PART II: LOCKS AND THE CONCEPT OF RESPONSIBLE DISCLSOURE v. IRRESPONSIBLE NON-DISCLOSURE

mwtobias@security.org

*This is **Part II** of an editorial that was prompted by the open letter in the May, 2008 issue of NDE magazine by Peter Field.*

Introduction

According to Peter Field, Medeco has now embraced and enlisted the support of the Locksport community. He cites their adherence to the concept of **Responsible Disclosure** as the principle reason for this apparent shift in attitude by the leading high security lock manufacturer in the United States.

In Part I, I examined the possible rationale behind this decision, and suggested that it was not done for purely altruistic motives. Jon King developed a wire pick and decoder to manipulate Medeco pins and open some of their locks. The public disclosure of this tool would constitute yet another attack on the "virtually resistant" security of Medeco locks. I believe the company decided to use this event as an opportunity to possibly re-introduce the implementation of special security pins (ARX) to prevent picking, decoding, and other forms of attack. They have been aware of these techniques for at least fifteen years, but have become timely and more relevant because of the Medecoder, as well as the release of our new book.

ARX PINS: Background

ARX pins, as I noted in Part I, were developed and introduced more than fifteen years ago, in response to a very sophisticated decoder that John Falle made available to government agencies. It used a fine wire to probe the channel at the base of each bottom pin. We believe that Medeco will be implementing certain changes in their locks to combat the Medecoder. It would be most logical that they begin using a form of ARX in their standard production line to accomplish this, because of the way in which the pick tool works, and their limited options to deal with this vulnerability.

If, in fact, Medeco supplies ARX pins, or a modified version, as standard in their cylinders, there are three important questions that need to be asked. First, why have they waited for fifteen years to do this? Second, will the pins make the locks secure against the Jon King attack, and more importantly, against the techniques we describe in our new book? Third, and perhaps most relevant, are they going to retrofit older locks to this “new” level of security, and if so, who is going to pay for it?

It is all about Cost

As to the first and second questions, I would submit that it is all about cost. Until now, Medeco did not believe they had to supply these pins, other than to customers with special needs, who were willing to pay extra for them. These pins are expensive to manufacture. In fact, Medeco management wanted to drop the ARX pin from production, but was wisely convinced by senior technical staff not to do so. The high security lock market is very competitive, so added manufacturing cost will likely be passed on to the consumer. Customers have many choices, and they may decide that other equivalent locks will meet their needs as well as Medeco. So, if the company chooses to implement these pins as their response to the Medecoder, why did they do so at this time?

The answer, I believe, is quite simple. The company is under attack from many quarters. Jon King is only the latest. More and more information is appearing on the Internet and other sources with regard to bypass techniques. So, Medeco needed to do something when Jon contacted them. I believe they used this opportunity to try to address not only the King attack, but the multiple bypass techniques that we developed and which may pose a far greater threat to Medeco. This may be especially true with regard to certain U.S. and foreign government contracts, and their specific requirements with regard to resistance against forced as well as covert and surreptitious entry.

If they do implement the ARX pin, or a pin that blocks access to the true gate channel at the tip of the pin, they will succeed in stopping the attack by the Medecoder. However, everyone should understand that the ARX pin may not be effective in stopping other attacks; including bumping and picking when using code setting keys.

The problem, as we discuss in the book, is that the ARX pin can provide positive feedback that will allow the lock to be opened, once the sidebar code has been set. This is the reason that we filed for a patent for the development of a pin to deter the very same bypass methods that we developed. We now can repeatedly demonstrate the vulnerability of these pins to bumping and picking attacks. Some locks with multiple ARX pins and varying depth increments can be reliably opened in as little time as thirty seconds. Sound impossible? We have already demonstrated certain bypass techniques for ARX pins to representatives of some U.S. and foreign government agencies.

Maybe the current Medeco description for their security, of "virtually resistant," actually defines the opposite of what this meaningless phrase connotes: virtually **not** resistant to attack!

Responsible Disclosure v. Irresponsible Non-Disclosure

The third question (fixing installed products) is perhaps the most important, and relates to the concept of responsible disclosure and the counterpart to that, which we identify as **Irresponsible Non-Disclosure.**

I would submit that the concept of Responsible Disclosure, with regard to a manufacturer, is not quite the same in the world of mechanical locks as it is in the cyber world, when a serious software flaw is discovered. A security vulnerability in software can be instantly "patched" without any direct material cost or requirement to take apart the affected computer. This is not the case with mechanical hardware.

For locks, it depends upon a number of factors as to whether it even applies, and how. I believe there are two scenarios that must be considered. The first is the discovery of a flaw **prior to** or a very short time after the introduction of a new lock or design. The other is a vulnerability that has existed for some time, and is present in a significant embedded base of locks that have already been sold and installed.

In my view, the real discussion should focus on full disclosure to the public. The relevant question is when they should be warned that a vulnerability exists, and the extent of that vulnerability. Peter clearly linked the concept of responsible disclosure with the fact that Jon King came to Medeco with his specialized bypass tool prior to making it available to the public. It apparently is this rationale that prompted Medeco to recognize the Locksport community and work with them, rather than simply acknowledging the contributions they have been making for quite some time in finding flaws in locks.

The clear inference is that the King attack was a new threat and that he and the Locksport community acted responsibly by (1) disclosing the issue to Medeco, and (2) waiting to publish full details or offering the tool for sale until Medeco could take remedial action to protect everyone with Medeco locks. So I repeat my initial question: where has Medeco been for at least the past fifteen years with regard to this vulnerability, unless they claim it never existed before?

I agree that once a vulnerability is found in a **new lock** design, prior to, or just after its introduction, the manufacturer should be notified and given time to effect a remedy before its publication or the sale of bypass tools to exploit the flaw. This can be easily accomplished with the execution of a mutual non-disclosure agreement between those that found the problem, and the manufacturer. Then, everyone is protected.

A defect in a new lock does not affect the consumer because there is no significant implementation of the lock with the vulnerability. This is vastly different than discovering a problem with locks that are currently installed, especially if the manufacturer enjoys a significant market penetration for its products, as does Medeco.

The second scenario is a bit more complicated and subtle, and involves the disclosure of a flaw or vulnerability in locks that are presently installed. The relevant issue has little to do with notification of the manufacturer of such a problem, other than for allowing them to fix it, going forward. In this event, I think that the public has a right to know precisely what the problem is, so they can make their own assessment of its seriousness. If the vulnerability currently exists in their installed base, it matters little whether the manufacturer is notified or not, unless the manufacturer is willing to fix the problem at the dealer and consumer level. The end-user can decide to accept the risk, or take some action, such as attempting to remedy the threat, or replacing the locks. And herein lays the crux of the problem: who is responsible for the costs in such event?

I do not believe that the notion of Responsible Disclosure applies in this instance, but that such a concept is really a legal dodge by the manufacturer to shield themselves from liability, rather than protecting the consumer. In the end analysis, it is all about money and liability. Manufacturers will claim that “new methods of bypass” are always discovered. In such event, a fix is implemented, but the lock maker claims no responsibility to retroactively remedy the problem. Their typical answer: either don’t admit the problem, or tell the consumer to buy new locks. Rarely will they bear the cost associated with a recall or other remedy because such costs could be prohibitive.

In this event, both the dealer and consumer may be left without a remedy, and even worse, may be vulnerable to a breach in security. Is the dealer supposed to continue to sell deficient or defective locks to their customers until they deplete current stock? Will the manufacturer tell the dealer of security flaws? These questions can also present serious liability issues for dealers, which most manufacturers would rather not address.

Some may argue with a philosophy of full disclosure, but once locks are pinned and installed, they are quite different than software. They can be fixed prospectively, but not retroactively without expense. So not publishing a vulnerability will not help the consumer, unless the manufacturer recalls every lock with the deficiency or defect, and fixes it. And even if a manufacturer were to agree to remedy a defect in every lock they have sold, it would be impossible to do so without notifying the affected consumers. In that event, everyone would know about the problem anyway. So we have returned to where we began: full disclosure so everyone is altered to the security issue.

There are very few manufacturers that will admit publicly there is a problem. It has far more to do with their potential exposure than it does with their fear of “educating criminals.” So, manufacturers use language like “incremental improvements” or “enhancements” to cover what they may perceive as design defects that could result in liability. There is no doubt that every lock manufacturer whishes to produce locks that cannot be bypassed. And when they discover problems, they will usually make those “incremental improvements” to deal with these issues to protect themselves and their customers. But again, this has nothing to do with locks they have already sold.

Medeco alludes to the fact that they will be sending out letters to all of their dealers and customers, once their “enhancement” is implemented with regard to the Medecoder. Will they claim that a “new” vulnerability has been “discovered” which, they may suggest, requires the implementation of ARX pins or other changes? If that is the case, then we would expect Medeco to pay all costs associated with the repining of all locks so affected, because it definitely is not a new threat. Otherwise, it becomes a marketing ploy to sell more products, based upon a new version of an old bypass technique.

I would submit that there is another side of Responsible Disclosure, and that is the immediate duty of a lock manufacturer to advise their dealers and customers of vulnerabilities that can directly affect their liability, safety, and security. If Medeco is “in business to protect people and property, and not to compromise their security,” then one would expect them to immediately notify their customers when they are aware of a serious risk that could affect many customers, especially those that that have purchased their locks to protect high value targets and critical infrastructure. The failure to do so, in my view, constitutes Irresponsible Non-Disclosure, and can have significant legal and ethical consequences.

The Medeco Deadbolt: A Classic Example

Last summer, we disclosed a serious vulnerability in Medeco deadbolts. We did not tell the public the precise method to open these locks, but did issue a detailed report to the security community. We notified Medeco almost three months prior to the release of our report that there was a serious problem with their lock design. They never asked what that problem was.

When we disclosed the problem (but not the details) at Defcon last August, Medeco then implemented certain fixes to make their locks more secure. According to several dealers, they never told anyone what the nature of the problem was, or why certain “incremental improvements” were made. Their customer service representatives downplayed the issue and stated there was no real security threat. They said that Medeco had made certain “enhancements” to fix a problem that did not exist, because they were the leaders in the market, and then had the temerity to state that now they were the only one in the industry that did not have this “problem.”

We detail this issue in our book, because the flip side of responsible disclosure is the responsibility of lock manufacturers to tell the truth to all who rely upon both their expertise in lock design and in their integrity to do so. The fundamental question is whether the end-user has a right to know the precise nature of a vulnerability. Consider the alternatives: perhaps they should be told that there is a problem, but not what it is. Or, maybe they should be told nothing at all, adhering to the old concept of Security by Obscurity. Neither of these alternatives, in my view, is acceptable, either from an ethical or legal standpoint.

Unfortunately, in our world of instant communications and the Internet, simply advising that there may be a problem will likely prompt a discovery and full disclosure of that problem in a very short period of time. So, why not properly advise everyone at the outset, unless the issues can impact upon national security? I find it rather disingenuous of Medeco to use the Medecoder as their rationale for embracing the Locksport community. While I applaud their decision, they should be forthright in their disclosure of multiple vulnerabilities in their locks, not only from the Medecoder, but to other forms of attack. Telling a customer the truth is always the best policy. Half-truths, innuendo, and misrepresentations will ultimately backfire and will lead to mistrust, placing consumers in jeopardy, and liability upon the part of the manufacturer.

While the company may effectively prevent the Jon King tool from being used in picking attacks, by the introduction of ARX pins or similar measures, there are other techniques, both old and new, that can completely compromise the security of these locks. Medeco is fully aware of these issues, and has chosen to artfully dodge them by denials and half-truths, by misleading advertising, by being less than candid in admitting to potential security vulnerabilities, and engaging in a disinformation campaign aimed at those that have dared to publish information about bumping and picking their high security cylinders.

We will squarely address these issues at Defcon, beginning with their attempt to retroactively alter their prior statements and press releases. These issues are fully documented in our book.

We will also specifically address and present information with regard to what we perceive as other very serious vulnerabilities that exist in Medeco locks, which have been discovered as a result of our research. Medeco has been supplied with this information months ago. They should publicly address the ability to bypass their forty-year old technology by bumping, picking, forced entry attacks, and the compromise of their key control. Their customers deserve to know and understand how these locks can be compromised, especially when they are used to protect high value targets and critical infrastructure. To do less, in my view, constitutes Irresponsible Non-Disclosure upon their part.

As we have done for the past three years, we again invite representatives of Medeco to take part in our presentation at Defcon 16, and to set the record straight, from their perspective, as to the security or insecurity of their locks. It would be a perfect forum for them to address specific issues that relate to key control, forced entry, and surreptitious entry of their various products, and to explain exactly what the term “virtually resistant” really means, and how they intend on making their locks more secure against the Medecoder and more sophisticated forms of bypass that use code setting keys.