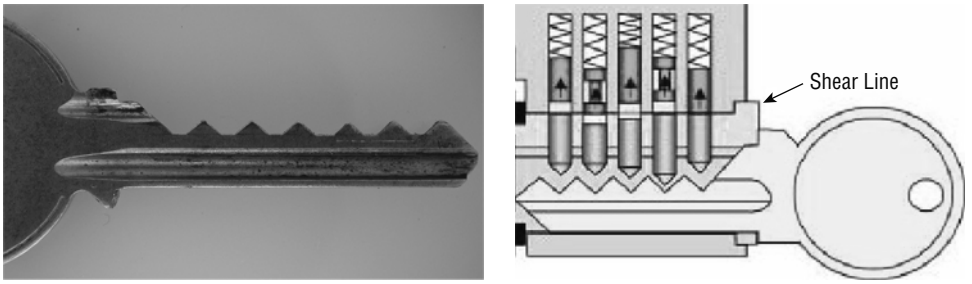


Figure 1-1a, 1b: A bump key can be produced from virtually any key blank for a pin tumbler lock by cutting all the bitting to the lowest possible depth. (a) A bump key for Postal Service locks. (b) What happens when the key is forced forward to cause the bottom and top pins to split at the shear line.

- *Shimming*: A technique in which fine wires are employed to compromise various lock types by exploiting tiny openings that allow the insertion of shims to access critical components.
- *Impressioning*: A technique in which an impression of a tubular pin tumbler lock is taken with plastic pens to produce a key.

The following examples demonstrate common design errors resulting from engineers failing to consider the basic laws of physics. These errors have cost my clients redesign expenses, product delays, recalls, lawsuits, federal investigations, injuries, and even deaths. Although this example list is not exhaustive, it does include all instances of insecurity engineering failures due to simple attacks that were covert and left no traces.

However, design failures are not limited to the application of the laws of physics. They are also about imagination and the ability to assess each lock component and how these components can be used to cause a compromise. They encompass every aspect of design, from key control to tolerances to the interaction of components. It's about the information derived from how each component works and what can be discovered about the inner working of a lock and, ultimately, the secrets that will enable it to be decoded or opened.

TIP **For more about lock-breaking techniques, see Chapter 12. In addition, you'll find multiple detailed lock images and diagrams throughout the book that illustrate critical parts of different lock types and how they work.**

The following examples detail the various types of locks and their design errors:

Spring-loaded locking mechanism: Many locks employ springs to retain critical components in place until activated by a key or other credential. Any spring-biased component is subject to potential compromise through the application of force and the laws of physics. Springs control other movable elements that can be subject to such attacks.

One design flaw was exploited by someone using a plastic screwdriver handle to release the locking mechanism of a newly developed laptop lock ready for production. A single strike with the plastic mass (i.e., the handle of the screwdriver) against the locked cylinder released the spring-based internal mechanism and unlocked and released the lock from the computer.

High-security cylinders with side bit milling and a sidebar: As described in Chapter 14, there are numerous techniques to make locks more difficult to compromise. One technique is the addition of what I call side bit milling with a second set of locking pins that interact with the key. The second set of bitting is designed to control more locking tumblers (see Figure 1-2).

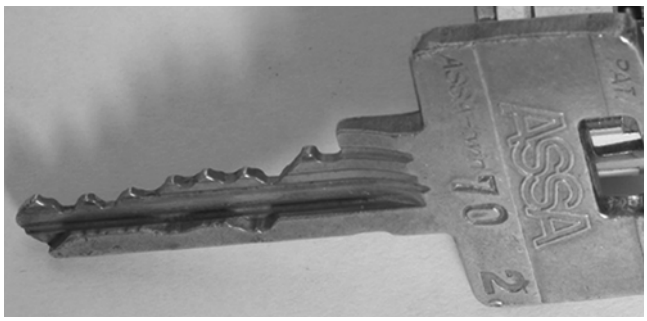


Figure 1-2: A key with side bit milling provides another security layer and can make picking and bumping more complicated.

It was believed that the design of this high-security mechanical lock with a secondary locking system using side bit milling pins would prevent bumping or another type of defeat. When attackers altered the physical design of the milling, I demonstrated that these locks could still be defeated, especially through lock bumping (which is more fully discussed and described in Chapter 18). Bumping, in the simplest of terms, requires using a special key that makes contact with all the pin tumblers in a lock and causes the pins to momentarily move in a way that allows the plug of the lock to turn.

The combination of energy and the modification of the milling was enough to defeat the system easily, even though the engineering team at the lock factory said it was impossible. They required an understanding of how this combination defeated their system.

High-security electronic cylinder: Many locks can be opened by applying force—striking them with hammers, plastic mallets, or other similar tools that can transmit energy to the lock's surface. This energy, in combination with internal components that rely on springs or the lack of springs to control the movement of critical parts, makes the locks vulnerable to this form of attack.

The manufacturer of this popular lock had no idea that the application of energy could easily and quickly defeat its high-security electronic profile cylinder and padlocks sold to foreign governments. This lock manufacturer's engineers had failed to imagine this form of bypass in its design and needed to understand the underlying theory of why their design failed.

Newton's First Law of Motion and electronic cylinders: The First Law of Motion states, "Every object will remain at rest or in uniform motion in a straight line unless compelled to change its state by the action of an external force." Many electronic cylinders rely on a worm gear to advance or retract locking elements when powered after a valid radio-frequency identification (RFID) credential is presented. A worm gear is a small motor that drives a spring or similar mechanism that is powered and turns when the lock is to be opened (or locked) (see Figure 1-3). As we discovered, these devices are subject to a simple form of attack. No one in the industry had connected the dots or realized that in seconds, the First Law of Motion could defeat these mechanisms produced by multiple manufacturers. The vulnerability affected many lock manufacturers because almost all relied on worm gears.

Figure 1-3: A worm gear is controlled by a small motor in electronic locks. The gear is turned when the motor is activated, which causes the gear to advance or retract a locking component.

NOTE **RFID is a technology that relies on a tiny passive radio receiver that requires no power. A signal transmitted from the lock energizes the receiver, which responds with a coded signal that validates the credential that energized it. RFID technology is used in thousands of different applications but is particularly well adapted to secure credentials in locks.**

Tiny entry points and openings for shims: Many lock designs have small holes or openings that allow for the entrance of fine shim wires to manipulate internal components, making it possible to open the lock. The Kaba InSync is a perfect example: a shim was inserted into the USB data port of this deadbolt cylinder and manipulated to release the locking mechanism (see Figure 1-4).

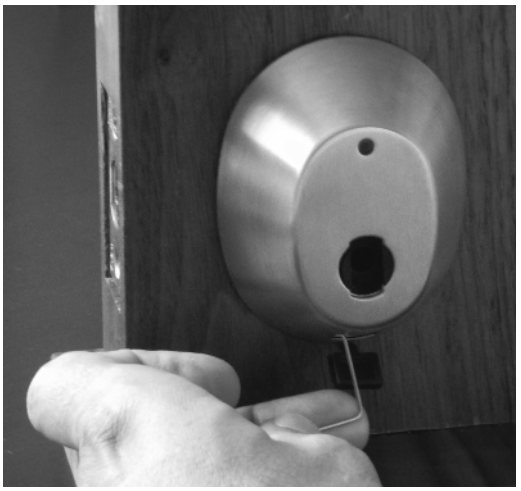


Figure 1-4: The Kaba InSync is a perfect example of a design failure to account for a small opening in the USB data port. This allowed the entry of a paperclip to bypass the release mechanism.

Virtual keyways with an internal sliding element: the *keyway* is the entry point for all mechanical locks. It controls which physical keys can operate the internal locking elements. Lock manufacturers figured out they could also create *virtual keyways*, which, as the name implies, are not equivalent to actual physical keyways. They are designed to simulate traditional keyways that mate with keys.

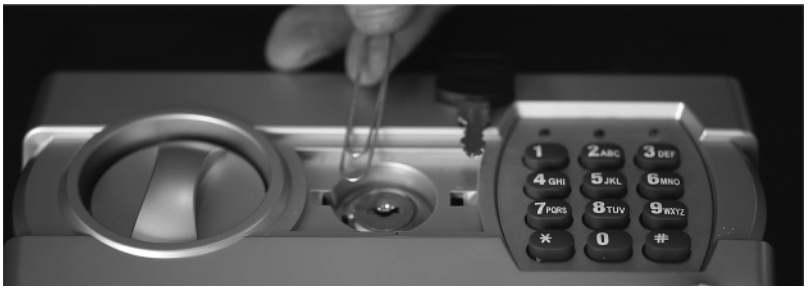
A clever but flawed concept in a new lock design used a form of virtual keyway. It was based on adding a sliding element to block access to the lock's sidebar until properly positioned by inserting a key. A *sidebar* is a very effective secondary locking system that many manufacturers employ to resist picking and other forms of attack.

In 2002, lock manufacturer Medeco introduced its m3-enhanced version of the BIAXIAL cylinder, in which a sliding element was added that moved laterally by a protrusion on the key's surface. This movement positioned the slider correctly, allowing the sidebar to engage in the plug. However, the team that introduced this concept failed to consider that the slider spacing was constant, regardless of the dimensions of the different slider combinations,

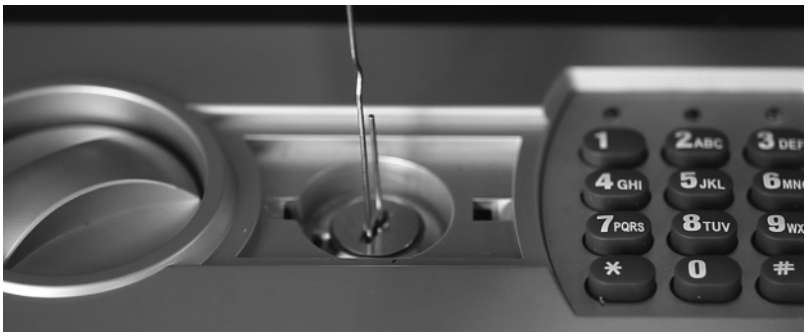
and that the required movement of the slider was precisely the diameter of a paper clip (.04"). All that was necessary to defeat this system was the insertion of said clip into the keyway, wedged between the plug body and the edge of the slider.

Electronic credentials and wire in a circuit board feed-through hole: A sophisticated electromechanical cylinder was defeated by fishing a tiny wire through a circuit board's feed-through hole to access and move the blocking rotor, allowing the lock to be opened.

Wafer locks and paper clips: A wafer lock, as described in Chapter 13, is a low- to medium-security mechanism that relies on the use of slidable tumblers, which are moved by the bitting of a key to the shear line, allowing the plug to turn. These locks are easily picked or manipulated (see Figure 1-5). The keys and their bitting can be configured to act on the wafers to move them in one or two directions.



(a)



(b)

Figure 1-5a, 5b: Reverse picking of wafer locks is common. (a) A popular gun safe with a wafer bypass lock that can be easily opened with a paper clip. (b) The paper clip is inserted into the keyway, torque is applied, and the paper clip is slowly withdrawn.

Many small in-home safes and other devices employ single- or double-bitted wafer locks. These types of locks can often be easily defeated by inserting

a wire, paper clip, or blank key and slowly withdrawing it with torque applied. In a reverse-picking attack, the wafers are trapped in place at the shear line because of the tension applied to the plug as a blank key or pick is withdrawn, one wafer at a time. This lock type is especially dangerous when used in gun-safe designs.

TIP ***Single-bitted*** **means the wafers are moved in one direction.** ***Double-bitted*** **means the wafers are moved to the top and bottom of the plug.**

Sophisticated push-button access control locks and the insertion of wires, pins, and paper clips: Advanced push-button locks employed by military, government, and commercial facilities can be defeated in many ways with wires, paper clips, and stick pins (see Figure 1-6). Their designers never conceived of simple attacks that could neutralize one or more security layers, notwithstanding the sophisticated electronic card-reading systems featured in the locks.

Figure 1-6: The Kaba 5800 electronic push-button lock could be defeated in six ways. I demonstrated these attacks at DefCon. One serious design failure was demonstrated by the insertion of a pin, wire, or pick tip through an LED mount to ground a contact on the PC board. This sent a remote opening signal to an electric strike at the door.

Vehicle anti-theft device and a shim: Makers of The Club steering wheel locking bar never considered how its ratchet design could be easily compromised in a few seconds with a five-cent piece of wire. Understanding how the locking mechanism worked and using that knowledge to defeat it led to my receiving a patent (U.S. 5,277,042) to fix the problem. The manufacturer's inability to imagine the defeat placed thousands of vehicles at risk of theft. The same security issue applies to handcuffs that can be defeated by circumventing the ratchet mechanism.

Simple key modification and electronic locks: iLOQ (from Finland) produced an award-winning and patented electronic cylinder that required no batteries. The designers of this lock series should have considered the fundamental design of how the lock worked and how design deficiencies allowed the lock to be set in a permanent state of unlocked status once a covert attack was implemented (see Figure 1-7).

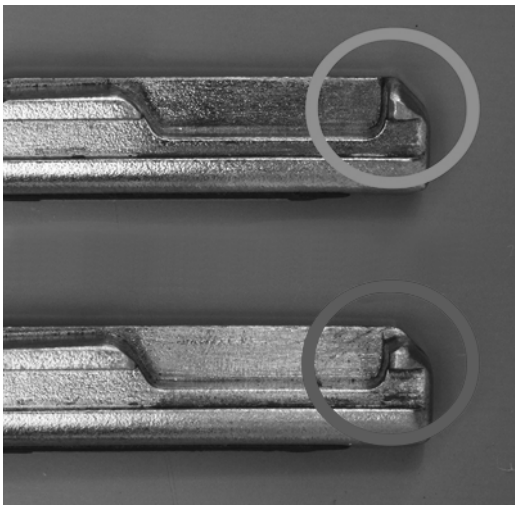


Figure 1-7: A simple modification to a valid key for an iLOQ electronic cylinder could result in it being permanently set with a screwdriver to unlock until reset. The top circle shows a nonmodified key tip. A small amount of material is removed (bottom circle) to defeat the lock's security.

Liquid injections and driver chips in safe and vault locks: The design of electronic locks, especially for safes, often requires an electronic driver chip to control motors or solenoids. Engineers never considered that you could destabilize these chips, causing a reset in critical integrated circuits by altering the impedance around the input contacts on the printed circuit board, which results in an electronic reboot that cycles the motor drives to open.

Wire access through keyways: In many instances, critical components can be reached through an open keyway. Many lock manufacturers have created serious security flaws by not closing and protecting the ends of plugs. A popular fingerprint lock can be opened in seconds by introducing a small wire into the bypass cylinder. This is also the case in file cabinet locks, key-in-knob locks, and even extremely popular locksets in which a release pin could be accessed through the keyway to completely remove the knob that contains the pin tumbler locking core (see Figure 1-8).

Plastic ballpoint pens and tubular locks: A failure to understand impressioning techniques in tubular pin tumbler locks has cost millions of dollars in

damages due to faulty lock designs. An engineer's lack of imagination failed to "connect the dots" in the Kryptonite bike lock case. (A more detailed description of this case can be found in Part VI.)

Figure 1-8: Open keyways, as shown in this deadbolt lock, can provide access to wires, shims, and other tools to manipulate a tailpiece.

KRYPTONITE BIKE LOCKS

The Kryptonite bike lock has been recognized as the premiere system for protecting bicycles from theft. The original design was based on the use of a tubular pin tumbler lock, which had a round key that is popular for many applications because of its low cost and simple implementation by manufacturers. The pins were configured in a circle rather than a straight line as in traditional mechanisms. The Kryptonite engineers failed to realize that the pins could be easily impressioned or decoded because they were all accessible simultaneously by an attacker. (The concept of impressioning is explored in Chapter 18.)

In the case of the bike lock, all that was required was a plastic ballpoint pen the same diameter as the opening (i.e., keyway) in the lock. If pressure was applied in a pumping action, the pen barrel deformed to precisely match the bitting values of the key. The failure to understand impressioning, the correlation of the diameter of the keyway to many pens, and the ability to produce a working key led to a recall of hundreds of thousands of locks.

Gun trigger locks and faulty key designs: Gun trigger locks are designed to prevent a pistol from being fired by blocking access to the trigger area by physically covering it. These types of locks are notoriously insecure and inexpensive and are sold mainly to protect access to guns by children. The tolerances between the plug (i.e., where the key is inserted) and the housing are generally poor. The gap created by this tolerance is called the *shear line*. It determines how the key works in the lock. Manufacturers of these locks can save money by

stamping rather than individually cutting the keys, so they can be mass produced. In this case, the producer of these locks not only stamped the keys but made the individual cuts almost identical and in a straight line, thus easily circumventing the function of the shear line. It meant every lock the manufacturer sold in the country could be opened by the same key, so a child could purchase a lock for $10 and have a key that would open the lock that was protecting the gun at their residence. Manufacturers producing inexpensive wafer or pin tumbler locks with bitting stamped at nearly the same level for each pin allowed gun locks to be opened with a straight wire or paper clip (see Figure 1-9). Design engineers failed to consider the ability to move all tumblers to the shear line due to their failure to understand the security of one of these mechanisms.

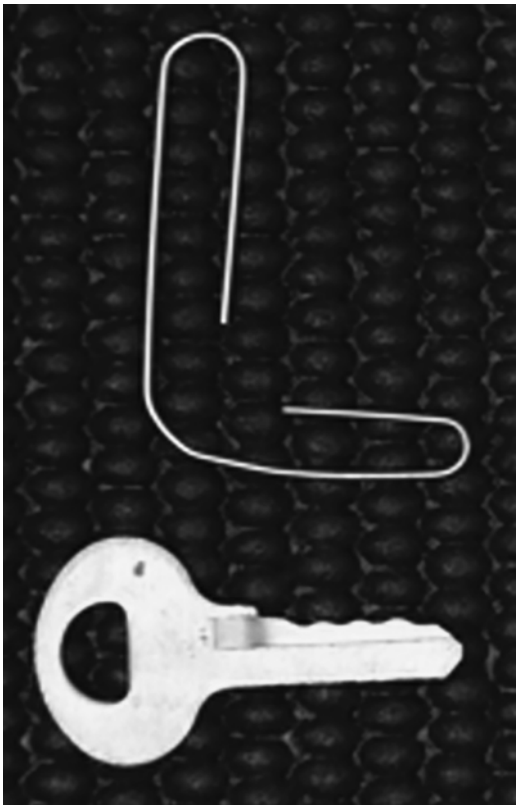
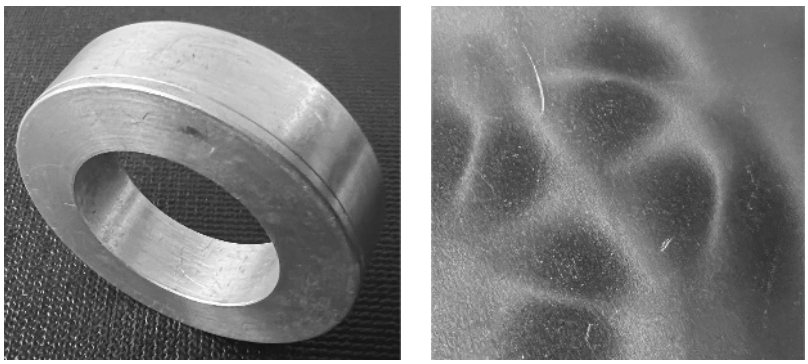


Figure 1-9: Several trigger locks for handguns were produced with stamped keys, all having essentially the same bitting values. A paper clip could lift all the wafers and open the lock in seconds.

Shims as drills in electronic cylinders: Using plastics in electromechanical and electronic cylinders creates serious security issues. In one instance, my security team partner and I used a fine shim wire as a drill bit to create entry holes into the lock face that were almost undetectable and enabled access to critical internal components.

Pin tumbler lock plug: Design engineers for one of the most popular and secure U.S. deadbolt cylinders should have considered what protects a pin tumbler lock from compromise via the keyway. This failure allowed the lock to be bypassed by introducing a small modified screwdriver tip to manipulate the lock's tailpiece element and attack and shear the endcap's retaining screws.

Magnetic fields and ferrous components in locks: Rare earth magnets have been very successful in moving internal components in many locks and electric strikes without a trace (see Figure 1-10). One of the most popular cases involved the Kaba Simplex 1000 mechanical push-button lock, currently used worldwide in banks, airports, pharmacies, government facilities, and many other venues. These prevalent locks could be opened in seconds because a ferrous element was critical to the locking function, and that component could be moved if a strong magnet was placed near the outside of the lock. When that occurred, the lock could be opened in two seconds. All it took to defeat it was an inexpensive magnet (see Figure 1-11).



(a) (b)

Figure 1-10a, 10b: Magnetic fields can move ferrous components within a lock to cause an opening. (a) The devil's ring, developed by Wendt, is the classic attack tool. It is a round metal enclosure with four magnets, as shown in (b) the visa mag film overlay that identifies each magnet.

Magnetic fields were also employed to open electronic cylinders with a small device called a "magnetic devil's ring," originally designed by Addi Wendt in Germany. The devil's ring was simply a round aluminum shell with four magnets placed in a circle to surround the outside portion of a locking cylinder. Rotating caused the lock's internal components to move and open. In my experience, lock design teams consistently forgot about the capability to manipulate ferrous materials with strong fields in locks and electric strikes.

Shims and combination locks: Numerous combination locks for computers and bicycles employ rotary discs that set a combination by the gate position for each number. Many manufacturers fail to consider the tolerances

between these discs. Thin strips of metal or shims can be used to probe the individual gates, allowing for easy decoding of the numbers to open the lock.

Figure 1-11: The Kaba Simplex 1000 mechanical lock was defeated by a rare earth magnet in seconds because a critical component that controlled unlocking was made of a ferrous material. Moving the round magnet near the lock was all that was required.

Now that we've reviewed the multitude of ways locks can be circumvented, let's consider what I think are the most important design rules when creating a lock's design.

Important Design Rules

> **It ain't what you don't know that gets you into trouble. It's what you know for sure that just isn't so.**
>
> ***—Mark Twain***

During my career, I've developed basic engineering rules that apply to locks and security hardware design. (If you wish to rush ahead, a complete listing is provided in Part VII, explaining why each rule is important.) I developed these basic engineering rules to take an alternative look at technical problems and minimize or eliminate the potential vulnerabilities existing in mechanical designs.

Basic engineering rules:

1. *The key never unlocks the lock*. Consider what actually unlocks the lock and how it or its credentials can be spoofed. Look for the path of least resistance to actuate the mechanism to open the lock. In most lock designs, the key controls another part responsible for allowing the lock to open. If the actions of the key can be replicated or simulated, then the key is not essential.
2. *Do not ignore the laws of physics or how they apply to attacks on locks*. One of the best ways I've found to defeat specific locking mechanisms is to rely on Newton's First and Third Laws of Motion. Many engineers do not correlate these principles with the ability to bypass locks and safes. As I note throughout this book, lock bumping is based on the Third Law of Motion: "For every action, there is an equal and opposite reaction" (see Figure 1-12). Bumping became a massive issue for manufacturers due to the vulnerability of most conventional and some high-security locks. It is based on the focused introduction of energy against pin tumblers. To combat this issue, some manufacturers introduced what they call *shock fuses*. These are designed to prevent the effects of bumping and other specific attacks against different parts via shock and vibration. Lock bumping has developed and expanded from its initial application of energy against pin tumbler cylinders to a more sophisticated method of attack for many different mechanisms.

(a) (b)

Figure 1-12a, 12b: The classic way to describe Newton's Third Law of Motion is with steel free-swinging balls. (a) The four balls are struck, and (b) the ball on the right is moved because of the energy transmitted as an equal reaction. This is the same theory of lock bumping with pin tumblers. When energy is applied to the base of pins by the key, the reaction causes them to move vertically across the shear line.

NEWTON'S LAWS OF MOTION

Sir Isaac Newton was a famous physicist who lived in seventeenth-century England. Most known for his studies of motion and gravity, he developed three laws of motion:

First Law of Motion: **An object at rest will remain at rest, while an object in motion will continue in motion with a constant velocity unless acted on by outside forces.**

Second Law of Motion: **When a force acts on an object, its acceleration is inversely proportional to its mass.**

Third Law of Motion: **For every action (force) in nature, there is an equal and opposite reaction.**

3. *Electrons don't open doors, mechanisms do*. Every lock with mechanical and electronic components that act in concert is vulnerable to attack. The junction of hardware and software must control something that moves, and that interface is always subject to compromise. Only mechanics control bolts and latches, whereas electrons only send signals to movable elements through motors, solenoids, magnetic coils, and so on.
4. *Locks are designed to be tested and attacked by bad guys*. You must assume that any designed lock will be subject to one or more attacks. It is important to try to envision all possible methods of attack against specific mechanisms when designing your lock. Consider every component, even if you assume it's irrelevant to the lock's overall security. Even the most insignificant part can be compromised and cause a cascade of events, resulting in the lock being opened.
5. *Whatever design is secure today certainly will not be tomorrow*. Methods of compromise are constantly evolving and being modified by clever attackers. New materials and tools and past design errors embedded into new locks are constantly being developed and exploited. Do not ever believe that what is secure today will be secure tomorrow.
6. *All security is about liability*. If people or property are injured due to a defective lock's design in a security system, the company that produced it can be held legally responsible.
7. *A lack of imagination in design and testing can lead to security vulnerabilities and failures*. The ability to analyze a mechanism and think about remote failure possibilities is important in lock design when considering a lock's vulnerability.
8. *All exploits ultimately replicate what the key does*. A correct key or code allows a lock's critical locking mechanism to be moved to a locked or unlocked position. Whether it's an actual or simulated key, lock pick, decoder, or special tool, its primary function is to replicate the actions of the key—to move the locking mechanism to an open position. If such a simulation can be accomplished, the lock can be opened without the key.

9. *All secrets in a lock are self-contained*. Whether it is a mechanical, electromechanical, or software-based lock, all the "secrets" or puzzle parts are self-contained, assuming that the intelligence running the lock is not networked or stored in the cloud. Locks should be thought of as puzzles that contain a set of secrets. If the secrets are deciphered and understood, then the lock can be opened.
10. *You cannot test against an attack if you have not envisioned the standards for testing*. The standards for testing locks, which are analyzed in Chapter 7, provide testing protocols that specifically include what I refer to as *hybrid attacks* that employ multiple modes and tools. Suppose that engineers do not fully understand what is possible outside the covert and forced-entry standards. In that case, they cannot fully assess vulnerabilities that may not be obvious if the standards are the only metrics. It's impossible to test for all attack types if your standards to test by haven't even conceived of those attack types.
11. *Adversaries can be incredibly resourceful and innovative*. Those planning and researching specific attacks against a lock may know much more than the designers who built the locking mechanism or system. It's often the case that the attackers understand your security and vulnerabilities better than you do. They constantly think about ways to attack, especially by collaborating on the Internet.
12. *Attacks may be low- or high-tech*. When assessing the potential for attacks against a new or current lock design, it's always tempting to think of them as high-tech attacks because simple ones cannot be conceived of. Some very sophisticated locks have been opened by extremely simple means. Locks and their mechanisms may be subject to either high-tech attacks or low-tech attacks that do not involve any technology. Never ignore one for the other.
13. *Design against likely attack vectors, not how secure a lock appears*. It is common for design teams to examine their current or new products and feel they're likely not vulnerable to forms of attack that they understand or can anticipate. In my experience, it's more important to concentrate on different forms of attack and work backward. Explore every conceivable way that other components and mechanisms could be compromised. Again, thinking outside the box is critical here because components that may seem to have no connection with security can become highly relevant. In one analysis my colleague and I conducted, the lead representative for a global U.S. company, in response to our claims of insecurity of one of the company's high-security locks, announced to the media that "I see no evidence that a system can be defeated. Therefore, it cannot." He later apologized, as his lock was indeed defeated because he could not conceive of a certain attack as viable.

14. *Suppose you don't believe you can open a lock. In that case, you probably will not be able to*. In my experience in compromising locks and security systems, negative thinking, especially when analyzing and attacking locks, usually leads to failure in such an endeavor because key indicators or paths are either ignored or missed.
15. *IT staff, risk management, security managers, police, crime labs, and locksmiths usually are not experts in finding lock vulnerabilities*. As access control systems migrate to becoming fully electronic, IT must always be involved. They must be able to fully understand system designs from the standpoint of security vulnerabilities. My experience with law enforcement and locksmiths has demonstrated that they need to become experts in discovering or assessing vulnerabilities to comprehend all vulnerabilities. The International Association of Investigative Locksmiths (IAIL) has this as one of their primary goals.
16. *Just because you're intelligent doesn't mean you can think like a bad guy*. Criminals and "bad guys" have different goals in compromising a security system or device. They usually want to gain access, steal assets or information, or sabotage infrastructure. Design engineers are employed to ensure that their products are secure against multiple forms of attack. They have very different motivations than bad guys. Unless they have experience working in law enforcement and interacting with criminals, these engineers cannot understand the thought processes and mentality of a criminal. Thinking like a bad guy requires a great deal of experience and insight into the mindset of someone who would cause harm.
17. *Just because multiple security layers are present doesn't mean all the layers are secure and the system cannot be compromised*. Virtually all high-security locks contain more than one security layer that must be appropriately activated to cause an opening. Although multiple security layers appear to ensure that the lock is more difficult to compromise by covert methods, they also provide an opportunity to do the opposite—create a vulnerability—if they are not designed properly. (Part IV describes many scenarios that allow locks with multiple security layers to be easily bypassed because their designers have yet to consider the possibility of attacks, especially hybrid attacks.)
18. *Insecurity engineering is far different from traditional mechanical or electronic engineering—the goals are entirely different*. Designing a lock requires mechanical engineering, materials science, and electrical or electronic engineering expertise if the system is electromechanical. In contrast, insecurity engineering is a different discipline that requires a thorough understanding of bypass techniques and the ability to project or foresee methods that could circumvent supposedly secure designs.

19. *Security can be viewed as an optimization problem, requiring many complex trade-offs and value judgments*. Designing a secure lock is a complex process involving many disciplines and thought processes that must be considered. Security is not just one factor, and it is not simply the hardware design. It encompasses possible failures, attacks, misuse, production defects, and use cases. There are often design trade-offs based on the complexity of manufacturing, materials availability, security, costs, convenience, human factors, management issues, and the projected user environment. In any project to design or modify a lock design, conflicting needs must be carefully considered and weighed to reach a consensus on the best way to proceed.
20. *Security starts when the project starts, not at the project's end*. If security is not the overriding consideration from the inception to the completion of a project, the result will likely be no security.
21. *Simple design errors can cause larger errors that experts will miss*. In my experience, every aspect of a lock design must be analyzed and assessed for the potential to cause failures in operation or security. The simplest design error can cause a cascading failure between related components, leading to significant manufacturing defects and security vulnerability. My rule of thumb: pay attention to everything and every component and their interrelationships.
22. *A security vulnerability may not be evident because there has been no incident*. In a serious product analysis that I conducted, a design defect that was latent for almost 20 years in the Medeco BIAXIAL pin tumbler lock surfaced in our research; it resulted in the compromise of many high-security cylinders. Do not believe there isn't a defect or vulnerability just because no one has reported a failure. No design is ever perfect.
23. *Sophistication in tech often means vulnerability*. Many believe that sophisticated or new technology means it's better and more secure. Often the opposite is true, because more layers of sophistication can mean more opportunities to defeat any one or more layers.
24. *The belief that all security devices can be defeated can mean none of them will be fixed*. I've often been told that all locks can be defeated with enough time and expertise. That attitude often causes management and design engineers to minimize threats and develop an "it's good enough" attitude in conducting research and development to produce a secure mechanism.
25. *Invest the time and research dollars in eliminating known vulnerabilities before going to market*. Recalls and redesigns are expensive. Unfortunately, management is always in a hurry to introduce new locks to their customers, with the attitude that any security issues are minimal and can be dealt with "down the road." This "down the road" syndrome can result in legal

liability and large damage lawsuits because the design and management teams simply did not want to wait until a product was secure. When analyzing a new lock design with defects, I have often asked management, "Are you willing to bet your company on not fixing a problem before a product release?" Take the time and money to invest in lock research to avoid big liabilities down the road.

26. *Bad guys do not follow the rules, standards, or attack modes*. Criminals, hackers, and attackers do not follow any rules regarding how they work or the techniques they choose to compromise a lock or system. The standards for locks and safes, detailed in Chapter 7, can provide a road map for how locks can be attacked in covert and forced entry mode, considering gaps in what the standards do not protect against. Design engineers must consider novel approaches to compromising their designs.
27. *Arrogance and a lack of knowledge can be the reciprocal of expertise in lock design*. A person who doesn't know they lack expertise can be the most dangerous and destructive to a design team. Many design engineers and managers think they know more about their product and its security than anyone else. This arrogance can result in serious ramifications, including liability and recalls.
28. *Never forget the Dunning–Kruger Effect and the phenomenon that the people who are the least competent in a subject often overestimate their skills*. People can overestimate their abilities, much to the detriment of a design project. Inflated self-perceptions can be fatal in terms of creativity and making errors in judgment about the efficacy of a lock design. David Dunning and Justin Kruger initially conducted a study in 1999. Their research looked at cognitive bias and focused on logical reasoning, grammar, and social skills. In the simplest terms, the Dunning–Kruger effect is the tendency of people with minimal ability in a specific area to offer overly positive reports of their ability. In judging the security of a lock, for example, this can lead to erroneous forms of thinking and conclusions.

Summary

This chapter introduced the premise of *insecurity engineering* and why it is important for every design engineer, product manager, and risk manager to understand. Many lockmakers are engaged in designing hardware that is inherently insecure, and they simply *do not know it*. After many years of working with different manufacturers, it was clear to my team that the simplest way to describe and understand the problem was to label it precisely as what it is: insecurity engineering.