NDE Magazine

Vol. 1 Issue 4

For Locksport!

ABUS PLUS CHALLENGE!

Six month long project wraps up with a win!

by Jaakko Fagerlund Pg. 12

INGERSOLL PICKING

by John Naughton Pg. 6

THE LAST WORD!

On Jon King's Medecoder Full Disclosure! Pg. 19

WHAT THE HECK

Is ARX? Mike Brewerton explains it all. Pg. 23

"I recognized that feeling coming over me like a warm blanket. I felt the need to pick a lock..."—pg.26

IN THIS ISSUE:

Pg. 6

NDE Magazine Is:

Staff: Executive Editor—Schuyler Towne

Managing Editor—Mike Brewerton

Online Editor—John Naughton

Contributing Editor—Michael Huebler

Photography: Ingersoll—Adam Ferguson

Forums: Bradley Klco, aka ILEx371

Graphics: ARX—SafetyOff

Ingersoll—Jon King

Barry Wels & Walter Kiczko, both contributors to this issue, at The Last HOPE conference in NYC.

"When you're the king of the hill, you become a target. Period."—pg. 23

Responsible Disclosure

BY BARRY WELS

What to pay attention to:

Most mechanical locks are not secure. It just takes a clever person to look at them from a different angle than the designer did, and the lock falls apart. Just look at the current status of locks: as soon as a lock becomes popular, a bypass method will be found. It may take a few years, but in the end most mechanical locks are proven vulnerable one way or another. Of course there are a few locks that still have not fallen, but that number is surprisingly small.

And, since there are a lot of clever people in the locksport community that look at locks differently, many new ideas will come from us. It will take the lock industry a while to get used to seeing their locks picked on YouTube, and receiving mail from eighteen year old lockpickers telling them their locks have vulnerabilities. But they will get used to it—they have no choice.

Whenever I find a flaw, I first look at how unique it is. For instance, when I discovered some Kensington laptop locks could be bypassed with a piece of cardboard, I did not notify Kensington. After all, a few weeks before that, the same locking mechanism (a tubular lock) used in Kryptonite bicycle locks was bypassed with a bic pen. By that time people already realized tubular locks can sometimes be compromised with simple tools, and the kensington trick was just a new lock that could be opened with an old idea.

In other cases the attacks we came up with were more unique, and we did notify the manufacturer. Now, when approaching a manufacturer, I always try to play by the following rules:

The Rules

1—Be professional: Always address the lock manufacturer professionally, using decent language. Keep logs of all e-mail correspondence.

2—Be honest: Only make claims on the research you conducted. Do not make assumptions about the lock's failure and be proven wrong later.

3—Be thorough: Tell them how many locks you have tested and how the lock was mounted, etc. Shoot some video and photos of your experiments.

4—Be clear: What is it that you want from them? Are you giving them time to fix the problem? Giving them time to prepare a press statement? Think before you mail or call!

5—Do not ask for money: This is important! Believe it or not the line between warning a company about a vulnerability and extorting them is very thin. In court, the most friendly "I think you have a problem" mail can be portrayed as an extortion attempt, even if you didn't have any wrong intentions. So, it is really important that you let them know from the beginning what your intentions are, and that this is not about the money. Also, be aware of not trying to force them into anything that could benefit you financially.

6—Be prepared: Sometimes lock manufacturers challenge our claims. In that case they usually want to send us some locks (or improved versions) they think/know we cannot open. I always have the following proposal ready: I want them to send me ten locks. These locks must have ten different pin combinations, but must otherwise be identical. This means the same profile, same pin types, etc etc.

And most important: each lock must be sealed individually. From these ten locks I will randomly select eight and disassemble at least a few of them to see what is inside. It is important to find out why the manufacturer thinks these locks cannot be bypassed when you know it must be possible. Once you have found the added extra (mostly a special pin in a unique spot, or them going beyond factory specifications), see if you can improve your attack to make it work on these new locks. The two remaining sealed locks you keep for demonstrating your attack when someone of the company comes to visit you, or when you visit them. This normally rules out any surprises, and what ever you do, do not accept a single 'black box' lock you are not allowed to take apart. If you do not succeed in opening this lock, they can (and most likely will) publicly claim you can not open their locks.

7—Do not sign NDAs: Another important one. Non-Disclosure Agreements will take away your independence and tie you to the manufacturer. Keep in mind that some of these companies will do anything to protect their reputation, including suing you out of your last penny.

Once you do go public with your attack, pay attention to add a disclaimer and make sure not to claim you can open any lock from that manufacturer or from that specific range of locks. In the bumping document I used the following disclaimer (and found out that only because of it, I was not sued by a big player in the high-security lock market):

> Important disclaimer: Please note that the above list does not mean to imply that every cylinder of a named brand and type will open readily using bumping. Locks are expensive and we are not a commercial testing lab, so we have had only a very limited number of testing locks available to us. The presence of a lock in the above list just means bumping worked at least once on a cylinder that we had access to. To us this means that type of lock is at least suspect, and further research is needed.

One more thing about number 5: the money. It may seem a pity that you cannot ask manufacturers for money for your clever exploit, but if you are any good, and if they recognize your talent, they might offer you the occasional job testing locks. After all, with a whole new generation of lockpickers on their way, manufacturers better make sure to hire someone with an open view to look at their locks before going to production. At times, manufacturers have approached me (and Han Fey) to test locks. In those cases we have no problem asking the same fee a decent lawyer would. Just keep in mind that the yellow pages are filled with good lawyers, but there are only a handful of good and reliable lock testers out there.

By now we know most manufacturers personally, or have easy access to them if needed. So, in case you find an exploit for a lock, and don't know how to address the manufacturer, or are in doubt how to continue, feel free to contact me for assistance: barry@toool.nl

Keep the conversation going online!

Share your thoughts on this, and all of the articles in this issue, at our new forums. If you want to discuss Barry Wels' primer in responsible disclosure with other readers, check us out @ lockpickology.com

Letter from the Editor

Dearest readers,

Everyone is working hard and hopefully not burning out here at the magazine. A couple of things quickly before we dive into the issue. Let's have a list!

- The Last HOPE: Was great! The Lockpicking Village was a hit, as Walter said: "We have locks, picks, and beer. What more could you want?" I had the pleasure of sitting next to Han Fey for three days straight, him selling Abloy Protecs, me hawking lockpicking doormats. Han is a funny guy. Incredibly knowledgeable, but when one potential customer asked him what made his locks special, Han simply asked for the man's glasses, locked them under the shackle of a Protec and said "Now you have a problem." He's a good salesman, moved a lot of locks! There were more physical security talks than ever and my only regret was the cancellation of the picking competition.
- 2 issues in 2 weeks: I can't even believe it, but the staff are gearing up to put out a new issue by DEFCON. NDE had its start at DEFCON 15 and I'm excited to launch Volume 2 at DEFCON 16. What can you expect? New gen of the Kwikset SmartKey, details of the RoboKey System from Stanton Concepts and a breakdown of the Drumm Geminy Shield, plus plenty more.
- DEFCON 16: I cannot wait to get to Vegas! This year I will be speaking on the morning of the first day. My talk is titled "How to Make Friends & Influence Lock Manufacturers" and reflects on some of the stories that have come across my desk during the last year with NDE. Most of the time you'll find me competing, running my field stripping competition or sitting at a Vendor booth selling merchandise. I may have overbooked my time this year...
- Great Moments in Locksport: We're launching a new feature here at NDE which should serve a dual purpose. We have composed digests of both the Medecoder and ABUS articles. First, they tie issues three and four together, and second, I hope they increase our accessibility. While we won't interrupt a good article to explain common terms, or explain how tension works, I believe some of our headier content can be appreciated by simplifying the technical parts and focusing on the stories involved. You will find the new digests immediately following their respective articles. Feel free to flip to them first! They should stand alone just fine. You can find the Medeco story on page 22 and the ABUS story on page 14. Print them for your friends!
- New forums: Thanks to our friends at Lockpickology.com (the same guys behind the incredible DIYTDS) we have forums for you to discuss articles, ask us questions, and offer your feedback on the magazine! The direct link is http://lockpickology.com/forum/viewforum.php?f=90 Keep your eye open for topic-specific links at the tail end of each article.

That's it for now. Enjoy the issue!

Schuyler Towne
Executive Editor

How NDE Works:

1. We pick a release date. If any of the big three conferences are coming up (HOPE, DEFCON & Dutch Open) we try to match our schedule to theirs.

2. We sift through any submitted story concepts we have received and discuss potential authors for articles we have pitched to each other.

3. Authors are assigned editors who will work with them from concept to completion.

4. Each editor typically has his work reviewed by a peer.

5. Photographs & other graphics are sourced for each article.

6. I propose an initial structure for the issue and begin to lay it out.

7. Test pages are sent back and forth between the editors until everyone is satisfied.

8. John publishes everything to the live website.

Ingersoll Picking Tutorial

BY JOHN NAUGHTON

Author's Note:

Please read this, & our previous article "Breaking Ingersoll" in their entirety before attempting to follow these instructions.

Ingersoll locks have always been of interest to the Locksport community. It's a fairly unique mechanism in what is quite a rare lock (especially outside of the UK) that intrigues collectors and spurs pickers to try and open them. The main reason it has continued growing interest is so few people can reliably pick them. This drove me up the wall too. I had one and just couldn't get the thing open.

Ingredients

1—Ingersoll brand, lever padlock (With working key)

1—Small flat head jeweler's screwdriver

1—Tension wrench (2 is better)

1—Hook pick or similar (Peterson standard hook is recommended)

Optional

1—Spare Ingersoll SC1 or SC71 lock to cannibalize for spare levers

1—Small Hammer to remove and replace retaining pins

Recommendations:

Before you start this tutorial it is probably best to point out that you should use a lock and tools that you do not mind damaging. Picking Ingersoll locks (like any lever lock) may require heavy tension. This will cause EXCESSIVE WEAR on the sidebar of the lock.

I recommend using the six lever 600 Series padlock for reasons stated in the breakdown article previously published in issue three of this magazine. I would also recommend using a pair spare of SouthOrd long twist flex tension wrenches. This is what gave me the best results and you will bend at least one out of shape following this guide.

I also recommend the Peterson short hook. I used the standard steel pick but government steel would be better. I have not seen any other commercial pick that had the required flat tip size and is also strong enough to spend a few hours in an Ingersoll.

I cleaned all of the parts of the lock to remove most of the grease. You will have the lock in pieces for a few hours with the constant assembly and disassembly. Many people I have talked to recommend leaving the grease in the lock and some have even recommended adding extra grease to slow the levers down. Older locks with lots of grease and dirt are supposedly easier to pick because of this, but in my experience it makes it harder to tell what's going on in the lock. It's your choice, but I had better luck practicing on a clean lock.

Finally, I recommend you remove the rubber seal from the cam mechanism that sits over one of the many retaining pins. This will provide better feedback until you are ready to return it for more realistic practice.

1—Getting Started—Open Feeling

The first thing to do is to remove the rubber seal from the lock to improve the feedback.

Assemble the core of the lock with two levers installed on the right-hand side of the lock. When done correctly you will see the gates of the levers in front of the side bar when it is pushed down and resting on them. I recommend using the front two levers at first.

Do NOT insert the core back into the body of the padlock. Instead press down on the sidebar with the index finger of your left hand. Unfortunately, because of the way Ingersoll constructs their padlocks this guide is not really suited to the left handed.

While pressing down on the sidebar insert the pick and feel around in the lock. This first part of the process is about finding the levers and not the internal parts of the core and keyway. Lightly press up on what you think is a lever, if you are pressing on a lever you will see it move in the lock.

Once you are confident you can locate each of the levers you should apply more pressure on the side bar and see if you can get each of the two levers to set in turn.

That should have been quite easy to do. Do this a few more times to get the feel for how much pressure is needed to lift the levers, and the difference between a set lever and a lever clicking in and out of place.

Once you are confident in the binding order of the levers, you should learn how to recognize the states of the levers by feel. First remove your finger from the sidebar and feel the levers, these are unbound levers. Now press on the sidebar and push the lever that normally binds first. The tension you feel is the friction of the sidebar on the lever. Push up until it clicks into place. STOP. Do not go to the next lever. Instead, lift that lever. You should feel a small amount of give and notice that it does not push back against the pick past that small amount. That is a set lever.

Now push up that last lever and move on to the next stage.

The Four States Of Levers

The levers can be in four different states, and you need to learn how to identify all of them to successfully open these locks.

Binding levers—A binding lever will give more resistance to lifting, followed by a solid click or jump. The lever will move quickly for about the width of its gate.

Set levers—A set lever will have a very small amount of give (under 1mm). It will not push back on the pick and will go no further than it already has without excessive force.

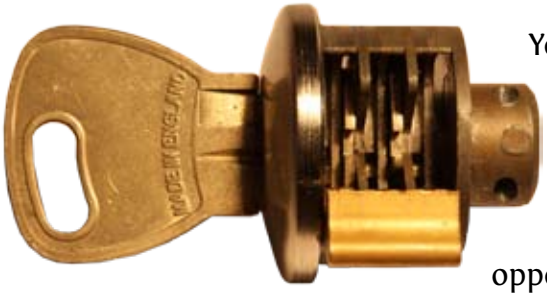
Unbound levers—Unbound levers are not yet binding against the sidebar. They will push back freely on the pick when raised.

Overset levers—An overset lever has been lifted too far, the gate is now behind the sidebar as it has traveled past. It will behave much like a binding lever but will appear to lift too far. It is something you will have to learn to recognize and deal with. They will carry on binding past the deepest possible cut, however you are not likely to determine this for most key bittings as you will hit other levers before you can push it past the deepest setting on a key.

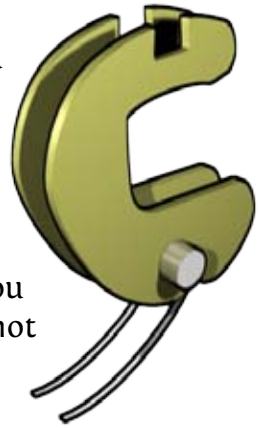
Install the third lever on the right-hand of the lock. It is important that you keep all levers on a single side of the lock at this stage. Remember you will need to remove the retaining pin that holds the levers in place to add or remove levers. Follow the same procedure and pick it several times. Once this is no longer a challenge you can stop and move to the next step.

2—Blind Feeling

Remove all the levers from the right-hand side of the lock and install two levers on the left-hand side of the lock. Do not install three. This will just frustrate you because there is a new binding order and you are not yet used to picking locks in this fashion.



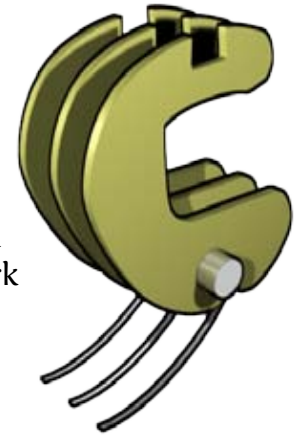
You are probably thinking you should try to pick the core of the lock in the body of the padlock by now and I also made that mistake. This exercise will familiarize you with picking the levers on the opposite side of the lock. You will find you hold the pick differently. I use the keyway as a fulcrum on the right-hand side and do not use the keyway at all on the left, but you should find what works comfortably for you.



This exercise also limits your ability to see the levers completely while still allowing you to see if you are moving them at all. This will help you find the levers as their staggered assembly leaves them in different places on the left side than the right.

Now follow the same procedure as before: lifting the levers one at a time to find the binding lever and waiting for the click. After you have done this three or four times, insert the third lever and try again. Do this until it is no longer a challenge.

Now remove all the levers from the padlock and place them on the desk in an organized fashion so you to not get them mixed up. From this point on you will need the operating key to work with the padlock.



3—Into the Padlock

Now that you can easily set three levers on either side of the core (or should be able to, before moving on to this section) its time to learn how to pick up the feedback you were getting through your index finger via the tension tool.

Don't forget: you WILL need a working key to the padlock.

Take the three levers for the right-hand side of the padlock and install them in the core of the lock. Now insert the key and make sure the gates line up and you can push the sidebar in so it is flush with, or recessed into, the core of the lock.

Leave the key in and insert the core into the body of the padlock. Rotate the core into the locked position. The two large grooves should be opposite the sidebar when properly installed.

You should reattach the faceplate of the lock and screw it in from behind with the two screws located under the shackle. This is not absolutely necessary but is recommended. Personally, I got bored of doing this although it does make it a little easier to pick up feedback as the core is held more securely in place. It is your choice.

Now insert the tension wrench into the opposite side of the lock from the levers. This will give you better feedback at this point as it can be inserted further. It will also allow you to pick in the fashion you just tried but with a different binding order as you are using a different set of levers. This is the right-hand side as you look at the lock with sidebar at the top.

I also noticed that if I placed the lock flat, with the top of the body of the padlock against the hard surface of my desk, it gave better feedback. Of course this is only possible as you have the lock partially dismantled with the shackle removed, but it may help you learn to pick the lock more easily.

Now you can begin to pick the lock with the three levers installed. You will notice that you are getting different feedback from the lock now because you are now feeling for slight rotations of the core rather than pressing down on the sidebar directly.

It is worth noting that if you are failing to open the lock, inserting the key and removing it to reset the levers can be a good idea. This could also be done with a blank key or another key of the same key-way.

Open? Great! You are half way there. Now we will do this three or four more times and then do it again with the other three levers from on right-hand side of the lock. You'll likely notice that you hold the pick differently when picking the levers on the right-hand side. Remember, move the pick around the lock not the lock around the pick.

Remove the core of the lock from the padlock body and remove all the levers, then replace them with the opposite set of levers. Reinstall the core into the body of the padlock and pick the lock a few times.

Now it's time to learn how to deal with levers on opposite sides of the lock. At this point you may want to put the lock down and walk away for a while. I think I would have done much better with this next step if I had taken a break, instead of continuing to pick well into the early hours of the morning and shouting at it.

Breaks are good. Take some time, step away from the lock and relax while you work.

Remove the middle right-hand lever from the core and set it down nearby. Now take the middle lever from the right-hand set of levers and install it in the correct position in the core.

Do not reinstall the core of the lock. We are going to pick this out of the body of the padlock again. This is where things start to get harder. Opposite levers will tend to lift the side bar as they are raised. In a manner similar to how a spool pin will reset a pin tumbler lock, lifting the sidebar will dislodge levers from their bound position.

We are doing this outside of the lock again so we can start to learn when a lever has been dislodged by levers from the opposite side. Once you have picked it a few times try it in the lock.

From this point on we will no longer be picking the lock outside of the body of the padlock, but feel free to remove the core again if you are really struggling. Make sure you ALWAYS test the core and make sure all the levers line up before you install the core.

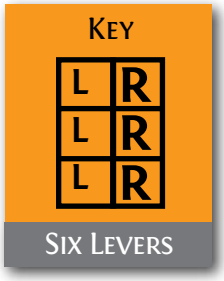
Install the final lever on the right-hand side of the lock and then pick the lock »

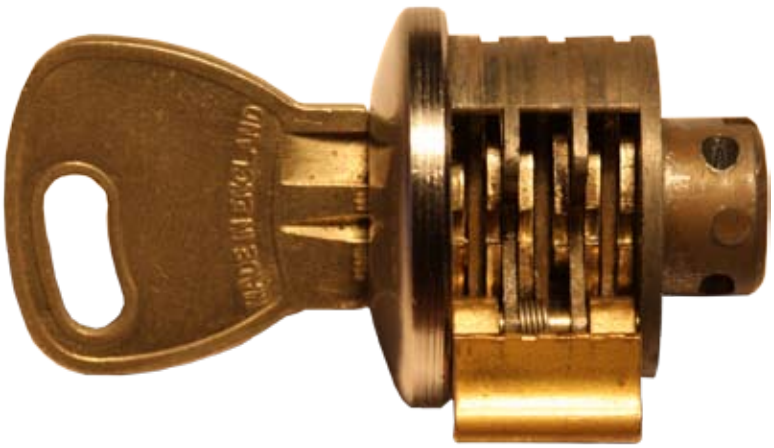
Now we are going to install more levers until we have a full lever pack installed in the core of the lock. First install a second left-hand lever in the lock. I recommend using the back left-hand lever but depending on the height of the levers in your padlock it may be easier to install them in a different order.

You will probably notice that picking times start to get much longer around now, don't let that put you off, just keep trying. Remember to take a break if you start to get frustrated.

If you have come to this point successfully you should be feeling quite smug right about now. You only have to install one more lever and you are basically finished. Install the final lever in the padlock and try it again.

The last thing you need to do now is reinstall the rubber washer on the cam on the back of the lock. This will make picking up feedback slightly harder but it is how you would find a lock in the wild so it is how you should aim to pick it. Replace the washer and install the core of the lock into the body of the padlock for the final time. Now, attempt to pick the lock.





Congratulations! You just picked a fully functioning 6 Lever Ingersoll padlock.

Have you picked it?

Tell us all about it at our new forums! Ask John about his technique or share some ideas of your own. If you want to talk about this, or any of our articles in this issue, check us out:

@

lockpickology.com

*Supplemental Material: John's photographer, Adam Ferguson, has provided us with incredible, high resolution photographs for these articles. Unfortunately we're not able to display them in their full glory in the magazine, but you can download all of the images on the Issue 4 release page. Thank you Adam!—S.T.

The ABUS Challenge

BY JAAKKO FAGERLUND

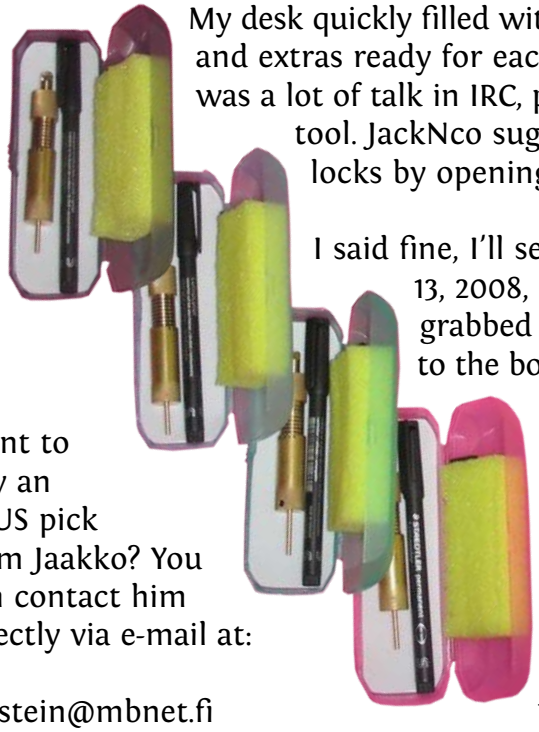
* BE SURE TO CHECK NDE ISSUE 3 FOR THE FIRST PART OF THIS ARTICLE: "ABUS PLUS EXPLOIT" FEATURING THIS AUTHOR.

Today I'm going to show you my progress on the improved version of the ABUS Granit 37/55 padlock that the ABUS factory sent me as a "challenge lock".

In January 2008 the lock was sent to me without keys or keycard. All I knew was that the discs inside were old & new, meaning some of the discs had the stamped number on them and some were the new non-stamped discs that ABUS introduced to their line of products as a countermeasure to my discovery, which was covered in a past issue of NDE Magazine.

It was somewhere around January or February when I got a small metal lathe ("a mini lathe" as it is better known) and some tooling for it. At that point I had no kind of training whatsoever for it. All I had were a few hobbyist websites, lots of free time and a few pieces of steel and brass to chuck in the lathe. I just had to do it and learn as I worked.

Fast forward a couple of months, I had plans made and knew where to get materials. I received some more tooling for the lathe from friends who were supporting this project: a milling attachment from Schuyler and a knurling tool from "unlisted". Because of those tools I was able to produce high quality ABUS Plus picks made from brass. This surprised me because I felt that the lathe was just a hobbyist tool and I had no formal training on lathe working.



My desk quickly filled with twelve of these beautiful tools, and soon I had cases, wrenches and extras ready for each, just waiting for buyers. During this manufacturing time there was a lot of talk in IRC, private messages mostly, with some ideas and opinions about the tool. JackNco suggested that I prove the tool's ability to pick and decode these locks by opening the "challenge lock" that ABUS had sent me half a year ago.

I said fine, I'll see if I can learn to use this tool and get the lock open. It was June 13, 2008, the clock ticking about 03:00 (yes, in the middle of the night). I grabbed the 37/55 and started picking it. I Inserted the tensioner all the way to the bottom, turned the butterfly disc and then one by one I manipulated the discs into "free" positions. I kept a table in front of me, crossing out numbers that were surely not in the key code and to keep my place if I had to quit before I solved it. I had gone through each disc twice and was half way down the cylinder on the third round when suddenly I felt the tensioner turn freely. My first thought was "Damn! It slipped again," but the tensioner stopped and the shackle dropped open. Wow, the feel of adrenaline rush, the excitement and joy and...well, my fiancé dropped me back to this world saying that the neighbors are sleeping.

Want to buy an ABUS pick from Jaakko? You can contact him directly via e-mail at:

einstein@mbnet.fi

I wanted to have proof and capture the moment, so I gave the camera to her and she took a few pictures of me with the open lock and the tool. I'm not that pretty, but get used to it, I will be here often!

After a few "woohoos" and "YEAHs!" I sat down again and decoded the now picked lock to get the key code. Took about a minute to go to each disc, read the angle from the tool and mark the corresponding number to a piece of paper. In the process I noticed that I filled my table during the picking process a little wrong, I had crossed over the number five cut from the end of the table. When I had the lock decoded, I sent an e-mail to ABUS with the key code 3612645 and CC'd the message to Barry Wels also, as he was the one who arranged the ABUS contact.

In the e-mail I also explained how I got the lock open and how much time it took. Looking at the table that I kept while picking, I had reduced the number of possible keys from the original 279,936 (6^7) to only 24,000 after manipulating each disc once. After the second round I had the number down to 486 different keys and, as said, half way through the third round the lock popped open.

Two days later, on June 15, 2008, I noticed an error in the key code I sent to ABUS. I had read the angle markings in reverse from my tool, so that a cut number one became six, two became five, three became four and so on, so I quickly sent a new e-mail to ABUS and Barry with the correct key code, 41651326. On June 19, 2008 I got a reply from ABUS saying that it was good that I sent the correction, as the previous message to them had been overlooked. I got a confirmation that the code I sent was indeed correct and that I would receive the keys and the key card in a couple of days.

Two or three days later UPS delivered a small package to me, with a description saying "keys." Inside were the keys, key card and a note from ABUS as a thank you.

I would like to thank Schuyler and unlisted for providing support in the form of tools, all supporters in #lp101 @ SlashNET, NDE Mag for covering the whole thing that started almost exactly a year ago (July 8, 2007), Barry Wels for inviting me to the Dutch Open 2007 and providing the ABUS contact, and ABUS for listening and being a great example of how things should be done and also for sending out the "challenge lock" as a gift. Finally, a special thank you to everyone who I didn't mention, you all have contributed to this and been friends (not that you still aren't!)

I hope to see you at the Dutch Open 2008 and that my tools will sell, because those things are my budget-to-be for the Dutch Open trip, so please, I would appreciate your support!

Cheers, Jaakko Fagerlund, Finland

Lock Talk

Discuss this article with readers, staff and even the author online at NDE's new forums!

@

lockpickology.com

"The ABUS Story"

Great Moments In Locksport

In June of 2007 a contest was announced by locksport legend "Zeke" to drum up some new talent in high security lock research. The results would lead to an amazing revelation and systematic changes to the ABUS Plus system.

Jaakko Fagerlund of Finland was at the center of the ensuing activity and kindly agreed to keep notes of his experience for publication in NDE.

The Exploit

The ABUS Plus system is a disc-detainer style lock. The attack exploited the individual code numbers stamped into the back of each disc. Though the numbers are not immediately visible from the keyway, a very clear impression can be made by inserting a T-shaped tool coated with adhesive and pulling the head back on the stamped disc.

Jaakko's Notes

– Sun Jul 08, 2007 20:48 –
An LP101 member "mh" from Germany sends me a message informing me that he has contacted ABUS and made them aware of this problem.

– Mon Jul 09, 2007 13:54 –
"mh" suspects the initial answer from ABUS came from the first level customer support:
"Nobody has opened an X-Plus lock without the proper key"—"the keyway has no surface markings"

– Thu Jul 12, 2007 18:46 –
Another message from "mh" and it appears to be a new response from ABUS:
"Thank you very much for your detailed description! The security level of the ABUS Plus cylinder – esp. concerning the so-called time resistance – is unique... We will gladly look into the issue and will follow-up together with our technical department, and/or R&D. Thank you for your efforts!"

The Fix Is In

ABUS fixed their problem and even sent Jaakko one of the new locks. This one had mixed discs, some with the stamping, some without, but no keys. Jaakko was invited to discover the key code on his own. If he could do it, they would send along the keys and code card as a reward.

A New Direction

With his former attack now obsolete, Jaakko needed a new plan. He began to work on a custom pick for the lock:

"I received a small metal lathe and some tooling for it. At that point I had no training whatsoever. All I had were a few hobbyist websites, lots of time and some steel and brass things to chuck in the lathe. I just had to do it and learn."

Before long he had plans, materials and various members of the community supporting his project. Donations of equipment allowed Jaakko to produce his ABUS Plus picks. During the manufacturing process there was a lot of speculation. Would it actually work? Jaakko would have to prove it.

The Challenge Lock

So, six months after lock first arrived, at 3:00 am, Jaakko finally attempted to pick the new lock:

"I said fine, I'll try and see if I can learn to use this tool and if I can get the lock open... I grabbed the 37/55 and started to pick it. Inserted the tension part, went all the way to the bottom, turned the butterfly disc and then, one by one, I manipulated the discs into "free" positions. I kept a table in front of me, crossing over numbers that were not in the key code. I had gone through each disc twice and was half way down on the third round when suddenly I felt the tensioner turn freely and first thought was "damn, it slipped again", but the tensioner stopped and the shackle dropped open..."

A few days later a package arrived from UPS marked "Keys." Inside were the keys, the code card, and a small note of thanks from ABUS. Jaakko Fagerlund had completed his study of the ABUS Plus system, picked the challenge lock and shared his story with the locksport community.

And we were proud to be there.

—NDE MAGAZINE

NDE Magazine
For Locksport!

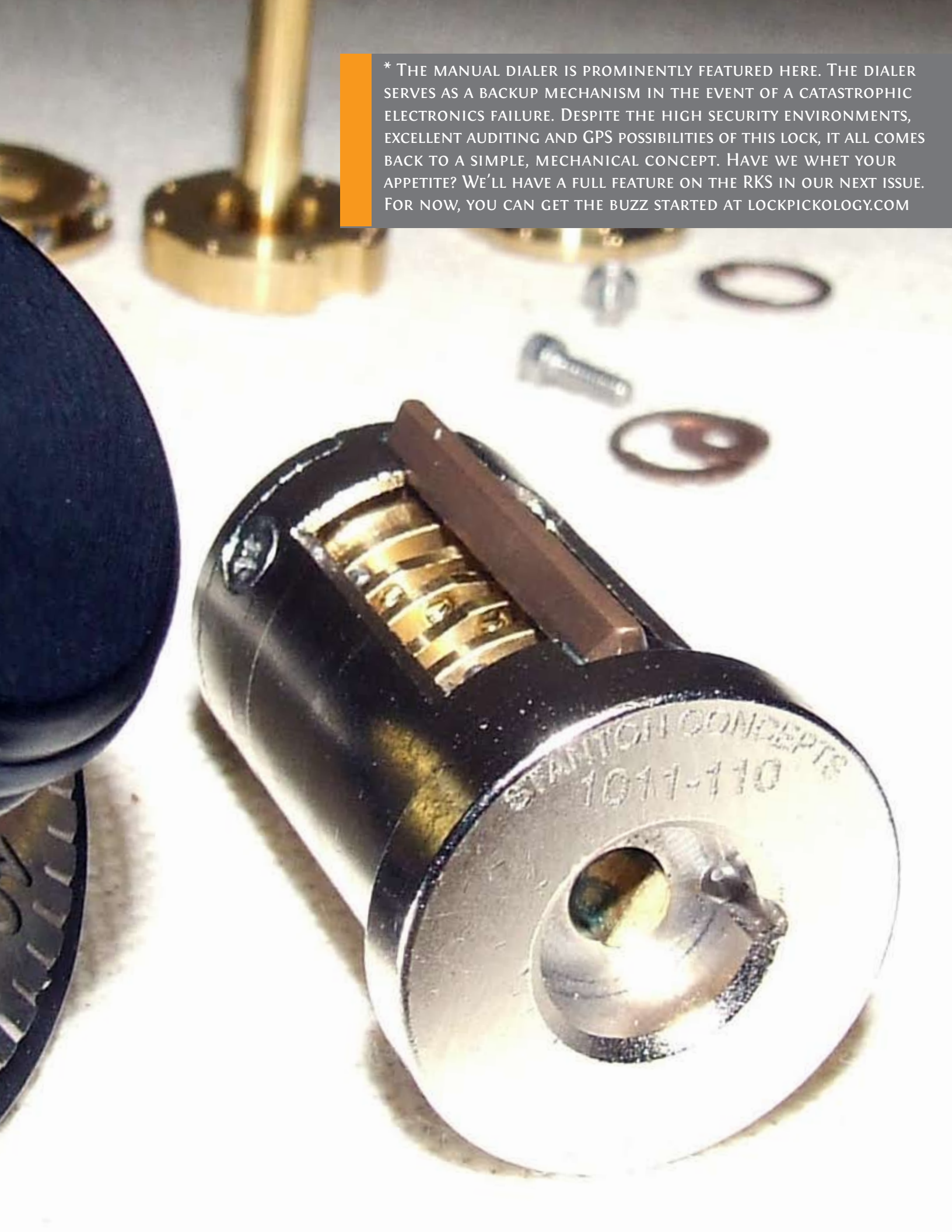
Timeline ...
From Discovery to Disclosure

- Jun. '07: Zeke Launches Contest
- Jul. '07: Exploit is Discovered — ABUS are Contacted & Respond Appropriately
- Nov. '07: Jaakko Speaks at Dutch Open
- Jan. '08: Challenge lock is delivered
- Mar. '08: Work Begins On New Pick
- Jun. '08: Challenge Lock Picked & Keys Delivered
- May '08: Inititial NDE article released

‹ 2007 | 2008 ›

* The RoboKey Cylinder. This beautiful, precise lock looks almost like clockwork when disassembled. You can see that each face is serialized, with no distinct keyway and the discs inside have flies like a safe...


16
12
8
4
0
60
56
52
48



* The manual dialer is prominently featured here. The dialer serves as a backup mechanism in the event of a catastrophic electronics failure. Despite the high security environments, excellent auditing and GPS possibilities of this lock, it all comes back to a simple, mechanical concept. Have we whet your appetite? We'll have a full feature on the RKS in our next issue. For now, you can get the buzz started at lockpickology.com

BY MIKE BREWERTON

Why Is Everybody Picking On Medeco?

When you're the king of the hill, you become a target. Period. Medeco represents approximately 70% of the high security lock market in North America, so it's safe to call them the king of this particular hill. At least for now.

Why am I picking on Medeco? Because I need to. As a locksmith, I like their locks and find them fascinating. Once upon a time, and not too long ago, Medeco was just about the only high security lock I dealt with. I've had other brands available to me, but until recently I've felt Medeco was simply one of the best options out there. Now, with all the new vulnerabilities I'm learning about Medeco, I'm starting to reconsider that position. I'm not dropping Medeco, but I am adding other options to my inventory. When it comes to security I'm blunt. I'm not afraid to tell my customers the ups and the downs of the options available to them. Sometimes my openness costs me business, but at least I can look myself in the eye in the morning.

Why is the Locksport community picking on Medeco? The adrenaline. There is a certain thrill when a lock that you're picking finally pops open. Until you experience it, that moment of triumph is almost indescribable, when you feel the last pin click and suddenly the lock turns under your tension wrench. That feeling is magnified many times when you're working on a lock many people call unpickable.

Why is Jon King picking on Medeco? Some people get a different thrill from "beating" a lock. While picking a single lock gets the heart pumping, the systematic defeat of an entire locking system is a deep, intellectual satisfaction that lasts well beyond the initial accomplishment. Jon King, inventor of the "Medecoder," once saw Medeco locks as The Holy Grail of lockpicking. He even said "maybe one day, I'll pick one once." Once! Looking back now, his words are comical, coming from a man who just last week, on camera and in front of hundreds of spectators, picked a six pin Medeco M3 in under three minutes at the HOPE conference. Stresses like that don't make picking easier. Sure, I'll bet the moment it opened he felt great, but he has done far more than that. With the invention of the Medecoder, he has conquered a generation of these locks.

What do you do with the information once you have beaten a lock? For some people it's all about the bragging rights, but the opposite side of that is "responsible disclosure," which is to use the information wisely. That is the course that many people, including Jon, have followed. Before going public with their discovery, they contact the manufacturer and give them a chance to respond and improve their product. On a similar note, look elsewhere in this issue for the follow-up article on Jaakko Fagerlund and the Abus Plus system. You'll find a story of a Locksport enthusiast who found a vulnerability in a lock which allowed it to be easily decoded, and he also developed a specialized pick for that lock. While his pick is still effective, at least for the time being, he worked with the manufacturer to render the simple decoding attack obsolete.

Locks are not a security solution on their own. They are just a part of it. A good security plan needs to be built in layers, so that if one part fails, other parts are standing by to pick up the slack. This applies to "secure" facilities like government buildings and banks and also to our homes and businesses. Are Medeco locks invulnerable? No. Is any lock invulnerable? Absolutely not. Lock companies need to constantly adapt and improve their products. They need to be proactive, not reactionary. I believe most manufacturers are making efforts in the right direction, but there remains room for improvement. That's where Locksport can help.

If you have found a new vulnerability in a lock system, or have invented a new pick or bypass tool and would like help interfacing with a lock manufacturer, please e-mail me and we'll see what we can do to help.

E-MAIL MIKE: MIKE @ NDEMAG.COM

The Last Word: Full Medecoder Disclosure

BY JON KING

* Recommended reading: A three part story about Jon King's discovery was published in NDE Issue 3.

Medeco Basics

The Medeco lock design has been a target for lock pickers since its release in the 1970's. These locks are used in some of the most secure facilities throughout the world. The United States Government in particular has a large number of contracts with Medeco. Many locksmiths regard them as "pick proof" or very close to it.

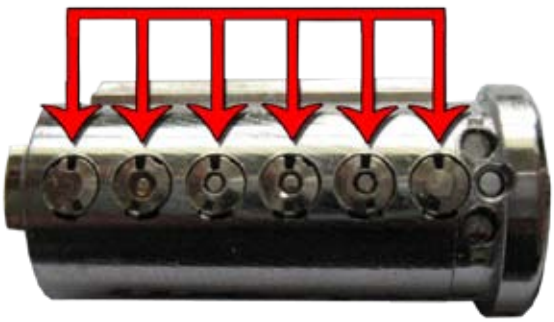
Many have attempted to develop tools and techniques to bypass Medeco locks; some successful and others not. The successful ones have usually only been available only to government agencies and certain locksmiths. The patent for the first Medeco decoder was filed in 1974 (US Patent #3987654) though I was unaware of it during development of the Medecoder. John Falle makes a government-restricted decoder which appears to exploit the same vulnerability as the Medecoder, but this assessment is based on photographs I have seen and not first hand observation. I believe that my Medeco decoder-pick, The Medecoder, is the first tool design available to the hobbyist that is able to handle the sidebar of most Medeco locks.

Medeco locks really do employ a fantastic design; the pins must both lift, like in a traditional pin tumbler lock, as well as rotate. There are three angles (left, right, and center) to which the pins can be rotated, and each bottom pin has a groove along its side. Unless they are rotated to the correct position, lining up the groove in the pin with a tooth in the sidebar, they prevent the sidebar from retracting.

This presents a unique challenge to the lock picker. How does one rotate small pins through the keyway, much less find the correct angle? The answer up until now has been: via pure skill.

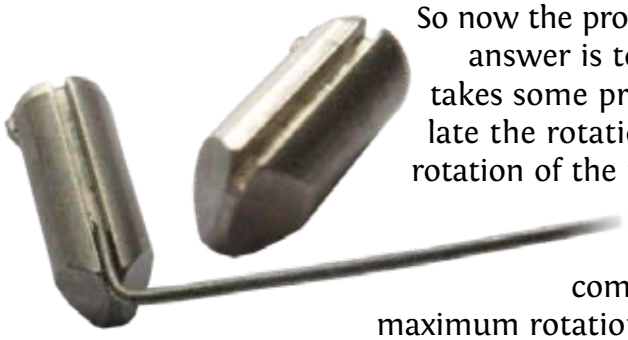
Feel The Groove

The vulnerability exploited by this tool lies in the sidebar groove in the Medeco bottom pins. The problem with the regular pins is that the groove into which the Medeco sidebar interfaces, extends the entire length of the pins, all the way down to the bottom, where they can reached by the Medecoder. The more secure pins—the Biaxial version is known as ARX—are not vulnerable because they employ a groove that is closed at the bottom of the pin. When the proper key is inserted, these grooves line up to match the teeth of the sidebar. If the rotation of these pins can be reliably manipulated so that they arrive at their final destination, we can defeat the sidebar.



The Evenly spaced sidebar teeth allowed for easy calibration of the Medecoder

These sidebar teeth are evenly spaced on every Medeco and thus exist at known positions. If we can map these positions outside the cylinder and align the rotation of the pin's grooves based upon these positions, we can pick the sidebar. This alone will not open the lock, but luckily most Medeco locks are not too difficult to pick to the shear line, at least for an experienced lock picker.



So now the problem remains: how do we control the rotation of the pins? The answer is to hook a small wire into the sidebar groove of each pin. This takes some practice, but it is much easier than trying to rake it or manipulate the rotation with a hook pick. So now we have a way to control the rotation of the pins and a way to determine the correct rotation of each pin.

Decoding is a bit more difficult to understand, but by comparing the known position of the grooves with their respective maximum rotation angles, you can determine the pin type (left, right, or center).

The Tool

If you can make and control a small wire capable of hooking into the sidebar groove of each pin, you have the rotation-control aspect covered. The next objective is to have a reliable way of measuring where the proper rotations are. Simply position the groove-grabbing tool inside a pre-measured scale (I use a hollow tube) and you're golden. So what we are basically doing is measuring how far into the lock the tip of the wire is, as precisely as possible, and comparing it to the proper final positions of the sidebar grooves.

This means we will need a basis for measurement. It has to be something that won't move, will be easily accessible, and remain consistent from one cylinder to another. There are a few good options, but I chose the plug face. So by measuring the reference scale by basing it on the plug face, you can get pretty good readings by simply butting the scale against the plug face and comparing it to a mark on the wire tool.

This Sounds Hard!

This all sounds much more complicated than it really is. Once you try it you'll see it's actually not so bad. The first thing you must do is pick the lock to the shear line while tensioning clockwise. It picks like a normal lock with a few mushroom top pins. What you must do is detect when the pins have been set to the shear line. On a normal pin tumbler lock this detection is pretty easy: the lock opens. It's a little tougher when picking a Medeco lock. What typically happens is a decent bit of plug rotation accompanied by a change in the way tensioning feels. The sidebar is spring loaded so when picked to the shear line the plug will feel springy under tension.

Next the wire part of the tool is inserted and you must start locating grooves. Holding the tool like a pencil, start to scrape the bottoms of the key pins. You should be able to readily hook into a groove. If you have difficulty, try holding the wire at about a 30 degree angle so the tip points slightly to the right. Once you think the wire has hooked a groove, simply push the scale tube forward and butt it against the plug face. If the index mark (on the inner shaft of the tool) is near a scale mark on the outside tube, this provides some verification that a groove is hooked, and into which pin you are hooked.

Take note where the index mark is in the relation to the scale mark. Next, slightly withdraw the scale tube to allow for full freedom of movement of the wire part of the tool. Slowly start lightening tension while wiggling the wire back and forth. If you are able to move the wire forward and aft with relative ease then its time to position the pin. If the index mark was aft of the scale mark, push the wire tool forward. If it was forward of the scale mark, pull the wire tool back toward you so that the marks on the tool line up.

Next apply tension, butt the tool against the plug face and check the marks again. If the marks now line up, great, move on the next pin. Once all of the pins have been lined up, the sidebar will be defeated. If the pins are also picked to the shear line (and the slider has been defeated in the case of m3), the lock will open.

So, Does It Work?

My results so far have been overwhelmingly positive. If you asked me last year if I thought I'd ever be able to pick open a Medeco lock at all (much less consistently), I'd have probably laughed. Picking most open-groove Medeco locks becomes almost easy with this tool. Everyone knows that the hard part is the sidebar and this decoder-pick really takes the difficulty out of that aspect of these locks.

I have run into a couple of keyways so far (a Medeco Classic, and a Biaxial) in which I could not effectively grab the grooves of some very low-setting pins. Other than that, hooking into sidebar grooves and controlling their rotation is pretty easy with practice. Even on locks with closed-groove pins, you can still handle any open-groove pins which might be present (not too hard to tell). This gives you a boost of confidence: "OK, I know for sure that pin is rotated properly," while you go after the closed-groove pins with another method.

For the locks it works on, the sidebar becomes a formality. It reminds me of the check pin on a Schlage Everest or even the slider on the Medeco m3. Granted, the Medecoder defeat is a little more involved than with these two examples, but it's not difficult after some experience with the technique.

Join the discussion at the new NDE forums. Let us know what you think of Jon's work. You can track us down right now @ Lockpickology.com

Editor's Note:
As we mentioned in issue three of NDE Magazine, Medeco asked us to withhold publication of this article for two months, to give them time to retool and close the vulnerability that is exploited by the Medecoder. That time has elapsed, and last week Medeco informed us that every new lock rolling off their production line now contains a mix of standard and ARX pins, rendering the Medecoder ineffective against them. (This does not apply to Medeco cam locks as they use a different design which was never vulnerable to the Medecoder).

For more information on this change, read the article "Medeco ARX High Security Locks" in this issue.

If you are a locksmith who services Medeco locks and would like to purchase a pin kit with the new style pins, the part number is KW-5004.

If you are an end user who has Medeco locks and would like information on upgrading your locks with ARX pins, contact your local locksmith for pricing.

-M.B.

"The Medeco Story"

Great Moments In Locksport

At a small kitchen table in an undecorated, sparsely furnished apartment in Virginia, sat the head of Medeco's R&D department and a 22 year old lockpicker. It would be an interesting conversation.

Jon King, a sailor in the US Navy, had invented a tool to reliably and systematically attack most Medeco locks. He wrote up his research, and agreed to release with NDE.

The Exploit

Medeco locks operate on a simple, but extremely effective principle. In order to open the lock, the key both lifts and rotates the pins, aligning both the standard shear line and a sidebar at the same time. The sidebar drops into a groove cut along the side of each pin when it reaches the proper rotation. John's attack is equally simple. Utilizing a thin wire in a meticulously calibrated shell he can hook into the bottom of the open grooves one after the other. Once in, a small mark across the barrel of the tool will either sit behind in front of, or dead on to a corresponding mark for the pin. From there, aligning the sidebar is simplicity itself. Just push or pull each pin until the marks line up and you're done.

"Hooking into sidebar grooves and controlling their rotation is pretty easy with practice...This gives you a boost of confidence: 'OK, I know for sure that pin is rotated properly...'"

First Contact

Peter Field is a brilliant engineer and the head of Medeco R&D. In 2007 he first spoke at the Dutch Open in Sneek, NL. He opened his talk this way: "Let me just say, in case no one else has, welcome to the industry..." and ushered in a long-awaited connection between locksport and manufacturers. When Jon came to NDE, NDE went to Peter.

Credible Threat

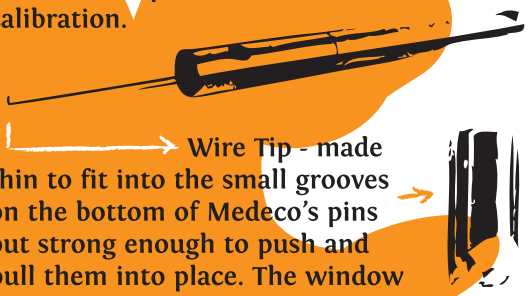
Peter reviewed Jon's research and decided to see it in person, driving across Virginia with a laptop, a camera and bag full of new pins. During the meeting it was revealed that an older tool which Jon's was often compared to was never useful as a picking aid, and completely ineffective against Medeco's Biaxial pins, which became standard in 1985. Jon's attack was the real deal, and Peter planned to respond accordingly.

ARX

The pins Peter carried with him were an old solution to a new problem. ARX type pins, save for a few exceptions, have closed bottom sidebar grooves. This means that there is no access to them for a wire, as in Jon's attack. The ARX system was actually introduced several years ago, but discontinued. The machinery wasn't abandoned, however and as soon as they were up and running Medeco began to produce new ARX pins kits and reintroduced them to every new lock coming off of the line.

The Tool

Jon took a hand-made prototype and, after success with his own model, had a few machined to provide ever more accurate calibration.



When Jon King sat down with Peter Field, bridging the gap between lockpicker and manufacturer, it was a huge step forward for our entire community.

And we were proud to be there.

—NDE MAGAZINE

NDE Magazine

For Locksport!

Timeline ...

From Discovery to Disclosure

‹ 2007 | 2008 ›

- Sep. '07: Jon First Picks a Medeco
- Nov. '07: Peter Field Speaks at Dutch Open
- Dec. '07: First Medecoder is built
- Feb. '08: Jon Approaches NDE
- Mar. '08: Han Fey Connects us to Peter
- Apr. '08: Peter, Jon & NDE Meet in VA
- May '08: ARX Pins in All New Locks
- Jul. '08: Jon King Releases @ The Last HOPE Conference

Medeco ARX High Security Locks

BY Mike Brewerton

*Special thanks to Peter Field for help in the research of this article & SafetyOff for graphics

In July 1994, ARX became commercially available to Medeco customers. The trademark "ARX" is an acronym for "Attack Resistance X-tended." They were optional features that could be special ordered, enhancing normal Biaxial locks, to improve resistance to picking, decoding and destructive bypass. According to Medeco literature, it was intended to be "a complete line of door hardware cylinders for customers that have sophisticated security threats." It was available for rim, mortise, key-in-knob/lever, and interchangeable core cylinders.

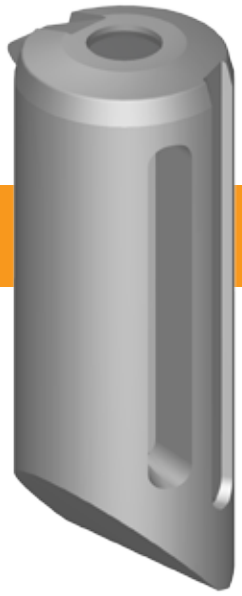
ARX features fall into four categories: appearance, drill resistance, picking resistance and decoding resistance.

Appearance

ARX locks can be ordered with standard Medeco markings, or with a blank face. By providing less information about the lock, it can potentially hinder anyone who attempts to reconnoiter or penetrate a target facility.

Drill Resistance

Normal Medeco cylinders have several features to provide drill resistance, consisting of hardened steel plates, rods and ball bearings placed at strategic drill points. Certain sizes of driver pins are also made of hardened steel. In addition to these standard features, ARX locks have a carbide rod which extends the length of the cylinder plug from front to back, on the side opposite from the sidebar. Every ARX bottom pin also has a steel rod of varying lengths, extending down the length of the pin. The pin inserts were effective enough as a drilling countermeasure that a random assortment of pins with these inserts later became a standard feature in regular Biaxial pin kits. This diagram shows a cross section of such a pin »



« Pins with steel inserts can be visually identified when removed from the lock since the end of the insert is visible on the top of the pin. According to the service manual, these extra features increase drill resistance by 500%.

Picking Resistance

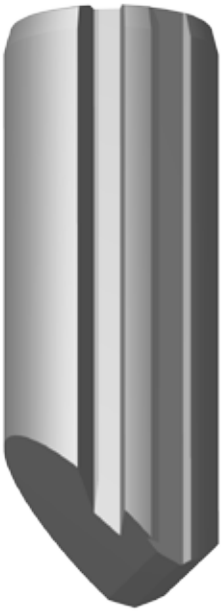
Medeco locks have always used mushroom pins to resist picking. The factory specifies that a minimum of two should be used in each cylinder. In addition to mushroom pins, ARX pin kits included an assortment of spooled top pins to further complicate picking. These pins have several rings cut into the circumference, making them look similar to serrated pins rather than traditional spool pins.

Decoding Resistance

In 1974 a company named Lock Technology made a set of tools to attack the original Medeco locks. This tool was not able to pick open the lock, but it was able to decode it so that a key could be made for use at a later time. The vulnerability in the lock that allowed this tool to operate were the grooves in the side of the bottom pins. Because the groove extended the full length of the pin, a thin wire could be inserted into that groove from the bottom. Medeco quickly closed this vulnerability and in June 1974 began using milled

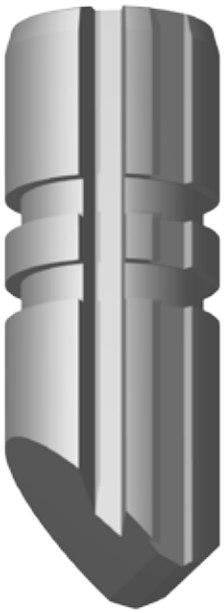
pins with the sidebar groove closed at the bottom. See the bottom center figure, below, for an ARX version of this pin. Medeco took legal action against Lock Technology, possibly for patent infringement since the tool used a modified Medeco key as part of the device. Lock Technology agreed to stop production of the kits and fewer than 100 were ever sold.

In the late 1970's another tool was developed to attack Medeco locks. This tool was able to compromise the elevation of the pins, leaving only the sidebar to secure the lock. In response, Micro-Milled pins were developed, with grooves that were closed on both the top and bottom. See the bottom right figure, below, for an ARX version of this pin. The downside of these pins is that due to the shorter sidebar groove, they cannot be used in pin stacks containing a master wafer.



Biaxial locks were introduced in 1985, changing the pin tip geometry so that they are offset either fore or aft of the center-line of the pin. This gave Medeco a new key control patent and doubled the number of bottom pin variations to 36; greatly increasing the potential quantity of key differs. They also changed the position of the locator tab on the top of the pins and the locator tab groove in the cylinders, as compared to original cylinders. Because of these changes, the decoders made by Lock Technology would not work on Biaxial locks. With no tools on the market to compromise them, Medeco went back to using pins with a sidebar groove that extended the full length of the pin, possibly also because of lower manufacturing costs with this method »

In the early '90s John Falle introduced a decoder for Medeco Biaxial locks. Medeco quickly responded by introducing ARX to thwart several different decoding methods. Pin styles included: ringed pins, milled pins with grooves closed at the bottom, and Micro-Milled pins with grooves closed on both the top and bottom. Milled pins were only produced in pin sizes three to six because pin sizes one and two are so short that if closed grooves were used on them, the grooves would be too short and would block sidebar operation even if the pin is correctly rotated. As mentioned earlier, the Micro-Milled pins still cannot be used in masterkeyed pin stacks.



Ringed Pins

Milled pin with closed bottom groove

Milled pin with closed top and bottom groove

I also learned of another type of decoder which may exist for Medeco locks, although I have been unable to positively confirm its existence, but it's far too interesting not to mention it. This decoder apparently uses an ultrasonic probe inserted into the keyway which would vibrate and bounce the stacks of pins, one by one. Allegedly, this decoder can precisely determine the weight of each bottom pin. By comparing the weights of the pins in a lock, to a chart of the known weights of all sizes of Biaxial bottom pins, a key could be produced for the lock. Apparently it was developed by a U.S. Government agency as a proof-of-concept and was never mass-produced. Production of an item like this by criminal elements was not considered likely, but there were concerns that use of such a device was possible by foreign governments engaged in espionage, so Medeco was asked to develop countermeasures for attacks of this type.

There are over 150 variations of ARX pins, compared to just 36 variations of the normal Biaxial pins. Within each size of pin, the variations were mixed at the factory, ensuring a random selection in each lock in order to resist traditional picking and decoding methods. The varied assortment of surface features on the pins also serves to randomize the weight of the pins. The steel inserts in the bottom pins are also made in varying lengths, further randomizing pin weight which should render the ultrasonic decoder ineffective.

The development of many features incorporated into Medeco ARX high security locks took place over a period of approximately twenty years, before being released under that name. Although the ARX system was eventually discontinued due to a lack of customer interest, the machines to produce the specialized pins have remained in the factory, unused. With the release of Jon King's Medecoder, ARX pins will now receive new life. The Medecoder utilizes a vulnerability that has been exploited by other tools in the past, but unlike those previous tools, the Medecoder can actually be used to help pick open a lock rather than simply decode the sidebar. Additionally, it is much lower in cost than previous tools, and can be even built by hand with limited resources, making it available to a much larger group of people. With this increased threat, Medeco decided it was time to resurrect ARX pins. In our communications with them, they requested a two month delay before we went public. This was to give them time to recondition those machines and resume production of the pins. Rather than being an optional feature, they will now be included in all newly produced Medeco locks.

Discuss the long history of Medeco ARX with us @ Lockpickology.com!

Pick a Lock With Squelchtone

BY WALTER KICZKO

*This was meant to be a recurring feature. See Issue #1 for the first "Pick a lock with..."

The Great Escape with Steve McQueen was on the small TV in the corner. The sounds of bassdrive.com filled the 100 year old house, and I sipped my Johnny Walker Black Label while hanging out on #lp101 in IRC. The clock hit 2:00am and I scanned the room for something, but at first I didn't know what. Then I recognized that feeling coming over me like a warm blanket. I felt the need to pick a lock.

I walked down the hallway to the kitchen to get my Peterson picks. I smiled as I walked past my latest score, perched haphazardly on the edge of my kitchen table: a free safe which was given to me after I helped the owner open it so he could retrieve the contents. He felt better getting a new one since this one's mechanism had gotten stuck one time too many. It's an old Sentry 1250 by the way. I know that you were wondering.

So I returned to my office, pick set in hand, but no lock to pick. I must have passed twenty of them on the kitchen table, and another dozen on the coffee table. The ASSA cylinders on my desk were tempting, but for 2 in the morning that is too much lock even for this picker. I lifted my rocks glass and took a sip. It's an acquired taste. The aroma of burnt wood barrels is also an acquired smell.

I found it: the perfect challenge. The biggest, BEST brand SFIC padlock you've ever seen...

I found it: the perfect challenge. The biggest, BEST brand SFIC padlock you've ever seen. It's an old model but I bought it new, and from what the seller told me it's an 8B772. It arrived last week and was quickly hung up on the peg board for display. I have the keys,

including the control key, but decided to not look at the bitting. My Peterson pick set has been busy fornicating. The case originally had ten picks and several wrenches. Now it contains 28 picks and 12 wrenches. I must preface this by telling you how big this padlock is. The body is one inch thick and two inches tall by two inches wide. It is a seriously heavy lock.

I chose my favorite half diamond pick, an HPC with a nice foam handle, and a SouthOrd twist wrench. The BEST D keyway has a nice little shelf for the wrench, almost like they put it there to help with picking. I find very light tension to be most effective with BEST cores, but this lock was proving a worthy adversary. Maybe it was the late hour, or the alcohol coursing through my veins, but I was now trying my TOOOL snake rake and the lock would not yield to my repeated attempts. There is something to be said for the fine machining and tolerances on these older locks.

I was done playing around, and took out a new Peterson short hook. It was SPP time. Raking is fun and all when trying to brute force a lock as fast as possible, but single pin picking requires finesse and skill. I think raking is like shooting deer with an AK-47 from ten feet. SPP is like shooting a deer with a .308 Remington from 300 yards.

A small pile of picks and wrenches was starting to accumulate on my desk. The hook didn't work. I was now trying a Peterson Gem with a red foam handle and a feather touch HPC double ended twist wrench. Normally that Peterson Gem only sees the insides of Medeco Keymark cylinders, but these were desperate times. Speaking of desperate times, why the hell did I pay $4.31 per gallon for premium gasoline today? Outrageous.

I had to put it down for a minute. It must weigh at least two or three pounds. I also had to try a key, something just wasn't right. But of course, the keys worked very smoothly with almost no effort. My pick-fu was not tight this evening. I released the tension wrench and heard all seven key pins click inside the lock.

The clock's hands advanced at a steady pace, and the Late Show had turned into the Late Late show. I was very impressed with this lock. It looks like it was made yesterday, but sports the classic BEST oval logo, as does the core. For anyone who thinks only the Germans and Japanese make things to stringent standards, this padlock has reassured me that Americans still make a good product. Or at least they did when this was made.

I broke out the TOOOL Falle clones. God they're beautiful, but my frustration with this lock had turned my soft touch into heavy handed attempts, nearly bending one end of the pick in a nice curve. Ten different picks now lay on the desk, neatly arranged next to four different wrenches. OK, that's a lie, they're not neatly arranged; it was a pile of entropy. The Falle clones didn't work by the way, and I reached to the shelf for a secret weapon. A friend asked me to get him some Peterson picks and I had offered to polish them up to get rid of any burrs or sharp edges. These picks have been wet sanded with 1000 grit paper. They are a superior weapon ready for battle. Another hour passed as I tried every pick in the set, but the padlock would not open. It was late, and I had met a formidable adversary. I hung this Best padlock, the largest I had ever seen, back on the peg board, between the ASSA Ruko 2 and the American 748 Shrouded. Another day my friend, another day.

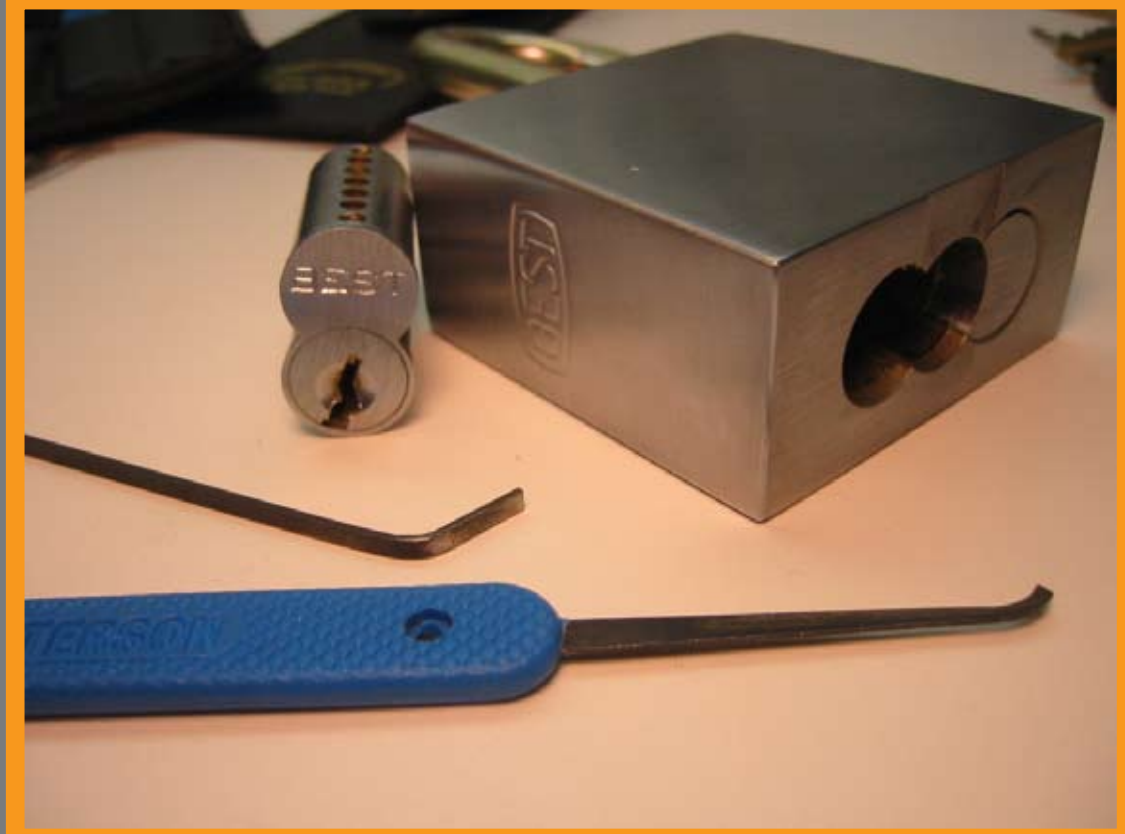
Another day my friend, another day...

Next Time in NDE

RoboKey System broken down & explained. Plus an interview with inventor John Laughlin & information on their new open source goals

High security one-two punch: Drumm Geminy Shield mounted on an Abloy Protec. Did we strike it rich? No! We borrowed it from Han Fey!

How the Kwikset Smartkey came to be. We will speak with Walt Strader, VP for Kwikset R&D about the history & their second generation.



Keep picking, my friends...