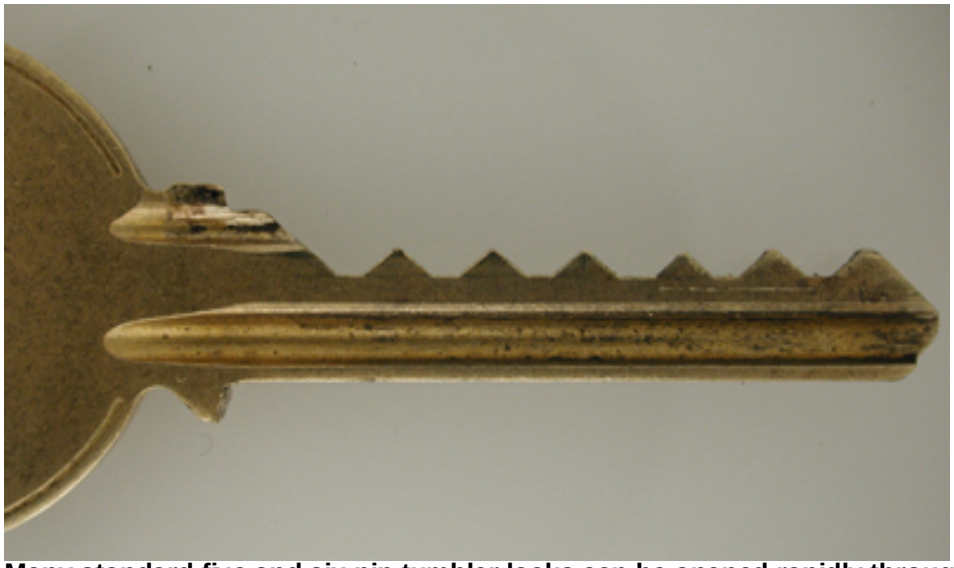
OPENING LOCKS BY BUMPING IN FIVE SECONDS OR LESS: IS IT REALLY A THREAT TO PHYSICAL SECURITY?

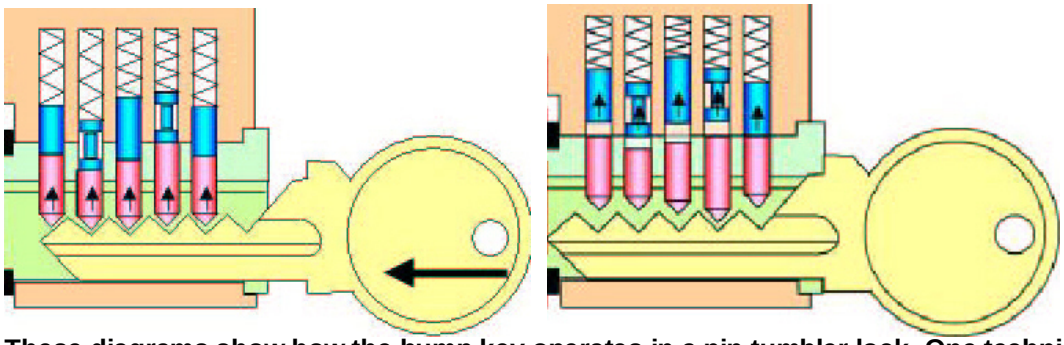
A TECHNICAL ANALYSIS OF THE ISSUES

Released on March 27, 2006 on http://www.security.org

The information contained in this report appears as part of a comprehensive treatment of bumping in the 2006 version of ***LSS+***, the Multimedia Edition of ***Locks, Safes and Security*** by the same author. Appreciation is expressed by the author to Barry Wels and Han Fey for their technical input and assistance in developing materials for this document. Our office is consulting with manufacturers to develop standards for testing cylinders against bumping. Currently, testing laboratories are not adequately addressing this issue. The author may be contacted at +1.605.334.1155 or mwtobias@security.org.



Many standard five and six pin tumbler locks can be opened rapidly through a technique known as bumping with a key similar to that shown above. Some high security locks can also be opened with this technique.



These diagrams show how the bump key operates in a pin tumbler lock. One technique requires that the key (left) be withdrawn by one tumbler position and then slammed into the lock. This will cause the top pins (right) to bounce and separate from the bottom pins, thereby creating a gap at the shear line that will allow the plug to turn.

SYNOPSIS: THE REAL WORLD OF BUMPING LOCKS

This analysis presents detailed information regarding the security threat posed by the “999” or bump key. Although there has been a significant amount of attention paid to the topic of late, there are complexities that must be understood to accurately gauge its impact upon security. As noted in the following material, the critical issue is the ability to obtain any key that fits the target lock. This requires the identification of the manufacturer and keyway so that a proper bump key can be produced.

If that challenge is met, then there is ample documentation that virtually all conventional pin tumbler cylinders are at risk. As will be noted in our discussion, the practical issues in obtaining keys depend in large measure upon the location of the target lock and whether it has a special keyway that may not be readily available. In addition, if the lock utilizes sidebar technology, then the task becomes a great deal more complicated and will likely result in failure.

To put this discussion in proper perspective, each of the following steps must be successfully completed in order to have a high probability of opening conventional five or six pin locks as well as “standard” dimple locks within a few seconds. None of the steps are particularly complicated, but failure at any stage can result in the inability to open the lock.

1. Possess or obtain any key that can be inserted into the lock. A key that has already been cut to fit any lock will work better than a blank, due to depth and spacing issues;
2. File the cuts to the deepest depth;
3. Use a bumping tool, such as the head of a large screwdriver, mallet, or “tomahawk” to bounce the pins and open the lock.

The bottom line: if an individual has a key that fits the keyway of the target lock, then bumping, (rather than picking, use of a pick gun or electropick) may provide the fastest method of entry and requires virtually no skill. Often, **locks can be opened in less than five seconds by bumping.** Bumping, in the view of the author, is a method of opening many pin tumbler locks that may not require any training as a locksmith or any significant skill set, although the technique is also utilized by professionals as yet another means of bypass. Some web sites are now offering bumping tools and precut keys for certain keyways, thus increasing the risk to the public.

Ultimately, the consumer is responsible for assessing the risk of an attack from bumping for currently installed locks. If poor quality hardware is in place, then in all likelihood, it can be compromised within a few seconds. The task can be more difficult as higher quality locks are employed. The term “quality” has many aspects and is based upon design, research and development, tolerance specifications and experience in the industry by the manufacturer. All of this comes at a price, and often the consumer is not willing to pay for better quality,

believing that it really does not matter. In the instance of bumping, it does matter, and the old adage “you get what you pay for” generally holds true.

There is no substitute for high security locks, but they come at a price. They are (or supposed to be) designed to resist both forced and covert methods of attack. As the Netherlands test and those conducted by the author demonstrate, this may not always be the case. World standards organizations had not considered bumping as a threat prior to the widespread exposure of the problem by Toool and others in Europe and America. As a result, certain rated locks may in fact have their high security certification withdrawn because of their vulnerability to bumping.

This document addresses the relevant technical issues with regard to the vulnerability of mechanical locks to bumping and the security threat that results. Law enforcement agencies, security professionals, locksmiths and the consumer need to understand the issues in order to accurately gauge individual risks. The author welcomes Inquiries and Input from readers.

COMMON QUESTIONS ASKED ABOUT BUMP KEYS

What exactly is a bump key?

A “999” or bump key can be any key that fits a particular pin tumbler lock and that has been modified so that all of its cuts are to the deepest allowable position, as defined by each manufacturer. The term “fit” means that the key will enter the keyway (the front of the lock), but it will not unlock it. To illustrate, all of the locks in an apartment complex are produced by the same manufacturer and have the same keyway, meaning that the key for apartment 101 can enter the lock of apartment 207 (or any other apartment), but will only unlock apartment 101 for which it was cut. Any key for any apartment in this example could be modified to act as a bump key and then could be used to open any other apartment within the complex, and potentially other complexes where the same or similar manufacturer’s locks are utilized.

Why is it called a “999” or bump key?

The term appears to have originated in Denmark about twenty-five years ago, when locksmiths began cutting keys for locks made by one specific manufacturer in their country to the deepest possible code depth of 9 for all positions. By way of background, each assigned depth is given a different “code” number by each vendor, so that their keys can be duplicated by this code without actually requiring the physical key. There are often ten individual coded depths, running from 0-9, where 0 is the shallowest and 9 is the deepest. Thus, the keys came to be known as “999” keys. The term “bumping” refers to the process of forcing the key to interact with the pin tumblers by “bumping” or rapping it with a plastic mallet while it is inserted into the lock. This entails hitting the head of the key,

causing it to rapidly move forward about .25mm. When the key is struck correctly, each of the bottom pins are “bumped” upward for a brief instant.

How difficult is it to make a bump key?

The critical issue, as discussed subsequently, is the availability of a key that fits the keyway of the target lock and the ability to create the proper cuts. Virtually any standard key can be modified to work as a bump key because by definition all of the cuts for any working key will be higher than those required for the bump key. Thus, the only requirement is the ability to file the cuts down to the lowest possible depth. As noted in the following discussion, keys, except for high security locks, are often easily obtainable and/or duplicated.

Can a lock be opened covertly by bumping?

The answer is both yes and no. Bumping requires striking a key while inserted into the keyway. Depending upon the condition of the lock, the technique employed, and the number of required strikes, there can be significant noise. In other cases, one strike may be all that is required. If the original bumping technique (that allows for the key to be withdrawn by one cut before being struck) is employed, then there may be very minimal noise. However, this is often not the case. The potential for making noise is a critical distinction between picking and bumping in terms of covert methods of attack.

What is the likelihood that someone has a key that will enter my lock?

Potentially, anyone that is in the same building, complex, or business will utilize the same locks and keyways, although this in part depends upon the lock manufacturer. That means that if a person has access to one or more keys, they can be modified into a bump key. Often, different buildings are engineered by the same architect. In such cases, the same locks may be specified because the architect is comfortable with one vendor. Contractors often specify what locks and keyways will be utilized in building complexes. If different facilities utilize the same locksmith, especially in less populated areas, the locksmith may recommend a particular brand of lock to all of his customers. Companies that have the same purchasing agent, hardware specifications, or special statutory requirements may likewise utilize the same locks and keyways. If there is a franchise or chain store operation in different cities, the corporate headquarters may require the use of the same locks in order to standardize their operations and increase security.

Commercial facilities that are master keyed often implement multiple keyways. Schlage, for example, utilizes keyways to differentiate areas within a building or complex. Some vendors, especially when utilizing small format interchangeable core systems, rely upon one keyway, which reduces overall security against

bumping. Implementation of multiple keyways should be considered because of the increased difficulty in obtaining keys from which to create bump keys.

Do we have high security locks or consumer grade cylinders, and what is the difference?

High security locks are significantly more expensive than consumer grade cylinders, but they can offer increased protection against most forms of bypass including bumping. Your local locksmith can tell you if your locks are rated for high security and carry a UL437 rating. In the United States, Schlage, Medeco, Assa, Mul-T-Lock, and Kaba are probably the most popular manufacturers for high security cylinders. Only locksmiths or national account representatives of the manufacturer distribute these locks, not retail outlets. In Europe, there are many more high security cylinders, some of which are subject to bumping.

What is the security of the locks in my facility against bumping?

This depends upon the hardware that is installed. If high security locks with sidebar technology are utilized, then you are more secure from an attack by bumping, as detailed within this report. You should check with your local locksmith or security consultant to determine the rating of your cylinders. If you are using consumer-grade pin tumbler locks, then in all likelihood, they can be rapidly opened by bumping, assuming that the variables that are detailed in this report do not come into play.

Our facility utilizes restricted or patented keys. Will these offer a deterrent against bumping?

Restricted or patented keyways do not prevent bumping. However, the answer is not quite that simple in some cases. The critical issue is the ability to obtain or replicate the blank and to create the proper cuts. Many keyways and associated blanks are not available through commercial channels. Unless a key can be obtained that fits another lock with the same keyway or one can be modified, then a bump key cannot be created. Patent and profile protection offered by some manufacturers may increase the difficulty of obtaining keys but will not in and of themselves prevent bumping.

Most mechanical keys can be reproduced through different casting techniques and there is no protection against this practice, However, this presumes that an original blank is available, even for a brief period, in order to take an impression. More sophisticated techniques are available, including the ability to photograph the front of the lock and then generate a key from the photograph. However, such procedures do not pose the same level of security threat as addressed in this document.

Is bumping easier to learn than picking or other forms of bypass, and thus does it create more of a threat to security?

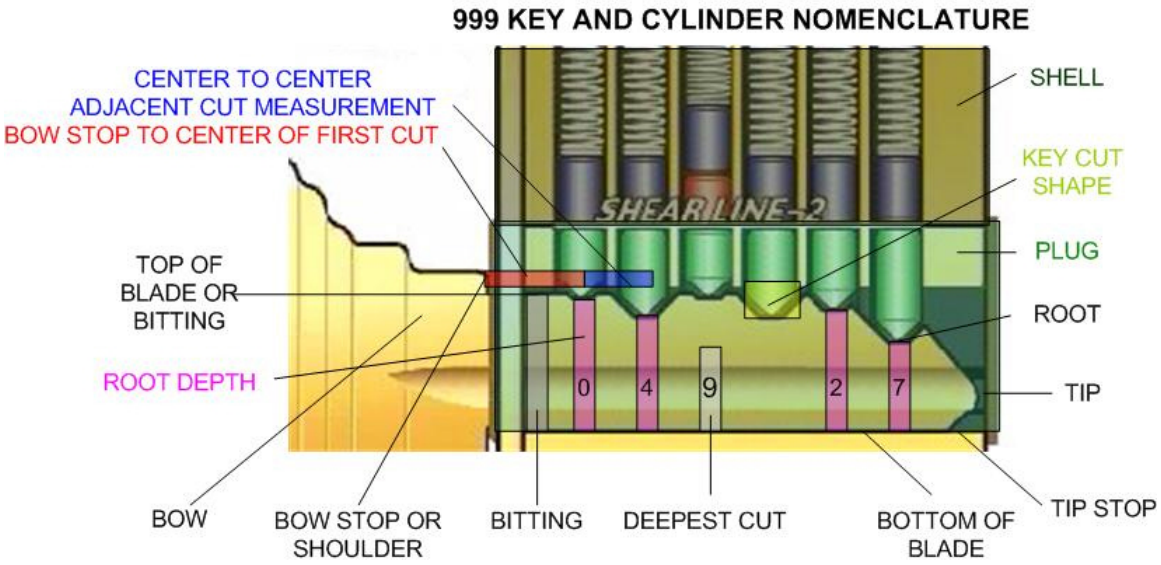
Bumping can be learned in less than an hour and requires almost no skill or special training. This is the primary reason for concern, absent other variables. In the worst case scenario, a would-be burglar can case a business or residence, then go to the local hardware store and potentially find the same manufacturer's lock. If that cylinder should have the same keyway as the target, then he can likely produce a bump key. Likewise, he can simply purchase a popular consumer brand lock, make a bump key for it and practice until he can open it. He then walks through a business or residential area, looking for identical cylinders and keyways. If he finds one and decides to commit a burglary, he will in all likelihood be able to open the lock.

What is the practicality of bumping as a method of entry?

It is extremely practical because of the required minimal learning curve to master the technique. If a bump key is provided to an individual intent on opening a lock, he will likely succeed if it is a conventional five or six pin cylinder or simple dimple lock.

If my lock is opened by bumping and I suffer a loss, will it be covered by insurance?

That would depend upon the terms of your policy. If proof of forced entry must be evident, then the theft may not be covered. Many policies exclude mysterious disappearance. In some cases, there will be forensic evidence of entry, but this is dependent upon many factors and is not assured.

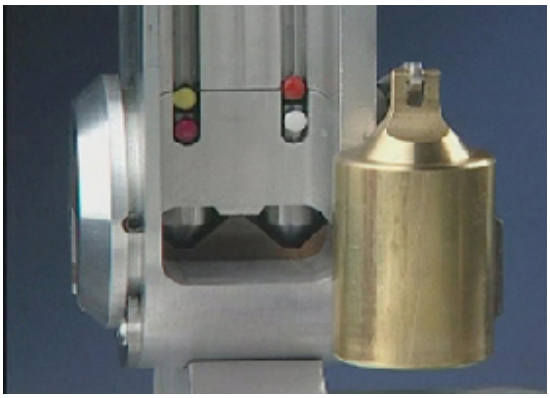


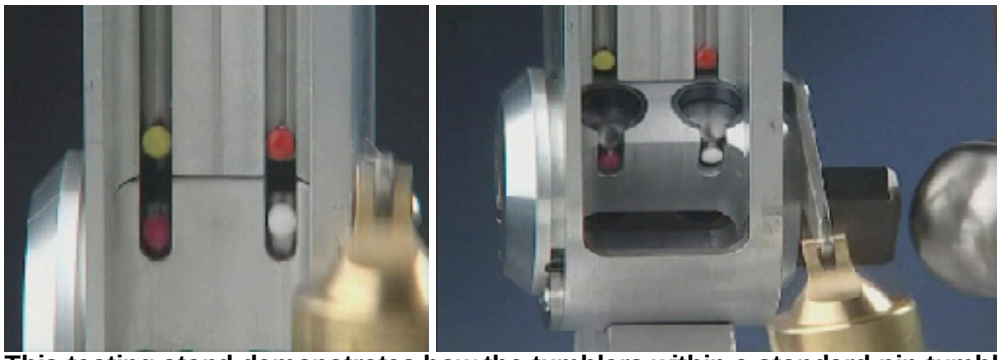
This diagram (from *LSS+*) shows the different components of a pin tumbler cylinder and associated key. There are a number of parameters that must be correct in order for a bump key to work properly. Of critical importance are the cut depth, spacing of cuts, and cut shape. Shown are different code depths (0,2,4,7) as would appear on a normal key for this lock. In order to create the 999 or bump key, each of the depths would be modified to the deepest cut (9). The cuts must be shaped correctly and the shoulder must be modified so the key can be pushed forward during the bumping process if the negative-shoulder method is employed. In addition, the distance between cuts (center-to-center) must be accurate.

THE BUMP KEY: AN INTRODUCTION

This report examines the procedure for opening locks that is known as bumping. It is a bypass method that uses a specially cut key to cause the pin tumblers to momentarily split across the shear line, thereby allowing the plug to turn. The original technique has been known by locksmiths and police for many years and was described in detail in ***LSS+*** but has only gained significant attention as the result of recent publicity in Germany and the Netherlands. Bumping was not considered a real threat to security until the technique was revisited in 2004 by members of Toool and other groups who determined that locks could be compromised by fashioning the bump key with what is referred to by the author as the “negative shoulder” method, detailed in a white paper that was authored by Barry Wels, Han Fey, and other members of Toool, “The Open Organization of Lock pickers” in the Netherlands and published by http://www.toool.nl and described in ***LSS+.***

Research was also conducted by Members of Ssdev "Sportsfreunde der Sperrtechnik" (Germany) in 2004, detailing a number of issues relating to bumping and its perceived threat to security.
For additional material regarding this subject, see
http://www.toool.nl/index-eng.php (main page)
http://www.toool.nl/bumping.pdf (original report)
http://www.toool.nl/bumpkey-alert.wmv (Nova television)
http://connect.waag.org/toool/ (bypass techniques)
http://connectmedia.waag.org/toool/whatthebump.wmv
(latest bump key presentation)



This testing stand demonstrates how the tumblers within a standard pin tumbler lock can be bumped through the application of energy to the base of the pins. A weight is utilized to replicate the actions of the "tomahawk" bumping tool to generate the required force against the key which has been inserted into this enlarged lock model (top left). In the photograph (top right) the bottom and top pins block rotation of the plug. In the photograph (bottom left) energy has been applied and the pin stacks (yellow-red and red-white) have momentarily been separated at shear line. The plug can now be turned. The Dolev anti-bumping pin prevents this practice. A video in LSS+ demonstrates this procedure.

In November, 2005, approximately 80 different models of locks that are sold primarily in the Netherlands were tested by the most prestigious and respected consumer protection research group, Dutch Consumentenbond. They are a private organization that evaluates products and alerts the public to defects or potential issues. These tests were conducted in conjunction with law enforcement agencies and members of Toool and utilized both skilled and unskilled individuals to open the locks. All of the locks were obtained directly from retail outlets by Consumentenbond.

The results of the tests have now been published and can be obtained from http://www.toool.nl and http://www.consumentenbond.nl. They clearly demonstrate that the vast majority of traditional mechanical pin tumbler locks that are utilized in the Netherlands can be opened in seconds by amateurs, unskilled in covert methods of entry. Even certain high security locks were compromised during the evaluation. No such testing has been accomplished in the United States.

Presently, there are no real standards to measure the security of a lock to withstand a bumping attack. Our office is working to develop such standards and methods of testing and will be evaluating different cylinders upon request. The testing procedures developed by Toool (the Green-Yellow test) are being integrated into the protocol. The author may be contacted for a draft copy of a proposed testing procedure to rate pin tumbler cylinders.

ANALYSIS

This report provides information regarding conventional five and six pin tumbler cylinders as well as dimple and sidebar locks. Bumping is not an issue with warded, lever, wafer or disc locks because their design does not rely upon a

shear line. The technique can only work when a pin stack, consisting of two or more pin tumblers, is momentarily separated. This analysis is solely based upon the perceived threat to security by the compromise of a lock by bumping. Other forms of bypass such as picking, the use of a pick gun, and the employment of an electro pick are not covered although each of these techniques may yield just as rapid results.

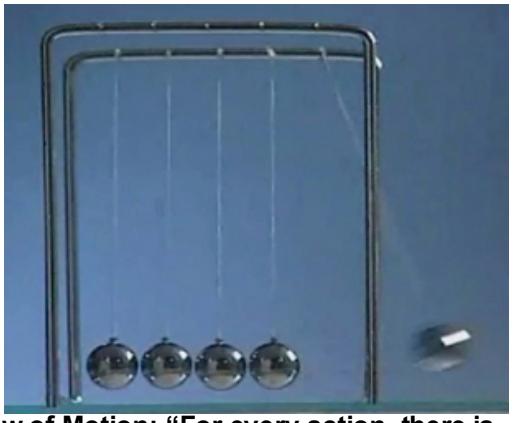
We differentiate two levels of attack: one that is based upon having no prior information or internal access to keys for a specific lock, and the other, available prior intelligence or inside information or access to keys, especially for high security sidebar locks. Obviously, the risk when there is prior intelligence may be greater, although as we shall show this is not necessarily true if certain brands and models of high security locks have been installed. The threat level is analyzed in terms of the difficulty in opening a lock, based upon required skill and the variables that may make the process more complicated and time consuming.

We view bumping as yet another method of bypass. The primary difference and principal danger is the ease in which it can be learned in comparison to other techniques and the lack of necessity of any specialized tools. Acquiring the needed skills is quite elementary. In fact, the Netherlands test demonstrated that lay people could view a short video that appeared on the Internet and then were able to open a high percentage of the locks that were tested with only a limited amount of practice. Although a person who just walks up to a lock with a bump key is not likely to achieve any success, once they understand the theory and have an opportunity to practice, they will, in all likelihood, have a high probability of success. Thus, the only real protection against bumping is the installation of certain high security locks that employ sidebar other designs, or anti-bump pins within conventional cylinders.

Bumping: A technical description

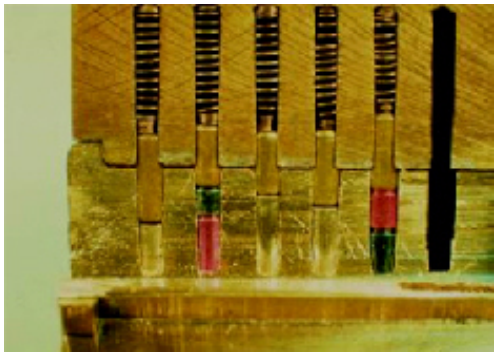
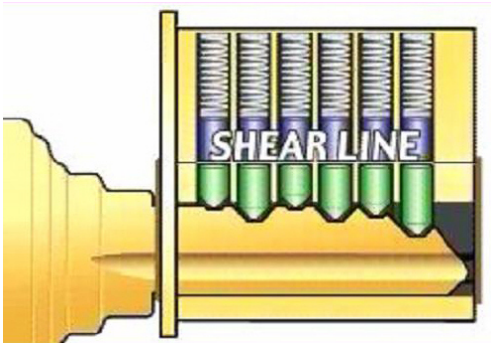
Bumping can be likened to rake picking or the use of an electric pick tool; many locks can be opened with minimal to no training because it is not necessary to understand any detailed theory behind the technique, In fact, bumping for the amateur may be far more reliable than the use of the pick gun because uniform transfer of energy is assured by the nature of the process.

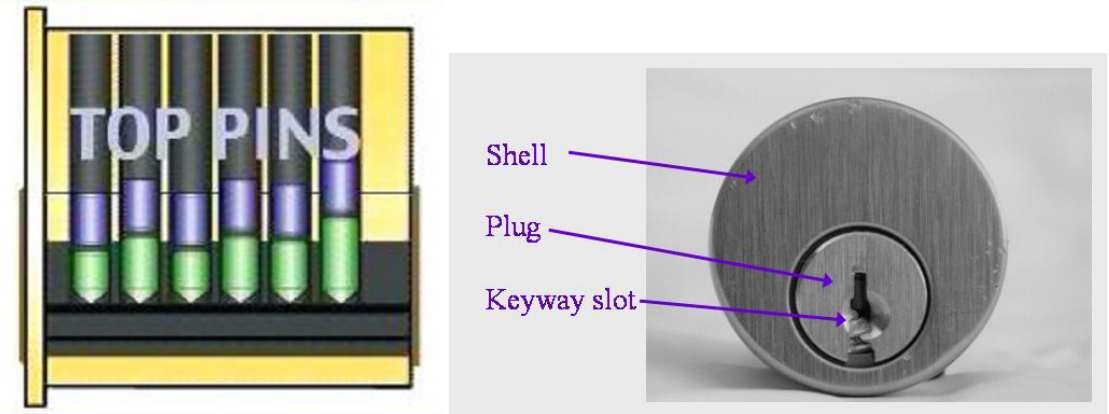
Bumping is the simultaneous application of energy to the base of all pins through a specially cut key where the depth of each cut is the maximum allowed. Once properly seated, the key is slammed forward with a bump tool, which is nothing more than a plastic mallet or similar device whose function is to generate a controlled burst of energy. Proper technique will result in opening the lock. Bumping occurs as the result of an inherent design issue within all conventional pin tumbler locks and is based upon a law of physics first developed by Sir Isaac Newton more than three hundred fifty years ago and discussed in ***Locks, Safes and Security*** and ***LSS+*** .

Sir Isaac Newton formulated his Third Law of Motion: "For every action, there is an equal and opposite reaction." When the first steel ball is struck on the left of the array, the energy is transmitted to the last ball on the right. This is precisely the theory upon which bumping is based. The left-most ball represents the bottom tumbler that makes contact with the bump key. The right-most ball represents the top pin within the lock. Little did Newton know when he formulated his physical law that he would be the father of bumping some three hundred years later!

Bumping occurs from the exploitation of the placement of two or more pins within each chamber and the ability to briefly separate these pins as they cross the shear line. When the base of a bottom pin is struck via the cuts on a key, the top pin is bounced upward. For a few milliseconds, there is a gap between the bottom and top pin. If torque is applied during this brief interval, there is nothing to stop the plug from turning.



These diagrams show how the shear line functions within a pin tumbler lock.

The threat from bumping results because it is a method for an unskilled individual to rapidly open a lock without really understanding the theory or developing any significant skill set. **Bumping, in the view of the author, is a method of opening a pin tumbler lock by one not trained as a locksmith.** The technique can also be utilized by a professional to accomplish a rapid bypass of a cylinder, but the skill set may be different, depending upon a specific cylinder and other variables.

We define the threat from bumping as a rapid means to open a lock by someone unskilled in the art of locksmithing or bypass. The concomitant side of this issue relates to the locks that are produced by manufacturers who have been identified as “insecure” because they can be opened by the bumping technique. In the view of the author, the labels of “not secure”, “can be opened by bumping” and “subject to bumping” require careful definition from a legal, technical and ethical perspective because the reliability and repeatability of such process may not be assured. Just because a lock has been sporadically opened by bumping does not mean it is inherently insecure.

Secondary locking mechanisms

Theoretically, all **standard** pin tumbler locks can be opened by bumping. However, this is an over simplification because of the introduction of many variables, identified subsequently. In addition, there are modifications to “standard” pin tumbler mechanisms that may be more difficult to compromise. The optimum use of the bump key envisions a five or six-pin tumbler lock that contains no other security technology.

Secondary locking technology cannot be bumped because a traditional shear line is not created. This would include sidebars employed by Medeco, Assa, Schlage and others that rely upon the rotation of pins (Medeco), or rotation and/or lifting of secondary elements (Assa and Schlage Primus), or interactive elements (Mul-T-Lock and DOM). Sliders that control sidebars (Evva) cannot be bumped either. For a lock to be a target of bumping there must be at least two

pin tumblers in each chamber that, in normal operation, are split at the shear line by movement of the proper key and otherwise block rotation of the plug.

Some models of locks produced by Mul-T-Lock, DOM and other manufacturers have incorporated certain features that are designed to make it more difficult to replicate a key. Interactive elements that change their position and which are embedded within the key are usually placed in one or more defined locations, rather than randomly. So long as the bump key contains the identical elements, it may be possible to open the lock, although the difficulty may increase. The underlying physical theory of bumping does not act upon these added elements. They merely add another variable and may prevent a successful opening because their primary function is interfered with by the forces that are created during bumping.

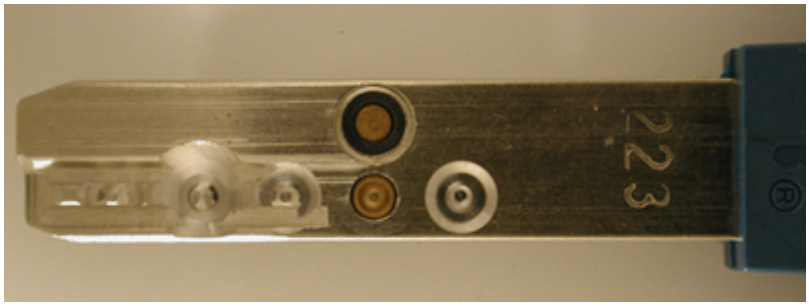
These interactive measures were not designed as an anti-bumping technology but for key security and to make picking more difficult. The Dutch test demonstrated that these elements can prevent locks from being compromised (Mul-T-Lock interactive and DOM-IX could not be opened during the formal test), but the DOM 6SR, the flagship of the DOM product line, was opened within seconds, even though this particular lock was equipped with anti-bump pins, two sidebars and one interactive floating disk which is active at a 45 degree angle straight through the key. There have been a number of independent reports and demonstrations from different countries regarding the ability to bypass these interactive measures and in fact some of these locks have been successfully opened by bumping. The real issue is the repeatability and reliability of such actions for a specific manufacturer. As has been emphasized in this report, the ability to open a lock one or more times is far different than opening that lock repeatedly with a high probability of success every time.

The members of Toool and others continue to develop methods to bypass these high security cylinders, based upon their specific design parameters. The issue in such cases raise three interrelated and relevant questions: (1) what is the required expertise, in terms of knowledge and tools, to produce a working bump key that may contain unique or modified geometry, (2) what is the skill set required to open these locks, and (3) what is the repeatability in such cases.

Although some models of some manufacturer's locks with sidebars or other security enhancements can be opened through the bumping process, there are caveats that must be understood in order to make this claim anywhere near truthful. Physically, the sidebar portion of a locking system cannot be bumped open. It does not matter whether it is a Medeco with its rotating and elevated pin tumbler design, or an Assa with its vertical finger pins, or a Schlage Primus with finger pins that are similar to the action of a Medeco pin tumbler and provide a completely separate locking system, requiring both rotation and lift of the finger pins. In the case of Mul-T-Lock, DOM and others, their interactive elements can make bumping difficult or impossible, but these locks have been opened by

bumping. However, in the view of the author, such occurrence may not be reliable or repeatable and are dependent upon a number of variables that may be specific or unique to each target lock.

If locks that contain secondary systems such as sidebars and interactive elements are to have a chance of being opened by bumping, then the precise character and dimension of these elements must be replicated within the bump key. That means that the correct sidebar code or interactive element must be present as well as the position of any moving piece or ball bearing. These elements must not be adversely affected from forward movement of the key during the bumping process. When the only variable is the shear line and the pin tumblers that cross it, then the lock will likely be opened. The moment that complicating variables come into play, the chances of successfully bumping diminish in proportion to the complexity of the secondary locking system. Although some high security cylinders may indeed be subject to bumping, it is usually as a result of a combination of factors within specific locks and bitting patterns. Such a combination of variables are generally not present in all locks, which explains why only certain ones can be opened.



These photographs show the interactive element within a Mul-T-Lock. The pin floats and is acted upon by internal components. Note that there are two elements because the key is reversible.

Bumping of the high security component of a lock is impossible because there is no sidebar design that utilizes a set of movable pins that can be split at a shear line. In the case of Assa and Schlage, the side pins that control the sidebar are in fact separate systems. Although Medeco incorporates a single pin to accomplish both lift and rotation, the sidebar vertical channel for each pin is not subject to bumping. There have been various claims that Medeco and Assa have been

bumped open. This is true for certain locks, but not entirely accurate because the procedure is neither reliable nor repeatable on any consistent basis. No claims have been made with regard to bumping of Schlage Primus. In the view of the author, their design probably precludes the practice.

In the case of Medeco and Assa, in order for there to even be a chance that one of these cylinders can be bumped open, the bump key must have the correct sidebar code as a precondition, thus requiring advanced intelligence about the target lock. Simply walking up to a Medeco or Assa with a bump key having a random sidebar code will never result in an opening unless that code happens to be the correct one. We concede that some high security locks may be opened on a one-time basis by picking, electropick, raking or bumping, but this has more to do with a number of variables that may randomly occur and by no means equate to a reliable method of bypassing the lock.

Further, if sidebars are used with sliders, such as employed by Evva, these locks cannot be bumped at all (3KS). Reporting that a certain sidebar lock can be bumped open is misleading because the statement cannot be applied universally to any model or manufacturer. In the author's view, the random ability to bump open a lock does not constitute any more of a threat than the ability to pick some locks. Reliability and repeatability within a limited time frame are the critical tests of a successful bypass technique.

From a factual, legal and ethical standpoint, the author believes that certain disclaimers should be attached to any statement or claim that any lock, and especially a high security cylinder utilizing sidebar technology, can be bypassed by bumping or any other technique. This is because opening one or a few locks misrepresents the ability to open a high percentage of such locks and does a disservice to both the manufacturer and the public.

The following disclaimers should be placed in any report regarding bumping of high security cylinders:

Only a limited number of locks have been tested, and therefore we only claim to have opened N locks during such testing; The fact that one or more locks can be opened does not necessarily indicate or imply that a substantial number of locks by the same manufacture can be opened in like manner; One lock may be opened within seconds, while another lock of the same model and design may be impossible to open, or may require substantial time to open; The manufacturer may have introduced enhancements to complicate or prevent bumping or other forms of bypass in subsequent models of which we are unaware; The locks that were tested may not accurately represent all of the locks produced by the manufacturer for a specific model or their ability to be bypassed;

There may be many variables, some of which are unknown, that would affect the ability of a lock to be opened;
The condition of the lock immediately prior to bumping may affect its ability to be opened;
The reader should conduct their own tests to determine the vulnerability of any specific lock or model.

Difficulties in Bumping

The following variables in manufacturer design and operating condition of a lock can affect the ability to open that cylinder by bumping and may determine whether amateur skills or greater expertise is required. These variables are referred to in defining the security threat level that results from bumping.

Variables that can affect the ability to open a lock by bumping

- Tolerance of internal components
- Availability of keys
- Ability to obtain depth and spacing data to create a bump key
- Ability to create the proper cuts
- How and where the lock is mounted (horizontal, vertical, near obstructions)
- Physical size of the bump key
- Secondary locking systems (sidebars)
- Number of pins per chamber
- Number of different depths of pins within the lock (the longer the pin, the more difficult it may be to bump the lock open)
- Location of locks
- Noise tolerance in area of attack and likelihood of detection
- Condition of springs
- Spring bias differential
- Anti-bump pins
- Lubricant and ease of movement of pins
- Concern with forensic indications of bypass
- Special requirements for the creation of a bump key
    - Special stop at shoulder (dimple lock)
    - Modification of tip to accommodate closed cam
    - Modification of shoulder to allow forward movement of the key

BUMPING: THE HIGHEST THREAT LEVEL

In order for bumping as a bypass method to pose a serious security threat, a number of criteria must be met. In summary, these would essentially require that *an individual that is untrained in locksmithing skills be able to easily obtain a key, modify it, insert it into a lock and open it within a few seconds without any special*

tools or expertise. In order that a statement could be made that a specific manufacturer model could be opened, repeatability and reliability in the bumping process would have to be demonstrated.

We view that bumping poses the highest security threat when the following conditions are met, defined in terms of eight issues: **skill set, time, prior intelligence, the key, the lock, bumping technique and tools, training, and evidence of entry.**

Skill Set

The lowest skill set is required and can be accomplished by an individual with no special expertise and minimal to no practice. The only actual information required to open the target lock would be the identification of the proper keyway;

Time

There is an ability to open the lock in less than one minute;

Prior Intelligence

No prior intelligence about the lock or facility is required;

The Key

It requires the possession of a key that will properly enter the keyway and which can be cut, or the bitting modified to the deepest value for each position (a bump key must contain all “9” or equivalent deep cuts). The key may be obtained from a retail outlet or by access to a blank key that is readily available through public channels;

The Lock

There are no security enhancements within the lock that require any special key modification;

Bumping Technique, Torque, and Tools

No special implements are needed other than a bumping tool with which to strike the key, and a metal file to create the bump key (or ability to code-cut a key);

The key must be fully inserted and then withdrawn by one position, or the shoulder must be slightly modified to allow at least .25mm forward motion of the key from its proper position, (where each bottom pin is seated at the root of its corresponding cut prior to bumping). The proper amount of torque must be applied to the key during the bumping process, and must be released at the

conclusion of each bumping cycle. The proper application of torque is critical and can determine whether the lock will be open. The timing as to when torque is applied is just as critical.

Training

No extended special training or practice is required;

Evidence or Indication of Entry

There is generally no forensic indication of bumping or that the lock has been opened by such means, and no apparent damage to the lock may result. Depending upon the design of the lock and the skill of the operative, there may indeed be evidence of deformation of pins or springs. In certain cases, repeated bumping may compress or distort components and render the lock unusable and in some cases, impossible to open.

Reduction of the threat level

Additional difficulties and variables will result in even less of a security threat. When one or more of the following conditions are present, bumping is considered a technique of bypass rather than a method to open a cylinder by an amateur. Depending upon the complexity of the variable, special skills, tools and techniques may be required.

- Consistent results are not obtained for all locks;
- Success is dependent upon one or more variables within the lock, such as:
    - Pin stack combinations
    - Length of bottom pins
    - Rotation of pins as was set by the removal of the last key
    - New or worn mechanism
- Requires special technique of bumping (hard, soft strikes and special torque);
- Requires a different mode of the application of torque;
- Requires more than one minute to open;
- Damage or deformation of tumblers, springs or other internal parts may occur;
- Requires a special key-cutting machine or there is increased difficulty in creating the required cuts on the key;
- If a dimple lock, specially cut key and shoulder-stop are required;
- Restricted blanks or sectional keyways are employed, and the availability of cut keys or blanks becomes more limited;
- Tip of the key must be modified;
- Extended bumping may be required to open the lock.

Any of the following issues may make bumping of a lock even more complicated and complex and are often encountered with high security locks. **The author believes that in such instances, bumping is taken out of the realm of the amateur and must be accomplished by a semi-skilled or professional technician.**

- Prior intelligence about the lock or facility is required;
- Secondary locking technology is utilized (sidebars);
- Knowledge of and ability to replicate the sidebar code for the bump key;
- Separation of conventional bitting from sidebar milling is required;
- The proper sidebar code must be employed on the bump key:
- The sidebar cuts may need to be modified to allow bumping;
- Multiple sidebar codes may be employed within one master key system;
- Special techniques must be employed to replicate blanks, such as the use of silicone casting or the Easy Entrie milling machine;
- Requires special action to make a key, such as:
    - Milling of wards or sidebar configuration on the key
    - Special depth cutting of conventional bitting
    - Knowledge of special depth or spacing information is needed to create the key.

ORDER OF DIFFICULTY TO BUMP OPEN THE LOCK

Bumping has several components, as previously identified. These are ranked in the order of difficulty to achieve and thus can affect the threat level. Unfortunately, these issues can interact so the task of evaluating the overall simplicity or difficulty of opening a specific cylinder becomes more complicated. Ranking is intended to provide an index as to the ease or complexity that can be expected.

1. THE KEY

A bump key (999 key) can be created by anyone who possesses or obtains any cut key that will enter the keyway of the target lock or who obtains a blank key that may be cut as a bump key. Interchangeable core, restricted keyways and sectional keyways do not affect bumping. So long as a person can obtain **any** cut key that will enter the lock, it can be made into a bump key.

A bump key can be produced by modifying an already cut key (or blank key) that fits the keyway of the target lock (or another lock that has the same keyway). A round, pippin, triangle or square file will suffice and can be purchased at any hardware store. The choice of file depends in part upon the bitting depth of the key that is to be modified.

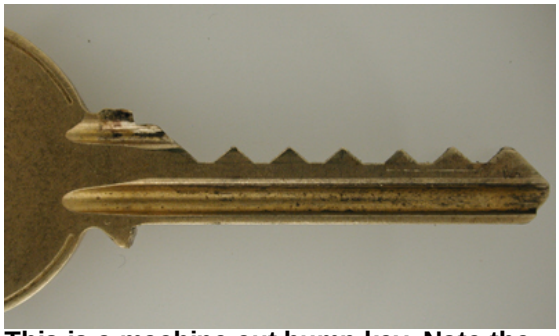
Hand-cut keys

Each cut must be individually filed to its deepest value. In some locks, the cuts may in fact be made slightly greater than the deepest code value, but depending upon the keyway and specific lock design, this may not be true.

Although this procedure appears deceptively simple, that is not exactly true. A certain amount of knowledge of the specific lock may be required in order to know the depth of the deepest cut. Different manufacturers have different depth and spacing specifications and they are by no means uniform. Thus, the operative must know how far to file the key for each bitting position. It may not be possible to ascertain this information from just a visual inspection of the key that is being modified and certainly the information is not evident from a blank key.

Cuts must be correctly formed and properly centered for each chamber. The ramps of each tumbler position must be uniform and parallel to each other, although a slight variance may be self-compensating as the key may actually deform the bitting surface as it slams against the pins. The peaks for each cut must be sufficient to properly make contact with the base of each pin and provide enough material to “bounce” it. If the cuts are too low and the peaks not formed properly, then the key will not properly interact with the tumblers and the lock will not open. If dimple keys or keys requiring special milling are utilized, then they may be difficult or impossible to cut by hand.

Machine-cut keys



This is a machine-cut bump key. Note the consistency in geometry of each cut. This key is far easier to produce than one that is made by hand and has a greater likelihood of opening the target lock.

Bump keys can be cut by code on a key machine that has that capability. These key cutters, whether hand-held punch or motor driven, are not generally available at retail outlets and are utilized primarily by lock shops, although they can be purchased readily from supply houses. Most locksmiths would refuse to produce a key with all “9” or equivalent cuts and would be likely to report any such request to law enforcement authorities.

Availability of a Key

A key (either cut or blank) for the proper keyway must be possessed or obtained in order to create a bump key to open a lock. **This becomes the most critical issue in success or failure of bumping.** The ease or difficulty of this task will depend on a number of variables, which may prove very simple to extremely difficult. Already, web sites are offering bump tools and precut keys for specific keyways, thus escalating the security threat.

If a key that fits the target lock is already possessed, then the lock can most likely be opened, assuming that it is a conventional five or six pin mechanism. Thus, an individual working in the same office building, for example, would likely have access to one or more keys that would enter other locks in the building, because all of the cylinders would likely be the same manufacturer and keyway. This is the simplest scenario.

If, however, the manufacturer and specific keyway of the target lock must be identified, the task can prove more difficult but not impossible especially if the brand and model are prevalent in the area. If the target is a mortise or rim cylinder or a padlock, then the manufacturer name will generally appear on its face, making identification more precise. If key-in-knob or lever handle in-line hardware is utilized then identification of the lock maker may prove more difficult, also complicating the task of obtaining the correct key.

Although a key can be acquired from many sources as noted below, there are two critical events that must occur: the correct manufacturer and keyway must be obtained, and the key must be of the correct length (for a five or six pin tumbler lock). A six-pin key can be utilized in a five-pin lock but the reverse is not true.

If an individual does not possess a cut key that will fit the target lock, then the alternative is to identify the manufacturer and keyway and obtain a blank key or a sample lock and cut key from a commercial (or other) source. For example, if Kwikset locks are the target, then similar locks having the same keyway could be purchased from the local hardware store, Home Depot, Wal-Mart, or Lowe's. This would provide a source of keys that could be modified for the correct depths, and also would offer test locks in order to gain proficiency in bumping.

If keys and test locks are to be obtained from commercial sources such as retail outlets, then the market penetration of the specific manufacturer will determine just how simple or difficult a task this becomes. Many manufacturers utilize a few standard keyways across the United States for retail distribution. This can make the task of obtaining the correct key much easier. If a certain brand of lock is popular in a given area, then it may be much easier to find a key. Simply observing a target lock and determining the proper key to fit it may become a daunting task, especially if less popular locks are utilized or special keyways or patented designs have been assigned, as in the case of many commercial or

government installations. In such instances, the threat of bumping becomes far less, unless there is already access to keys from sources that are defined below.

Sources of keys that fit the target lock

One source for keys would be the random selection of another lock, based upon possession of a key that enters the keyway of that lock. In this scenario, an individual would randomly try a key in a lock. If it entered the keyway, then, depending upon the kind of lock, it may be bumped open after modifying the bitting. An individual may already have a cut key for another lock with the same keyway, such as might be the case of a tenant in the same building, dormitory, apartment house, housing project, or commercial building tenant. Employees or people that have keys for limited access to a location could also create bump keys. Or, one might borrow a key to a restroom within a target building and copy it or just fail to return it. Finally, an individual could obtain the name of the locksmith for a target building and purchase the same locks under a pretext.

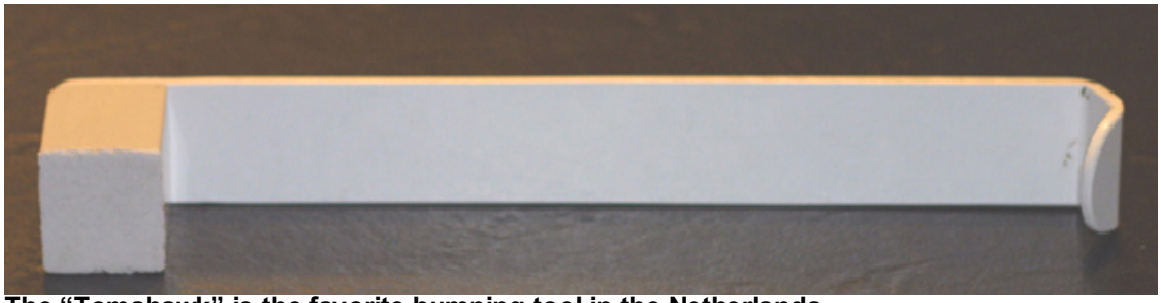
2. THE LOCK

The easiest locks to open are a five or six-pin conventional cylinder or simple dimple lock. If sidebar technology is utilized then the lock will not be opened by an amateur attack without prior intelligence.

3. CUTTING THE 999 KEY

The 999 key must be cut so that all bitting positions are the deepest cut that is specified by the manufacturer. If the cuts are too shallow the lock will not open. In certain cases, if the cuts are too deep, the bitting will not properly move the pins, although in certain locks, the cuts can be one half to one cut deeper with no affect. All of the cut angles must be parallel and consistent so that energy is transmitted at the same time to each pin. In certain cases, the key will form itself after several blows if the angles are not identical. The shoulder of the key must be reduced to allow the key to move forward about .25mm, if this bumping technique is employed. If too little material is removed, the key will not work.

4. BUMPING TOOL



The “Tomahawk” is the favorite bumping tool in the Netherlands.

The bumping tool may be any implement that can create a momentary shock or burst of energy to the head of the key. A special “Tomahawk” tool was developed in the Netherlands by Kurt Zuhlke specifically for this purpose. The author believes that this design works the best for bumping. In the United States LockSport hobbyists have commercialized a similar tool to the Tomahawk coined the “Ke-Bump”. The Ke-Bump is readily available in the United States.

There is a modified tool, made of laminated leather that also works quite well. However, any tool that provides a hard surface can be utilized, such as a screwdriver handle or wooden or plastic mallet. The real requirement is that the tool has enough mass to create sufficient energy to bounce the pins while allowing control by the operator. The Tomahawk is made of plastic with the correct density and amount of flex in the handle.

5. TRAINING

Training is perhaps the simplest part of bumping, although obviously if the operative does not understand the theory and has not had a chance to practice, the likelihood of success is greatly diminished. In one instance, the author handed a bumping tool and six-pin cylinder to a reporter who had previously watched a short demonstration of bumping. Although she had no idea of the theory or proper technique, she was able to open the lock in about five seconds. The real danger of bumping, as discussed previously, is the ability (unlike picking or other forms of covert attack) to learn the art in a few minutes.

Assuming that the proper bump key has been produced, the operative needs to learn five skills to successfully bump open a lock:

- How to position the key in the lock;
- The amount of force necessary to apply to the head of the key;
- The correct amount of torque to apply;
- The proper timing between bumping and the application of torque;
- How to repeat the process when the lock does not open.

These issues may appear more complicated than they really are. In the Netherlands test and in the personal experience of the author, the technique of bumping can be easily mastered by most people in just a few minutes. This, again, is the danger of the technique; no real skill set is required to successfully open most locks.

SPECIFIC SECURITY SOLUTIONS

Certain locks are secure against bumping. These are generally high security cylinders, often with a UL 437 or equivalent rating. Some manufacturers have implemented patented anti-bumping pins within their standard cylinders that will also frustrate the practice (Moshe Dolev in Israel and others). As noted in our

earlier discussion, some locks are not subject to the practice at all. As a result of the work done by the members of Toool and others, several manufacturers have begun implementing changes that will frustrate or eliminate their vulnerability to this form of attack.

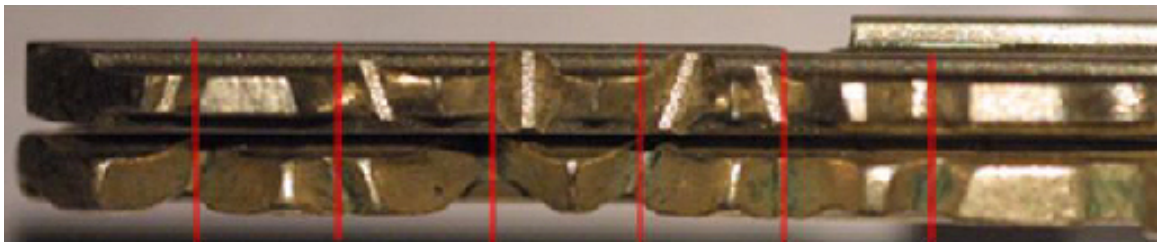
The following locks are noted for their resistance to bumping.

Schlage Primus

The Schlage Primus utilizes similar side millings to Assa, but the locks are more secure because the finger pins must be lifted and rotated in order for the sidebar to align properly.

Although the Schlage Primus and Assa were created by the same inventor, the Primus design is quite different in terms of its resistance to bumping. In Assa configurations, the finger pins are only **lifted** but not rotated. The elevation of the pins allow alignment of individual gates within each finger pin to the sidebar. In contrast, the Schlage Primus, like the Medeco integrated pin tumbler, requires that each finger pin be *both lifted and rotated* to allow the sidebar to retract. The tolerances between each pin and gate makes it virtually impossible to move the bump key horizontally (having the proper sidebar code) and still maintain finger pin to gate alignment. Thus, it is virtually impossible to bump the lock, even with the correct sidebar code on the bump key. If the key is physically split, then it is theoretically possible to use the upper portion to bump the conventional pins, but proper seating of the sidebar millings is critical and there is generally some interaction between the side millings and bottom pins that make this option almost impossible to achieve.

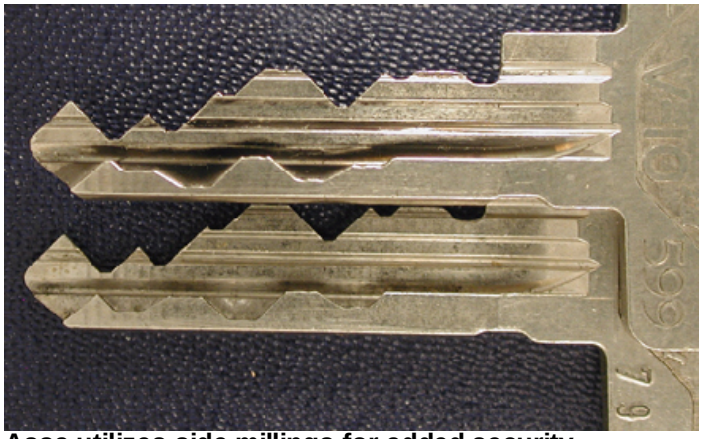
Medeco



This is a top view of the bitting angles for the original Medeco (bottom) and the Biaxial. In the Biaxial design as shown by the vertical red lines, there are twice the number of possible angles for each tumbler position. Each pin tumbler is both lifted and rotated to the correct position in order for the sidebar to properly align. The M3 adds another layer of security.

Some Medeco Biaxial locks have been opened by bumping, but this claim is deceiving for a number of reasons. Unlike Primus and Assa, Medeco integrates a sidebar with conventional bitting within each pin tumbler. Pins are both lifted and rotated by the bitting of the key in one combined action. Thus, if the correct sidebar angles are cut on the bump key and the bitting for the conventional pins is created in such a way that the key may be bumped in a forward direction without affecting rotation, then the lock can sometimes be opened. Although this process can be accomplished it cannot be reliably repeated and can result in damage to springs. This will make the process difficult or impossible to repeat on the same cylinder. A Medeco cylinder can never be opened by bumping without the correct rotation angles for each fore and aft position being cut into the 999 bitting. The M3 does not offer any significant advantage in security against bumping. The author has tested some cylinders and was able to bump them without difficulty with the correct sidebar code.

Assa

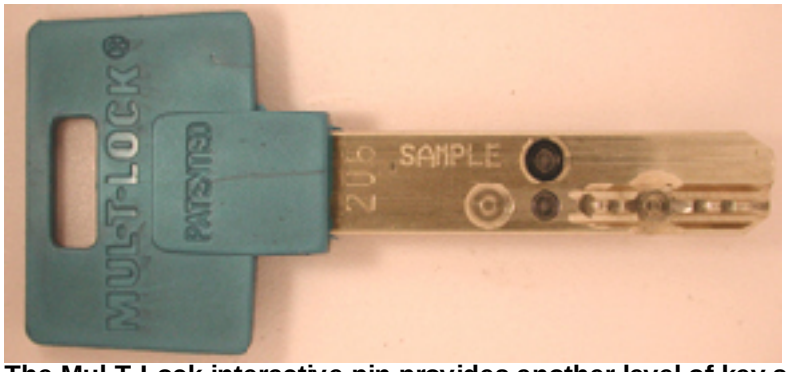


Assa utilizes side millings for added security.
The photograph shows two keys with different sidebar codes.

Some Assa sidebar locks can be bumped open with the correct sidebar code. As with Medeco, prior intelligence is required; the sidebar mechanism cannot be bumped without the proper code being cut into the bump key. Assa is easier to open in this fashion than Medeco because the sidebar bittings are separate from the conventional bitting. This allows for several possible options. If the side millings are not multiplexed (V10 and later designs), then there can be enough horizontal tolerance to allow the slight forward movement required of the bump key without affecting the interaction of the side milling to the finger pins. Additionally, theoretically, the side milling portion of the key can be physically split from the conventional bitting. In such a scenario, the portion of the key that

controls the finger pins is set in position prior to bumping. The top portion of the key can then be moved forward without affecting the operation of the sidebar. The same caveat applies for Assa and Schlage Primus; this process is not practical.

Other Designs

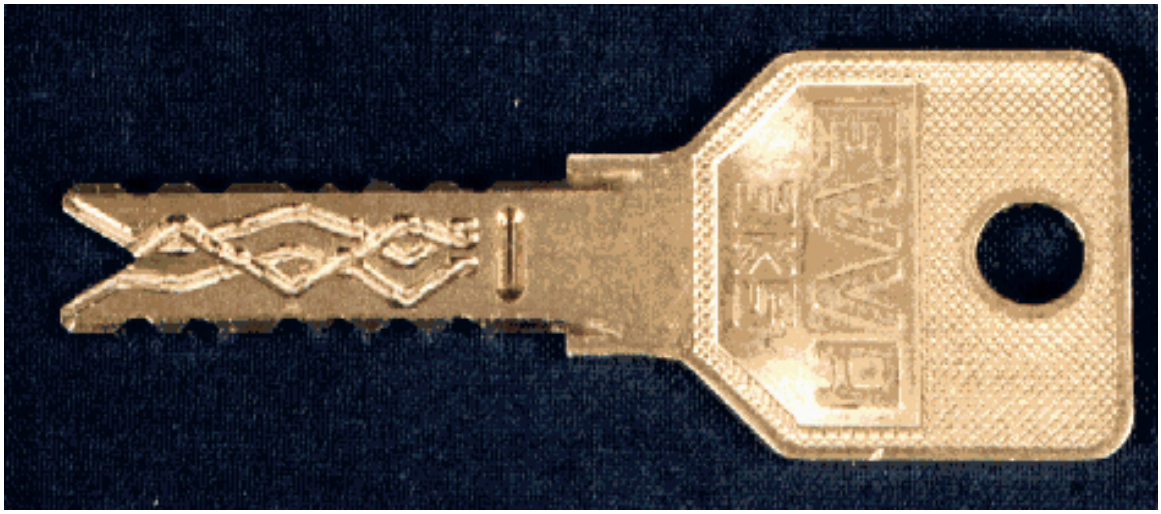


The Mul-T-Lock interactive pin provides another level of key security.

Other high security lock designs may also frustrate bumping attempts. The Mul-T-Lock is a pin tumbler dimple lock that utilizes telescoping pins and in some designs, interactive pins. In the Netherlands test, certain models of Mul-T-Lock were bumped open, while others with interactive pins could not be opened during the test, but reportedly have been opened, but not consistently or with repeatability. The author has bumped open several Mul-T-Lock cylinders models (7x7, Interactive, Classic) but again, this only represents a very limited sample. Mul-T-Lock has reported that they have taken steps to prevent bumping.

Other dimple designs will likewise frustrate bumping. Kaba, for example, produces locks with multiple rows of pins, set at different radial angles. These locks are virtually impervious to bumping, while in contrast normal dimple locks are quite simple to open.

Evva (Austria) utilizes a design in some of their locks that outwardly appears from an examination of the key to be a pin tumbler lock, but actually utilizes sliders. These locks cannot be bumped open because there is no shear line; only sidebars.



The Evva 3KS is based upon the use of 13 sliders to control two sidebars. The key is a composite of intersecting tracks that guide the sliders. The photograph shows the interaction of a slider and track. This system is secure against bumping.

In some models, DOM utilizes an embedded ball bearing within the key that can also frustrate bumping.

DOM-IX series

Summary

Virtually all conventional pin tumbler locks, regardless of manufacturer, are subject to bumping and a large majority of them can be opened by this technique. The ability, however, to open high security locks that incorporate sidebar designs is neither reliable nor repeatable. Although some of these locks have been opened, there are significant limitations that must be considered in assessing the security risk when such cylinders are employed.

Medeco, Assa, Schlage Primus and many other manufacturers all utilize sidebars to increase the security of the lock and prevent or seriously reduce the risk of bypass. Although certain models of Assa and Medeco have been bumped open, this was done so only after the bump key was cut with the proper sidebar code, Without this critical information the locks could not be opened. Even with the correct sidebar code, the results are certainly not assured, reliable or repeatable because there are many variables in the process, as noted in the previous discussion. The requirement of prior intelligence and the ability to replicate a blank minimizes the risk of bypass of sidebar locks to an acceptable level. Finally, if the correct sidebar code is known, then it may be more practical to extrapolate the top level master key, (as described in chapter 31 of ***LSS+***), rather than attempt to bump open the lock.

The consumer must assess their individual security requirements and the likelihood that they will be a target of bumping. If they perceive the risk as significant, then high security locks that are certified to resist bumping should be installed. It should be remembered that there are many methods of covert entry that range from simple to extremely sophisticated. Bumping is perhaps the simplest form of attack, but as has been described in this document it is not without limitations and certain caveats.

The unauthorized bumping of a lock constitutes forced entry and possession of a bump key would qualify as a burglary tool. In this regard, there is no difference between bumping and other forms of covert entry. Criminal investigators and police personnel should be alert to anyone possessing a key with the bitting in

each position cut to the same deep depth as shown in the photograph. No lock is ever keyed in this fashion.

Finally, old keys should be destroyed when the combination to locks are changed so that they cannot be converted into bump keys.

Marc Weber Tobias is the author of ***Locks, Safes and Security: An International Police Reference,*** and ***LSS+***, the Multimedia Edition. He has authored five police textbooks and is a practicing attorney and security consultant. His clients have included government agencies, corporations, and lock manufacturers. Additional information can be found at www.security.org.