THE MEDECO® DEADBOLT DESIGN: Disaster Waiting to Happen?

An example of a Medeco deadbolt cylinder that can be bypassed in seconds with simple tools by attacking the screws that retain the end-cap on the plug.

This detailed report and video demonstration is only being released to locksmiths and security professionals. Please do not disseminate its contents outside of the security community.

Introduction

Incredibly, it appears that since the introduction of the current method of securing the tailpiece to the plug no one has discovered or exploited what we perceive as a potentially serious security vulnerability within the Medeco deadbolt hardware. We believe that this attack primarily affects the **m3** but also may place at risk certain Biaxial keyways[1]. At least since the m3 was introduced (and maybe for the last twenty years) it would appear that a disaster has been waiting to happen: the simple, unskilled, rapid, and very effective bypass of the security of this lock in about thirty seconds. It is, in our view, a classic case of insecurity engineering and a failure of imagination on the part of those responsible for product design, testing and review. It appears that UL did not consider this issue either when they certified the lock under UL

437. Evidently this issue was not contemplated when the keyway was widened in the m3 to implement the slider.

The method of interaction between the plug and tailpiece, in our view, raises possibly serious security concerns with legal and ethical implications for Medeco, locksmiths and any facility that deploys such hardware. Lest the reader believe that we are unfairly targeting Medeco, such is not the case; there are other major manufacturers that have similar design deficiencies that are potentially placing the people that rely upon their expertise in lock and hardware design at risk.

I have notified Medeco on several different occasions during the past two months suggesting that they should re-examine their deadbolt design because it could be easily bypassed. They have never requested further clarification or information nor even acknowledged the communications so I can only assume they have been aware of the problem for some time and are engineering a fix or they do not believe it is important enough to warrant such action.

Medeco, as has been pointed out in other articles, is one of the acknowledged leaders in the high security lock and hardware industry in America. They have a global presence and millions of organizations and people around the world rely upon their expertise. They are one of the companies that set the standard for quality, reliability, and excellence for high security products. So when we find this type of design issue perhaps everyone should step back and examine how this occurred and more importantly how to prevent such design failures in the future. If this article accomplishes that, then the criticism that is sure to follow from the release of this information will be worth it.

Let us be very clear: Medeco is not the only guilty party and many in the industry know it. I believe the real problem is two-fold. In the first instance it is a failure in the ability of design engineers to conceive of and test for real world threats to their products. Most design engineers know how to make things work but they do not know how to break them. It is impossible to properly design a security product without having extensive knowledge with regard to attack techniques. I would submit that most design engineers do not have such expertise. Medeco in fact does, which is why this is so perplexing and troublesome.

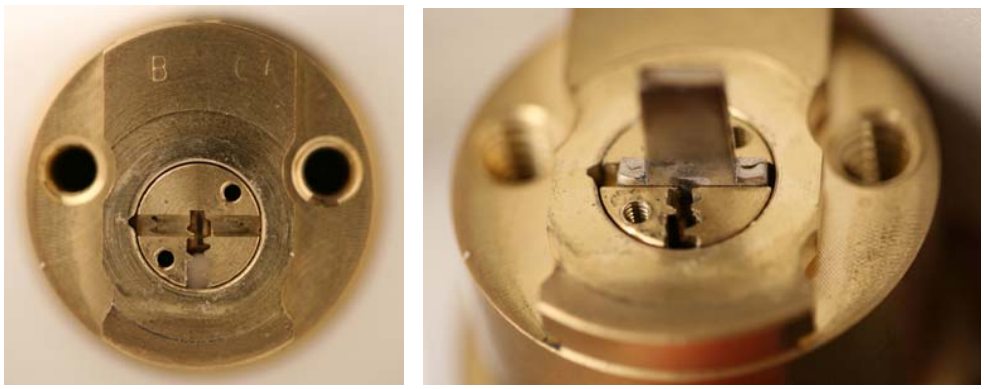
The other half of the equation is the standards to which these products are tested. We would submit that neither UL nor BHMA effectively test for some of the attacks that occur or are likely to occur in real world scenarios. If they had then the method we describe to bypass the Medeco deadbolt would have been detected years ago and made impossible through proper engineering.

Exploits of hardware and software designs are occurring regularly yet nobody seems capable of really addressing these problems. Locksmiths and security experts are quite aware of such bypass techniques. Hundreds are chronicled in ***LSS+*** and other texts. Yet manufacturers continue to make deficient or defective designs that place their users at potential risk. Even though others continue to produce bypass tools to open these locks, designs are often not changed or worse, the manufacturers are ignorant of such vulnerabilities. The real problem: where does that leave the public? They are rarely aware of security vulnerabilities in the hardware they believe is secure? This is especially true in UL 437 or BHMA rated locks.

The Medeco Deadbolt Design: A Failure of Imagination

We discovered this problem almost by accident. We were researching and documenting a similar vulnerability in another deadbolt lock of a major manufacturer and decided to look at the Medeco as an afterthought, believing that no such design issue could ever occur. Then we remembered a possibly related service problem that would crop up from time to time; a lockout or inability for the user to withdraw the key from the plug. The culprit was loose or stripped screws that retained the cap at the end of the plug in the Medeco cylinder. This in part led us to the bypass method we are describing.

Within the Medeco deadbolt design the plug is mechanically linked to the tailpiece because it is locked within a horizontal channel as shown in the photograph. A steel end-cap retains the tailpiece and plug as an assembly with the use of two countersunk screws. The tailpiece in turn controls the extension or retraction of the deadbolt.



The rear of the plug contains a channel within which the tailpiece is seated. This provides the linkage to transmit movement to the deadbolt mechanism.

Our bypass method requires the following steps:

- **Insert a specially designed breaker tool into the top of the keyway so that it abuts directly against the tailpiece;**
- **Apply sufficient force to shear the heads of the two retaining screws by striking it with a hammer;**
- **Insert a small tool that is shaped to mate with the end of the tailpiece;**
- **Push the tailpiece forward at least .120″ so that it is no longer within the channel at the rear of the plug;**
- **Turn the tailpiece to retract the bolt.**

This exploit can usually be accomplished in about thirty seconds with no apparent visible damage. Three strikes with a hammer are generally sufficient to shear the screws.

The same technique, of course, could be used by saboteurs to render the lock inoperable in order to block access to a secured area.

A special breaker tool was developed for five and six pin locks to apply extreme pressure on the tailpiece in order to shear the heads of the screws at the rear of the plug.

A simple screwdriver has been modified to manipulate the tailpiece.

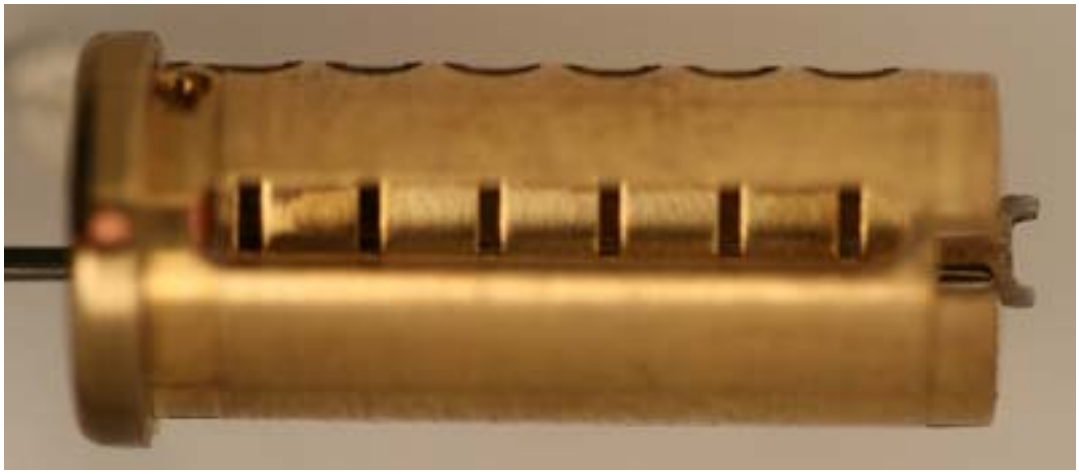
The manipulation tool is formed to precisely grab the edge of the tailpiece that abuts the end of the keyway.

We are able to accomplish this exploit because of what we perceive as three design deficiencies within Medeco cylinders. We should note that this technique does not work with dual deadbolt cylinders because there is not sufficient clearance to push the tailpiece outside of the channel in order to turn it. This also suggests the remedy for this problem. The exploit works best when the lock is mounted on a standard thickness door (1 3/4").

Perceived Design Deficiencies

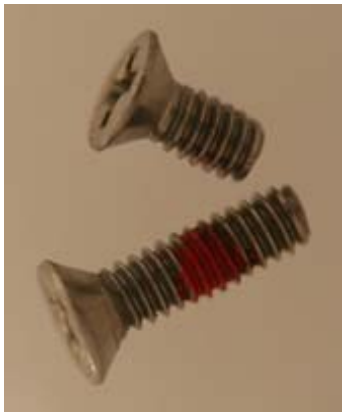
We believe that three primary design deficiencies allow the m3 and perhaps some Biaxial locks to be quickly and easily attacked with inexpensive and simple-to-construct tools.

When the retaining screws are sheared the tailpiece is pushed forward approximately .120″ in order to clear the horizontal channel within the plug. The tailpiece can then be rotated to control the deadbolt, as shown in the right photo.



These photographs show the manipulator protruding through the end of the m3 keyway. The tailpiece can be easily turned with this tool.

Medeco Deadbolt Security: Two Screws (loose or broken)



Virtually the entire security of the deadbolt locking system relies upon two tiny screws. Once the heads are sheared there is nothing to prevent the tailpiece and end-cap from being pushed forward.

Medeco elected to use two tiny screws to secure the end-cap to the plug. We believe this is a critical problem with the current design. Why? We measured the outside diameter of these screws at about .083”. That means that virtually the entire security of this lock and related system in fact relies upon these two tiny pieces of metal! The excellent security of the actual cylinder, sidebar technology, slider, ARX pins and other advanced features that has set Medeco apart are irrelevant in this attack. That is why it is so dangerous in our view.

This is a five-pin plug that has been compromised by shearing one of the retaining screws and driving the other from its bore.

Widened Keyway in the m3: The Real Problem

The manipulating tool is inserted to the end of the m3 keyway in order to access the tailpiece after the breaker tool has sheared the heads of the retaining screws.

We believe the second problem is the widened keyway in the m3. Although it appears that there is nominally only a difference in width of about .007" between the Biaxial and m3 it is sufficient to allow the insertion of our manipulation tool to successfully lock into and rotate the tailpiece. I am quite certain that this method of attack was never contemplated in the m3 design because it had apparently not been an issue with the Biaxial (which has employed essentially the same method of linking the plug to the tailpiece for many years).

No protection for the end-cap

The third issue that allows this attack to occur is the lack of protection of the end-cap that links the tailpiece to the plug. We propose a temporary fix for this problem by placing a metal block or washer to stop the tailpiece from being forced backward. The screws can only be sheared if

the end-cap is free to move, even slightly, so the obvious remedy is to block its movement.

The Real Problems

There are two fundamental issues that need to be addressed if we are going to improve the security of the products that are relied upon by the public: re-define the standards to include new testing criteria, and be certain that design engineers are educated and fully understand common methods of bypass.

Standards

In my view the real problem is product testing against real world threats, not just those that are enumerated in the testing protocol for UL and BHMA. Unless you subscribe to the philosophy (which I do not) that no lock is really secure and there is always a bypass method then why are UL and BHMA and other standards organizations not testing for such simple attack methods?

In a recent meeting with a representative of UL I proposed that UL437, which is ostensibly the high security standard together with BHMA/ANSI 156.30, be rewritten to more closely follow the European methods of testing. Why define the methods of attack, rather than establishing security levels based upon anticipated expertise of the attacker and needed time to protect a facility.

Locks would be classified based upon a perceived threat criteria that would take into account the type of facility, value of protected assets, layers of security, anticipated detection times, and expertise of those intent on breaking the system. The technique, at least for covert and semi-covert attacks should be largely irrelevant to the standard. If the lock can be opened or compromised within a defined time then it fails and does not receive the certification.

UL 437, for example, states that a certified lock must withstand a picking attack for at least ten minutes. Yet we can demonstrate the ability to reliably open some UL437 certified cylinders in a minute or two by picking, and sometimes less time with other methods of bypass for which UL or BHMA may not test. The consumer relies on these standards yet we would argue that some locks do not meet

them and should not be so certified. The Medeco m3 cylinder and deadbolt are certified to be secure against forced entry for five minutes. In certain cases it is not, as demonstrated in the video.

Competence of Design Engineers

Perhaps lock manufacturers should have two separate engineering groups that evaluate security products: the design team and a vulnerability assessment team. Each should be tasked with foiling the other's success so that in the end, both teams win by producing secure products that cannot be bypassed with wires, paper clips, magnets, vibration, shock, bumping and other relatively simple attacks. Checks and balances are always good; why allow the fox to run the henhouse?

Fixing the Medeco Deadbolt Problem: Ethical and Legal Issues

If Medeco believes that the disclosed method of bypass is indeed a serious security problem then I would submit that they should immediately notify every Medeco dealer worldwide to be certain that they and their customers are aware of the potential threat from this method of attack. Medeco should move to fix this problem quickly. From the legal standpoint I believe that every locksmith would agree that once on notice they have both an ethical and legal obligation to insure that their customers are protected against this form of attack. Who bears the cost for the fix is a good question but is not relevant here. I would submit that it is imperative to address the problem before there is a significant breach of security.

Conclusion

Most design engineers forget what I believe is the cardinal rule in analyzing locks and security systems for bypass: "the key never unlocks the lock." That statement may seem illogical but remember that in most cases the key **actuates the mechanism** that is responsible for controlling the real locking hardware. Every locksmith knows that if you can access that component then the lock and all of its high security functionality is irrelevant. The Medeco m3 deadbolt attack is a classic example.

I would imagine that Medeco never contemplated this mode of attack nor that it could be accomplished when they initially designed the linkage between the tailpiece and plug for the Biaxial. After all, even if the screws became loose or stripped they would theoretically prevent the release of the end-cap and therefore would prevent the tailpiece from being manipulated by the method shown. The problem, of course, is reliance on two tiny screws for this function. Such issues should not escape those responsible for the overall design of security hardware, especially when it carries a UL or BHMA/ANSI rating.

It would be my hope that everyone in the industry assesses just how they test for vulnerability in their products. Perhaps the only way to insure that the label of "high security" actually means something is to challenge UL and BHMA to withdraw certifications of those who do not produce products that truly provide the protection they advertise.

If you have any questions or comments, please contact the author at mwtobias@security.org or at +1.605.334.1155. Additional information regarding this and other methods of bypass is contained within the new edition of ***LSS+,*** the multimedia edition of ***Locks, Safes and Security***.

[1] We have only been able to test an extremely limited sample of Biaxial keyways. It would appear that popular Patriot and G3 keyways are wide enough to permit our manipulation tool to be inserted to reach the tail piece. Additional tests must be conducted to verify this and to determine exactly which keyways are susceptible to the attack. The issue is primarily with the insertion of the manipulation tool and not the breaker tool. The m3 keyways appear to be wide enough to allow virtually all of them to be bypassed.