Journal of Physical Security 6(1), 10-21 (2012)

Lock Opening by Bumping: Physical Analysis and Secure Lock Designs

Alexei Toropov, Ph.D.
Dierre Spa, Italy
tel: +393476701025, e-mail: alexei.toropov.dierre@gmail.com

Abstract

There are various techniques for defeating locks based on exploiting vibration. In recent years, one of these techniques for manipulating cylinder locks, called "bumping", has become widespread. The problem is that a large variety of mechanical locks can be opened quickly, in a non-destructive manner by using simple attack tools. We studied the physical phenomena responsible for the vibration techniques of lock opening. We considered the period of time during which the pins of a cylinder lock remain separated as a function of natural frequency, damping properties, and lock design parameters. On the basis of this analysis, we suggest some changes to lock design and assembly that can enhance the security of the lock and resist bumping attacks.

Key words: locks, security lock, lock picking, bumping, design of secure locks

Pin Tumbler Cylinder

When people talk about "the cylinder lock " or "the pin tumbler cylinder", they have in mind the classic locking mechanism invented by Linus Yale in 1861. The concept is so simple and effective that it remains the basic design principle of modern locks. The mechanism essentially consists of two main parts: the housing and cylindrical plug with axial keyway. See figure 1. A number of holes have been drilled up to the keyway in the transverse direction through the housing and the plug. In each hole, there is placed a key pin, a driver pin, and a compression spring. When the proper key is inserted in the keyway, each cut on the key has the correct depth which allows a coincidence between the shear lines of the key pins and driver pins, and the shear line of the housing and plug. When this occurs, the plug can be turned and the lock unlocked. If, on the other hand, the corresponding depth of the cut on the key differs from the correct value (either too high or low), the cylinder will not rotate.

If we assume that the number of different depths varies from 6 to 9, and that the number of the pin pairs is equal to 6 (which is typical for many standard cylinder locks), then the number of possible code combinations can approach half a million. Such a large value means that, despite being enclosed in relatively limited dimensions, the Yale mechanism provides significant levels of key uniqueness and security.

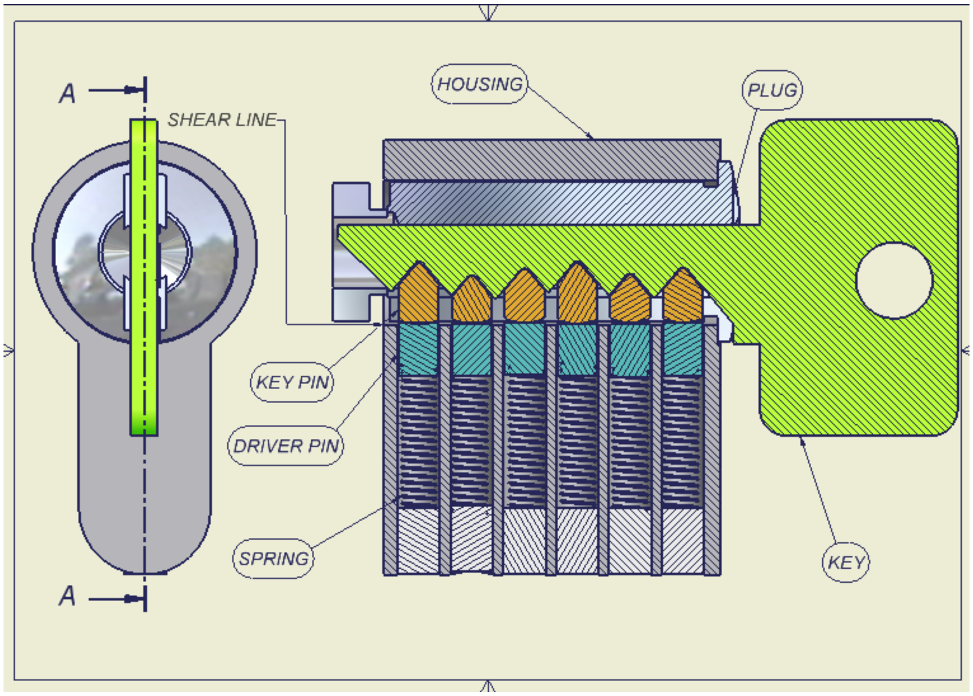

Figure 1 - The pin tumbler cylinder.

In recent years, however, it has become widely recognized that all cylinders which employ this classic Yale design are at risk due to the simple and easily applicable techniques based on the movement of the pins due to the impact or vibration applied to the lock in different ways. These can include the use of picking guns such as the "snapper pick"[1], through more sophisticated attack tools utilizing electric motors. All these attack techniques rely on the fact that the key pin and driver pin can be separated for a brief instant of time. During this small period of time, the skilled operator attempts to turn the plug of the cylinder.

One of the most successful of such vibration attack methods is "bumping", described in detail elsewhere.[1,2] In contrast to other vibration methods, bumping allows the simultaneous, synchronized movement of the pins. Bumping requires use of a bump key. This is a key which can be inserted into the keyway, and that has all cuts at every position at the maximum possible depth. In addition, the tip and the shoulder of the key must be milled for some fractions of a millimeter. If this bump key, once inserted, is hit by some impact tool, it transfers energy to the first pin of the lock. The first pin then transfers the energy to the second pin, which moves away from the first one, until the spring causes it to rebound back.[2] This approach allows the major types of pin tumbler cylinders to be opened quickly, without damage, through the use of simple tools.

The bumping technique has been investigated previously from the theoretical point of view [1,2] but only one part of the whole system of elements was considered, namely the kinematic behavior of the key pins and driver pins during purely elastic impact.

The Behavior of Cylinder Parts During Bumping

The tools used for bumping are shown in figure 2. The schematic model for bumping is depicted in figure 3, where M_h and V_h are the mass and velocity of the bump hammer, respectively, and M_k and V_k are the mass and velocity of the bump key. The values of velocities correspond to the values after impact.

For this model, we assume that the impact between all parts is purely elastic, and that they move without friction. This approximation is close to realty for low initial displacements just after the parts collision.

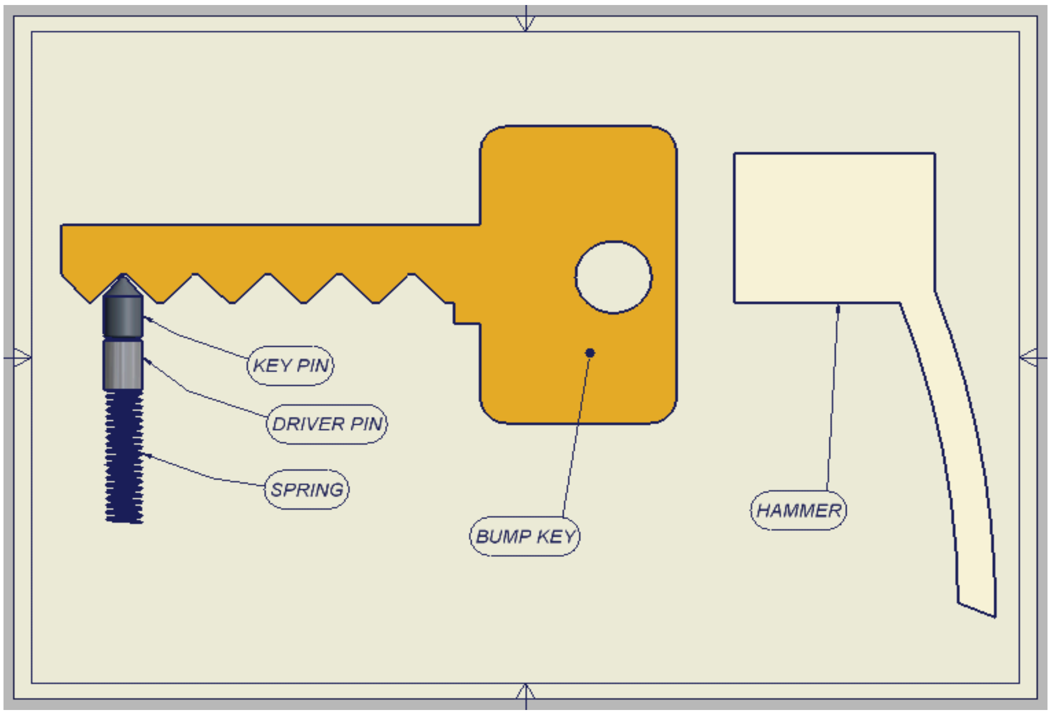

Figure 2 - Bumping components.

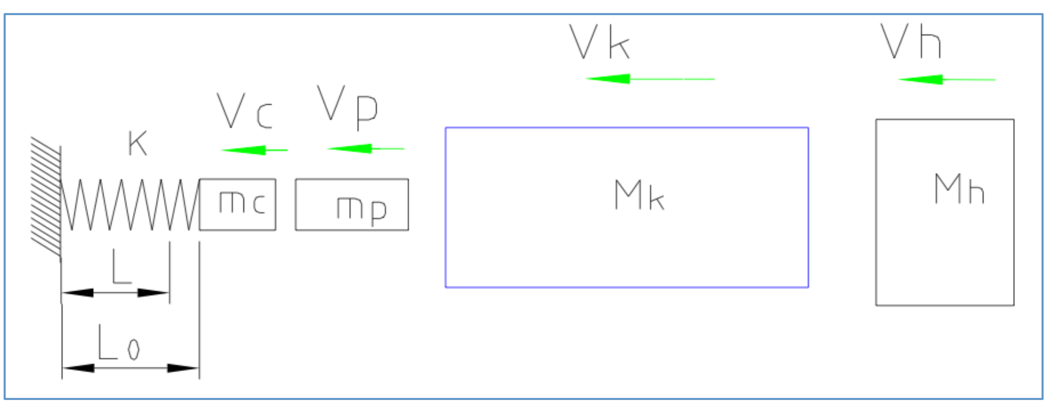

Figure 3 - Model representation of the bumping process.

The bumping procedure initiates with striking of the bump key with the hammer. If the hammer's initial velocity is V_0, the subsequent behavior of the hammer and bump key can be described by applying the following physical laws:

$$M_h \cdot \overline{V}_0 = M_h \cdot \overline{V_h} + M_k \cdot \overline{V_k} \qquad \text{the law of conservation of momentum} \qquad (1)$$

$$\frac{M_h \cdot V_0^2}{2} = \frac{M_h \cdot V_h^2}{2} + \frac{M_k \cdot V_k^2}{2} \qquad \text{the law of conservation of energy} \qquad (2)$$

In equation (1) we assume one-dimensional displacement of the parts before and after the collision, therefore the vector values of momentum can be substituted with their scalar values.

From (1) and (2) we can obtain the velocity of the bump key after collision:

$$V_k = \frac{2 \cdot V_0}{\frac{M_k}{M_h} + 1} \qquad (3)$$

Equation (3) leads to the interesting conclusion that the velocity of the key after impact does not differ significantly from the velocity of the hammer before impact, even if the mass of the hammer is considerably greater than the key mass. In fact, in the upper limit case where the ratio $M_k/M_h \rightarrow 0$, the key has only twice the hammer velocity, and when $M_k \sim M_h$, we have $V_k \sim V_0$. Thus, for purely elastic impact, the mass of the hammer has little importance (over a reasonable mass range) for successfully opening the lock with bumping. Probably more critical is the handiness and convenience of manipulation.

The same approach can be apply to estimate the velocity of the key pin. We assume that a purely elastic collision occurs between the key and the pins. In this case, equation (1) becomes:

$$M_k \cdot V_k = q \cdot m_p \cdot V_p + M_k \cdot V_{1k}$$

The vector values of velocity have been substituted with their scalar values. But due to the changing of the pin movement direction, we insert the coefficient *q*, which depends on the angle between the direction of key movement and the plane of collision with the key pin. This coefficient is equal to 1 for a frontal (**π**/2) collision, whereas $q < 1$ for angles of collision less then **π**/*2*. For real keys, we assume that this angle ranges between **π**/*2* and **π**/*4* , and *q* is bounded by ½ < q < 1. Combining this equation with the energy conservation equation, we find the initial velocity of the key pins just after impact:

$$V_p = \frac{2qV_k}{\frac{q^2 \cdot n \cdot m_p}{M_k} + 1} \qquad (4)$$

where n is the number of pins in the cylinder, usually equal to 6 or 7. Others terms are shown in figure 3.

We assume that the mass of the pins is significantly less than the mass of the key. This is reasonable because typical dimensions for the driver pins are ø3 x 5 mm, corresponding to about 0.3 grams (for brass), whereas the mass of the key is around 15 - 25 grams. Thus, $q^2 \cdot n \cdot m_p << M_k$, and taking into consideration that $V_k \approx V_0$ for the majority of situations, the pin velocities can be estimated to be:

$$V_c \approx V_p \approx \gamma \cdot V_0 \qquad (5)$$

where $1 < \gamma < 2$. Here we have made the reasonable assumption that the velocity of the key pin is nearly equal to velocity of the driver pin, due to the elastic collision between them and their nearly identical mass values, along with their same direction of movement. Hence, we can conclude that the initial velocity of the driver pins during a bumping attack doesn't differ significantly from the velocity of the hammer.

Obviously, for bumping attacks the following rule is valid: the longer the time period when two pins (key pin and driver pin) are separated, the more likely the bumping will succeed. Therefore, it is useful to estimate this period of time, and identify the most important parameters responsible for the changing of this value.

Because the mass of the driver pin is the same order of magnitude as the key pin, the velocity of the driver pin after impact is approximately equal to V_p. The kinematic behavior of the driver pin after impact can be precisely described by the force balance equation, well known in the form of the differential equation for a harmonic oscillator [3, 4], without taking into consideration the gravitational force:

$$m_c \cdot \frac{d^2x}{dt^2} + c \cdot \frac{dx}{dt} + k \cdot x = -F_0 \qquad (6)$$

where x is the displacement of the pin from the initial position, dx/dt and d^2x/dt^2 are the velocity and acceleration of the driver pin, respectively, c is the friction coefficient, and k is the spring stiffness (or spring constant). The sum of the forces in the left part of the equation (6) are set equal to the force F_0 caused by the spring, when mounted into the cylinder with some initial compression deformation.

The damping ratio $\varsigma^2 = \frac{c^2}{4 \cdot k \cdot m_c}$ critically determines the behavior of this system.

There are three clearly distinguished kinematic behaviors of the system:

1. The undamped situation (no friction) where $c^2 << 4\ k\ m_c$

2. The damped situation. This occurs when the friction forces are sufficiently strong to change the kinematic behavior of the key pins and driver pins, but at the same time, the pins can still move without much resistance: $c^2 \leq 4\ k\ m_c$

3. The over damping situation when the friction force significantly obstructs the moving of the pins. This case has no practical relevance for bumping a pin tumbler cylinder because with over damping, the pins can barely move and the cylinder won't operate properly.

Undamped Situation

In this case, equation (6) reduces to

$$m_c \cdot \frac{d^2x}{dt^2} + k \cdot x = -F_0 \tag{7}$$

If we substitute the variable $y = x + \frac{F_0}{k} = x + \Delta L$, where

$$\Delta L = L_0 - L \tag{8}$$

is the difference between the free (L_0) and mounted (L) lengths of the spring (see figure 3), we can rewrite (7) as follows:

$$m_c \cdot \frac{d^2y}{dt^2} + k \cdot y = 0$$

which has the well known solution $y = A\sin(\omega_0 \cdot t + \phi)$, where A and φ are the amplitude and phase of oscillation, which depend upon initial conditions of the pin, and where $\omega_0 = \sqrt{\frac{k}{m_c}}$ is the natural angular frequency of oscillation.

Substituting for y, we obtain: $x = A\sin(\omega_0 \cdot t + \varphi) - \Delta L$

Based on the initial conditions at t = 0, we have x = 0 and dx/dt = V_c at the start of motion of the driver pin just after impact, and at t = t_{max}, we have $x = A - \Delta L$ and dx/dt = 0 at the point of maximum distance of the driver pin from the key pin. Given that the period of separation of two pins is twice the time to arrive up to the point of maximum deflection, we have finally:

$$\tau = 2t_{\max} = \frac{1}{\omega}\left[\pi - 2\cdot\arcsin\left(\frac{V_c^2}{\omega_0^{\ 2}\cdot\Delta L^2}+1\right)^{-1/2}\right] \qquad (9)$$

This expression gives the exact solution of the time interval at which two pins are separated. It should be noted that for all real designs of a pin tumbler cylinder, the following condition will be always satisfied:

$$\frac{V_c^2}{\omega_0^{\ 2}\cdot\Delta L^2} = \frac{m_c\cdot V_c^2}{k\cdot\Delta L^2} >> 1$$

This is due to the fact that the velocity of the driver pin after impact is around a meter per second, but the distance of the spring pre-compression in the mounted state (8) can't be greater than a few millimeters. So, for a reasonable range of pin mass and spring stiffness, the above parameter is much larger than 1. As a result, the expression (9) can be rewritten in the simpler form:

$$\tau = \pi\cdot\sqrt{\frac{m_c}{k}} - 2\cdot\frac{\Delta L}{V_c} \qquad (10)$$

Equation (10) leads to some qualitative conclusions regarding resistance to bumping of pin tumbler cylinder locks in the undamped state. As can be seen, by increasing the stiffness of the spring (k) and the distance of pre-compression of the spring in the mounted state, along with decreasing the mass of the driver pins, it is possible to improve the bumping resistance due to the fact that the time, τ, diminishes. In order to do some quantitative estimations, we will considered realistic locks, but to cover a whole range of different designs, we take into consideration 2 extremes cases: one with a very high spring stiffness and extremely low pin mass, along with the maximum possible pre-compression deformation of the spring; and a second case with a very soft spring, maximum mass for the pins, and low pre-compression deformation of the spring.

"Soft" Design

Figure 4 shows various parameters for the lock components, based on a realistic design for a pin tumbler cylinder. The driver pin dimensions are ø3x5 mm. We will assume the spring is made of phosphor bronze, as is often used in real locks due to its high corrosion resistance and good performance, but this kind of spring coupled with pins made from brass can result in an increased susceptibility to bumping. Using the physical characteristics, shown in figure 4, we can calculate the value of spring stiffness and the natural frequency as $k = 29\,{}^{N}\!/_{M}$ and $\nu = \frac{\omega_0}{2\cdot\pi} = 49\,Hz$, respectively.

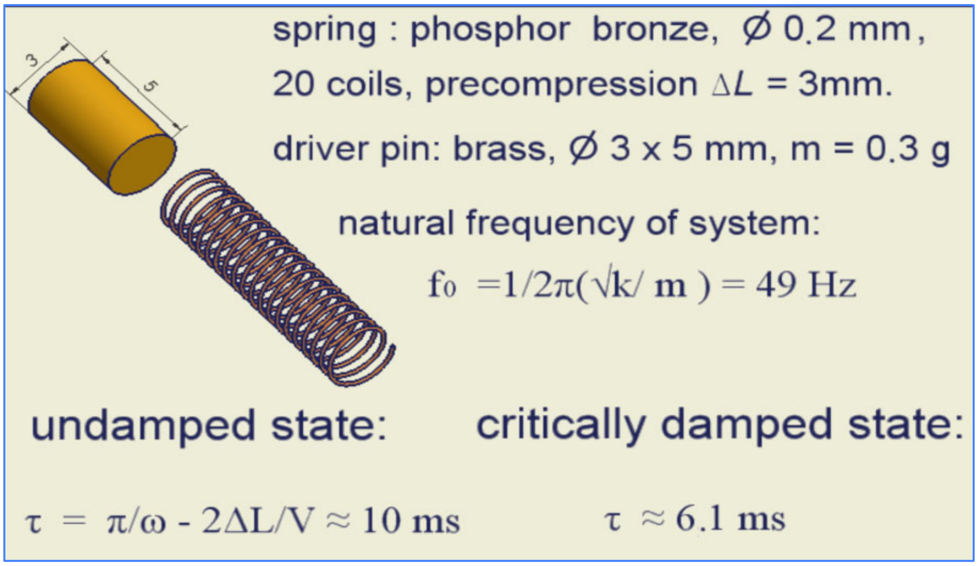

Figure 4 - Design parameters for a "soft" locking mechanism.

The average velocity of the bump hammer can be varied in the range of 6 to 10 meters per second. Taking into consideration that velocity of the pin is approximately the velocity of the hammer (5), we presume in our estimate that $V_c \approx 15 \, M/_{\sec}$. Thus from equation (10) we can obtain the time interval for when the key pin remains separated from the driver pin, before the spring rebounds it back. During this interval of time, the lock cylinder can be turned without the presence of the correct key. It can be seen that this interval is equal to 10 milliseconds for the undamped situation. Due to the fact that an actual lock with the design shown in figure 4 can easily be opened by bumping, we can suppose that a value around 10 milliseconds puts a lock at risk.

"Rigid" Design

This situation suggests some useful countermeasures without making major modifications to the lock. It is necessary to substitute only two elements without changing geometrical dimensions, as shown in figure 5. The brass driver pin used for figure 4 can be replaced with a stainless steel one which has a central hole, in order to significantly decrease the mass (from 0.3 to 0.1 g). The second element to be modified is the spring, now made from stainless steel using a wire with a greater cross section. This increases the spring stiffness to k = 140 N/m.

As a result of these 2 changes, the time period when the pins are separated is equal to only 1.9 milliseconds. Taking into consideration that a real lock designed as described in figure 5 is very difficult to bump, we presume that a value of 1 to 2 milliseconds is near some threshold value for easy opening via the bumping technique. This value seems to be a plausible because a reaction time under 1 millisecond is challenging for most people. It should be noted that in order to make more precise evaluations of the threshold value, it is necessary to obtain more experimental data.

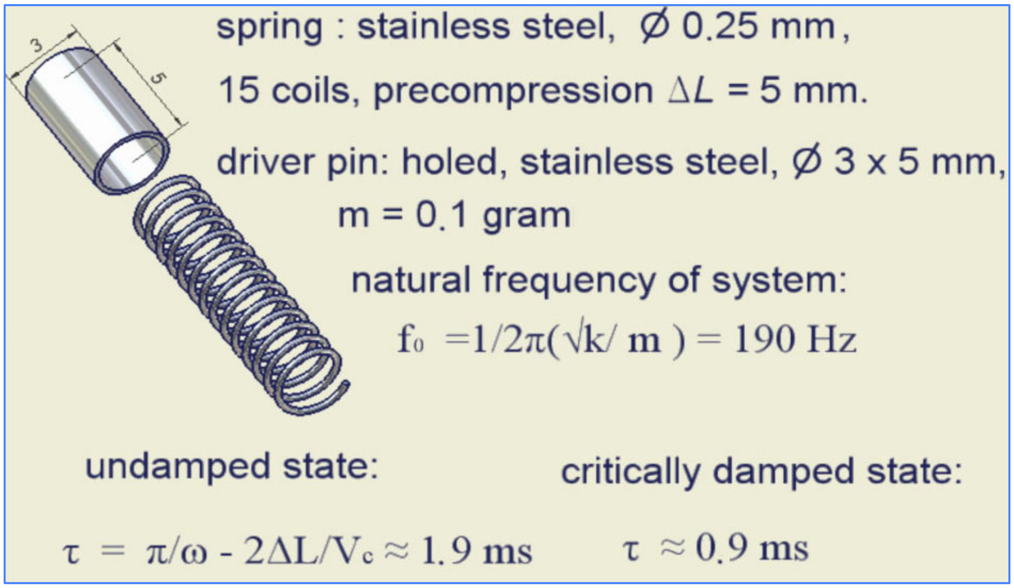

Figure 5 - Design parameters for a "rigid" locking mechanism.

Damped Situation.

In any event, a more realistic scenario is the damped situation. This is because a real lock accumulates dirt, dust, pollen, particles, oil, etc. so real locks will never be found in the pure, undamped situation. Equation (6) in this case has the general solution, obtained from equation [4] using $y = x + \Delta L$ which is:

$$x(t) = A \cdot e^{-\varsigma\omega_0 t} \sin(\omega_1 \cdot t + \varphi) - \Delta L \qquad (11)$$

where $\omega_1 = \omega_0 \cdot \sqrt{1-\varsigma^2}$ is the angular frequency of the damped system.

Using the same initial conditions as those used to find expression (9), and assuming $\frac{V_c^2}{\omega_0^{\ 2} \cdot \Delta L^2}$ >> 1, which is the case for real locks, the time period for which the key pin and drive pin remain separated is:

$$\tau \cong \frac{2}{\omega_1} arctg \frac{\sqrt{1-\varsigma^2}}{\varsigma} - 2 \cdot \frac{\Delta L}{V_c} \qquad (12)$$

As can be seen, equation (12) for the damped situation becomes equation (10) for the undamped situation when the damping ratio $\varsigma \to 0$. On the other hand, the time interval (τ) exponentially descends to the critically damped value at $\varsigma \to 1$ where

$$\tau \cong \frac{2}{\omega_0} - 2 \cdot \frac{\Delta L}{V_c}$$

Figure 6 shows the behavior of the time interval, τ, with increasing damping ratio. The dashed orange line near the solid line indicates the threshold value.

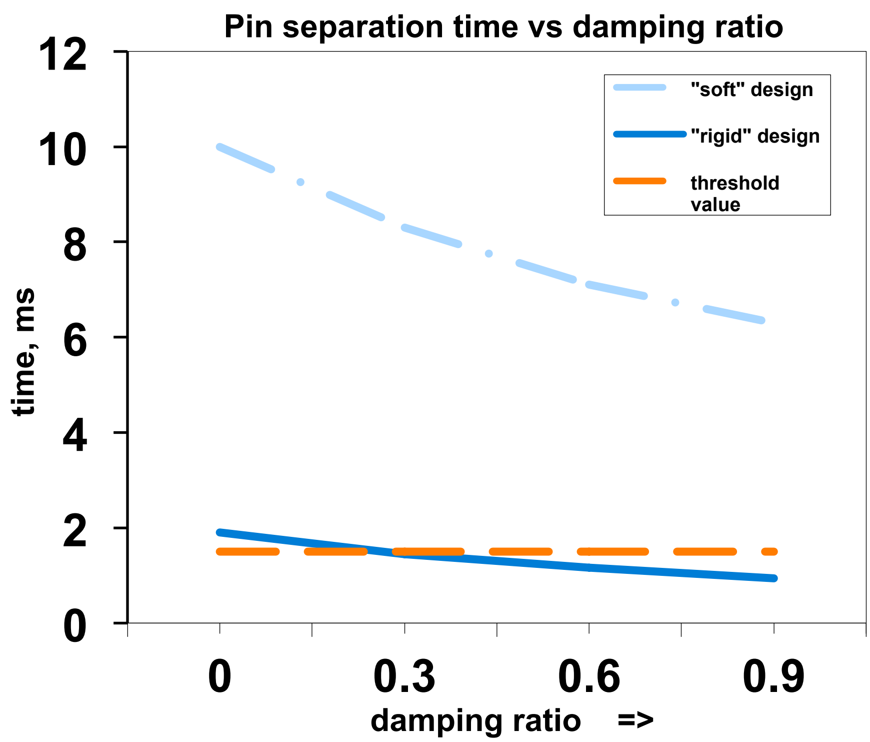

Figure 6 - A graph of the pin separation time, τ, as a function of damping ratio, ζ.

Discussion

Important practical conclusions can be made from the graph in figure 6. First, with the passing of time, the resistance to bumping of the cylinder can only improve due to the inevitable accumulation of different types of dirt and contamination, which increases the damping ratio. Second, if an attacker sprays into the cylinder some substance like dense oil, in order to try enhance the possibility of opening by bumping, he is making a mistake. This action increases the resistance to bumping, as shown in figure 6. Moreover, it can be noted that the most effective results for opening the cylinders by any vibration technique (including bumping) will be achieved when the lock is very clean.

The graph in the figure 7 shows the behavior of the pin separation time with increasing natural frequency of oscillation of the spring/driver pin system.

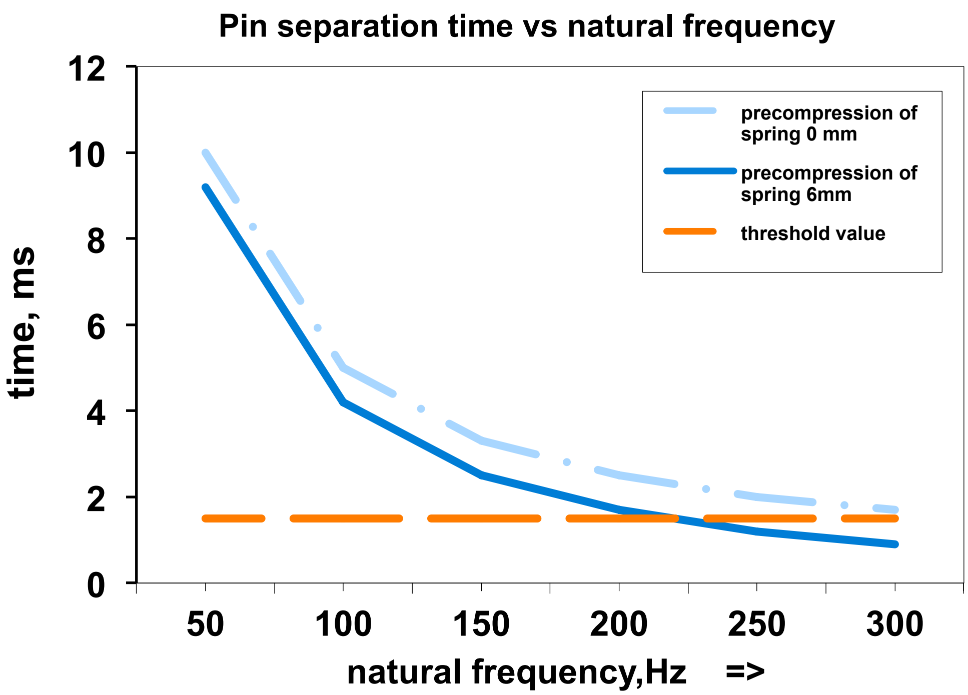

Figure 7 - Pin separation time interval, τ, vs. natural frequency, $f_0 = \omega_0/2\pi$.

It can be seen that the pin separation time decreases hyperbolically with an increasing stiffness-to-mass ratio. So called "soft" mechanisms, which have a natural frequency of oscillation less than approximately 200 Hz, are at risk of being easily opened with bumping.

Note that the value of the spring pre-compression, ΔL, has a relatively low influence on the pin separation time, which is also the case for the velocity of the pins (and hammer). Various locking mechanisms can be evaluated from this point of view. For example, the "radial system" employed by KABA and other manufacturers uses very small pins due to the limited space available in non-vertical directions. These locks, even with a medium range of spring stiffness, result in large natural frequencies. As a consequence, this type of lock is very difficult to bump.

In contrast, mechanisms used by some expensive locks constructed in classic Yale manner, such as the DOM 5-pin, Pfaffenhain, Corbin 5-pin, Zeiss IKON 5-pin and others, have relatively heavy pins. They use springs with low to medium stiffness, and can be easily opened, as has been shown by Barry Wels and Rop Gonggrijp [1]. Evidently the stiffness of the spring cannot be increased infinitely because at high values, the key won't enter the cylinder. The value of stiffness at about *200 N/m* can be considered as the maximum allowable for exploitation reasons. Therefore, to enhance bumping resistance, it is possible to act on both elements: the spring and the driver pin. The mass of the driver pin can be decreased in various ways: by decreasing its external dimensions, by drilling a hole (as shown in figure 5), or by using low density materials. Equation (10) can be used to estimate the bumping (or other vibration attack) risk for each kind of cylinder. All input parameters of this expression can be easily measured, and reasonable values for the driver pin velocity can be assumed. See the discussion around equation (5).

In the beginning of the discussion, the assumption was made that the masses of the key pins and driver pins are similar, and as a consequence, the velocity of the driver pin is equal to the velocity of the key pin. But sometimes these masses are significantly different, and this fact must be considered in the analysis. Suppose, as above, that a purely elastic collision occurs between the key pin and driver pin. Then, using conservation of momentum and energy before and after the collision (see equations (1) and (2)), we can obtain the precise relationship between the velocity of the driver pin (V_c) and key pin (V_p): $V_c=2V_p/(1+m_p/m_c)$. Finally, the driver pin velocity can be expressed by means of the velocity of the hammer V_0 (a value which can be easily measured). Thus, combining this equation with (10) and (5), we can obtain the expression for a more complete estimation of bumping risk:

$$\tau = \pi\sqrt{\frac{m_c}{k}} - \frac{\Delta L}{\gamma \cdot V_0}(1+\frac{m_p}{m_c})$$

Another important parameter of the cylinder lock is the natural frequency of oscillation. The maximum value at which the cylinder can be operated more or less normally (we presume at about *200 sec*$^{-1}$) can be estimated more precisely by collecting experimental data. Moreover, the value of the natural frequency can also be used as a quantitative parameter for judging a lock's resistance to bumping, and could be included in the standards such as EN 1303 for cylinder locks.

Acknowledgements

I would like to express my gratitude to the anonymous reviewers who helped with suggestions, editing, and improving the English. A very special thanks goes to the editor for assistance with editing, corrections, and clarifying the principal results of the paper.

References

1. Burry Wels & Rop Gonggrijp, *Bumping locks*, Toool – The Open Organization Of Lockpickers. *http: //www.toool.nl/bumping.pdf* - January 26,2005

2. Marc Weber Tobias, *A Technical Analysis of Bumping*, - Investigative Low Offices, *http://*www.security.org - April, 4, 2006.

3. Harmonic oscillator*, http//en.wikipedia.org/wiki/Harmonic_oscillator*.

4. Serway, Raymond A.; Jewet, John W. (2003), *Physics for Scientists and Engineers*. Brooks/Cole. ISBN 0-534-40842-7.