Physical Security and Cybersecurity: Reducing Risk by Enhancing Physical Security Posture through Multi-Factor Authentication and other Techniques

Samuel Moses B.S.
Cyber Security Research Lab
Brigham Young University

Dale C. Rowe Ph.D.
Cyber Security Research Lab
Brigham Young University

Abstract

Physical security should be a fundamental part of our cyber security architecture and defense. Access controls, a key cornerstone in physical security, have become a weaker defense. The most common access controls, mechanical locks and proximity cards are no longer enough. New technologies and attacks have made it easier, more effective and cheaper to defeat these current systems. Today's thoughts on physical security posture needs to change because of the increasingly associated risk to data and critical resources associated with a physical breach. This paper brings a new perspective to physical security, multi-factor authentication, and other techniques to better an institutions overall security architecture.

1. Introduction

Physical security is fundamental in protecting information systems and services. Physical security is used to protect a company's premises, sites, facilities, buildings, people, information, and other assets [1]. It is an important part of protecting the confidentiality, integrity and availability of resources. It is vital to develop physical security in a way that can effectively secure critical resources, infrastructure and systems. The 'CIA triad' consists of confidentiality, integrity and availability. Security controls are designed to protect these aspects of information systems. Properly designed and maintained access controls are the cornerstone of securing and controlling organizations assets. They control how resources are accessed, and reduce the risk of unauthorized modification or disclosure [2]. However, many of today's physical security controls are insufficient. Relying on mechanical locks or proximity cards as a sole access control to secure the facilities is not enough. Mechanical locks always have some vulnerabilities that have some inherent risk and the proliferation of 3D printing makes it easier, more effective, and cheaper to exploit them [3]. Attackers can even decode keys from a distance using methods of optical decoding. RFID Proximity cards, another common security practice are also vulnerable to a variety of man in the middle and relay attacks [4]. Magnetic stripe cards are simple to clone using low-cost, readily available equipment and next to no technical knowledge. Even the latest biometric controls have been shown to be lacking [5].

This paper will discuss some of the key components of physical security, how new technologies have improved attack methodologies against current authentication techniques, and how multi-factor authentication can mitigate the risk of unauthorized physical access.

The author's experiences include several years' operating a student penetration test team on a college campus and developing curriculums for graduate level classes in penetration testing, incident response, information security and social engineering. A penetration test includes a negotiated security assessment proposal document consisting of the scope and rules of engagement, a permission memo and full verbose details of both procedural and technical measures. After the penetration test is complete, a comprehensive security assessment report is produced. This consists of a review of the penetration test findings, a timeline of the attack and the teams recommended mitigation techniques to better secure customer systems. These reports are confidential and we are unable to disclose specific information from penetration tests. Any examples shared in this paper will be based on real experience from actual engagements, but some details will be changed to help protect the privacy of our clients.

2. Physical Security Controls Types and Risk

Physical security is a critical part of an effective security plan. When properly leveraged it establishes policy, technical controls and education designed to provide appropriate risk reduction for an organizations assets and resources. As well as protecting against

malicious attacks such as theft, vandalism and sabotage; security planning should also provide protection against natural disasters such as floods or fires. The focus of this paper's discussion on physical security is focused more on the man caused attacks. ISC(2) suggest that security controls can be categorized into 6 control types: preventative, detective, corrective, recovery, deterrent and compensating: [6].

Preventative – controls meant to prevent unauthorized actions. Examples of preventive controls would include, locks, biometrics, mantraps, etc.

Detective – controls meant to send alerts during or after an attack. Example of detective controls would include job rotation, mandatory vacations, recording and reviewing security cameras.

Corrective – controls meant to restore systems to normal after unwanted or unauthorized activity. These normally only have limited capability to respond without user interaction. Example include antivirus solutions, intrusion detection systems, and business continuity planning.

Recovery – controls meant for after a security incident has occurred. Recovery controls are meant to restore functionality of the system and organization. Examples include reinstallation of Operation Systems and data restored from backups.

Deterrent – controls meant to discourage actions. Examples include "Beware of Dog" or "Security System" signs.

Compensating – These provide a supplementary or alternative solution to a control that is too expensive or difficult to implement.

Compensating controls are an important type of control, particularly when discussing physical security. A compensating control is an additional security control installed to help compensate for any weaknesses in another control [6]. To better illustrate this, the following is offered as a scenario we have previously encountered:

The Company under test had recently installed high security doors that required a biometric fingerprint to authenticate. In comparison with other more traditional methods this appears to be a good security control. However, due to delays caused by the scanner and multiple attempts being required to authenticate, it was noticed that users had started propping the door open due to the inconvenience they feel having to scan in. The result being the entire access control mechanism was defeated. Access for our team was as simple as walking through an open doorway. In fact, it was thanks to just one team-members observance that the security control was even noticed.

Despite this dramatic failure of a physical access control system, a simple example of a compensating control could be a policy published about not keeping doors propped open. Employees can then be trained as to the risks of such actions. Finally this policy could be enforced with an additional control that triggers an audible alarm for that any door left open longer than 30 seconds.

Alone, the fingerprint scanner introduced an increased risk of a physical breach caused by users propping the door open. Coupled with additional simple compensating controls helps to mitigate this weakness without significant additional expense. This is why compensating controls exist, to help support and secure the infrastructure by addressing weaknesses found in other controls.

Best practices would recommend that a series of these controls be installed to protect a company's assets. It has been our experience that physical controls are often weak and lacking. In nearly all penetration testing engagements that involve a physical assessment, even the most stringent logical controls have been defeated by poorly designed or implemented physical controls.

Recently, there is an increase of more technically advanced attacks such as phishing campaigns, VPN brute forcing, ransomware and DDOS attacks. Due to the 'hacker story' these more technical attacks are highly reported in the media and are often foremost on our thoughts when reviewing security plans. This can result in underestimating the criticality of physical security in favor of mitigating those of higher technical merit. It is important to be aware that physical security breaches have resulted in significant data losses and outages with little to no technical knowledge from the attacker. Hard drives or even laptops with gigabytes of data company data are easy targets for theft. Physical access to servers allows attackers to use known procedures or back door entry processes to break into the system using the console. Keyloggers readily available from online stores are usable by individuals with very little security knowledge to cause significant data breaches, illegal activities and system wide outages.

Many information systems are in-fact designed with the built-in ability to circumvent technical security controls using physical methods (i.e. CMOS password reset, local administrative credential recovery/reset, hard drive access by remote-mount). These procedures allow legitimate system administrators to recover from forgotten credentials or accidental lockouts. With this in mind, the criticality of effective physical security is obvious. These capabilities help reinforce the importance of making sure servers and equipment are in a physically secure location such as a secure network operations center or a server room [7]. In penetration tests, it is commonly considered that once an attacker has physical access to

a machine, it is game over because hackers turn these legitimate safety controls against the system administrators and have full administrative access, in full control of the system and its data.

As well as impacting the confidentiality and integrity of data, security planners should consider the impact of attacks directly targeting the availability of systems. This is another easy target if an attacker has physical access to your devices. Such attacks may be as simple as unplugging devices, cutting wires, or even damaging equipment causing hours, days, and even weeks in repairs depending on the extent of the damage. Consider the potential impact of physical damage caused to a power-grid high-voltage transformer. Transformer coils of this scale are expensive and most utility companies have a very limited supply of replacements.

Attacks against system or information availability almost always incur cause a financial loss due to the damage of the equipment as well as costing money in potentially excessive downtime and man-hours in recovery time spent restoring service availability. Technical attacks may be more common, but physical attacks can also cause a crippling monetary loss to an organization.

Security professionals need to ensure the physical security of a company is being addressed that the organization is fully aware of the risks they may be exposed to. Hackers tend to gravitate to the path of least resistance. If physical security is not properly addressed, then hackers can easily steal valuable data or disrupt critical services by exploiting simple vulnerabilities in a company's physical security.

3. Access Control Principles

Access controls are security features that control how users and systems interact with other systems and resources. This ensures that these privileges are kept to the authorized personnel only. The basic principles of access control are identification, authentication, authorization, auditing and accountability. These are commonly contained within the acronym 'AAA', although one should note that identification and accountability are not obvious from this.

Identification - subjects supply identifiable information such as usernames, user IDs, and account numbers.

Authentication - verifying the user's identification though some predetermined process such as using a passphrase, PIN, biometrics, and passwords.

Authorization - determines that the subject may access the resource. Roles are assigned to users to grant permissions of what operations that they are allowed to perform.

Auditing – logs of all previous stages are kept to ensure the effectiveness of these steps.

Accountability - Audit trails are reviewed to ensure that from identification to data access, users are accountable for their actions on, and interactions with a system. [2].

An effective physical security access-control system should incorporate all give AAA steps. Biometric scans, passwords, and physical keys are examples of the authentication method to evaluate whether a person is who he or she claims to be. Once a person is properly authenticated, the authorization control can determine if the person has the proper access rights to enter.

An example that goes through all five of these access control principles would be a person passing a security checkpoint. The person would offer up their ID, then the guard would check the ID to verify their information. Once verified the guard, the guard would ask for the passphrase. The person would offer up the passphrase. With successful authentication, the guard should verify they have access to the requested facility. At this point, they may be granted access and the guard would record this in a logbook. If unsuccessful, the guard would redirect or even detain them depending on policy. Then if an incident occurs past the security checkpoint, an audit can be performed to confirm which persons had access to the facility. This overall process leads to accountability where users attempting to access resources can be held fully accountable for their actions. Properly implemented access controls that provide accountability in either a physical or digital environment provide non-repudiation.

Access controls are a corner stone for physical security. Weak access controls create opportunities for an attacker to breach a company and as discussed above can cause devastating losses to a company. This is often a weak point in a companies' security that needs to be strengthened. Part of the weakness is due to companies' current access controls becoming outdated. Physical security *needs* to evolve with changes in threat and their mitigation brought about by new technology.

4. Mechanical Access Controls Exploited Through New Technologies

One of the oldest and most used forms of access controls are mechanical locks. Mechanical locks are vulnerable to a variety of attacks. The three most popular attacks on mechanical locks are lock picking, impressioning, and copying.

We draw attention to the fact that mechanical locks, when used as a standalone control, do not meet the requirements of AAA. The only aspect of AAA that is

met is that of authorization, that the proper holder of the key is authorized to do so. But even this is not sufficient for auditing and accountability due to the lack of identification and authentication.

One new technology that has further weakened mechanical locks in particular is 3D printing. This has made all three previously listed types of attacks more effective, resulting in current mechanical locks being woefully insufficient as a standalone control.

4.1. Lock Picking

Not always the most effective, lock picking is the most known attack on mechanical locks. A small torque is applied to the keyway of the lock or cylinder and the pins are pushed up until the pin tumblers sitting on top of the pins engage the shear line. This attack requires the appropriate tools on wafer locks, tube locks, and other kinds of locks using a variety of techniques including raking, scrubbing, and bumping [3].

With 3D printing, a person can easily and cheaply manufacture any specialized tool for lock picking. When using torsion wrenches or other force-applying tools there is the stronger-boding polymer process or the metal printing process. For permanent or reusable tool manufacturing, a person can design and implement a prototype version in a cheaper and more readily producible plastic format. These prototypes can then be evaluated and iterated upon to develop a more precise tool. Following that, to provide longevity and strength a final version can be made using a metal printing process [3].

4.2. Impressioning

The decoding of the bits on a target lock is performed through impressioning. A prepared key blank is used to make a copy of the key for the target lock. The blank key is placed in the lock, torque is applied, and the key is moved against the pins. Binding friction slightly marks the pins on the blank. The key is then removed from the lock, inspected for marks, and cut with a file. Cuts are made one bit-depth at a time, and the process is repeated. If successful, the attacker will have a working key. This process has its own complications. If impressioning is not done correctly, an attacker could possible apply too little or too much torque or force and cause missed biting marks, false positives, or damage the target lock [3].

While vendors have attempted to protect the distribution of high-security key blanks, it is now possible to 3D print blanks. Using a key sample, which can be gathered through reconnaissance or a photograph, 3D printing provides another avenue of attack that makes creating blanks for locks cheap and easy. 3D printed keys are stiff but malleable plastic keys also make it easier for leaving impressions and marking the keys. Easy access to 3D printing facilities ensures that attackers can access blanks, circumventing the security practices put in place by limiting blank distribution [3].

4.3. Copying

When making a copy of a key a person needs an exact duplicate of the key's bitting. The techniques to get this key bitting include lock picking and a pin lock decoder, but each of these techniques are very intrusive. A more covert option would be to take measurements and decode the key's bitting but even that takes time and has the possibility of the owner noticing their missing key. All these techniques require physical access to the lock or key, which puts an attacker at greater risk. Previously, this was part of the advantage of mechanical lock security, but now there is a method of optical decoding that has become a threat, and allows an attacker to decode the bitting on a key from a distance [8].

Optical decoding is based on four assumptions: 1) The target key "type" is known; 2) A key face can be approximated by a 2D plane; 3) Absolute metric measurements are known for a reference image of a key; 4) A user supplies point correspondences between these reference measurements and their location in the target key. Of the four assumptions all are minor hurdles except the second one. A picture of the key needs to be taken so a precise edge detection can be taken, and could otherwise introduce errors when modeling. To test the limitations of this option, an experiment was done using a camera costing under $2,000 dollars, from 195 feet away the key image was captured and was able to be correctly decoded [8].

After the key has been decoded, 3D printing is the next logical step. If the goal is to have a permanent key, or a key as close to the likeness as possible, a metal printing process should be implemented. An exact duplicate is even possible, including the numbering, logos, and even including simulated wear when properly modeled. This can be extremely helpful when combined with social engineering since the key will not only work but can be seen to look ~~to~~ the part. Using social engineering an attacker can even gain an official key. Using a key designed to appear worn, the attacker can turn it in to a facilities officer, requesting a new official key. No longer would a forged key be in circulation, and the attacker has an official real key [3].

There has always been some weakness to the access control offered by mechanical locks, but now with the developments of 3D printing and optical decoding the security offered by these locks is even weaker. Indeed, we propose that mechanical locks

should now be considered a deterring control as they no longer offer effective preventative capabilities (we do concede that transponder-equipped mechanical locks with transponder verification still offer primitive preventative control capabilities. Such keys are commonly found in automobiles to release an engine immobilizer).

Security needs to change as new technologies are developed. An attacker no longer needs physical access to the lock or key to make a copy anymore. They can now take a picture, even from great distances, and be able to print their own keys to use to break into the buildings and have access to any systems they want. Using mechanical locks as an access control has become a greater risk.

5. Proximity Cards Continue to be Under Attack

Different types of badges are being used as access controls today. Some badges use a magnetic strip that a user needs to swipe for entrance but it appears industry as a whole is moving away from this technique. There are two different types of proximity cards: passive and active. Passive cards are the more widely used type, which have a limited range and must be held close to the reader unit. The card can be left in a wallet or purse, and by holding the wallet or purse close to the scanner it will be able to read it. Active cards, otherwise known as vicinity cards, are powered by an internal lithium battery. They have a greater range (up to 2 meters), and are often used for an application where the card is read inside a vehicle, such as security gates. With active cards the battery eventually runs out and the card needs to be replaced every 2 to 7 years [9]. Between the two, the industry standard is moving towards passive proximity cards.

Proximity badges are used in many places today. Companies may use these badges to gain access to both computer systems and physical locations. Some organizations such as transit authorities, busses and subways may use them as a means of taking payment. While using badges for access control can overcome the security vulnerabilities of mechanical locks, many doors maintain a mechanical lock to use in cases where the power might go out, or other technical issues could arise. However, since employees are using their badges to scan in and out an attacker's access to the get a copy of the key is much more limited. Additionally, as the use of a key only occurs in extenuating circumstances, key use is abnormal and should be thoroughly examined. Simple reed-switches can be used to identify times where the door has been used in the absence of a proximity card. Due to the reduced key usage, attacks on mechanical locks are forced to go back to the older practices where they need physical access to the lock to be able to decipher the bitting of the key, which puts them more at risk.

Using proximity cards for access control helps mitigate the risk created through optical decoding and 3D printing, but they have their own weaknesses. There are a variety of attacks that can be used, in this paper we will bring up two: Man in the Middle and Relay Attacks.

5.1. Man in the Middle

For a man in the middle attack, an attacker is essentially acting as a middle man intercepting a transaction and then passing it on. The attacker acts as a card reader taking the information on the card then relaying the information to the true reader. This allows the attacker to sniff the traffic between a card and a reader stealing its access credentials, which would allow an attacker to impersonate the card. A Man in the Middle attack makes is possible to alter data as its passed through [10]. This attack may thus provide higher privileges than those held by the legitimate card owner.

5.2. Relay Attacks

A relay attack is where an attacker relays communication between the reader and the authentication card or token. A successful relay attack allows an attacker to possess a copy of the card. For a relay attack, one needs two devices to act as the card and the reader. They establish a relay channel and establish a connection which the reader and card is unable to distinguish from the true one [11].

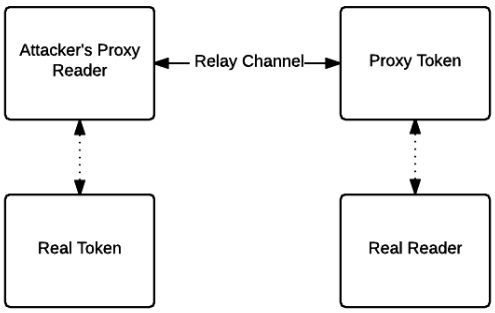

Figure 1. Relay Attack [7]

A relay attack circumvents most application layer security mechanisms and the attacker only needs to relay the communication between a token and a reader for a transaction. With this attack even high security tokens that implement strong modern encryption techniques are at risk [11].

There is danger to an organizations property and data when an attacker has physical access to our

devices. There are different access controls out there, but the two most popular ones are proximity cards and mechanical keys. Both of these have weaknesses in them that an attacker can exploit to gain access to our internal systems. Changes in policy and security architecture are needed to more effectively manage the increased risk to our facilities and people.

6. Authentication Principles

Security is something everyone is concerned about. Using authentication as a primary access control is common practice, however the methodology needs to be updated. There are many modern authentication systems that seek to increase organizational security. Valid authentication methods are guided by a set of principles 1) something you know, 2) something you are, and 3) something you have. Other less-common principles in modern authentication systems may include someone that you know, your location and the access-time. Location has limited utility in physical-controls as the assumption is the requester is physically present. Access-time may also be left until the authorization stage in many systems. The 'someone-you-know' principle however, while less-common, can create a vulnerability that can be exploited through social engineering.

The first principle, based on the idea of *something you know*, is the use of credentials held in the individual's memory such as a password or a PIN. A person will remember this passcode and, when challenged, the individual needs to be able enter the password of PIN to enter that location or site. We use this type of authentication every day in our lives. Our email passwords, our ATM PINs, the passcodes on our phones, all of which fall under this principle of something you know and commonly use. Passwords still are the most prevalent form of modern authentication used to verify who a person is. Some banks are now requesting elements of a password or PIN rather than the complete word or number to mitigate the risk of shoulder-surfing (where an attacker watches you enter a password) and keylogging.

Something you are is the authentication principle based on physical or biological characteristics of someone as a person. Using biometric technology, a system can verify a user's identity from their physical characteristics. Current practices use one or more of four biometric methods to establish a user's identity to an acceptable level of confidence. These methods have been shown to offer enough uniqueness and reliability to be effective. The first biometric factor is fingerprint scans, a tool that has been in use by law enforcement and government agencies for decades. Throughout this time, it has been proven to be a reliable and unique identifier for authentication. Second is scanning the retina or iris of one's eye. These scans analyze the arrangement of blood vessels or the patterns of color in the eye to confirm someone's identity. The third option for using physical attributes of authentication is voice recognition. A voice print analyzes how someone says a word or sequence of words which can uniquely authenticate an individual. Fourth and lastly is facial recognition. This method uses the unique features present on one's face to identify and authenticate the individual [12]. A newer mechanism in current research involves the observation of an individual's gait, or posture as a feature.

Third is the principle of *something you have*. This is something you might have in your possession such as a proximity or magnetic card, a key, or a cellphone. Cellphones are a great modern-day tool for authentication. Different applications have code generators, or a phone can receive a text to verify who you are. Since a phone is often something a person keeps on them it makes for a great modern form of authentication. Cellphones can also be multi-factor authentication devices in their own right with fingerprint scanners, pin-numbers and passcodes. Thus used as an authentication device, a cellphone may fulfil all three primary authentication principals.

The most common form of authentication that follows the principle of something you have is a key. Keys are used everywhere from people using them to secure their homes, places of business, and cars. Asides from the previously discussed limitations of keys as a physical security control a general disadvantage of using *something you have* is if the device is lost or stolen, authentication may no longer be possible.

The last principle we shall discuss for physical authentication is based on *someone that you know*. This principle is not formally considered one of the three primary authentication principles but still has merit, particularly in having an expedited ability to offer short-term, temporary access. For example, given a policy may stipulate that a manager or authority must approve all requests to interact with a specific asset or group of assets. In some cases, this is even required to be completed in person with the manager and user both there.

This principal revolves around an element of human-trust where the approving authority has some method to know the user making the request. This is usually by prior familiarity with either the individual or the request. The reliance on the human-factor opens this policy to being targeted by social engineering attacks. Knowing enough information to act like a user belongs, or name-dropping appearing to know the people they need to gain access is an attack used in this area. Social media has created this weakness to be stronger with the proliferation of personal details

across the Internet. The disadvantage of this authentication principle is the human factor.

There are strengths and weaknesses to each of these authentication principles. Despite their weaknesses, most physical controls are based on the '*something you have*' or '*something you know*' principals.

As we mentioned in our conclusion to section 4, mechanical locks are incapable of satisfying AAA access-control requirements. With this in mind, many organization may find themselves lacking any physical access control whatsoever.

7. Multifactor Authentication on Physical Access Controls

Each of the discussed physical access controls has various advantages and disadvantages. Being aware of their flaws and creating hybrid multi-factor access control platforms can be very effective in comprehensively and effectively minimizing the risks of a physical security incident. Multi-factor authentication is offered when the access-control mechanisms require more than one authentication principal to establish the user's identity. The most common form of multi-factor authentication is two-factor authentication. This is so-named as it verifies authentication using two different principles.

Multi-factor authentication adds an extra layer of protection. The best multi-factor authentications combine more than two different types of validation into an access control: 1) something you know, 2) something you are, 3) something you have, and 4) someone you know. Mixing the different principles of authentication offers the best security.

In some situations, the same authentication principal may be used to provide multi-factor authentication. This usually relies on multiple users authenticating together (and thus indirectly fulfils the *someone you know* principal). An example of dual authentication is when a user has one key for the door handle and another key for the deadbolt. In this instance the user is still using multi-factor authentication, but they both use the same authentication principle, *something you have*.

However, in the instance when a user can login to their email with a password, then be prompted by a second password, both factors are based on *something you know*. While it can be argued that this offers an extra level of security, because an attacker would have to know both passwords to get access then the same method to obtain the first password is typically effective obtain the second. Thus established best-practices require the second form of authentication to be based on a different principle. For example, in the above example, the user might be texted a time-limited numerical code to validate that they have their cellphone. By combining *something you know* with *something you have*, the system becomes more resistant to one form of attack and confidence in a user's identity is increased.

Many consumers today use multi-factor authentication often without realizing it. The use of ATMs for example, requires an ATM card, which is *something you have*, along with a Personal Identification Number or PIN. The PIN, which is typically four or more characters, is *something you know*. Thus multi-factor authentication systems do not have to be disruptive or inconvenient, and can actually become intuitive if well designed.

Securing email by dual factor authentication is also becoming more common and many email providers now offer this option. Email providers offer to send a verification code to a user's phone upon login. When a user logs into their email they first input their password (*something you know*) and then are prompted to enter a verification code. This code is sent through a text or application to the user's phone (*something you have*). The user has now authenticated themselves twice to better secure their email. This may seem time consuming to logging into one's email, but by just adding a couple of seconds a user has added another layer of security. A weak or stolen password no longer by itself has the ability to cause account compromise. And today, almost everyone has their phone with them all the time. For Payment Card Industry (PCI) compliance, when using a Virtual Private Network (VPN) a user is required to use two-factor authentication. This is normally completed through a password and a second authentication type such as a number generating dongle that a user is required to enter in.

Each of these implementations of multi-factor authentication discussed has been more about the technical aspect of security. As stated before, physical security's importance is often underestimated in favor of more technical attacks, but the same principles applied in these security improvements can be used to better enhance our physical security. Combining different authentication principals will add additional protection needed for physical security. This needs to become standardized as a best practice to ensure that physical security can keep pace with new attack vectors.

Implementing properly designed multi-factor authentication using distinct principal types can significantly reduce the risk of a successful attack. A proximity card relay attack has had only limited success when a systems has failed to implement effective multi-factor authentication [11]. Attackers who might be practiced and prepared to attack and pass mechanical locks can now be prevented by facing a

second form of authentication such as a PIN or a fingerprint scanner. Using these different forms of authentication in conjunction with one another will better enhance the security posture of a company.

8. Layer Physical Security Controls

Defense in depth is a common principle in cyber security that involves layering security controls across a system. For example, network security across multiple layers might include a border firewall, compartmentalization, web application firewall, intrusion detection systems, and internal firewalls. Access controls and antivirus software provide additional layers of security on top of this [13].

Defense in depth, or security layering is designed to provide a greater resilience against security breaches. This concept should also add levels of protection to physical security. Applying defense in depth to physical security should also plan for contingencies in the event of a physical access-control breach by requiring additional controls for attackers to face before accessing critical resources.

Combining control-types can provide a comprehensive physical security plan. For example, a fence can act as both a deterrent and a preventative control, but if an attacker were to circumvent this, locks on doors provide a further security control. Furthermore, door alarms can be set so that after hours, their opening triggers an alarm and notification. This detective control should be handled by security guards to provide further detective and a corrective security controls.

Applying defense in depth principle to physical security provides better overall protection of resources and helps defend critical resources in incidents when one security control gets breached.

9. Built-In versus Bolt-On Security

Built-in security is a term used to describe the designing and inclusion of security features when a plan, architecture, or program is still being developed. Bolt-on security is a term used to describe the addition of security features after a plan, architecture, or program has already been completed and developed by attempting to help make an already in-use system more secure. In security it is a better practice to build in security feature in the initial planning and developing stages versus bolting on security features. However, bolt-on security is far better than attempting a plan, architecture, or program without trying to include any security features as it will open up even more vulnerabilities for hackers to attack. The best practice in development, even when it comes to physical security, is to build the security features into the plan from onset.

For example, if a building is to be located in a high flood-risk area this needs to be prepared and planned before the building is started. Trying to prevent the risk of a flood after the fact would be costly, less effective and inefficient. To better protect and secure our building and resources, security professionals should review the company's needs and the development plans from the outset. Even with this example, improving the building defenses against flooding with a bolt-on approach would help reduce the risk exposure and would be better than leaving the building completely exposed to flood damage.

Remodeling can also leave an organization exposed to physical threats. This type of weaknesses was revealed after a penetration test of a department. After remodeling and space reassignment, a physical penetration test was requested. The remodel consisted of updating and moving around some office areas. To accommodate for increased faculty they decided to move their main department entrance to ensure all faculty offices would be behind the locked department entrance. In theory, this move would mean that anyone trying to get into a professor's office would have to get past the double doors with a high security lock, then the professors' door lock. Potentially, a good implementation of the defense in depth principle. Hackers and security professionals look at things differently and strive to take the path of least resistance when exploiting vulnerabilities. In this case, it meant slipping into the building at night and checking above the tiled room to see if the double doors had a physical firewall above the suspended ceiling. A firewall in physical security is a wall designed to help stop fires from spreading past a certain point by creating fire resistant hard walls to help segregate rooms. This increases protection against unauthorized intruders by preventing users attempting to circumvent physical security controls.

Moving the double doors down the hallway, created vulnerability discovered in the penetration test because the original firewall above the doors had not been relocated during the remodel. Thus the team was able to easily exploit the vulnerability by having one team member slip through the tile ceiling, drop on the other side and open the doors using the emergency escape handle to provide access. The plan to better protect two more offices by putting them before the double doors created an easily exploitable vulnerability, which put all the offices and department files at risk. Additionally the original intent of the firewall (to slow the spread of fires) had been completely negated as the suspended ceiling firewall no longer connected with the fire-retardant security doors to provide an airway barrier. With proper

security planning before the remodel, this vulnerability could have been rectified before any construction work commenced.

Hackers target the easiest vulnerability with the least resistance and physical security tends to be one of these vulnerabilities. To breach a system, hackers often chain a series of easy exploits together. This is commonly known as a kill-chain. Vulnerabilities in physical security opens many new avenues of attack.

10. Social Engineering Awareness Training

Exploiting the fourth authentication principle, someone you know, is often completed through social engineering. Social engineering is the use of persuasive techniques that target human nature to convince people to conform to one's own desires [14]. When performed properly, a person will not even realize they have been a target or are under attack, and it causes the target to willingly give valuable information or access to an attacker.

When focusing on physical security with social engineering, the focus includes non-technical hacking such as shoulder surfing and tailgating. Shoulder surfing is when an attacker will observe a target entering in their password, and then reuse it to later defeat a security control. Within the context of physical security an attacker may attempt to view and memorize a door code so that they can gain entry at a later time.

Tailgating is another simple nontechnical attack that can give an attacker instant access. Tailgating is when an attacker follows an authorized employee or group of employees through an entrance to gain access. Sometimes attackers will be carrying heaving boxes or a stack of papers, so an employee will feel like they are being polite and doing them a favor by holding the door open, when in reality the victim just gave the attacker access to an area they were unauthorized to be in.

The best defense in these situations tends to be user training. There are other measures that can be taken to help as well, such as requiring badge swipes and adding covers to keypads to help defend against these type of attacks. To defend effectively against social engineering attacks, users require regular awareness training and need to understand the potential consequences that seemingly insignificant oversights can have in an attacker kill-chain. An attacker can follow a group of employees into the building, then walk out with a laptop full of company secrets, but if a company has trained its employees to report anything suspicious and required badge swipes this type of attack would be less successful.

We can attempt to secure our infrastructure the best we can, but the weakest point in our security will be the human element [14]. Training the people to better understand the attacks to defend against them and to understand the risk if a breach occurs can help secure our data and physical resources from social engineering attacks.

11. Conclusion

Technology often gets developed quickly and security is slow to follow. It is essential for security to evolve and change to keep up with these advances. We recommend that mechanical locks are unsuitable as a preventative control given advances in 3D printing and optical decoding. In security planning these should be seen as a deterring control and not part of an effective AAA strategy.

Proximity cards have offered a different solution from using mechanical keys but have weaknesses that allow attackers to clone cards for access. Man in the Middle attacks can even allow attackers to elevate their access level to a higher authorization than the original card allowed. We encourage the use of such controls as part of a wider AAA implementation as they offer the ability to effectively authenticate individual users and maintain audit capabilities when properly implemented in a multi-factor authentication system.

Physical security breaches offer attackers a wide variety of ways to damage a company including but not limited to: property damage, availability, and data loss. Damage like this can jeopardize a company's reputation and can require little to no technical knowledge to perform.

Social engineering is a dangerous threat. Targeting the human element by manipulating goodwill and human nature allows attackers access to unauthorized areas and potentially critical resources or data. These attacks often require little to no technology, but can cause still be the cause of serious financial loss with a significant impact to confidentiality, integrity and/or availability.

Layering physical security controls by applying the defense in depth principle can better protect a company's assets. Preparing to include security features from the start will also better establish a more secure architecture. Awareness training will better prepare people to defend themselves against letting attackers use their own human nature against them.

Security professionals must be vigilant in planning physical access controls. Concepts and principles designed to protect information systems from technical attacks provide an effective method of designing and establishing physical security.

It is vital we ensure the security of our people and data from physical attacks, not just technical attacks such as hacking and phishing. Solutions should include multi-factor authentication, defense in depth, including

security and the security team at the beginning of changes and development, and training people to be aware. Designing the security infrastructure properly, a security professional can more effectively manage risk and protect the organizations assets.

12. References

[1] M. Perry, Effective Physical Security (Fourth Edition), Fourth. Elsevier Inc., 2013.

[2] S. Harris, ALL IN ONE CISSP EXAM GUIDE, Sixth Edit. McGraw-Hill, 2013.

[3] B. Doyle, C. Goettel, L. Broadbent, and D. C. Rowe, "MAKER: Call a 3D Locksmith – How 3D Printing can Defeat Physical Security," in Proceedings of the 2015 ASEE Annual Conference and Exposition, 2015.

[4] F. Brown and S. Shubham, "RFIDiggity: Pentester Guide to Hacking HF/NFC and UHF RFID," in Defcon 23 Archive, 2015.

[5] K. Cao and A. K. Jain, "Hacking Mobile Phones Using 2D Printed Fingerprints," MSU Tech. Rep. MSU-CSE-16-2, vol. 16, no. 2, 2016.

[6] E. Conrad, S. Misenar, and J. Feldman, Eleventh Hour CISSP, 3rd Edition. Syngress, 2016.

[7] S. Moses, D. C. Rowe, and S. A. Cunha, "Addressing the Inadequacies of Role Based Access Control (RBAC) Models for Highly Privileged Administrators : Introducing the SNAP Principle for Mitigating Privileged Account Breaches," vol. 6, no. 3, pp. 583–591, 2015.

[8] B. Laxton, K. Wang, and S. Savage, "Reconsidering Physical Key Secrecy : Teleduplication via Optical Decoding," Security, pp. 469–478, 2008.

[9] "Proximity Card," Wikipedia The Free Encylopedia, 2015. .

[10] M. Meriac, "Heart of Darkness - exploring the uncharted backwaters of HID iCLASS security," 27th Chaos Commun. Congr. Berlin, no. December, pp. 1–13, 2010.

[11] G. P. Hancke, "Security of Proximity Identification Systems," Univ. Cambridge Comput. Lab., no. 752, 2009.

[12] M. Owens, "Biometrics and User Authentication," SANS Institue InfoSec Read. Room, 2002.

[13] D. C. Rowe and K. A. Rowe, "Space - The Final Cyber-Frontier? Adopting space industry practices for critical systems cyber-security," in Proceedings of the 2013 BCS International IT Conference, 2013.

[14] S. Moses, N. S. Baker, and D. C. Rowe, "Helping the Human Element : Educating in Social Engineering," 2016, no. ASEE 123rd Annual Conference.

