Replication Prohibited: Attacking Restricted Keyways with 3D Printing

Ben Burgess
University of Michigan
baburges@umich.edu

Eric Wustrow
University of Michigan
ewust@umich.edu

J. Alex Halderman
University of Michigan
jhalderm@umich.edu

Abstract

Several attacks against physical pin-tumbler locks require access to one or more key blanks to perform. These attacks include bumping, impressioning, rights-amplification, and teleduplication. To mitigate these attacks, many lock systems rely on restricted keyways and use blanks that are not sold to the general public, making it harder for attackers to obtain them. Often the key blank designs themselves are patented, further discouraging distribution or manufacture by even skilled machinists.

In this paper we investigate the impact that emerging rapid prototyping—or 3D printing—tools have on the security of these restricted keyway systems. We find that commodity 3D printers are able to produce key blanks and pre-cut keys with enough resolution to work in several commonly used pin-tumbler locks and that their material is strong enough to withstand the requirements to perform the aforementioned attacks. In addition, in order to demonstrate the low skill requirements necessary to perform these attacks, we develop a tool that automatically generates a 3D printable CAD model of a key blank using only a single picture of a lock's keyway. This tool allows us to rapidly manufacture key blanks for restricted keyways that were previously difficult to make or buy. Finally, we discuss possible mitigations for these attacks that lock manufacturers, installers, and users can perform to protect their assets.

1 Introduction

Locks are a central component of modern society, providing defense against opportunistic and dedicated attackers alike. Locks employ a wide variety of mechanisms to ensure only the owner of a certain key or code is able to open the lock. Of these various types, *pin tumbler locks* are commonly used to protect a wide range of valuables including homes, offices, data centers, and banks. Pin tumbler locks work by placing an inner cylindrical plug within an outer housing with several pins in drilled shafts between the two cylinders. Without the proper key, the various sized pins mechanically block the inner plug from rotating. However, when the correct key is inserted, the pins are raised in a specific configuration that allows the inner plug to rotate freely, opening the lock.

In addition to overt brute force attacks such as drilling and cutting, there are many known non-destructive attacks on pin tumbler locks including lock picking [23], bump keys [23], decoding color-coded pins [15], teleduplication [11], and rights-amplification in master-keyed systems [1]. With the exception of picking, which requires attacker skill or luck when attacking well-made locks, all of these attacks depend on the adversary having access to *key blanks*. Key blanks are keys that fit inside their respective locks but are not yet cut to a specific key biting. With access to a blank, an attacker can easily cut it to be a copy of any key, create a bump key, or test other key biting variations.

Many key blanks can be purchased cheaply from hardware stores or online. These blanks—such as SC1 and KW1—are commonly used in home locks and are not intended for high-security applications. In higher security applications, lock manufacturers offer customers *controlled blanks*. These blanks are more difficult for an attacker to obtain because manufacturers often hold patents for their design and only sell them directly to customers who have purchased a large volume of locks from them. Customers with smaller systems have the cuts for their system randomly generated by the lock manufacturer and are only provided pre-cut keys to these codes. Some key-control systems include keys specifically designed to be difficult to produce by standard manufacturing methods (such as CNC milling), further ensuring all keys must come from the manufacturer directly.

In this paper, we show that it is currently practical to use consumer-available 3D printers or services to produce keys and key blanks, even when the blanks are controlled, patented, or specifically designed to be difficult to manu-

facture. To demonstrate this, we develop a tool that can automatically generate a CAD model of a key blank from a single image of the lock itself. Generally made from plastic, we show that when properly designed, 3D printed keys can be durable enough to withstand use in operating locks and are strong enough to throw latches multiple times. Although 3D printed plastic keys are not ready to replace metal keys in everyday benign uses, we show that current 3D printers and materials are more than capable of facilitating attacks, lowering the bar for clandestine operations. To investigate the possibility of using a 3D printed key as a normal key in everyday use, we additionally test 3D printed metal keys.

Contributions:

- We develop a tool for rapidly producing 3D printable key models from a picture of the lock itself.
- We test the robustness of 3D printed keys across various materials including plastic and metal and over several keyways commonly used in practice.
- We describe applications and specific attacks that this new technology makes practical or lowers the cost for performing.
- We discuss several defenses to this growing threat and offer mitigations that lock manufacturers, installers, and users can perform to protect themselves from these styles of attack.
- We release our tool as an open-source project; code and a demo are available at https://keysforge.com/.

2 Background

In this section, we present background on pin-tumbler locks, controlled blanks, master key system vulnerabilities, and rapid prototyping as they apply to our attack.

2.1 Pin tumbler locks

Pin-tumbler locks are the most popular type of mechanical lock, with a history dating back potentially thousands of years [21]. Modern pin-tumbler locks are comprised of three main components:

- A brass plug with a specifically shaped channel cut into its length, called the *keyway*.
- A brass housing which contains the brass plug.
- Brass pins of varying standard lengths placed inside pin chambers.

The brass plug is placed inside the brass housing, and pin chambers are drilled perpendicular to the length of the housing. In a basic (non master-keyed) pin-tumbler lock, two pins are inserted per chamber. These pins block the plug from turning unless the pins are raised so the space between the two pins lines up with the interface–or sheer line–between the plug and housing. A working key cut with the corresponding code of the bottom pins in each chamber will align each pin-stack across the sheer line, allowing the plug to turn and the door to unlock. The setup described above is illustrated in Figure 1 with each pin chamber comprised of both a red and blue pin.

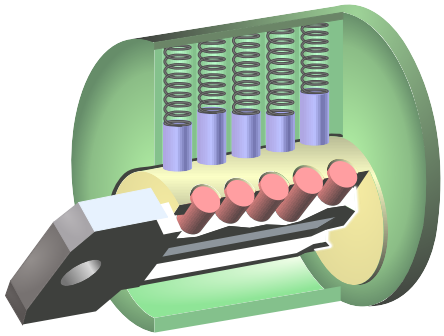


Figure 1: A view of the inside of a pin-tumbler lock with the correct key inserted [24].

2.2 Controlled blanks

Unauthorized copying of keys is a concern for both businesses and residential lock users. Temporary keys given to contractors or service workers run the risk of being copied without the owner knowing, even if the original key is returned. With standard key blanks any person who has possession of a key for a short amount of time can make a copy of the key. In some circumstances, it is even possible to copy a key from a simple picture or observation of it. These attacks can be aided by the use of telescopes or telephoto lenses to obtain pictures of keys from far away [11]. To mitigate this problem, lock manufacturers designed and patented proprietary keyway channel designs. Patented keyway designs ensure that other third-party key blank manufacturers cannot produce blanks that work in these locks. An attacker that is able to obtain the cuts of a restricted key will still find it difficult to copy this key, as typical hardware stores that copy household keys will not carry these blanks, and even locksmiths may be unable to purchase them. Copies of keys in these systems are generally done by the lock manufacturer, who authenticates copy requests with corresponding proofs of purchase, identity verification, or key cards.

2.3 Master key systems

In a master-keyed system, there are multiple locks, each with a specific key called a *change key*. In addition, there is also a special *master key* that is able to open all of the

(a) 3D printed nylon plastic Best G key

(b) 3D printed brass SC1 key

(c) Brass KW1 key, twisted 90 degrees

Figure 2: **3D printed keys** — Keys printed in both nylon plastic and brass along with a brass key deformed due to excessive torque.

locks in the system. Thus, each lock has two keys that can open it: the lock's specific change key and the system's master key. In some systems, there are multiple layers of masters, such that subsets of the locks can also be opened by the group's *submaster key*.

To master key a lock, additional pins are placed in some or all of the pin chambers. This allows there to be two or more possible key cuts that will align the pin stacks across the sheer line. The master key will use one of the cuts while the change key will use the other.

Privilege escalation Although master-keyed systems are convenient for users, they can introduce additional vulnerabilities such as privilege escalation attacks. Matt Blaze described one such attack which would allow an attacker to easily derive a master key to a system from a low-level change key [1]. In this attack, an adversary with access to a single change key and access to its corresponding lock can efficiently query the lock to determine the master key cuts for each pin position and derive the system's master key.

The attacker must first obtain a set of blank keys for the keyway he is trying to attack.The attacker then cuts this blank key identical to the change key except on one position; the remaining position is left uncut. This effectively isolates querying a single pin stack, as all of the other pin stacks will be aligned due to the key being identical to the change key at these other positions. This key is then tested in the lock and if it opens, the attacker learns the master cut on the targeted pin stack. Otherwise, the attacker files down the cut at this position to the next lowest value (skipping the change key cut) and tries the key again in the lock. Eventually, the key will open the lock and the attacker learns the cut of the master key on the targeted pin stack. He then repeats this process, starting with a new key and querying a different pin stack until all of the master pin positions have been learned in all the pin stacks. At this point, the attacker can now cut a master key to the system. A common defense to this known attack is to use restricted keyways, making it difficult for an attacker to obtain the N blank keys needed to attack an N-pin lock system.

2.4 Rapid prototyping

The increase in availability of prototyping tools such as 3D printers have allowed people to create intricate models and designs at home for relatively low cost. 3D printers, including Makerbot Replicator [13], Printrbot Simple Metal [16], Ultimaker 2 [22], Formlabs Form 1+ [3], and Cubeify Cube 3 [2], are now available in the $500–5000 price range. Services such as i.materialise [5], Kraftwürx [8], Sculpteo [17], and Shapeway [18] even allow people to upload their model and have it professionally fabricated on high resolution commercial 3D printers for a small fee. In addition to plastic, these services also offer "printing" in metals, including brass, stainless steel, sterling silver, titanium, and even gold. While these materials can be significantly more expensive (e.g. $\$16/\text{cm}^3$ for brass, $\$600/\text{cm}^3$ for 14K gold vs. $\$1.50/\text{cm}^3$ for basic plastic), as we quantify, these prints are significantly stronger than their plastic counterparts.

Plastic printing process The majority of desktop 3D printers (with the exception of Formlabs Form 1+) use fused deposition modeling (FDM) to "print" a 3D model one layer at a time. The print head is a heated element that extrudes a thermoplastic—typically acrylonitrile butadiene styrene (ABS) or polylactic acid (PLA)—and is moved in two dimensions over the printing surface by computer-controlled servos. After a layer is deposited, either the print head or build plate moves vertically, and the process repeats for the next layer. Since the plastic is heated to a specific temperature as it is extruded, each layer partially melts with the previous layer, forming a single object. An example of the result of this process using nylon plastic is shown in Figure 2a.

Metal printing process Metals such as brass, sterling silver, titanium, and gold are printed by first printing in wax using a specialized FDM printer. A plaster mold is then created around the wax print and placed in a furnace to melt the wax out. Next, molten metal is poured into the now empty cast to create the finished product [19]. An example of the result of this process using brass is shown in Figure 2b.

Stainless steel is printed by depositing a layer of stainless steel powder onto the build plate and then placing drops of glue on the layer, similar to FDM. The resulting glue-powder model is carefully removed from the build plate and placed in an infusion process which replaces the glue with bronze. This results in a very durable all-metal key [20].

3 Strength Testing

To evaluate the viability of using both metal and plastic 3D printed keys in attacks against restricted key systems, we produced several designs of keys, had them printed in several materials, and measured how much torque they could withstand before breaking. We chose three common keyways: SC1, KW1, and Best G. For each keyway, we created a 3D model using OpenSCAD (a 3D modeling suite), with random cuts on the keys. After prototyping these models using a MakerBot Replicator 2, we contacted a 3D printing service to fabricate them in several materials including nylon plastic, acrylic plastic, alumide plastic, brass, bronze, and stainless steel.

To test the maximum torque each key could withstand before breaking or permanently deforming, we used a CEDAR DID-04 torque screwdriver which provides 12 torque readings per second and measures up to 35 inch-pounds. We created a notch in a socket to fit the key bows to connect the key to the CEDAR DID-04. We mounted the lock cylinders for each keyway in a bench-top vice and combinated the locks such that they would not open for any of the keys (providing resistance for us to turn against).

We also used the torque screwdriver to measure the torque needed to open a collection of common locks in order to compare the breaking strength of each key to forces they might experience in real-world scenarios. We classified a key as successful if the minimum force required to break the key exceeded the maximum force required to turn the lock. We classified a key as possibly successful if the average force to break the key exceeded the average force required to open the lock. If the average force to break the key was lower than the average force to open the lock, we considered the key unsuccessful in that lock. These results are summarized in Table 1.

3.1 Testing procedure

All of the keys were first numbered to allow us to take notes on the way the specific key broke and to also find the broken key corresponding to a certain test in the future. We mounted the locks into a bench-top vice and the key to be tested was cycled in and out of the lock several times without turning it in order to remove some of the 3D printing artifacts, easing the removal of the key from the lock once the key broke off. The key bow was then inserted into the notch in the torque screwdriver's socket and torque was applied to the key bow.

For each trial, the maximum torque a key could withstand before permanently deforming or breaking was recorded along with corresponding notes regarding how the key broke. In our notes, we classified a key as a *clean break* if it completely broke into two pieces. A key was classified as a *partial break* if the key bow remained attached to the key blade but only by a very narrow section of plastic/metal. A key was classified as *deformed* if the key blade largely remained attached to the key bow, but a significant amount of bending between the bow-blade junction was observed. We tested two metal keys and four plastic keys per keyway per material (for a total of 6 keys per metal material and twelve keys per plastic material). To test the factory made keys, an analog torque wrench capable of measuring up to 100 inch-pounds was used.

To measure the torque required to open each lock, a factory made key was inserted over three trials into the lock to be tested and turned using the torque screwdriver. The key was turned until either the padlock or door opened.

3.2 Plastic

Most plastic key breaks were classified as clean breaks with the exception of the alumide plastic keys whose breaks were usually classified as partial or deformed breaks. Thus, some benefit to printing in alumide plastic exists for real use, since a key which has deformed or partially broke is still removable by the user without specialized tools. However, the alumide plastic's sandy texture makes removal exceptionally hard in the event of a clean break due to the friction it creates inside the lock. Other materials, including nylon, PLA, and acrylic, were comparatively easy to remove with broken key extraction tools due to their smooth texture.

The plastic keys ordered from our 3D printing supplier, with the exception of alumide plastic, would not be able to reliably open an office door or padlock. The alumide plastic was the most durable plastic from the 3D printing service, and keys printed in it would be able to open a standard office door and one of the weaker padlocks tested. Surprisingly, the PLA keys printed on the MakerBot were the strongest plastic keys we tested, with an average breaking strength exceeding that of even the alumide plastic.

Material	Brass	Bronze	Stainless Steel	Arcylic	Alumide	Nylon	MakerBot PLA	Factory Blanks
Cost	$25.03	$25.03	$10.73	$8.28	$3.08	$2.55	$0.08	$0.50
Average Breaking Torque (in-lbs)	29.5	29.8	34.1	1.59	3.21	2.07	5.29	55
Crash Bar (4.7 in-lb)	●	●	●	○	○	○	◐	●
Various Padlocks (3.0 in-lb)	●	●	●	○	○	○	●	●
Door Unlock (2.6 in-lb)	●	●	●	○	●	○	●	●
Door Latch (1.3 in-lb)	●	●	●	◐	●	◐	●	●

Table 1: **3D printed key strength** — The average breaking torque for keys made from each material (across the three keyways tested) was taken, averaged, and compared to the torque required to open locks in four common lock categories using factory blanks. A filled in circle indicates the material's minimum strength was stronger than the maximum required strength for the application; partially filled means its average was higher than the average required strength; and not filled means its average was lower than the necessary strength.

This would allow them to open office doors and our set of various padlocks with ease. The acrylic, nylon, alumide, and PLA keys had average breaking torques of 1.59, 2.07, 3.21, and 5.29 inch-pounds respectively, approximately 6–10% the strength of a factory made metal key.

The most expensive plastic was acrylic at over $8 per key while the other plastic keys from the 3D printing manufacturer cost approximately $3 per key. Acrylic was also the weakest material with an average breaking strength of approximately half of the alumide key. Alumide may seem like the most cost effective and strongest option, but once the texture is considered, nylon may be the best choice if a desktop 3D printer is not available. The MakerBot was the most cost effective and quick solution with a per key raw material cost of $0.08 and average print time of approximately 20 minutes compared to the two-to-three week turn around time from the service. This does not take into account the initial printer purchase cost which would significantly raise the per key cost if the printer is purchased solely for printing keys.

3.3 Metal

Unlike plastic keys which can be printed cheaply and quickly using desktop 3D printers, metal keys are generally only available from 3D printing services. Thus, the cost of the metal keys as well as the time it takes to procure them increases, with typical manufacturing and ship times ranging between two and three weeks.

With the exception of stainless steel keys, the metal keys we tested either partially broke or deformed in failure. Although they were stronger overall, stainless steel keys broke cleanly and without warning. In addition, stainless steel keys can be abrasive to the lock, which is made of brass (a much softer metal). Long term use of stainless steel keys can even lead to the keyway being reshaped, potentially to the extent that factory made keys are less reliable or no longer work in the lock.

All of the metal 3D printed keys tested were strong enough to withstand opening torques for our locks. In one instance (stainless steel SC1), the key withstood the maximum torque our tool could measure (35 inch-pounds). The brass, bronze, and stainless steel keys on average withstood 29.5, 29.8, and 34.1 inch-pounds respectively. Compared to factory made keys, which break at approximately 55 inch-pounds of torque, the metal 3D printed keys were slightly weaker, though this difference would not be noticed in everyday use.

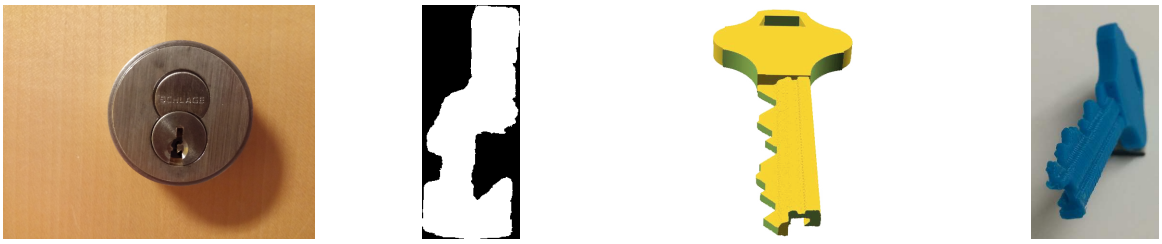
Although stainless steel was the cheapest and strongest material, its abrasive surface, clean breaks, and lower feature detail (compared to that of brass or bronze) make it less desirable for long term use. In contrast, brass's failure mechanism of deformation gives it an advantage over other materials, as approaching failure is very obvious to the user. In some cases, brass keys could be rotated almost a complete 90 degrees without breaking, as shown in Figure 2c.

4 Model Generation

Although the ability to 3D print keys is useful for attacking restricted keyway locks, it requires an accurate CAD model of the keyway's shape to create a model of a blank key that fits into the respective keyway. Such a model can be created manually using measurements from a real key but requires time and at least a minimal amount of skill. As an alternative, an attacker could use an outline of the lock itself (rather than a key) to develop the model.

In this section, we detail how a CAD model of a key blank for an unknown keyway can be *automatically* created from a single picture of the lock itself. We describe our implementation and discuss examples of keyways that are conducive to automatic model creation using our tool.

Given such a tool, an attacker simply needs a single straight-on picture with high resolution and contrast (such as one taken with a modern smartphone camera) of the



(a) Picture of lock (b) Keyway detection (c) Model generation (d) 3D printing

Figure 3: **Automatic key blank generation** — Our tool takes an image of a lock (*a*), automatically detects the outline shape of the keyway (*b*), and produces a 3D model of a blank (*c*) that fits in the keyway. A MakerBot Replicator 2 3D printed key (*d*) produced using the generated key blank model is illustrated.

face of the lock. Given this image, our tool detects the outline of the keyway, determines the scale of the outline, and creates a 3D model that consists of this outline extruded with a simple standard key bow placed on the end. This effectively creates a key blank that will fit in the keyway in question. The tool can optionally "cut" the blank to a specified code (based on the A-2 standard) to more quickly enable an attack. Figure 3 details the steps of our tool.

We implemented our tool using Python with the OpenCV and Scikit image processing libraries. To create the final 3D model of the key, we used the OpenSCAD modeling suite which uses a textual language for describing models.

4.1 Keyway outline detection

In order to obtain an outline of the keyway, we observed that in images of locks, the keyway generally appeared dark compared to the rest of the image. Our tool leverages this by converting the color image of the lock to a black and white image using thresholding. Each pixel below a certain intensity is converted to a black pixel, while everything else is set to white. Due to image brightness and contrast variation, the intensity value to threshold around must be determined for each image. One approach is to allow the user to manually specify this value. Our tool uses a heuristic to automatically infer the threshold for the image. This heuristic iterates across potential thresholding values (e.g. 0 to 255) and for each resulting black and white image generated, performs blob detection to find the largest contiguous region of black pixels. If the threshold value is too high, the largest contiguous blob will contain the outline of more than the keyway. In contrast, a threshold value that is too low will contain at best a small amount of the keyway outline. To find the optimal threshold, we observe the total area of the outline as the threshold is increased. Figure 4 shows the area of the largest contiguous blob for a sample image as the threshold is increased. There is a sharp increase in blob area after the optimal threshold for finding the keyway has been achieved. After this optimal point, the SFIC housing or mortise gets included in the outline, and the area increases dramatically. Therefore, our tool uses the first threshold value before this sharp increase to extract the keyway outline.

4.2 CAD model generation

Once the keyway outline has been obtained, our tool generates an OpenSCAD model that consists of a key blade (with optional cuts) and a bow. To generate the key blade, our tool scans each row of pixels in the keyway outline obtained previously to generate rectangles that are extruded for the length of the key blade. Each black-white edge in a row in the keyway image is the beginning of a rectangle that ends at the next white-black edge. This results in a rectangle per row of pixels in the outline image in the OpenSCAD file. To further improve the rendering time, we coalesce adjacent rectangles that have the same width. The set of extruded rectangles is placed in a union block with our OpenSCAD template that contains a standard key bow.

One shortcoming of this approach is that the result from the keyway outline component may have fragments or miss pieces altogether due to the effects of thresholding. To reduce the problem of fragmented images, we allow the user to specify that their image has no overhangs, such as those found in the Schlage Everest series. This allows us to scan each row from left to right looking for a black-white boundary and once found rescan from right to left looking for another black-white boundary. The corresponding row's rectangle spans those two boundaries, even if there are sections missing in the middle. By scanning an image this way, any missing parts in the center of the image (such as is caused by the first pin in the lock being visible in the picture) are eliminated since only the left- and right-most boundaries are considered.

The approach discussed above allows us to generate the key channels and mimic the 2D keyway outline in

OpenSCAD. However, the model is still in units of pixels with no scale. To determine the correct scaling factor from pixels to inches, we take the constant SFIC keyway height, 0.320 inches, along with the bounding box height of the mask of the keyway and divide them to generate the inches per pixel ratio. This scaling factor is inserted into our OpenSCAD template.

Given the bounding box (and orientation) of the extruded keyway, optional user-provided key cuts can be included in the model. Since the height and length of the blade are known, our tool can cut standard A-2 pin cuts, as well as a tip contour and tip stop, to ensure the key is inserted to the correct depth in the lock.

4.3 Tool validation

We verified that our tool produced accurate and usable models by testing it across several pictures of six distinct keyways. We then printed the models using a MakerBot Replicator 2 and verified each fit in its respective keyway. We found that although the models generated by the tool were quite accurate, our printer overprints the model by about 10%, causing the keys to be too large to fit in the keyway. We modified our tool to accept a manual overprint correction amount. Alternatively, a nail file or light sandpaper could be used to remove excess printed material.

We note that our tool is not able to produce working keys for lock designs that have hidden checks for a legitimate key when these features are not visible from the front of the keyway. However, keys for keyways with security features that are visible from this angle (such as the overhangs used in Schlage Everest keys) can be reproduced easily. We also note that the user may have to manually tweak the tool or image if the front pin of the lock is visible, such as when photographed in bright environments. This can be solved by either taking the picture in a lower light environment, manually editing the image, or manually adjusting the threshold value the tool uses.

5 Related Work

Although 3D printing is still emerging as a technology, there have already been several works related to keyway modeling. The most notable of these was the PhotoBump tool which was created by Jos Weyers and Christian Holler [4]. PhotoBump allows a user to take a picture of an IKON SK6 keyway and generate a bump key that works on the lock. However, although the authors claimed the tool could work with other keyways, the tool has not been released, and no additional keyways have been demonstrated. In contrast, our tool has been tested across a range of keyways and is open source.

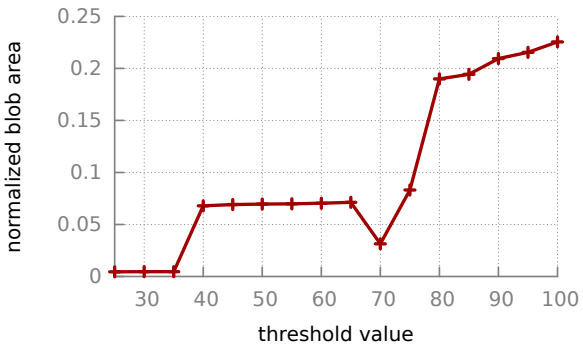


Figure 4: Normalized blob area vs. threshold value for an image with an optimal threshold value of 35.

In 2013, David Lawrence, Eric Van Albert, and Robert Johnson showed how 3D printing could be used to bypass restricted keyways by 3D printing a Schlage Everest key [10]. OpenSCAD was used to develop the blank but was manually created, unlike the automated approach we present[1].

Services such as KeyMe and Keys Duplicated allow users to take a picture of a key and have it reproduced with a traditionally manufactured blank and mailed to them [6, 7]. Although these tools recognize the cuts on the key (similar to what was done in the Teleduplication work), the blank is recognized by markings on the key blade or the shape of the bow. This allows these services to create high quality keys but limits the keyways that they can work with to a small set of pre-modeled designs, which excludes restricted keyways. Our approach automatically generates the key blank from a picture of the keyway profile and can thus work for a much wider range of keyways, including restricted keyways.

In 2013, KeyMe expanded their service to allow users to 3D print their house keys [14]. This allowed them to offer users a variety of materials along with exotic key bows. However, the models are pregenerated and selected based on the picture the user provided, preventing users from using the service to copy any restricted keyways.

6 Discussion

3D printing gives attackers a new tool in attacking physical systems. In this section we will discuss implications of this capability, as well as potential countermeasures that lock manufacturers, locksmiths, and users can implement to protect themselves from these attacks.

[1]Our automatic keyway modeling tool would not have been able to fully produce the Schlage Everest key due to the dual set of cuts it features. However, this could be accomplished with a small modification to the generated OpenSCAD file by the user.

6.1 Attacks

Key duplication The most obvious attack enabled by 3D printing is copying existing keys. With 3D printing, restricted keys, "Do Not Duplicate" keys, or otherwise difficult to obtain key blanks are a significantly smaller obstacle for attackers. Traditionally if a malicious user was given one of these keys, they would have a difficult time making a copy of it, even if the key was in their possession for an extended period. However, with 3D printing, this user can now make a copy by creating a model of the key blank shape and copying the cuts from the given key to it. This model can be printed in either plastic or robust metal for a reasonable cost ($10–30).

Teleduplication with restricted keys Beyond simply copying a key in the attacker's possession, teleduplication attacks can be used to copy keys remotely. These attacks normally employ a powerful lens or telescope to photograph the key and then software or manual inspection to determine its cuts. These attacks were traditionally limited to keyways that the attacker could obtain blanks for, however, the methods to produce restricted blanks described in this paper could be combined with these attacks to allow the attacker to copy restricted keys as well.

Bump keys Many locks are vulnerable to bumping, an attack in which a key of all low cuts is inserted just short of all the way in the lock, struck with a small hammer or mallet, and turned in quick succession. The key is pushed abruptly into the lock causing the pins to transfer some of this momentum to the upper pins. If all of the upper pins happen to be above the sheer line at the exact moment the key is turned, the lock will open. This attack was previously limited to non-restricted keyways due to the difficulty in procuring restricted key blanks, but 3D printing and rapid prototyping can be used by attackers to overcome this obstacle.

Privilege escalation As mentioned in Section 2.3, there is a known privilege-escalation vulnerability in master-keyed systems, such that an attacker with legitimate access to one lock in a system (and its corresponding change key) can effectively query the lock to learn the system's master key. The attack requires N blanks and $N(M-1)$ trials for an N-pin lock with M different possible cuts per pin. One defense to this attack is to make obtaining blank keys difficult by using restricted keyways. Even with CNC or custom milling or filing, the multiple number of blanks required makes this a tedious attack at best. However, with 3D printing, an attacker can print out all $N(M-1)$ keys in plastic at low cost (possibly only a few dollars for a typical SFIC lock system if the attacker has access to a 3D printer). As each trial key only needs to turn the lock's plug and not any mechanical spring or latch assembly, there is little risk in breaking keys due to excessive torque, even across the large number of trials. Once the master key is obtained, it can be produced in metal for a more robust version. In practice, we estimate this attack can be done with less than $100 and an hour of time (excluding time spent on production and/or shipment of the printed blanks).

Key reuse Key cuts, like passwords, are often chosen by users improperly. Different systems maintained by the same locksmith may reuse prefixes or entire sequences of cuts from one system to the next, perhaps out of laziness or convenience. This is a dangerous oversight that could allow attackers that have keys or masters in one system to easily get equivalent access to another system, much like how password reuse gives attackers a wider breadth of compromise. Normally, if these buildings do not share the same keyway (i.e. one is using a Best keyway, while another is using a Medeco keyway), it would be difficult for an attacker to test for this kind of key reuse in practice since blanks for the systems would need to be obtained. However, with 3D printing, this is made remarkably cheap for the attacker.

6.2 Countermeasures

3D printing and software tools pose a number of threats to physical key systems. In this section we present defense measures for lock manufacturers, locksmiths, and users alike.

Non-mechanical locks As 3D printed keys interact exclusively with mechanical locks, the use of (or inclusion of components of) non-mechanical locks, such as electronic or magnetic locks, may protect against these attacks. One example is the EVVA MCS magnetic lock that uses alignment of magnetic pucks in the key to change the orientation of magnetic discs in the lock. However, we note that non-mechanical locks—including electronic locks that pair with smartphones such as the Lockitron [12] or Kevo [9] smart locks—introduce a large new attack surface not present on purely mechanical locks.

Active keyways 3D printing attacks using the tool we presented in this paper could be thwarted or discouraged by having a mechanical check for legitimate keys in the keyway. Electronic and magnetic checks, if implemented correctly, could discourage even manual 3D modeling and printing of keys. For example, if legitimate keys have active spring components (such as in the Mul-T-Lock design) or additional sidebar or finger pins (such as in the Keymark X4), these may be difficult for a 3D printed key to reproduce accurately or may require additional knowledge from an attacker. Similarly, locks that have thinner keyways will provide some resistance to attacks with 3D printed plastic keys due to durability concerns.

However, as 3D printing technology continues to improve, this defense may be short-lived.

Trap keyways Specialized locks exist that can be configured to "trap" or capture a certain key when it is used. These locks utilize telescoping pins in conjunction with a plug that has smaller diameter "trap" holes next to the actual holes for the pins. The locks are pinned so that when a key that should be trapped is used, at least one telescoping pin is above the sheer line thereby allowing the telescoping pin to expand into the smaller holes that were created, effectively preventing both the lock from rotating and the key from being removed. These locks could also be used to prevent rights elevation and bumping attacks since the attacker would inevitability hit a trap cut on at least one of the pin stacks.

6.3 Tool

To facilitate improvement of our tool and identify its limitations, we are releasing it as an open-source project. Additionally, we are running a website interface that allows users to upload a picture of a keyway and download a CAD model of a key that will fit in the lock. We hope that this tool helps illustrate the vulnerability in many restricted keyways in use today. By releasing it to the public for use, we also hope to discover keyways (restricted or non-restricted) that resist this attack. Such keyways may hold lessons for both current implementations and new keyway designs. Our code and tool are available at https://keysforge.com.

7 Conclusion

3D printing is a powerful emerging tool that dramatically lowers the cost of physical manufacturing. As it applies to physical security, 3D printing antiquates the notion that we can have physical tokens such as keys that are hard or expensive to reproduce. Current high-security locks rely on this notion, using restricted keyways to prevent key copying and other powerful attacks. However, as we have shown in this paper, these protections can be defeated relatively inexpensively using 3D printed keys. Not being limited to plastic, these keys can be printed in metal and in practice are as robust as legitimate blanks from the manufacturer. As these capabilities improve, lock manufacturers will have to explore alternative designs in order to provide the level of protection previously realized using restricted keyways.

Acknowledgments

The authors thank Matt Blaze, Brad Campbell, Shane DeMeulenaere, Prabal Dutta, Branden Ghena, Pat Pannuto, and Drew Springall for their valuable feedback and for assistance with 3D printing tools. This material is based in part upon work supported by a National Science Foundation Graduate Research Fellowship and by the Morris Wellman Faculty Development Assistant Professorship.

References

[1] Matt Blaze. Cryptology and Physical Security: Rights Amplification in Master-keyed Mechanical Locks. *IACR Cryptology ePrint Archive*, 2002:160, 2002.

[2] Cubify. Buy a Cube 3D Printer. http://cubify.com/cube.

[3] Formlabs. Form 1+ SLA 3D Printer. http://formlabs.com/products/form-1-plus/.

[4] Christian Holler. PhotoBump: Working Plastic Bump Keys for any Profile. http://unlocked.own-hero.net/2014/07/10/preview-photobump-plastic-bumpkeys/.

[5] i.materialise. 3D Printing Service i.materialise. http://i.materialise.com/.

[6] KeyMe. Copy Keys, Solve Lockouts. https://key.me/.

[7] Keys Duplicated. Copy Keys Online using your Phone. https://keysduplicated.com/.

[8] Kraftwürx. Professional Quality 3D Printing Services in 85 Materials. http://www.kraftwurx.com/.

[9] Kwikset. Kevo. http://www.kwikset.com/kevo/.

[10] David Lawrence, Eric Van Albert, and Robert Johnson. Key Decoding and Duplication Attacks for the Schlage Primus High-Security Lock. https://www.defcon.org/images/defcon-21/dc-21-presentations/Lawrence-Panel/DEFCON-21-Lawrence-Johnson-Karpman-Key-Decoding-and-Duplication-Schlage-Updated.pdf.

[11] Benjamin Laxton, Kai Wang, and Stefan Savage. Reconsidering Physical Key Secrecy: Teleduplication via Optical Decoding. In *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS)*, pages 469–478, 2008.

[12] Lockitron. Lockitron, 2014. https://lockitron.com/.

[13] MakerBot. Replicator Desktop 3D Printer. http://store.makerbot.com/replicator.

[14] Michael Molitch-Hou. Emergency and Custom Keys from Shapeways and KeyMe.

[15] Deviant Ollam. Practical Lock Picking: A Physical Penetration Tester's Training Guide. 2012.

[16] Printrbot. Assembled Printrbot Simple. http://printrbot.com/shop/assembled-simple-metal/.

[17] Sculpteo. Online 3D Printing Service for your 3D Design. http://www.sculpteo.com/en/.

[18] Shapeways. 3D Printing Service and Marketplace. https://www.shapeways.com/.

[19] Shapeways. Brass 3D Printing Material Information. http://www.shapeways.com/materials/brass.

[20] Shapeways. Stainless Steel 3D Printing Material Information. http://www.shapeways.com/materials/steel.

[21] Schuyler Towne. Rethinking the Origins of the Lock, 2015. http://schuylertowne.com/research/rethinking-the-origins-of-the-lock.

[22] Ultimaker. Ultimaker 2. https://ultimaker.com/en/products/ultimaker-2-family/ultimaker-2.

[23] Barry Wels and Rop Gonggrijp. Bumping Locks. https://toool.nl/images/7/75/Bumping.pdf.

[24] Wikimedia Commons. Pin Tumbler Unlocked. http://commons.wikimedia.org/wiki/File:Pin_tumbler_unlocked.svg.