The Four Types of Lock

Deviant Ollam

As a lecturer, auditor, and trainer in matters of physical security, I am fond of pointing out that your network and data are only as safe as your infrastructure itself. You can have the best firewall ruleset around, but it doesn't matter if someone gets into your server room with a console cable. You can communicate with other branches of your company via encrypted VoIP sessions, but someone can probably still listen in if they are in your wiring closet with some alligator clips and a buttpack. And you can have proper user permissions and access controls, but none of that will prevent data compromise if someone marches your hard disks right out the door. Physical security *is* data security.

A number of wonderful talks and white papers (not to mention media reports of intrusions and TV shows like *Tiger Team)* have helped to drive home this point... and yet there exists no simple, clear cut framework for physical security in a networked world. We see terms like "pick resistant" and "high security" on the packaging of products on store shelves. We speak with locksmiths who describe their wares as "restricted" or even "unpickable"... but what does it all mean?

How does one make heads or tails of the multitude of locks on the market today? Hopefully, this analysis will help you cut through all the marketing pabulum and understand the fundamental distinctions between various lock designs. By realizing which locks provide real security and which locks only give a false *sense* of security, you can make decisions that can help your facility become much more secure.

Strong vs. Weak Design

On the surface, the title of this talk might seem peculiar. Even individuals with little to no advanced study of security hardware can instantly recall far more than four designs of lock they've seen at various times in their life. From the old-style lever locks to modern safe dials... from puny wafer locks on file cabinets to heavy-duty rotating disk mechanisms with robust keys... from padlocks to deadbolts to locks seated within doorknobs... we see a multitude of designs and mechanisms every time we leave the house. How could I hope to distill things down to a mere four categories?

Simply put, the *design* of a lock matters significantly less than its *operation.* If a lock is resistant to compromise and can keep out an attacker, it doesn't matter if it was produced from blueprints drawn up in the last year or if it was designed and fabricated in the 19th century. If you'll permit me to make a temporary leap to another type of physical security hardware—the firearm—my analogy may become all the more relevant. Picture a revolver and a semi-automatic pistol.

The old six-shooter might seem like an antiquated design and the pistol might be viewed by some as the only device suited to our modern age. But in a tough spot, if given the choice between a .22 caliber pistol and a .357 revolver... which would provide greater security? Just as old designs can be made powerful, new designs can be implemented weakly.

It's not simply the *mechanism,* it's the *implementation.* Understand that, and the rest can become clear to you.

The Four Types of Lock

While I'll be the first to admit there are any number of unique and inventive designs that might not conform perfectly to categorization in the world of locks and physical security hardware, I can say with confidence that it is rather trivial to group nearly all locks on the market today into four simple categories: **Basic** Locks, **Resistant** Locks, **High Security** Locks, and **"Unpickable"** Locks.

As opposed to considering design features and mechanical function exclusively, the way in which I evaluate and categorize locks primarily concerns how they behave in the face of an attacker.

Each type of lock has its place and its function; what matters most is the application of locks in situations where they belong, and the avoidance of weak locks in sensitive situations that call for a higher grade of security.

Lockpicking and Lock Bypassing

It is slightly beyond the scope of this paper to discuss the intricate details of how lockpicking and other methods of lock compromise work. There are a multitude of resources on the internet discussing this topic, including my own previous Black Hat briefing paper entitled The Ten Things You Should Know About Lockpicking.[1] Furthermore, both the hobby of lockpicking for sport as well as academic research interest into lockpicking has become widespread. Feel free to visit the Lockpick Village instructional areas at popular security conferences or read more on the web about lockpicking for additional details on this topic.

My key focus on how locks and physical security hardware can be compromised pertains to the techniques, tools, and training required for achieving covert access. Anyone can kick in a door or break a window. The real risk to privacy

[1] Please be aware, while I am proud of the material in that paper and accompanying presentation, locks are no different than other security equipment... new facts come to light and once-revered technologies sometimes fall from favor when weaknesses are exposed. While the bulk of that previous work's content remains relevant, some of the highly-praised lock designs that were well-respected back then have since been compromised. Most notable in this vein are the products of Medeco and the new Kwikset "Smart Series" locks... while they remain more robust than low-grade, off-the-shelf locks, they have been exposed as weak in a number of ways that are not adequately described in my earlier paper.

and data security lies with non-destructive entry into a facility. Can an attacker with limited skill and basic tools open a lock in ways that aren't immediately apparent? What designs of lock can thwart even a well-trained agent of espionage?

Basic Locks

Most locks available for purchase at hardware stores and other non-specialty retail outlets are what I call "basic" in design. They incorporate no special protections and are trivial to pick or bypass. Either via brute force "raking" attacks or finesse "lifting" attacks with lockpicks, nearly all basic locks can be opened in short order... both by skilled attackers as well as novices with a modicum of practice. Locks of the "wafer" design are particularly notorious. I cannot think of a single means of implementing a wafer lock design in a way that makes it anything more than the weakest type of "basic" lock. There is also the matter of attacks that require essentially zero skill... methods such as bumping or shimming can be attempted with success by total novices and this is, of course, a very real concern.

Particularly troubling is the fact that nearly all locks which are "included" in mainstream office products (such as desks, file cabinets, storage boxes, luggage, etc) are of this "basic" design. Featuring no special protections or methods of stifling attack, nearly all office furniture and catalog-purchased corporate equipment can be opened in seconds. Any "security" they provide is entirely notional and wholly unreliable for business purposes.

Resistant Locks

Occasionally one can find items on the shelves of a hardware store emblazoned with terms like "Pick Resistant", "Commercial Grade", "Hardened", or any number of other popular buzzwords. While some of these items are legitimately a step up, many others offer no significant protections beyond the "basic" level.

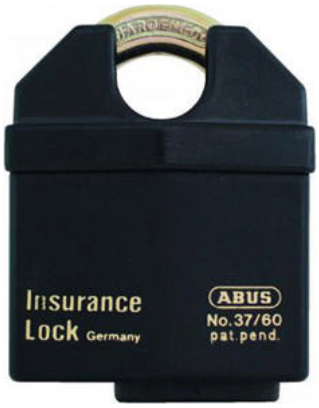
In my mind, a "pick resistant" design sets itself apart by incorporating features which would prevent an average attacker from easily opening the lock in under five minutes and which fully mitigate the potential for "wholly unskilled" attacks like bumping or shimming.

The use of features like anti-pick pins (also called "security" pins and sometimes referred to by name with terms like "spool" or "mushroom") and tight, jagged

keyways that frustrate the use of typical tools can make a lock more resistant to basic picking. Padlocks that incorporate what is known as a “double-ball” mechanism and keyed locks that utilize “anti-bump” pins can adequately quash the risk of zero skill attacks.

Unfortunately, there exists no standard for packaging and labeling locks that incorporate features such as this. Most locks that prominently extol themselves as being “commercial” or “hardened” are referring primarily to the construction of their outer housing and shackle and therefore are touting resistance to brute force attacks with crowbars or bolt cutters as opposed to finessed, covert attacks.

High Security Locks



While many store displays and catalog listings (and even many locksmiths) might lump the following locks and the immediately preceding locks into a single category, I feel there is an important distinction to be made and a very valid reason for understanding what makes a “high security” lock, in my view.

While both a “resistant” and “high security” lock are wholly non-susceptible to zero-skill attacks like bumping and shimming, they perform quite differently when set against finesse attacks with covert entry tools.

The previous category of “resistant” locks contain features that will *frustrate* and *interfere with* the use of basic lockpick tools... but they do not ultimately *prevent* compromise with these tools. In the hands of a person with some training and understanding of how locks work, a typical lockpick kit of the style sold on the internet or at “spy shops” will open a “resistant” lock.

A “high security” lock, on the other hand, employs mechanisms that completely block and render nearly useless most “typical” lockpicks. An attacker with anything less than stellar skill would be unable, in my definition, to open a “high security” lock in under a half an hour. Even a skilled attacker would require specialized tools and techniques to compromise a high security lock in anything less than five minutes. The fact that non-standard tools and techniques are required in these scenarios is the key parameter of this category.

The security implications of this distinction are significant. While it is not possible for most corporations to cover 100% of their facility with security cameras or passive infrared alarm systems, it is within the budget of nearly all companies to monitor a video feed or have a security guard pass by a sensitive

area like a server room or records room once or twice an hour. By selecting high-security locks for their most important installations and incorporating these locks into a larger security model that involves monitoring and incident response, it can dramatically increase its overall security posture.

The use of anything less than a "high security" lock, as defined by these standards, leaves an organization open to a great number of attacks. Persons who can social engineer their way into a building may easily be able to bypass internal security doors and access private data covertly (even if lockpicking isn't their core area of expertise) if lesser locks are the norm at a given facility.

"Unpickable" Locks

Naturally, the use of quotes in the name of this final heading is a must. We in the security world know all to well the folly of vendors who have chosen to label a product as "unhackable" or "impregnable" and their inevitable comeuppance in the press when a flaw or weakness is revealed.

However, that said, I do believe that there does exist one final category beyond the "high security" designation when it comes to locks and access control mechanisms. There are a small number of products for which there is no known bypass or compromise attack. While it is not wholly unbelievable that a highly skilled attacker, given enough research, might be able to open one of these "unpickable" locks without the proper key or token or combination... in my view it could never be done in under thirty minutes and would *always* require special tools and perhaps a multitude of special (and perhaps self-researched) techniques. Even then, it is quite likely that most attacks would involve more than the "covert" types of action most commonly associated with lockpicking. Some degree of commotion and conspicuous disturbance would likely be a feature of even the most meticulous attacks against "unpickable" locks.

While it may seem unsettling that someone with enough skill, research money, and dedication could open a door in your facility secured with what I would refer to as an "unpickable" lock... I would assert that if an unauthorized individual can squat by a secure entryway and methodically (and perhaps loudly) utilize a variety of nonstandard instruments in the door for upwards of a half an hour without being noticed or challenged... then you have a larger problem with your overall security model.

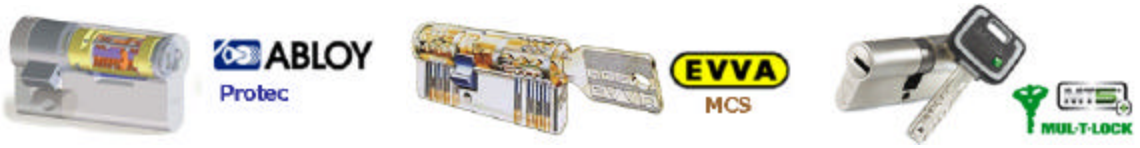
Where "unpickable" locks truly exhibit their virtue is in the fact that to compromise them, an attacker must almost certainly attempt acts of gross

devastation or otherwise render the mechanism damaged in an easily detectible fashion. There are a number of "unpickable" locks available for purchase in small, inexpensive form factors. These locks can be cut with large bolt cutters or even smashed apart with sledgehammers or door rams. What value do they have, then, in the face of attack? It is simple... their virtue is in the fact that any attacker has *no other option* than to act in a destructive fashion.

If the morning shift employees arrive at a facility and discover the server room door off its hinges or a filing cabinet with the drawers badly pried and misshapen or a safe with large scratch and pry marks around the combination dial and door plates... these are all cause for alarm, indeed, but they are plainly obvious and will trigger immediate response actions on the part of security staff. Policies that are in place can be followed without delay and efforts surrounding evidence collection and protection, as well as data inspection and recovery, can begin.

In matters demanding the highest security, the greater risk is *non-destructive entry*... since it affords the victim no means of adequately identifying the intrusion and responding properly. By *forcing* an attacker to take a destructive route (by use of "unpickable" locks) it practically *guarantees* you peace-of-mind in the absence of any signs of attack. If things look well-in-order, you can rest assured that no one has covertly bypassed your security perimeter without your knowledge.

Presently[2] there are three conventional lock mechanisms that I would designate as "unpickable."



The Protec rotating disk design by the Abloy group, the Magnetic Code System key by the Austrian company Evva, and the latest offering by the Israeli Mul-T-Lock company – their MT5 series – are all exemplary designs that I would happily pit against the most skilled lockpickers in either the sportpicking or research communities.

There is also an option for electro-mechanical security in the form of safe locks that merits the "unpickable" designation. The X-series electronic safe dials by

[2] As noted in an earlier footnote... please understand that attack developments and security compromises in the physical sector are just as common as in the digital realm. While all efforts have been made to ensure that facts and details in this paper are accurate, one would be best served by speaking with highly-security-conscious locksmiths and/or physical security researchers before making any product purchase or infrastructure installation.

the Swiss company Kaba Mas (formerly Mas Hamilton) have been the absolute, unquestioned standard for protection of top secret materials by governments and corporations for nearly two decades. There is no significant research leading one to believe that these products are in any risk of being unseated from their top ranked spot anytime soon.

Where to Buy, Where to Use

It is very easy to believe that locks that I have described in the "basic" design have no real purpose. This is not true. If you secure a simple access panel with a basic lock, you usually remove the possibility of it being accidentally bumped ajar or carelessly opened. Additionally, even if they are easily bypassed, any individual (especially someone who does not belong in a given part of a facility) who is found in the presence of such an open panel would be at pains to explain how it became unsecured. Provided that you are not protecting *critical* infrastructure, basic locks can (and often do) secure things like circuit breakers, display cases, and utilities like water spigots or electrical outlets.

Remember, locks cost money... and higher-grade locks can come with significant price tags. If you have a small shed that your building and grounds staff uses to store $50 worth of lawn care tools, it makes little sense to invest in a $100+ lock for protection in this case.

Pick resistant locks are sometimes available for purchase at local hardware stores (again, be mindful of the lack of any real standards in the packaging and labeling for locks of this caliber) and, despite what you might believe, these are often suitable for residential installations. Unless you live in a particularly high-crime area or have especially valuable corporate secrets in your home (if you work from a home office, say) you will never experience attackers attempting to covertly enter your dwelling. You can ask essentially *anyone* with ties to law enforcement if they have ever seen (or even know of) a case in which a private residence experienced an illegal entry (for larceny, assault, or any other purpose) by means of lockpicking. I am quite confident that you will not find anyone with such a case on record. It simply doesn't happen.

Bad actors who would seek to enter a *home* are most often low-level street criminals with zero training and no time or desire to learn finesse techniques. Brute force attack is the name of the game nine times out of ten in residential matters, resulting in broken windows or forced doors. On rare occasion, there have been alleged reports of some tactics like bumping or shimming being used in acts of petty larceny, but even these are very uncommon.

Overall, if your home is protected with a lock that can eliminate those “zero skill” attacks and perhaps even resist some picking attacks for good measure, you are not going to be seen as a low-hanging-fruit and petty criminals will direct their efforts elsewhere.

High Security locks–those incorporating advanced pick resistance and usually employing wholly new and distinct mechanisms–are suited for areas that house and store sensitive material, data, or records. Remember, the key distinction of “high security” is that a person without special training or knowledge would have no chance of successfully attacking the lock in under thirty minutes... and *anyone* who could possibly compromise the lock (even a highly skilled individual) would have to make use of specialized, non-standard tools beyond those found in an off-the-shelf lockpick kit. With the use of such specialized tools and techniques, a “high security” lock should be able to resist even skilled attack for five minutes or more.

It is highly uncommon for proper High Security locks to be found available for purchase anywhere other than at a professional locksmith’s shop or from online specialty suppliers.

Locks of the highest caliber and in the final category, designated “unpickable” by some, are suited for the most sensitive installations... where it is essential that absolutely *any* compromise of security result in clear and obvious signs after the fact.

While some locksmiths may be licensed dealers of these highly specialized products, often the best means of acquiring hardware of this caliber is by ordering products from suppliers online, sometimes from overseas.

Conclusion

The merits and respectability for many security products are always changing. New exploits and attacks may appear tomorrow that shake the reputation of a lock considered unassailable only a week prior. The best means for ensuring your own physical security is the planning and implementation of multiple systems in layers, arranged so that a failure of one segment does not cascade into others. This, coupled with attention to security bulletins and reports by lock researchers, can ensure that your facilities, equipment, and data remain secure in the face of both skilled and unskilled attack.