Part I: Acceptance of the Locksport Community by Medeco and the concept of Responsible Disclosure

© 2008 Marc Weber Tobias

I read with interest the May, 2008, edition of Non-Destructive Entry Magazine (#3). What immediately caught my attention was the emphasis on Medeco locks, and an open letter from the company, written by Peter Field. The article addresses two primary issues: the recognition of Locksport contribution to security, and the fact that Medeco is taking steps to correct what they evidently perceive as a "new" vulnerability in their locks, occasioned by the development of a picking tool by Jon King.

I have known Peter for a long time, and from my perspective, he is one of the brightest engineers on the planet, with regard to lock design and innovation. He has been the chief architect of Medeco products almost forever, and the company has flourished because of his talents, insight, and creativity.

For many years, I have consulted with lock manufacturers in the United States and Europe with regard to the analysis of bypass techniques for their locks, and how to prevent or deter such attacks. This is often a complex problem, involving technical, legal and ethical issues. As a lawyer, I have advised clients as to how to protect them from liability for deficient and defective lock designs, and related corporate policies. Specifically relevant to the NDE article and the concept of responsible disclosure, I have counseled that my clients adopt a policy of full disclosure about vulnerabilities unless the release of such information would impact national security. Many have subscribed to this philosophy.

Four years ago, I began speaking publicly about the need for the lock industry to embrace, listen to, and exploit the talents of Locksport members. ALOA referred to them as hackers, criminals, persons of questionable character, and other derogatory and mostly uninformed and inaccurate descriptions. The HOPE 2006 conference that Schuyler Towne refers to was one of the hacker forums wherein Matt Fiddler and I specifically addressed this issue. In 2004 at HOPE, we did the same thing, and solicited feedback from the participants of the conference with regard to cooperation between the hacker community, manufacturers, and law enforcement. The response in 2004 and 2006 was mainly positive, but went largely ignored by manufacturers.

This prompted ALOA to advise me that I had violated their Code of Ethics, which forbids associating with “persons of questionable character.” They were referring specifically to the attendees at HOPE, which included representatives of federal law enforcement agencies, the Department of Defense, and other security professionals.

They sent the message that if I spoke at any more conferences, I would no longer be a member of ALOA. I appealed their ruling, and they never responded. I am still a member, and have been so for more than fifteen years. And I have continued to support Locksport groups in the media and lectures, and have repeatedly advocated full disclosure upon the part of lock manufacturers as the best means to insure the security of the public and improve the quality of products. As Schuyler aptly points out, Security by Obscurity does not work, and is an inherently flawed premise. There are no more secrets: the Internet and the instant proliferation of information are responsible for that fact. Some in the locksmith community still will not accept this fact, nor will they accept the premise that the consumer has a right to know and understand security vulnerabilities in the locks that they purchase and rely on to protect them.

When Barry Wels and I gave our presentation at HOPE in 2006, and then Matt Fiddler and I spoke at Defcon the following month, we all introduced bumping to the American consumer. That, as everyone knows, caused an instant furor. The public was concerned, the locksmiths were dismayed, and ALOA was furious. That organization made their views known in an editorial in August, 2006, to which I responded. Those editorials can be found on my blog at **http://in.security.org**.

As an aside, now that Medeco has recognized the Locksport community, I am wondering if the fundamental thinking by ALOA will change. Will the trade organization and its members now agree with one of their major supporters (Medeco) and acknowledge the Locksport community and the valuable contributions they can offer?

Schuyler Towne and Peter Field are quite correct in what they wrote in NDE: the issue is responsible disclosure. But I would submit that this concept is different in the world of physical security, than it is in the cyber world. That principle has always guided how and when I have written about security vulnerabilities in locks and related hardware. But there are variables and distinguishing issues that exist with regard to deficiencies or defects in locks, in comparison to bugs or

vulnerabilities in software code. As a lawyer and technician, I may have a different and broader perspective with regard to such issues, and the legal and moral right of the public to understand vulnerabilities that can directly impact their lives and property.

Based upon Peter’s open letter, it would appear that Medeco has now embraced working with the Locksport community. As we noted in our book, it is actually not the first time they have done so. I laud them for publicly adopting this policy, but in my view, such a decision does not stem entirely from altruistic motives.

Medeco is well aware that their locks are vulnerable to attack by many different techniques, including bumping, picking, decoding, and the compromise of their key control. Just look at how Medeco has modified their disclaimers in the past eighteen months with regard to bumping and picking. They have gone from “bump proof” to “virtually bump proof” to “virtually resistant.” We documented how they subtly changed their advertising and retroactively altered their press releases because they knew their locks were vulnerable. The real question is whether this knowledge translated into what I would refer to as the other side of Responsible Disclosure? Did they notify their dealers or customers, especially those in the federal or state government, of such vulnerabilities? The answer, from our investigation, is no.

For the past eighteen months, my associates and I have been involved in a detailed and comprehensive research project to develop entirely new methods of forced, covert, and surreptitious methods of entry for the Biaxial and m3 cylinders. The result of that research, and every detail along the way, has been provided to Medeco, (other than copies of our three separate patent filings). This “full disclosure” has taken the form of video, locks, keys, code tables, diagrams, charts, and demonstrations at the factory and in the field to management at Medeco. We even provided an advanced copy of our book at least four months ago for their engineers and counsel to review. We repeatedly encouraged them to seek an injunction to block publication, or to have the government classify the information, if they believed that it would be contrary to national security.

Of even more interest is the inference that Medeco was unaware of this “new” method of compromise that Jon King developed to pick their cylinders. I had a long discussion with Jon last month with regard to his decoder and technique. I credit him

with being very creative in solving the problem of how to control and manipulate the chisel-point pins within a Medeco cylinder. This allows them to be rotated in order to align the sidebar leg to the true gate channel. It is a clever solution to a forty year old problem. But it is not unique, and Medeco knows it.

There have been several variations of tools for decoding and manipulating Medeco pins that have been patented or available to government agencies. Jon just made it a lot simpler to accomplish. According to Medeco, its use can potentially affect perhaps twenty percent of their locks. So, Medeco used the NDE forum to announce that they would be improving the security against picking, for locks that they have been advertising as “virtually resistant” to such attack!

In 1976, the company sued Lock Technology Company to stop them from producing a pick tool and technique to reproduce Medeco keys. Medeco lost this lawsuit, although most in the industry believe they won it. In 1994, the company, in response to the development of another decoding tool that was produced by John Falle in England, introduced the **ARX** pin. ARX is an acronym for **A**ttack **R**esistance **X**-tended. The Lock Technology case and the development of the ARX pin are significant because they both relate to security vulnerabilities in Medeco locks that stem from the ability to probe and manipulate the bottom pins by using the true gate channel. This is the same method of attack that Jon is employing to feel-pick these locks.

This specially-designed ARX bottom pin was designed to prevent John and others from decoding the true gate channel by probing the tip of the bottom pin with a fine wire. The government and some commercial customers employ these pins to add another layer of protection against pick and decoding resistance. As we have documented, they are only partially effective in preventing certain methods of bypass that we discuss in our book.

So for Medeco to now claim that they are making incremental improvements to their locks to protect against this “new” threat is not quite the full story. We believe that Medeco will shortly announce the implementation of the ARX pin for all of its m3 cylinders in an attempt to prevent the use of the bypass methods developed by Jon, and those that are disclosed in our new book.

If Medeco claims that they were not aware of the method to pick their locks that Jon King developed, then I would suggest that you read the Lock Technology patents and other prior art and

draw your own conclusions. If they in fact implement ARX pins in all of their cylinders, then they are doing so fifteen years after the fact. The significant question is why and why now?

Peter talks about standards. As we note in our book, we believe that the standards, those enumerated in UL 437 and BHMA/ANSI 156.30, are precisely the problem. In our detailed analysis, we talk about why we feel that these standards do not go far enough in protecting high value targets or critical infrastructure.

Manufacturers, such as Medeco, tout these standards as an assurance that their locks are secure against defined threats, especially for high security applications. “Defined’ is the operative word, because the standards do not protect against many threats that can allow Medeco and other high security cylinders to be opened in seconds. They only protect against “defined” standards that do not contemplate many forms of attack.

For those of you that may be unaware of BHMA/ANSI 156.30, this is the civilian high security standard for locks. In discussions with BHMA, I have pointed out what we perceive as the deficiencies in their current standard. We have asked them to look at our methods of bypassing Medeco and other cylinders, with the view to addressing these methods of compromise in a new standard that is based upon “real world testing” rather than specifically defining each method of bypass.

Finally, Peter and Schuyler address the concept of Responsible Disclosure. While I certainly agree that we should not be educating criminals as to techniques to bypass locks, there is a problem in this logic, which Schuyler correctly identifies. The consumer has a right to know of deficiencies or defects that can affect their security. The problem is that locks are quite different than software. Code errors can be fixed with updates that can be instantly implemented without any cost of materials. Patches can be effected remotely to fix a security vulnerability. This is not the case with locks.

And often the criminals are far ahead of the consumer in their knowledge, so is it wise to keep that knowledge from the consumer, commercial security officer, or government agency? The real problem, and the irony of embracing the Locksport and hacking community, is that Medeco and other manufacturers often do not know how to bypass their own locks! That is very obvious, for if they did, they would have taken the necessary steps to properly design their cylinders against such techniques. This

fact can be no more graphically illustrated than by Medeco's insistence that their locks cannot be bumped or picked by the methods we developed and attempted to explain to Medeco since 2006. The fact that Medeco could not open their own locks does not mean that they cannot be opened by others, using those same techniques!

So it often falls upon the Locksport enthusiasts, hackers, or security professional, outside of the lock manufacturing community, to demonstrate vulnerabilities that should have been discovered by the manufacturer before offering their products for sale. In my experience, design engineers learn how to make things work quite well; they rarely are educated in how to break them. That is a fundamental problem. If locks were designed properly, hackers and others would not be able to circumvent security. It is about time that manufacturers recognized that the more minds that are evaluating their products, the better.

So, when Peter says that Medeco and other lock manufacturers are reluctant to publicize potential threats to their products, primarily because they do not want to teach criminals how to decipher their mechanical puzzles, I would submit that this statement is not quite correct, nor does it tell the whole story. While there is no question that every lock manufacturer is "genuinely concerned with the security of their customers," there is another side to this issue, and that is money and liability. And at the end of the day, there should be no illusion as to why lock makers are in business: it is to make money, first and foremost.

Advising a manufacturer of a design defect is the right course of action. Unfortunately, most manufacturers have been unwilling to listen to the Locksport community, instead calling them hackers and criminals. This is clearly changing. In Europe, Toool has been responsible for a shift in attitude, primarily upon the part of some major manufacturers. And the realization by Medeco that they can have a valuable ally by using individuals with diverse backgrounds, to test their locks, is an important step forward. The question is the effect of advising a manufacturer of a problem, and when to notify the public. This is the real issue.

While I completely embrace responsible disclosure, thus giving a manufacture time to fix a problem in a new design, I do not quite subscribe to the theory of giving a manufacturer time to address all problems, especially if they have existed for quite awhile, the locks have achieved significant market penetration,

and the issue likely will not be remedied by the manufacturer without cost to the consumer.

***

In ***Part II***, I shall address this issue, and why the concept of responsible disclosure is a technical, logistical, legal and financial minefield for lock manufacturers.