Mechanical vs. Electronic Locks

Security implications of the two paradigms

Independent Security Evaluators | www.securityevaluators.com

October 12, 2014

MECHANICAL VS. ELECTRONIC LOCKS

Abstract

Electronic locking mechanisms introduce new attack vectors as compared to mechanical locks, but if properly designed, there are no inherent flaws with systems that have such attack surfaces. Furthermore, hardened electronic locking systems introduce significant security upgrades over more traditionally deployed mechanical locks. However, the entire premise of security advantages in electronic locks is based on the condition that such a system has had security properly built in, as validated by design assessment, implementation assessment and security assessment. This paper analyzes the various security implications associated with deciding between mechanical and electronic locks for use in access control of physical premises.

Overview

When an emerging technology starts to become adopted, the market often divides into two very distinct mentalities: (a) those who are overly eager to adopt the new technology – possibly without full regard to the consequences, and (b) those who are exceptionally wary of the security or privacy implications – possibly without full understanding of the benefit. In either case, a poor risk-based decision is made. This condition is typically seen in the case when choosing between mechanical and electronic locks. This relatively new technology coupled with ever newer platforms for innovation, such as mobile phones, radio frequency identification (RFID), and the Internet of things, repeatedly leads the market back to the risk-reward drawing board. It is important to recognize that locks are only one component of an overall access control scheme, and a business should not rely solely on locks to secure a premise.

This paper aims to clearly define a lock-based security model in the digital age, articulate and compare the benefits and disadvantages of mechanical and electronic locks, and help businesses understand risk in order to make the best risk-reward decisions when choosing between these options for physical access control.

USE CASE

A lock is generally meant to control physical access between two areas, either keeping someone or something out, or in, unless authorized to traverse that boundary. Access control is the primary security objective.

Threat Model

A threat model articulates the assets and associated adversaries who would be interested in those assets, in order to determine best security approaches for a given system. When it comes to locks, whether or not a lock can be defeated under certain conditions may not matter in every situation, and concerns may vary. By understanding the assets being protected, the threats to those assets, and the access and attack surfaces available to those threat actors, businesses can determine what matters most in a given situation, and appropriately weigh the security or privacy concerns against real world risk.

ASSETS

Whether mechanical or electronic, all locks protect the same assets:

- **Persons**: Locks are one component of physical access control mechanism meant to prevent physical and emotional harm, including but not limited to assault or harassment.
- **Property**: Locks are one component of physical access control mechanism meant to protect personal possessions of varying ranges of value, stored in an ostensibly secured room/house/ etc

- **Information**: Locks maintain access to privileged information, which can be leveraged for corporate espionage, state-sponsored intelligence gathering, or other forms of physical or emotional harassment.
- **Business Opportunity**: For entities such as hotels, bed & breakfasts or other rental properties, if an attacker can subvert access controls in order to utilize a temporary use space without paying, monetization strategies for the business are undermined.
- **Reputation**: For entities such as hotels, bed & breakfasts or other rental properties, there is implicit trust between the renter and the business that personal safety is guaranteed. If an attacker were to circumvent a lock in order to violate a renter's sense of safety, the business could suffer reputation damage.

THREATS

Any business must build out a unique threat model that is specific to that business' own assets, but generally speaking, these are some of the adversary categories that may or may not apply:

- **Targeted Attacker**. Motivated by personal agendas, this attacker usually knows something about the victim and is motivated to attack that victim for personal gain or retribution. This type of attacker can range widely in skill level, access to resources and time.
- **Opportunist**. Not typically very motivated to attack, but will do so if an easy opportunity presents itself. Characteristics of this attacker can vary but typically would be lowly skilled and with minimal access to resources or time.
- **Nation States**. Motivated by political interests, they are very well funded, highly skilled, have tremendous access to resources and time. This type of attacker may not be interested in attacking the typical individual homeowner, but very interested in attacking a high profile individual, a business or government entity.
- **Organized Crime**. Motivated by profit, they operate like a business. They are well funded, highly skilled, with tremendous access to resources and time. This type of attacker may not be interested in attacking the individual homeowner, but very interested in attacking a high profile individual, business or government entity.

ATTACK SURFACES

Locks can be attacked via a number of surfaces:

Surface:	Applicable to:
1) The lock itself.	Mechanical; Electronic
2) The key(s).	Mechanical; Electronic
3) Storage of the keys.	Mechanical; Electronic
4) The key holder (i.e., the user).	Mechanical; Electronic
5) The key-lock communications.	Electronic
6) The backend systems supporting the lock security system itself.	Electronic

It is important to note that while certain attack surfaces (e.g. key-lock communications and back-end systems) do exist with mechanical locks, practical exploits of these surfaces are not readily prevalent. By contrast, electronic locks introduce practical exploits against these attack surfaces. However, discussion of this new type of access control also highlights the often-overlooked severity of existing attack surfaces in mechanical locks, such as key storage.

Analysis of Attack Surfaces

Since lock systems differ most prominently with regard to attack surfaces, this is where the focus of the risk-reward decision making should be made. This section walks through each attack surface, compares the lock types, and rates the locks with a metric of advantage vs. disadvantage in terms of security. Adversaries typically choose the path of least resistance when pursuing asset compromise.

I. THE LOCK

The lock is the device that controls access to the protected area. If a lock is easily defeated, it will likely be targeted directly. If it is difficult to defeat, the adversary may choose to circumvent the lock entirely, breaking through a window, a separate door, drilling the lock out of the door, or stealing the locked container (e.g. in the case of a safe). The lock itself need only be stronger than the weakest links available in the anticipated attack. In other words, of the variety of attacks discussed below, a business may want to associate less weight on the possibility of advanced attacks (e.g., those that require key theft, malware, or advanced cryptographic skills) if the lock is deployed adjacent to a more easily defeated mechanism, such as a glass window.

Accepting that both lock types can be circumvented with equal difficulty, when comparing the mechanical and electronic locks directly we examine how easily the locks themselves can be defeated, either by causing them to open without an authentic key (a.k.a., authentication bypass), or to fail to open when an authentic key is present (a.k.a., denial of service). One very important factor to consider is whether or not the electronic lock additionally has a mechanical interface to fall back upon.

Mechanical locks. Mechanical lock picking is a skill that can be mastered through practice and enhanced by industry tools. For the most part, skilled criminals can readily obtain these abilities and tools, and mechanical locks can withstand only seconds-to-minutes of attack before defeat. This is hardly a high barrier for preventing advanced/targeted attacks, however, we *do* consider these locks to provide some level of security and comfort against unsophisticated adversaries, or adversaries with limited ability, need, or desire to target assets. It is important to recognize that these mechanical locks are inherently weak.

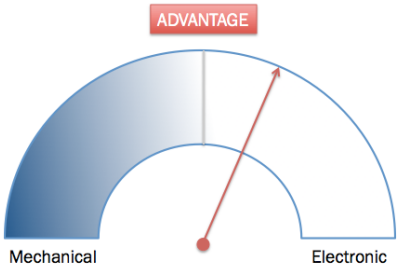
Electronic-mechanical hybrid locks. Most electronic locks have a mechanical interface to fall back upon. This can be useful when a power source fails, memory has become corrupted, or some other unforeseen situation occurs that disrupts the electronic interface. However, the mechanical interface comes with all of its inherent security deficiencies. As a corollary to the earlier statement that a lock need only be as strong as the weakest link required to circumvent it, we can say that so long as the electronic interface is no weaker than the mechanical interface, the electronic interface is *at least* not weakening the lock.

Making that very determination would depend on a case-by-case study, but if designed and built properly, there are no inherent issues with an electronic interface as there are with mechanical. Poor designs or implementations may expose an electronic lock to defeat through disruption or manipulation of power sources, connecting leads to the lock, or directly interfacing with exposed ports, but if properly shielded and designed in a fail-safe manner, these issues are avoidable.

For all intents and purposes, with regard to the lock attack surface there are no significant advantages for a hybrid lock over a strictly mechanical lock. If anything, we may consider a hybrid lock to have only negligible security

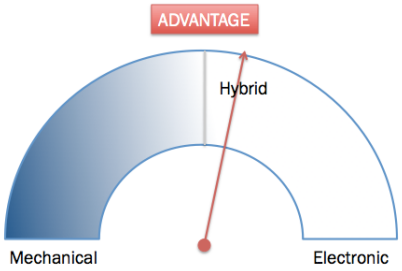
implications with regard to this attack surface, only because there exists the *possibility* of additional attack vectors, and even then that attack would need to be functional within the already present window of seconds to minutes for attacking the mechanical interface – an unlikely circumstance.

Electronic locks. Some locks have only an electronic interface, i.e. lacking an exposed mechanical interface., may have an inherent advantage since there is no weaker mechanical interface available to defeat. In this case, the same attacks above regarding the electronic interface of a hybrid lock are applicable, e.g., manipulating power, circuitry, or ports, but as stated these attacks are not inherently possible, and preventable through proper design and implementation. Therefore, electronic-only locks, if built properly, will only be defeated using sophisticated, lock-specific techniques, rather than the seconds-to-minutes window for defeating a mechanical lock. The advantage here leans strongly toward electronic-only locks.



Lastly, with regard to denial of service, both locks are inherently susceptible. For mechanical locks, old tricks such as super glue or breaking off a key in the hole can damage and prevent a lock from opening. For electronic locks, signals may be jammed, power drained, or circuitry damaged resulting in a lock failing safe, i.e., staying locked. Comparing the two, denial of service attacks against electronic locks require much more sophistication, making them the better choice. However, if preventing denial of service is crucial, the best choice is a hybrid lock. The dual interfaces provides two targets to be disrupted before the attack can be successful.

Businesses should be sure to keep perspective with regard to denial of service attacks. On one hand, the threat of denied service is likely secondary to preventing access, making the benefits of hybrid locks possibly less significant than the advantages of electronic-only locks. On the other hand, denial of service can cause safety concerns or an expensive hassle if locks are caused to fail regularly, possibly trapping persons or preventing access to needed medicines, weapons, or other items.



II. THE KEY

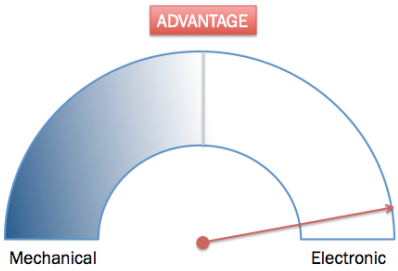
Perhaps the most recognizable distinction between mechanical and electronic systems is the key itself, which presents very different attack surfaces between these two lock types. The key is the component that authenticates and authorizes the key holder to the lock, opening it. Generally, possession of a key always grants access, and without the key access is denied.

For mechanical locks, a key is typically a piece of metal with a protruding blade outfitted with teeth such that the arrangement of the teeth is *ideally* unique. In practice, however, a unique arrangement for most mechanical keys is not possible and there will thus always exist duplicates. Other mechanical key formats exist, such as tubular keys, double sided keys, and more. While some are less susceptible to the attacks described in this section, for this examination we treat them all the same.

For electronic locks, rather than a physical arrangement of components representing the key, the key is represented as a digital number. That number is stored on a variety of media, from magnetic stripes and RFID tokens, to smartphones, smartcards, and other tokens capable of performing complex computations. Since the numbers can be sufficiently large, it is possible to create *truly* unique keys.

Key management. The most significant aspect to *the key* attack surface is that mechanical keys cannot be easily revoked. This represents an overwhelming security risk as cost and difficulty routinely trump security in practice. When a mechanical key is lost, stolen, or copied, it can then only be revoked by rekeying or replacing the lock, and usually involves reissuing keys to all valid users. This process is expensive and many lock owners weigh the risk-reward tradeoff between replacement and possible compromise, and choose to accept the risk. In essence, the lock owner chooses to *trust* all previous key holders, even temporary key holders. Electronic lock systems (depending on the design) can nearly eliminate the expense and burden of key revocation, and better eliminate unnecessary trust. This greatly increases the likelihood of proper key revocation and mitigates the aforementioned risk.

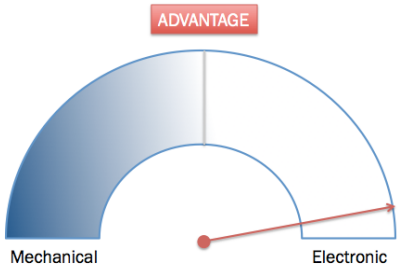
Depending on the business needs, this is possibly the most significant aspect of security differentiation between the two lock types. Any business or homeowner that routinely wishes to grant and revoke access to different parties (such as vendors, employees, tenants, maintenance workers, friends, or guests), must choose between permanently trusting those parties once keys are returned or replacing/rekeying the locks in order to revoke the keys. In the electronic setting, since key revocation is trivialized, the choice to revoke keys is simplified and far more likely. Given this business or personal need, the security advantage is greatly in favor of electronic locks.



Forging keys. Assuming for a moment that perfect key management is established and practiced, there are still key forgery attacks against both lock types that could result in bypassing the locks' security. A successfully forged key is any key that grants the holder access through the lock. This could be a replica of a valid key, but is more broadly defined as *any* key that an adversary can create to successfully grant access through the lock. The ease of forging a key is dependent upon a variety of factors and boils down to access. The first three levels of access are easily understood in both mechanical and electronic contexts. The last three levels of access may have analogous mechanical implications, but are largely disregarded until electronic locks are part of the equation.

1) From scratch. At this level, the adversary has no key and no knowledge of the key. The scenario is equivalent to approaching a never before seen lock, and attempting to create a key which grants access. For certain mechanical locks, creating forgeries from scratch is trivial. Some lock types have such a limited key space that an adversary can simply obtain or create them all. For other locks, creating an outright forgery is difficult, but not impossible. It has been demonstrated that molds can be made, and keys constructed after repeated probes of the lock itself. To do so would take specialized skill, patience, and a non-trivial amount of time with the lock itself. That said, the forgery of a mechanical key from scratch is likely far more difficult and time consuming that simply picking the lock to gain access, so the usefulness of these attacks is questionable.

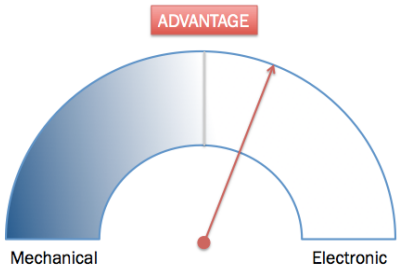
With electronic locks there are many more considerations. Unlike mechanical systems where forgery techniques are likely to work across models, manufacturers, and even lock types, there is such a wide variety of ways in which electronic locks may be designed that simply enumerating attacks is unhelpful. Some electronic lock systems have been shown to use incremental and predictable identification numbers as keys, others have default master keys, while others still provide sufficient information from the lock itself to predict and forge a key. Some locks have implemented strong cryptography, and are unlikely to be broken under these conditions. What is important to realize is that while some electronic lock systems' designs are deeply flawed, this doesn't *have* to be the case – these issues are not inherent and a strong design and implementation can prevent these attacks.



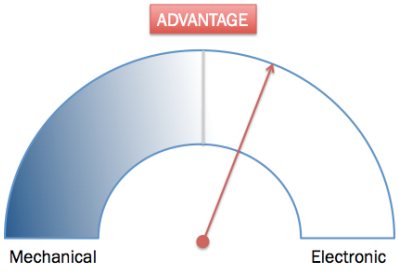
2) Proximity to a key. A step up from the adversary having *no* key, is the adversary having temporary or proximal access to a key, such as being momentarily handed a key, having line of sight of a key, etc. Some mechanical keys under this condition are highly susceptible to key forgery attacks. There have been demonstrations that forgeries can me made easily from key imprints in bars of soap, tracings of keys on paper, and keys can even be reproduced from photographs. Unlike creating a forgery from scratch which most likely requires access to the lock, creating a proximal

forgery of a mechanical key prior to attack may be simpler or provide better cover than even defeating the lock through picking.

With electronic locks, just as performing a forgery from scratch has many considerations, performing a proximal forgery does as well. There are no inherent vulnerabilities in electronic keys that make proximity to a key an issue, but depending on system design and implementation there are ways in which these keys can be forged. Some transponders that have a hard-coded broadcast identifier used as a key can be easily obtained by simply querying the device in the field. Other transponders that use weak cryptographic operations to prevent copying have been shown to be beaten with only two queries. The take away again is that while flawed systems exist, the paradigm is not inherently flawed, and strong cryptography can be used to prevent the copying of keys.

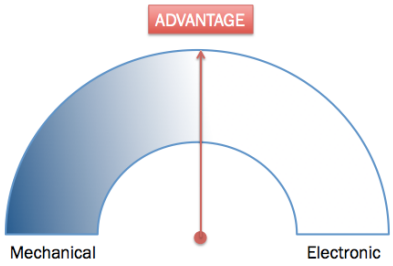


3) Possession of a key. Full possession of a key is the kiss-of-death for most mechanical keys. There are no mechanical keys that cannot be copied with extended physical access to those keys. Some keys may require special equipment or skill, but it is always possible. Electronic keys, in theory, are all susceptible to forgery given sufficient time as well, but technologies and techniques exist for making replication incredibly difficult, and the equipment and skill to do so may be unobtainable depending on how advanced the technology is. The take away here is, if done right, electronic keys provide far superior defense against possession of key forgery attacks.

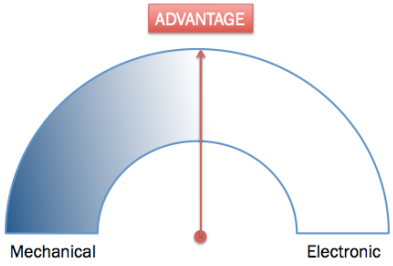


4) Proximity to a key in use. Proximity to a mechanical key in use provides no additional information, in fact, it may be harder to gain information from a key in use than sitting still. An electronic key on the other hand exposes an entirely new attack surface while in use: the key-lock communication protocol (discussed again below). There is no question

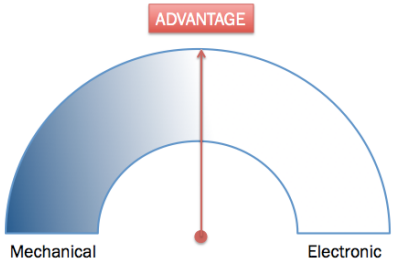
that additional attack surfaces provide different points of exposure, but again, this is not an inherent flaw. Key-lock communication protocols, like all communication protocols, can be designed to withstand eavesdropping attacks that could result in key forgery.



5) Inside access to the lock. With mechanical locks, it generally doesn't matter whether or not an adversary has temporary access to the protected area. Being behind a locked door generally doesn't afford the adversary the ability to forge a key any more than being locked out. This is not always the case for electronic locks however. Electronic locks typically have some form of key-enrollment procedure, sometimes built in to the lock, a master key, a key-enrollment device, or through accessing a computer system. If these devices or interfaces are available to an adversary within the protected area, they could be used to forge a key through a false enrollment. Again, however, these flaws are not inherent to electronic locks, but may be apparent in flawed system designs or poorly configured installations by users. This attack surface should be understood by both designers and users.



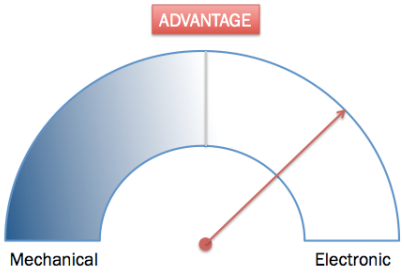
6) Backend access. Mechanical locks simply have no networked backend, while electronic locks thrive on this component. In fact, backend access is an inherent risk to all connected electronic locks with third-party management. Developers and administrators of the backend could potentially create back doors or forge keys that could be used to grant access through any lock, if so inclined. Even so, this is not all that different from employees at a mechanical lock manufacturer holding the requisite skills or master keys to gain access through the locks they produce. Therefore, the additional backend access should not be of significant concern to consumers and small-to-medium sized businesses. Large enterprises or government facilities with exceedingly valuable assets should remain wary of vendor-operated backend networks.



Summary. As can be seen above, with regard to *the key* attack surface, mechanical locks offer no inherent security advantages, while well-designed electronic lock systems can offer strong, effective, and well-defined security advantages over mechanical locks. The key management benefits alone should sway the decision maker – when considering similar pricing tiers, superior security can be immediately realized – and there are additional advantages beyond that with regard to key forgery resistance. Understand, however, that with any electronic lock system poor design or implementation can quickly nullify this advantage and leave the lock owner worse off than before. We state only that there are no inherent disadvantages with electronic locks, and that businesses should demand proof of sound design, implementation, and security assessment.

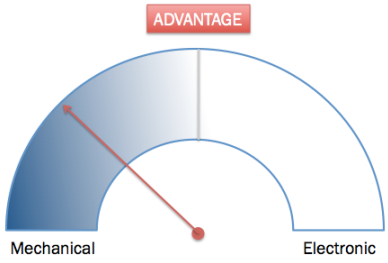
III. THE KEY STORAGE

If attacking the lock fails, and the keys cannot be forged, the adversary may move on to the next most readily available attack surface: the storage of legitimate keys. The goal is to obtain a legitimate key and use it to grant access through a lock. Once again, the mechanical systems have inherent disadvantages. Mechanical keys are physical, tangible objects, and remain in that form whether in use or at rest. Electronic keys can be encrypted at rest, and only made available with the contribution of a second authentication factor, such as a PIN, password, or biometric reading. This represents a massive security advantage for electronic systems. Whether keys are happened upon by chance, or located in a targeted attack, obtaining the electronic key can be made more difficult by requiring additional knowledge beyond knowing the key location.



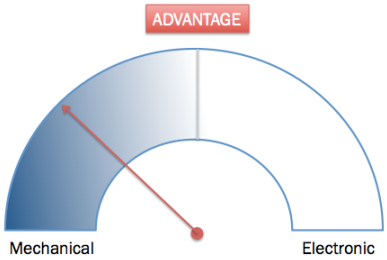
IV. THE USER

The next most promising attack surface is the holder of the key, i.e., *the user*. Attacks against the user of a mechanical system are analog, in-person, high risk attacks. These attacks would include physically stealing keys, convincing a user to hand over the keys, or convincing a user to grant access through a lock. These attacks do occur, but they are generally high risk and easily detected. For electronic systems, social engineering attacks against the user are more subtle and not as easily detected. Depending on the nature of the system, phishing attacks, devices infected by malware, false locks, and other trickery may be possible to fool unsuspecting users into handing over the information needed to grant access through a lock. It may be unfair to lump all electronic locks in to one category and declare *the user* attack surface as a rich target – not all systems will store keys on mobile phones, link locks with email accounts, permit backups, etc. – but the human element is without a doubt an inherent security weakness in all security systems. It is possible, and highly recommended, that electronic lock systems assess and mitigate social engineering attacks against users, and protect data at rest from malware, but when it comes to users the edge goes to mechanical locks, simply because launching these attacks in the physical setting is far less likely to succeed.



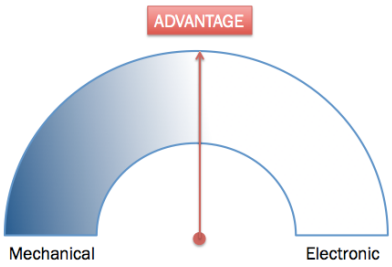
V. THE BACKEND

Mechanical locks do not require backend infrastructure. Electronic locks on the other hand often integrate with a supporting backend. This backend affords the electronic systems many of the security advantages already discussed above, including key management, back up, audit, ease-of-use, etc., but that very backend becomes an additional, and potentially vulnerable attack surface. Rather than target the user or their keys and locks, depending on the systems' design, an adversary could target the backend infrastructure and if able to find vulnerabilities there, could leverage those vulnerabilities to forge keys, or indirectly manipulate locks in the field. This attack surface can be large, complex, and involve numerous components which, if poorly designed, implemented, or configured, could invalidate many security properties that the electronic locks have to offer. Such vulnerabilities are not inherent, and would only result from improper design or implementation. It is true that mechanical locks will never suffer from vulnerabilities on this attack surface, and so they have an inherent security advantage, but electronic systems can be secure from attacks against that backend as well assuming proper security has been built in.



VI. THE PROTOCOL

Electronic locks introduce another attack surface not otherwise seen in mechanical locks: The key-lock communication protocol. Mechanical locks generally interface with keys through physical contact, but electronic locks can communicate over a variety of other media, including radio signals and infrared, each of which can be eaves dropped upon, manipulated, or forged from a distance. Even so, this does not lead to inherent flaws. For the protocol, while it may be more easily targeted, it can be designed in a manner such that it is secure.



Additional advantages of electronic locks

So far, we've discussed each attack surface by which an adversary might approach defeating a lock system, but it is important not to overlook the additional advantages offered by electronic locks that are not possible with mechanical systems. Logging, auditing, intrusion detection, monitoring, and remote or automated locking/unlocking each offer new and superior security usage scenarios that traditional mechanical locks are incapable of without an electronic security system counterpart. Electronic locks also provide the opportunity to provide single use keys, time-constrained keys, and other special key situations that best manage authorization and limit trust.

Design Validation

Many of the security benefits introduced by electronic locks are based on a system being properly designed and properly implemented. Without proper hardening, the very same security benefits of electronic locks become significant attacker ingress points. The academic research community has consistently demonstrated that many digital systems suffer from design and/or implementation flaws that leave ostensibly secure systems vulnerable. It is highly ill-advised to assume that a system is properly secured, without proper third party documentation to support such an assumption.

Overall Assessment

The distinctions between mechanical and electronic locks are intricate and non-trivial. In most settings, electronic locks offer far more benefits than drawbacks as compared to mechanical locks. It is sensible to be cautious when adopting this new technology, but not so timid as to deny the numerous advantages electronic systems have to offer over mechanical ones.

Mechanical locks fall short compared to electronic locks in the three primary attack surfaces that the two types share: The lock, the key, and key storage. In each of these areas, electronic locks offer opportunities for improved and additional security features that mechanical locks inherently cannot provide. Electronic lock systems do expose new attack surfaces, which should not be taken lightly, i.e., the user, the backend, and the protocol. However, when considering the advantages introduced by electronic locks, especially as it pertains to, key management, prevention of key forgery, and all of the *additional advantages* of logging, auditing, etc., these new attack surfaces are very often considered acceptable risks. As always, each business should carefully decide based on their own threat model and use cases.