3D Printing in Lock Picking

Byron Doyle
Brigham Young University
School of Technology
265 Crabtree Building
Provo, UT 84602
byrondoyle@gmail.com

Colby Goettel
Brigham Young University
School of Technology
265 Crabtree Building
Provo, UT 84602
colby.goettel@gmail.com

Dale Rowe
Brigham Young University
School of Technology
265 Crabtree Building
Provo, UT 84602
dale_rowe@byu.edu

ABSTRACT

Physical security analysts have always sought to overcome challenges in security infrastructure using novel approaches and new technology. One of these challenges is preset mechanical lock mechanisms.[1] 3D printing technology provides a valuable tool for those interested in attacking or bypassing locks high-security locks. Practitioners can create key blanks or even complete replicas from key data such as physical key measurements or photographic evidence.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*unauthorized access*; J.6 [**Computer-Aided Engineering**]: Computer-aided manufacturing—*CAM*

1. INTRODUCTION

Keyed locks are generally vulnerable to a variety of attacks, but due to the enormity of designs and technologies used around the world today each lock typically requires a different technique to exploit or bypass. For example, simple pin and wafer locks can be picked with moderate skill, but more complicated locks with sidebar mechanisms make picking impractical without specialized tools and a high degree of skill. Impressioning is a technique common to many types of locks. This technique allows an attacker to create a copy of the key for the target lock. However, it requires a decent amount of skill, as well as key blanks specific to the target lock type. Having a key copied is an option as well, but due to the control of key blanks and cutting facilities for high-security locks, as well as the inherent difficulty there may be of obtaining the bitting[2] of the original key, this may not be feasible. With 3D printing, all these attacks can be made more effective, and especially in the case of high security locks, become much more effective.

[1] A locking mechanism that is opened by predefined key.
[2] A code that defines the key cuts that will properly open the target lock.

To understand how these manufacturing techniques can be useful, we must first look at the benefits and drawbacks themselves. Next, we can evaluate some popular attacks on keyed systems. Finally, we can combine these two approaches to understand just how the application of 3D printing technology can render even very high-security locks irrelevant in the proper circumstances.

2. 3D PRINTING TECHNIQUES

3D printing, a form of rapid manufacturing, is a broad field comprised of many different techniques that can produce products in a variety of different materials. Some of these techniques are more useful than others for the penetration of physical security systems. Of particular note are fused filament modeling, stereo lithography, and direct metal laser sintering.

2.1 Fused Filament Fabrication

Fused filament fabrication (FFF)[3] is one of the most common 3D printing techniques, and also one of the cheapest. Relatively high-quality models are built out of various types of plastic via a machine that lays down traces of material in patterns, building up layers in the z-axis (Valavaara).

This method is particularly useful because of its proliferation: a 3D printer with the accuracy required to produce basic key blanks can be purchased for under $500. If that route is not available, there are many online services that offer prints using this method that are extremely high-quality and fairly cost-efficient.

In general, fused filament fabrication is perhaps the largest area of new material development due to the relatively high adoption rate in the consumer market. Typically, prints are produced in either ABS[4] or PLA[5] plastics, but many different materials can be used to suit the task at hand. FFF-manufactured parts have very different properties depending on the material they are made from; thus it is important to choose the right material for the application. ABS plastic offers a good balance of hardness and flexibility; both are important when producing parts such as thin key blanks. PLA

[3] Also called fused deposition modeling (FDM).
[4] Acrylonitrile butadiene styrene, a very common thermoplastic used in the manufacture of cheap, mass-manufactured parts.
[5] Polylactic acid, a biodegradable thermoplastic made out of various renewable resources such as corn starch and sugar cane.

is more rigid, but more likely to snap instead of bending.

Of particular interest to this topic may be nylon.[6] 3D printing-specific nylon materials are designed specifically to offer an extremely wide range of characteristics depending primarily upon the temperature they are printed at — this builds off of the innate properties of the material. Relatively hot temperatures will yield an extremely strong bond in the part, as well as a harder result overall. Cooler temperatures result in a more weakly bonded, more flexible part. In addition, nylon is extremely abrasion-resistant, important for working in locks without leaving behind plastic shavings.

2.2 Stereolithography

Stereolithography (SLA) is the original 3D printing process, first patented in 1984. This process is characterized by the transformation of a liquid photopolymer into a solid by a laser or other curing light element (Hull). In most situations, this process produces some of the highest-resolution models available.

The cost of stereolithography equipment is generally more than FFF equipment. Consumer-level printers are appearing on the market in the $2000 to $3000 range. These machines provide a build volume[7] large enough for models such as keys while still maintaining a relatively low cost. Online 3D printing services can provide larger, higher quality prints as well; these may be valuable when producing larger batches of parts.

High resolution is very important when considering the design of complex keys and key blanks. In addition, the higher resolution and bonding method of this process can produce stronger models, though this varies with the type of material used. This printing process necessitates the addition of support sprues to the model; these must be taken into account when designing precision-driven projects such as keys, as the connection points between the part and the sprues leave small bits of material that must be carefully filed away or removed by some other means.

Materials for SLA machines are more limited in variety than their FFF counterparts. Photopolymers for SLA printing generally resemble ABS after being cured during printing. Unlike thermoplastics, however, photopolymers will continue to cure as long as they are exposed to ultraviolet light. Depending on the material used, parts made with photopolymer liquids can become brittle over time as they over-cure through exposure. Materials research continues to mitigate this effect, but because of the material development cost, the relatively low demand, and the relatively high production cost, liquid photopolymer materials are often quite costly.

2.3 Direct Metal Laser Sintering

Direct metal laser sintering (DMLS) is a manufacturing method that creates solid metal parts via exposure and bonding of fine metal powders to a high-power laser (Das and Beaman). This process differs from others in that it can create full, solid metal parts which rival or exceed the strength of cast parts and, in some cases, even forged parts. In addition, parts produced with this process are extremely accurate and typically have a very smooth finish.

The benefits of this process may be less obvious, as equipment for DMLS is not available directly to consumers. However, DMLS is now a common format available through online 3D printing services, making it especially useful when custom one-off tools are required, or when a controlled key blank distribution system (such as with many high-security locks) must be circumvented.

Even without investing in manufacturing equipment, DMLS parts are typically expensive. For this reason it is usually better to use another form of 3D printing to produce early prototypes. Only after the design is finalized should the part design be sent off for manufacturing. DMLS may therefore be thought of as an option to enhance the efficacy of other 3D printing techniques.

Many different metals can be used with DMLS; the material only needs to have relatively stable thermal properties over its melting point. As the technology progresses, more and more metals are made available for use in manufacture. Titanium is a very popular material as it is light, strong, and corrosion resistant. Steel and brass are also popular, but are more often offered on online printing services as parts cast from a 3D printed wax or sand model. These parts typically offer good strength, but their surface finishes are not as accurate.

3. POPULAR ATTACKS ON KEYED SYSTEMS

3.1 Lock Picking

Lock picking is certainly the most famous attack on keyed systems, though not always the most effective. A small torque is applied to the keyway of the lock or cylinder of the lock, and the pins of the lock are pushed up slowly until the pin tumblers sitting on top of the pins engage the shear line between the lock cylinder and the lock body (Error: Reference source not found).

This attack can also be used on other types of locks such as wafer locks and cylinder locks with the appropriate tools. Wafer locks are opened in much the same way as pin tumbler locks with one key difference, brought on by the geometry of the lock: the shear line is wide and the wafers all engage a single large slot. This allows for a great amount of play in the workings of the lock, making picking much easier. Tube locks are easier to pick for a different reason: they only require a special tool, conveniently called a "tube lock pick." The tool is engaged with the lock, and torque is applied on and off while the tool is gently pressed down. The binding of the pins against the shear line of the lock impression the bitting of the tube lock into the lock pick.

In addition to single-pin picking, a number of attacks across multiple pins can be used. Raking, scrubbing, and bumping are three of these methods. Raking and scrubbing generally fall together as the two techniques experienced lock pickers use to quickly open easy-to-bypass locks. These techniques

[6] A common grouping of aliphatic polyamide thermoplastics known for their high strength.

[7] The total volume in which a 3D printer can construct a part; the limiting factor to the size of any one print job.

are most useful, however, when combined with skillful single-pin picking: problematic pins can be set, and then raking or scrubbing can be used to set the rest. Bumping expands on raking by using specialized key blanks made specifically to set all the pins in the target lock at once. With the proper tools and some practice, lock bumping can open even very hard to pick locks.

Raking is performed by dragging a tool lightly across the bottom of the pins while applying light torque to the lock cylinder. As the tool bumps against the pins, they rebound against the pin tumblers which should rise above the shear line and set. This can be done very quickly to open simple locks. This technique varies greatly depending on the tools used, the target lock, and the attacker's preferences. Many different pick shapes can be used for raking, but typically half-diamond, hook, and snake shapes are preferred. The target lock's geometry also affects how raking is performed, or if it is even useful at all; this is typically a function of the pick shape in contrast to the keyway[8] shape.

Scrubbing is a variation of raking: instead of dragging a tool across the pins, a wide, flat tool is used to push groups of pins up and down in a "tooth brushing" motion. In this way the attacker is effectively attempting to pick multiple pins at once. This technique is extremely useful when raking fails due to restrictive keyway shapes, or when the target lock's pins are very close together. Scrubbing may also be preferable if the spring tension on the pins is very high — a common trait of padlocks and other locks meant for outdoor use. When not chosen by necessity, scrubbing may only be used instead of raking because of preference; however, both raking and scrubbing are equally useful.

Bumping is a variation of the raking technique using a specialized key blank, cut just past the deepest pin depth on all pins with ridges in-between. This tool is called a bump key, or "999" key, so-called as the key is cut to a modified all-nines bitting. The bumping technique is performed by pulling the bump key slightly out of the lock, applying light torque, and then lightly "bumping" the key with a wooden hammer or other apparatus to strike all the pins at once. This forces all the pin tumblers above the shear line at once, opening the lock.

3.2 Impressioning

Impressioning consists of using a specially-prepared key blank to make a copy of the key for the target lock via physically decoding the target lock's bitting. The blank is placed in the lock, torque is applied, and then the key is moved up and down against the pins; any pin at the improper height will be bound against the sides of the lock body and cylinder. This binding causes the pins to pit the blank slightly. The key is then removed from the lock, inspected for pitting, and cut with a file where pitting is found. Cuts are made for one bit-depth at a time, and then the process is repeated. This can be done for all pins in the lock at once under normal circumstances, and should result in a working copy of the key for the lock if the attack is successful. The attacker needs only make note that the proper torque and force on the pins is used. Too little torque or too much force and pins will slip, causing missed bittings. Too much torque or too little force and the pins will bind in the wrong places, causing false bittings. In either case, the target lock could be damaged.

Caution should be used when employing this technique, mainly as improper use can lead to positive indications of an attack on the lock system. In some cases, locks may degrade quickly and seize or bind; many shear forces are being applied to the inner bearing surfaces of the lock in an unusual manner. Care should also be taken to thoroughly clean the filed blank before re-inserting it into the target lock if discretion is required. Leaving loose metal shavings inside the lock is a fairly obvious giveaway, as filings from regular use typically differ from those resulting from cutting with metal files.

3.3 Copying

The main feat in making a copy of a key to a foreign lock is gaining access to the key's bitting. This can be done via certain lock picking techniques, such as using a cylinder lock pick, impressioning, using a pin lock decoder, or by gaining physical access to the key in some way in order to take measurements or a cast. All of these techniques can be quite intrusive, however.

One technique for decoding keys from a distance developed by Laxton, Wang, and Savage involves taking photos of a key from a distance and then using a computer vision algorithm to decode the bitting. This proved equally successful up close and at a distance using telephoto lenses. Utilizing this technique removes the attacker from the immediate vicinity of the key owner, and is thus much less intrusive. With even more powerful optics it seems feasible that this technique could be used to not only capture key information without the risk of notifying the target, but also to keep the attacker completely out of view. In combination with common key manufacturing facilities, this obviates the security of sole key ownership entirely in the case of common locks, as blanks are freely available and copies can often be manufactured without producing the original.

Copies of keys that result from impressioning are also extremely useful for providing the bitting for a lock. Because they must open the lock for the attack to be successful, the original impressioned key can be regarded as the lock's decoded bitting. This can then be used to create copies of the target key that appear genuine in order to facilitate a more successful attack.

This is especially true of keys for high-security locks; typically high-security blanks are only provided by the lock manufacturer, and so all keys will look very similar. Depending on the manufacturing techniques used, the very slightest detail can be copied, producing very realistic functional facsimiles.

Attackers should consider the idea that an entirely new key is being produced during the copying process. In the case of a common key type, this may just mean considering that the key will look brand new. High security-keys, however, have more exploitable features; thus care must be taken when

[8]The cut in the lock cylinder through which the body of the key passes.

making copies in order to dimension not only the working parts of the key, but the aesthetic portions as well. If photos of a target key are taken, an exact replica can be made; the replica can be weathered to match the original, serial numbers can be matched, and logos can be copied. These features all add up to a key that has history in a social context; it can be used in social engineering attacks as well as to open doors.

4. AUGMENTING ATTACKS WITH 3D PRINTING

The attacks described above can all be augmented by 3D printing in a variety of ways, depending on the printing processes and materials used. One notable use of the technology is the ease of making specialized tooling[9] to attack high-security locks such as the ASSA Twin series. These locks have a coded sidebar preventing the lock from turning independent of the top pins. Both blanks, spare parts, and even discarded cylinders are carefully controlled.

4.1 Lock picking

3D printing technology allows the cheap manufacture of specialized tools for lock picking. To facilitate a lock picking attack against a Twin Series lock, a special torsion wrench with the correct sidebar bitting built in could be printed. The top bitting may be unknown as it is unique to each lock, but sidebar bittings are set by region. Thus any sample key from the target site may lead to a more complete exploitation of the security system.

In the case of torsion wrenches or other force-applying tools, a stronger-bonding polymer process (such as stereo lithography) or a metal printing process (such as direct metal laser sintering) may be more useful than the cheaper, and more common, fused filament fabrication process found in consumer-level 3D printers. The designer must decide how much torque is required for the application, and how that torque will be applied through the tool. The designer can choose a manufacturing process using this information.

For permanent or reusable tool manufacturing it is useful to design and implement a prototype version in a plastic format as it is cheaper and more readily producible. These prototypes can then be evaluated and iterated upon as needed; to provide longevity and strength in the tool a final version can be made using a metal printing process. This might be especially useful for creating specialized tools that are not specific to a certain lock bitting, but are specific to an application; for example, a bypass tool for a lock with a common vulnerability found during the picking process.

Bump key manufacturing benefits greatly from this process as well, especially in the case of high-security locks. Bump keys are normally made out of stock key blanks; however, manufacturer controls limit this process in the case of high-security locks. To circumvent this, a complete bump key can be designed, tested, and then printed in metal. As bump keys are only specific to the type of lock and not the bitting, such tools are still useful when the target lock has been exploited.

[9]Specialized equipment used for mechanical processes.

4.2 Impressioning

The applications of 3D printing for impressioning are a natural extension of the applications in lock picking. ASSA is deliberately very protective over key blank distribution and key cutting for their locks, as it increases security for their customers. However, with 3D printing, a blank can be manufactured for the lock based on any cut key sample and rough specifications of the lock; both of these are easily acquired via proper reconnaissance or photography and computer vision.

In practice, creating blanks for high-security locks using low-cost 3D printing tools is very easy. Figure 3 shows a 3D model created from physical measurements taken from samples of ASSA Twin Series keys; this model has been used to successfully print key blanks on a consumer-level FFF 3D printer. These key blanks were printed in polylactic acid, a stiff but malleable plastic. Impressioning with plastic blanks manufactured in this fashion should work quite well if used in conjunction with a torsion wrench to apply torque to the lock, after the sidebar bitting is modeled into the blank.

In some high-security locks it may be possible to impression the sidebar when the top-bitting is known but the sidebar bitting is not (for example, if a picture of the back of an original key is used to decode the lock). In this case, a key with a coded top bitting and a blank sidebar would be printed, and impressioning would be performed as usual. Depending on the lock's sidebar mechanism this may not work — the ASSA Twin Series uses a sidebar mechanism where this is not possible. Other locks with sidebar mechanisms may have more success, such as Medeco high-security locks.

If correctly designed, blanks can be used repeatedly for the same type of lock without care for specific fitment within the same lock model. Once such a design is achieved for a high-security lock, the blank can be publicly released. Once this is done, the blank distribution-limiting in the lock system's environment is no longer a security factor. It may actually become a liability as the availability of printed blanks could exceed legitimate ones.

4.3 Copying

After a lock or its key is decoded by impressioning, computer vision, or other means, a true copy of the key can be made via 3D printing as well. At this point, a metal printing process would be desirable if the goal is to have a permanent key. Otherwise, a copy could be printed and torque applied with a torsion wrench. In both cases this implies a persistent threat to the keyed system: even if the copy is recovered by the affected organization, another can be made without need for special tooling or blanks.

The usefulness of 3D printing in key copying is perhaps the most obvious, but warrants extra consideration, especially where detail is concerned: if properly modeled, an exact duplicate of a key can be made, down to the numbering on the key, logos, and even simulated wear. During a penetration test this may be extremely useful as a social element: in addition to the key working, it can also be shown to personnel as proof that the attacker is supposed to be there. For example, a copy of a key can be made, worn down, and then taken to a facilities office under the pretense that it no

longer works. The key can then be traded for a new, properly serialized key from the organization — the forged key is no longer in circulation, the attacker has a real key, and the original key will stay in circulation until it is turned in or audited.

5. CONCLUSION

The capabilities of 3D printing technology have posed a persistent threat to organizations' physical infrastructures for quite a while. This is done via clever manipulation of lock picking, impressioning, copying, and other means. Essentially, the supply chain control paradigm for high-security physical locks will no longer stop a determined attacker from gaining physical access to what those locks are protecting. For this reason, new security models need to be put in place for physical security, and lock manufacturers need to stop relying on outdated supply chain control and choose to innovate.

The methods presented here can be used to create custom tools to address even the most obscure physical security platforms. A clever attacker no longer has to worry about security through obscurity in the physical space, and can fill his toolbox with items meant specifically to address the physical security weaknesses of a targeted organization. These tools afford the same flexibility to the attacker in the physical space as he already has in the digital space. Keys can be copied and used without notification of the original's owner. Systems can be reverse-engineered without leaving evidence behind. Security access controls can be bypassed entirely.

In addition, 3D printing is advanced enough that complete copies of legitimate keys can be made, akin to copying organizational IDs or badges. These can be used in social attacks as well as to open doors and gain access. For security professionals, this means looking at physical security threats in a new way, as attackers are not necessarily impeded by physical access restrictions as they once were: they now have a toolset that gives them the ability to produce what was once a trusted credential out of raw materials and some time. Those relying on the presence of a serial number and an earnest demeanor may want to re-evaluate.

6. REFERENCES

[1] T. O. O. of Lockpickers (TOOOL), "Introduction to lockpicking," Retrieved April 2004.

[2] ——, "Assa twin systems (part 1) the unparalleled security system," Retreived April 2014.

[3] B. Laxton, K. Wang, and S. Savage, "Reconsidering physical key secrecy: Teleduplication via optical decoding," Retrieved April 2014.

[4] V. Valavaara, "Topology fabrication apparatus," Patent US 4 749 347 A, Retrieved April 15, 2014.

[5] C. Hull, "Apparatus for production of three-dimensional objects by stereolithography," Patent US 4 575 440 A, Retrieved April 15, 2014.

[6] S. Das and J. Beaman, "Direct selective laser sintering of metals," Patent US 6 676 892, Retrieved April 15, 2014.