#2

NDE

Medeco Breakdown

Springtime in Manitoba

Attention:
Motion Sensor Vulnerability

Losing your touch?
Try picking underwater!

AND MORE!

For Locksport

April 2008

Note from the Editor

After NDE was first released at Defcon 15 there was no doubt that that this publication was going to be a big hit in the locksporting community. If you haven't noticed, we haven't exactly have been keeping up with our monthly publishing deadlines as originally promised. I would like to assure everyone that NDE is not dead, and we are planning on publishing a little more often then at the current rate (every six months?). I am pleased to announce that as of recently, Mike Brewerton, John Naughton and I will be taking over most aspects of publication of this magazine. Of course Schuyler will remain involved as much as possible as Advisor and President of NDE. We are always looking for new content so feel free to submit an article for consideration. Thank you for reading.

Doug Farre
Editor In Chief

NDE Staff

Editor In Chief:
Doug Farre | doug@ndemag.com

Content and Webdesign:
John Naughton | john@ndemag.com
(aka JackNco)

Senior Editor:
Mike Brewerton | mike@ndemag.com

President and Public Relations:
Schuyler Towne | schuyler@ndemag.com

Writers and Other Staff:
Beyond
John Fraser
Mitch Capper
James Laird
Jon King
Josh Nekrep

Photography By:
Mitch Capper
Jeremy Lau

Digital Graphics By:
Safety Off
Schuyler Towne
Doug Farre

Thank you:
Brady Nock
Steve Pordon
Walter Kiczko

Table of Contents

Don't Forget....

Tell us how you like our magazine. This is a magazine for the community, by the community. Everyone appreciates feedback for their hard work, so please take a bit of time and let us know. Let us know at www.ndemag.com

Updates in the Community

Tobias to Release Recent Medeco Bypass

Marc Tobias has some exciting information to be released in June, regarding vulnerabilities in the Medeco M3, and possibly more. He and Matt Fiddler will be releasing details at HOPE and Defcon this summer. In a related topic, be sure to stay tuned because the next issue of NDE will feature some Medeco exploits from a member of our own Locksport community.

Mark Your Calendars

2008 Dutch Open Announced

Barry Wels and our friends over at TOOOL sent word that the dates for the next Dutch Open have been set. This year the Open will be held in October to offer visitors a unique opportunity, as the Essen Security Show will take place right before the Open begins. The physical security show is one of the largest on the planet, and it is a great experience for returning and first time visitors alike. The full schedule (including the Security Show) is:

October 8(Wednesday)- 20:00-23:00 visit the regular Toool meeting in Amsterdam
October 9(Thursday)- Wake up early and visit the security show in Essen. In the evening drive to Sneek. (people not attending Essen can go directly to Sneek)
October 10 (Friday)- Presentations and workshops.
October 11(Saturday) - Championships (lockpicking, impressioning, combo manipulation (?)) Champions are honored at the 'Dutch Open party' later that evening.
October 12(Sunday) - Final presentations and the end of the event.

As you can see they also added an extra day for presentations which means they have more room for speakers and workshops. There is a current call for papers which has a deadline of July 20, 2008. There is already one world class speaker who will be presenting, so submit soon to get your presentation or topic in!

The Dutch Open is a great event where security experts and lock pickers around the world come together in Sneek (The Netherlands) to compete and share information. The number of seats is limited to 100 and is on a first come first served basis.

For more details or to contact Toool please see:
http://www.toool.nl/blackbag/?p=176

- Mitch Capper

2600's Last HOPE Conference

The last HOPE (Hackers on the Planet Earth) will take place on July 18, 19, and 20 at the Hotel Pennsylvania in New York City. Locksport International hopes to have a strong presence there, at what may be the final HOPE conference. In addition, TOOOL.US plans to continue to help by provide the Lockpicking Village. Conference attendance is $75 per person. More information can be found at www.thelasthope.org.

Defcon 16

The biggest wildest hacker con takes place on August 8th - 10 in Las Vegas at the Riviera Hotel and Casino. TOOOL.US will be there with the usual, also the Longhorn Lockpicking club will be visiting the conference for the first time, planning to help run some of the events. Special room rates are available for $98 a night, conference attendance is $125 per person. Stay tuned, big plans are in the making.

Security Awareness:

Motion Sensor Vulnerability

By Beyond

Motion sensors, or motion detectors, are popular additions to any access control or security related project. These devices have an electronic sensor that detects changes in motion within its line of sight. These lines of sight can be adjusted by the access control specialist to accommodate a small area, say three to five square feet directly below the sensor, to a much larger area depending on the capabilities of the motion sensor. They can be used as part of an alarm system to detect intruders and can also be used as a part of an access control system to trip relays and unlock a door for a person exiting a facility. When a motion sensor is used in this application, they are sometimes referred to as a "request to exit device" or as a "request to exit sensor." This article discusses a vulnerability that can result when they are used as part of an access control system.

The vulnerability is based on a premise upon which the majority of all access control/security solutions operate: that if you possessed the credentials to enter a secured area to begin with, you don't need to present them again to get out. They employ this by adding a motion detector near the inside of an exit doorway and tie that sensor into the system itself. As a person leaves they will trip the motion sensor, which in turn activates a relay, momentarily unlocking an electric locking device and allowing the person to exit. The reason this creates a vulnerability is because it is often very easy to trip the motion sensor from the outside of the door, and many technicians don't adjust the motion detector to account for this. The sad fact of the matter is that standard settings are not always appropriate for every installation. Any object can be used to trigger the motion detector as long as it comes into its line of sight, therefore unlocking the door.

Exploiting the vulnerability can vary with each situation, requiring a unique approach. Many times it will not even be possible given the location's hardware, but more often than not the vulnerability can be made possible with ample willpower and determination. How do you go about setting off one of these motion sensors? Any motion, of course, but it

doesn't have to be your motion. It can be the motion of any object fitted through a gap, as long as is able to move in the sensor's line of sight.

Many commercial facilities use double glass doors which, despite many tolerances being measured to the thousandth of an inch, are still susceptible to having a piece of paper penetrate their meeting point. This paper is more than enough to trigger the motion detector and allow entry. Other physical factors can allow for this vulnerability to occur, so don't think you need two double doors for

this to work. Mail slots, peep holes and just about any other access points incorporated into the door or its surroundings can be capitalized upon to allow this vulnerability to work. Old, sagging doors and worn weather stripping can create small gaps big enough to stick a small object through and trigger the motion detector. Improperly installed hardware can also leave large gaps through which an object can be passed.

Normally, this vulnerability should only work during business hours because the motion detector/relay should be turned off after hours since no one should be there in the first place, and a fire alarm would be handled via another device. However, since most access control techs aren't trained as well as they should be, they will often not set restrictions in the system's software. This makes the vulnerability even more rampant, sometimes allowing the vulnerability to continue to work outside of business hours. To their defense, it is often a tough compromise between functionality and security. You have to account for people approaching the door at weird angles and other random scenarios to make sure the system works appropriately. At the same time, you can't be too liberal or your system will be flawed.

The factors that go into customizing an access control system for the users' specific needs can either help this vulnerability work flawlessly or shut it down completely. Access control/security technicians need to be made aware of this vulnerability so they can prevent it. While its existence is common knowledge amongst many in the business, it is unknown to others, and this needs to change.

Up and Coming:
A look inside the International Hardware Fair

Completely Stainless Steel Lock

Stainless Steel Cylinder (Profile): Every part of cylinder is made out of 100-percent stainless steel, from the housing to the roller. They are anti-rust, durable, and provide high security (anti-drill).

Luen Hing Metal Manufactory
Hong Kong
info@luenhingmetal.com

Key Programming For Commercial Vehicles

From the mid 1990's passenger vehicles have been fitted with transponder immobiliser systems, which have increased considerably in complexity over the past 12 years. Originally, if a customer needed additional or replacement keys / remotes they would have no option but to go to the franchised dealer, which could be expensive and inconvienient. In 2000, Advanced Diagnostics developed key programming equipment, allowing independent workshops and locksmiths to offer a service to customers who needed additional or replacement keys / remotes. Transponder technology is also fitted to commercial vehicles and until now, the franchised dealer was the only option the owner had.

Advanced Diagnostics have launched the latest development for key programming, aimed at the commercial vehicle market. The "AD100Pro Truck" will be capable of programming keys for both 12v and 24v immobiliser systems on all-makes of vehicles. The unit is a flexible and portable, hand held tester, designed for anyone involved in Vehicle Immobiliser Systems, Transponder keys, Key Cutting and programming. Product functions: Reads diagnostic trouble codes (dtc), clears diagnostic trouble codes, reads immobiliser identification's, clears rCUansponder key memory, programs new transponder keys into ecuECUg andram's new remote keys. Product features: Fast update speed, USB PC interface, Vehicle diagnostic cables, Large LCD touch screen display, Standard & Beta Software on your unit at the same time, Large memory, Enhanced language capability (certain markets), Enhanced security, Internet updates.

Advanced Diagnostics Ltd
Nuneaton
Nordirland UK
shaun@advanced-diagnostics.co.uk

Up and Coming: New Master Lock® Combination Padlock

Sneak preview of the soon to be released article by Michael Huebler (a.k.a mh) about this fascinating new padlock. Look for his publication on www.toool.nl in the near future!

This is a combination lock with a new and unique user interface: Instead of turning a wheel to certain numbers, a knob has to be moved on two axes – Up, Down, Left or Right – in a sequence, quite similar to a game console joystick.

The combination sequence can be reprogrammed by the user, and it can have any length.

To start, the user pushes the shackle into the lock – this clears the combination inside the lock – and then the user has to move the knob in the correct sequence. The original factory combination is [Up, Down, Left, Right].

Once the combination has been entered correctly, the shackle can be pulled out.

Manitoba in the spring is what lockpicking is really about. As the great Canadian prairies begin to shake off the chill of winter one can almost feel the relief that radiates, much like the new sun, through the hearts of those simple prairie people. As new life springs forth in every nook and cranny Manitobans begin to yawn and stretch, reviving themselves from yet another winter hibernation. And despite all this hustle and bustle, a young boy sits perched over a workbench covered in carbon steel dust as he grinds out a new set of summer pick tools.

"They'll think I'm so cool!" he quietly rejoices, thinking about how he'll be showered with praise this summer at Grand Beach. "When they see I can pick locks, that will make me cool."

The boy, not quite like most his age, had spent the cold winter months buried deep in the archives of Lockpicking101.com, a website that first sparked his interest in this exhilarating hobby they called "Locksport" - not that he really knew who "they" were, exactly, though they mostly seemed like decent people. He had poured over post after post, devouring every speck of information on the subject he could find. He had learned all about things they called sidebar locks, single pin picking, raking, and impressioning. He had even developed the rather snobbish attitude toward something called bumping that seemed to be shared by much of the community. "Bumping! Pffftht! That's for babies and criminals" he had declared to his parents over dinner the night before. They smiled and pretended to understand what he was talking about, though he knew that they didn't.

His parents had been a little uneasy with his new hobby at first. If he was willing to be honest with himself, he could understand why. But that didn't make him like it any more. They did come around - eventually. Perhaps it was all the time and effort he had been putting in at the workbench. Maybe it was that they finally realized that he was responsible. The truth he wouldn't understand for many years to come was that they were just happy that he was doing something at home

where they knew he was safe rather than 'out there' with who knows what kind of people.

And so as the months of spring dragged on he got more and more restless, eager to showcase his talents for the pretty girls in their first bikinis at the beach this summer. He just knew that he'd be a hit. He practiced regularly until he could easily open just about any lock he could get his hands on - not that he had access to any of the really cool locks. But he was content with his progress. Actually, he was pretty proud. Yup. Those girls would be all over him.

On June 30th, just two days after school was officially over, his parents loaded up the pop-up trailer and corralled the family into the back of the Dodge Caravan that he hated terribly. But today it wasn't really so bad. For today marked the first day of his incredible summer. Within an hour they'd be pulling up to their summer-long camp site at Grand Beach. His little sister would bother him much of the way out but today he didn't really mind. Today he was ready for anything.

They pulled in to the site shortly after and began the long and painful process of unpacking and setting up camp. His dad set off to start the camp fire that would cook their first summer camping meal. He watched with great amusement as his father made a semi-feeble attempt at playing Boy Scout. After several minutes of blowing on a pile of twigs and dead grass he finally stood up and stretched, proclaiming that it was, in no uncertain terms, entirely too wet to start a fire. The boy thought about going over and helping his dad, but realized that he couldn't possibly win on that one. Either he'd fail too and feel foolish, or he'd succeed and make his dad look foolish. Either way, he had a whole summer ahead of him and there wasn't any sense in starting it off on a bad note. Instead he offered to go fill up a water jug for his mom.

As he strolled down the path toward the old Artesian well he kept a close eye on each camp site he passed. Any one of these tents or trailers could contain the prize he hoped to claim this summer - the girl of his dreams. Having not found her by the time he reached the well he grumbled something under his breath and began to fill the 20-liter jug. Once it was full he lifted it up and gasped at the sudden weight. He set it back down carefully, only then realizing just how heavy 20 liters of water can be. He poured some of it out and put the cap back on, once again lifting it. It was still heavy, but he was determined that he wouldn't pour out any more of it. He hoisted the jug up onto his shoulder and began the long and unsteady walk back down the path to his camp site.

As he was coming up to the last rounded corner on the path his foot slipped off the path, only for a moment, but it was enough to set him off balance. Heshrieked as he stumbled sideways and lost control of the jug. It launched itself from his shoulder and began rolling across the grass in front of him. Just then he heard a high-pitched laughter emanating from behind him. Who would dare laugh at his misfortune, he thought as he spun around, a scowl already forming on his face. And as he turned about his breath caught in his chest. There before him was, quite possibly, the most beautiful girl he'd ever seen.

"Are you ok?" she asked, though it was clear by her expression that she was less concerned with his well being than she was elated to have seen him fumble in the first place.

"I... I'm fine" he stammered.

"My name's Jen" she said.

This was it! He knew it! This was his moment.

"I'm Doug" he barely got out in the whispered, cracking voice of the only barely post-pubescent

teen he was.

"Do you need a hand?" she asked?

He took a deep breath and steadied himself for what was to come next. "No, I'll be ok. I just didn't see that rut." He tried to sound as manly as he could but knew he'd failed miserably. He walked over to retrieve the water jug knowing he'd probably just blown it. Much to his surprise she continued.

"So you out here all summer too?" she asked, and inside his heart lit up. She was interested! And so it continued with the meaningless small talk for the next several minutes. They talked about what schools they each went to, how much they hated sleeping in a trailer, how much they looked forward to spending hours at the beach. Until finally the discussion turned to other interests.

"I pick locks." he said with great enthusiasm.

"Oh", she paused, "that's kinda creepy".

His heart sank. Within the next few minutes he tried to explain why, tried to get her to understand what was so cool about lock picking, tried in vain to win her heart. But it was no use. The minute the words had left his mouth he knew that he was finished. How could it have gone so wrong? He was absolutely sure that his ninja-like skills would be a hit with the ladies. Within a few minutes she had excused herself saying "Maybe I'll see you around sometime".

He didn't see much of her that summer. He had bumped into her once on the beach while she was with some friends. She let out a quick "Hi" and carried on her way. As she got several feet away he could hear her snickering with her girlish friends.

As he sat by the campfire one late August night, a Group 1 Schlage in his hand and a short hook prodding mindlessly away at the pins, he came to realize something. Picking locks is really much like Manitoba in the spring. He had spent so much time waiting with great anticipation for the glorious summer that he totally overlooked the process of learning itself. He missed the spring. He'd heard the line before 'It's not the destination, but the journey' and now he was starting to understand that.

He sipped some more hot chocolate and set the lock down for a break, content in the moment of new understanding. It's really just about picking locks.

As the night stretched on he thought about the cold months to come and knew that he'd be just fine.

Makeup and Breakup of a Medeco Biaxial Lock

- By John Fraser | (aka Unbreakable)

Introduction

In this article, I will discuss the Medeco Biaxial high security lock. Medeco biaxial is one of the most well known and used high security locks in North America. It combines a normal pin tumbler lock with a rotating pin and sidebar design. This concept was first developed by the Mechanical Development Company (Medeco) in 1968. Medeco is currently an Assa Abloy group company.

Here you can see a mortise Medeco 51s Biaxial lock with a brass finish and a Z keyway. This is the lock I will be breaking down, picking, and making a cutaway out of. Medeco locks are available as rim, mortise, interchangeable core, key in knob, cam, and switch locks. Medeco locks, depending on their type, are available in 4, 5, 6, and 7 pin models.

The External Parts

The face of the lock is clearly stamped with the Medeco name and symbol. In the lower left there is the 51s stamp, indicating the lock is 51s series lock, and below that there is a UL stamp to indicate the lock is UL certified.

Looking at the back of the lock all you can see is a stamp, and a cam. The cam interacts with the other parts of the lock to retract the bolt or latch in the door.

One excellent feature of the Medeco locks is that instead of using standard sheet metal slide on pin covers, which are easy to bend and ruin, Medeco uses a small hex socket screw. The covers are easily removed with a 5/64" Allen wrench.

Fig. 1- Face of Medeco 51s lock with Z keyway

Fig. 2- Rear of Medeco Biaxial lock showing the cam and cover

Fig. 3. Top of Medeco Biaxial lock showing the removable pin covers

In order for a key to open a Medeco lock, it must fit the keyway, have the right depth cuts, and the right angular cuts. Most Medeco keys have a square head, with an eagle on them, as well as the patent number, the Medeco name, and "RESTRICTED DO NOT DUPLICATE" stamped on them. The key has six depths available for each pin, and the angles on the key are either center, 20° left, or 20° right. The angle in the valley of the key, where the key touches, is 86°. Medeco locks can be masterkeyed; however the master key must have the same angular cuts as the operating key, and every other lock in the system it operates.

Fig. 4- Medeco Biaxial key.


Fig. 5- Medeco keys, showing the different cut angles on the keys

Medeco also uses key tags or keycards with their locks. The key tag or card has the information needed to duplicate the key. Medeco originally used key tags, but they have since moved to credit card sized cards with all the information needed to duplicate the key on them. This also works as protection against illegal key copying, and is explained in the "Key Control" section.

Key Control

Medeco values key control very highly. Their locks are available in four distinct levels of key control.

Fig. 6- Medeco key tag, with information on it used to duplicate keys

Starting with the lowest level, Medeco's signature program is for customers who are not very concerned with key control. In order to get additional keys made, customers simply have to go to the locksmith from whom they obtained the lock, and they can then have additional keys made. Due to the keys used for the signature program being widely available, keys could be copied by unauthorized people. Level I uses the AIR keyways.

The card program is for customers looking for more key control than the signature program offers. With their new lock and keys, customers are issued a key card. The customer then signs this card after receiving it. In order to copy a card on the card program, the locksmith needs the card that contains the control data. The locksmith must also verify that the customer's signature matches that on the card. Level II uses SKY keyways, which offer a higher level of protection than the AIR keyway.

Contract restricted key control is for businesses that are looking for a special keyway. After entering into a contract with Medeco, they are assigned a special keyway. Once they are assigned this keyway, they can only obtain new keys through a Medeco factory, after having proven their identity. Keys are never distributed to distributors.

The factory program offers the most key control possible. Keys are factory restricted, and are only available to that customer. Key blanks are never sold or distributed. The keys for these locks came precut, and each key in a set is also identified by number, for example 1 of 4, or 3 of 7.

The Internal Parts

The plug is made of brass, and it contains four hardened steel anti-drilling rods. Three of these are at the top of the keyway, and they are to keep someone from drilling out the bottom pins in the lock. The fourth is on the right hand side of the lock, at the 3'oclock position. This is to prevent drilling of the sidebar. Although drilling is possible, these hardened steel rods make it very difficult to drill out the lock in a short period of time.

Fig. 7- Top view of plug, showing hardened anti-drill rods and pin chambers

Fig. 8- Side view of plug, showing sidebar hole and slots, and one hardened rod

The lock also contains two hardened crescents. This is to prevent the top pins in the lock from being drilled, as well as to keep the sidebar from being drilled. These crescents are located at the 12 o'clock and 3'oclock positions in the lock. They are nested in the cylinder itself, and they are removable.

Fig. 9- Hardened crescents.

Fig. 10- Crescent's position in cylinder

At the front of the sidebar, there is a hardened ball bearing, also to thwart drilling attempts. The tiny sidebar springs force the sidebar out of the pins grooves when the sidebar is in line with the sidebar groove in the side of the cylinder. The sidebar fingers fit into the slots in the key pins.

The Medeco biaxial key pins (bottom pins) are made of nickel plated CDA340 hard brass. They are available in six different sizes As you can see from looking at the pictures below, each pin has a long chisel face and a short chisel face. Pins also have a sidebar slot, as well as a 0.015" flat at the bottom of the pin, which is offset 0.031" to the left or the right of the centerline of the pin. Each pin has a 0.135" diameter, which is 0.020" larger than the standard pins in a pin tumbler lock. Each pin also has a slot cut in the side of it. The angle may be 0° center, 20° left, or 20° right. These angles are in relation to the tang, or locater tab on the pin, which is located along the true centerline of the pin.

Fig. 11- Sidebar, with springs and hardened ball bearing

Fig. 12- View of a pin stack

Fig. 13- Side view of pin showing long and short chisel face

There are 6 types of Medeco biaxial pins, and they are K, B, Q, M, D, S. While there are only three angles available (20° left, 0° center, or 20° right), there are six pins, each of which is available in 6 heights. Each angle may be a fore or aft pin. Fore pins have the long chisel face to the right, and the chisel point offset 0.031" to the left of the centerline, whereas aft pins will have the long chisel face to the left, and the chisel point offset 0.031" to the right. K, B, and Q are all fore pins, and M, D, and S pins are all aft pins. These pins have excellent wear resistance, because only the sides of the pins touch the key, and the small flat never contacts the key. The wear is spread out over a large area, instead of being focused on a small point. This, combined with the use of hardened brass, leads to excellent wear resistance.

Fig. 14- The six different types of pins.

Each of these pins is available in six lengths

Each key pin also contains a small tang, or locator tab. This locator pin fits into a groove in the pin chambers in the plug, and in the bible of the lock. The purpose of the locator pin is to keep the pins from over rotating. If a pin were to complete a 180° turn, then it would lineup with the key, but the sidebar slot would be on the wrong side of the lock, and you would be unable to open the lock. The pin also contains a steel pin. Not only is this pin hard to drill thru, but they are all different weights. This throws off the weight of the pin, and makes one particular method of decoding impossible.

Also, each key pin contains a shallow sidebar slot, to discourage and further frustrate picking attempts. If the sidebar lines up with this slot, it can only retract part way, and therefore the lock cannot open.

Fig. 15- Top view of a pin. The tang is the protrusion on the left hand side. The indent roughly opposite it is the sidebar slot. The center circle is a steel pin.

The driver pins (top pins) usually contain at least one mushroom pin. Many locks contain two or three of these mushroom security pins. These pins also frustrate picking attempts. Some locks, such as mine, may also contain a hardened steel pin, which is located in the pin stack closest to the face of the lock. This is to making drilling difficult. Not only is the steel hard to drill through, but a drill bit will spin it around without cutting into it.

Fig. 16- Side view of a pin. The true sidebar slot is on the left, the false one is one the right.

The cylinder itself is made from brass, and is different from normal pin tumbler locks in four main ways. One is the slot milled down the side for the sidebar, and the other is the groove for the locator tab in the bible of the lock (where the pins go). The two other differences are the screw in pin covers, and the holes for the hardened crescents. All of these are shown in figures 3, 7, and 10.

Operation

To open a Medeco Biaxial lock, the user must insert the correct key into the lock. The correct key will fit the keyway, and it will have the right cut depths and angle cuts. If the key fits the keyway, and has the right cut depths, then it will raise all of the pins to the correct height. This will raise all of the pins to the shearline. When the user turns the key, the sidebar is forced into the pins. If the correct key is used, the slots will line up and the plug will turn freely. If the wrong key is inserted, then the sidebar will be unable to fit into the slots, and the plug will be unable to turn, since the sidebar is blocking its rotation.

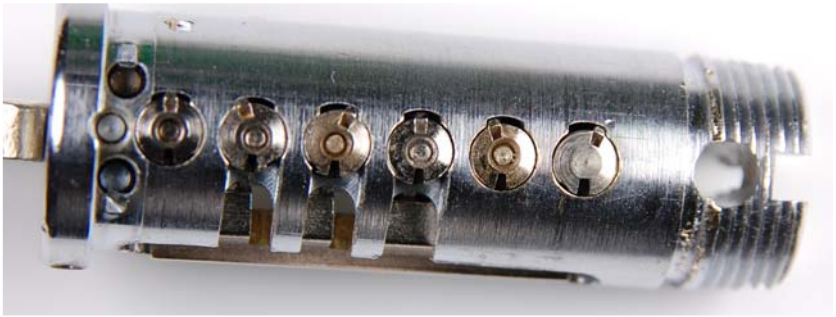


Fig. 17- Medeco Plug, with the correct key inserted.

Coming Next Issue: How to pick a Biaxial Lock!

Picking Your Way to the Surface

Doug Farre

I wondered how today's lockpicking was going to be different than any normal day of picking. On Mondays and Wednesdays I help teach a beginner scuba course at the University of Texas at Austin, and today one of the students brought an underwater camera with him to class. I figured I couldn't pass up the opportunity to throw a few locks in the indoor pool after class and give it a shot. When you're a lock picker and a scuba diver, it only makes sense to do both at the same time, right?

I had a decision to make, this wasn't a locksport meeting where we just dump our supplies everywhere and hope they make it back in our possession at the end of the evening; this was going to be a tactical underwater demonstration of pure skill. At least I hoped so. I laid out a large knapsack full of tools. I had pick guns, bump keys of all flavors, every pick in the book and numerous other tools. Choosing some of my favorites, I put together a small set of tools that would fit nicely in the cummerbund of the buoyancy control pocket on my diving gear. I decided on an HPC emergency set and a short hook. In addition, I had a few theories about bumping locks underwater that needed to be tested, so I brought along a Masterlock bump key.

Excitement was flowing through my veins. All my tools were lying out by the pool deck, and I even got in a quick lesson to some of the onlookers before class started. The head of the scuba program at the University, Peter Oliver, had previously showed interest in picking locks and, to my surprise, had already read the L.I Guide to Lockpicking. I gave him a five piece set and he managed to open a four pin padlock on his first try.

I chose a rustproof Masterlock #3, a brass Pacific Padlock, a brass Masterlock #175, and an Ilco five pin rim cylinder. I started to think to myself, "these locks are pretty easy, I hope no one looks at these choices and questions my picking ability." I just want to assure everyone, that I chose these locks for sake of demonstration. I mean, what if I ran out of air while I was decoding a Medeco Biaxial with wension wrench and a hookater that could be life threatening!

As class came toward an end I could feel my anticipation rising. Eventually, I couldn't wait any longer and snuck away from the group to begin my adventure. I descended slowly to the bottom with a bag full of locks, and my cummerbund pocket full of picks. Inhale…1 2 3 4 5…exhale…1 2 3 4 5… Relaxation is the ultimate goal of scuba diving. Underwater, you are totally at peace, all you hear is the noise of your breathing and the low churning of the filter pumps.

I laid all my tools down and took the locks out of their bag. Water rushed through them like an empty pipe, and bubbles rose towards the surface. I took my regulator out of my mouth and placed a Masterlock up to my ear and shook; nothing. I didn't hear the normal sound of ill

manufactured components clacking against each other. I don't know why I did that, it just seems like something I normally do to a lock. First step listen, next step feel.

Putting my regulator back in, I took out my short hook pick and tension wrench and went for the Masterlock. Still ultimately relaxed, I move the tools in the keyway. First pin, second pin, third pin… pop! Too easy, or was it? It was just a Masterlock I tell myself…

I am a very high energy, high strung person. I am mostly violent with my picks, bending and breaking them on a regular basis. Having a high energy personality leaves little room for patience, so you can imagine how picking locks may be somewhat frustrating for me, unless I find a nice state of relaxation. This is unfortunate, however, because relaxation is a state that is fairly hard for me to find.

The student with the camera was still in class, so I kept practicing. I grabbed the Pacific and took a deep breath. Inhale…1 2 3 4 5…exhale…1 2 3 4 5... I moved the tools in the keyway, and felt the first pin, then the second, then pop! It was a record. That Pacific and I were one. We were like salt and pepper… peanut butter and jelly... yin and yang. I was intensely focused like I had never been before. I was just me, the lock, and my breathing. It seemed nothing could hold me back. I grabbed the Ilco next and of course it was the same thing! Pop! I was feeling great. I tried the 175 bypass and yes, of course it worked underwater.

Bump keys underwater? Well, as you might have guessed, it didn't work. I'll try again another time with higher quality locks, but there is no doubting the fact that the friction caused by the water in the pin housing prevents the phenomenon that normally allows creating a gap at the shear.

Then I see Jeremy, one of my students, swim over to me with his underwater camera. I had already relocked all the locks before he approached, knowing that I should be able to impress him and the camera (considering my previous success). I picked up the Pacific, and began my attempt.

"Hmm," I thought to myself, "something isn't right here."

I couldn't get the lock open. I knew something had to be wrong with the lock. I moved on to the Master, and finally the Ilco. Nothing! I couldn't open a single lock. Jeremy remained hovering over me taking pictures of my failed attempts. I imagined that Jeremy was secretly laughing at me, shielded behind all the scuba gear. I just wanted to tell him "Man I swear, I just had them all open!" Although I doubt he cared very much.

I told myself the "locks must be getting cold", or "the temperature was be changing the spring tension", and even "maybe they have already started to rust?" Irrational thought is a symptom of nitrogen narcosis, a serious medical problem scuba divers may experience when too much nitrogen builds up in the blood stream after staying too long at depth. However this wasn't nitrogen narcosis. My irrational though was due to something completely different.

I took a deep breath. Inhale…1 2 3 4 5…exhale…1 2 3 4 5… Then the Ilco fell open in my hands.

Stage fright? Impossible! I suddenly realized that I had been breathing much faster after Jeremy came over and began taking pictures. I was also was thinking about how the pictures are going to look, and how much time I had left before I had to get out of the pool. I was no longer

experiencing the Zen like concentration levels that I had previously described. That was why my locks wouldn't open!

I heard the alarm go off, time to get out of the pool.

As I finished up the rest of my responsibilities at the pool and walked to my car I realized that I had come across a revelation today. For me, the revelation was that being at the bottom of a pool, isolated from the world, made me a good lock picker (as long as no one was watching). But more importantly, as cliché as this may sound, in order to be a successful picker, you must find that special connection between you and your tools. You must find the situation where locks will fly open for you on cue, with the softest touch, and the slightest effort. The situation where you find yourself opening everything you have in your collection, and wishing you had more.

With this epiphany in my heart, I finally reached my car, and what I saw my made my heart sink. I discovered a large orange boot on my front wheel due to unpaid parking fines. Securing the boot to my wheel was a large American padlock. I thought to myself, If only I could get my car to the bottom of the pool…

A note from the President:

I hope Doug doesn't screw this up. You know, like I did. I was talking to Doug the other day and told him that I have made a lot of mistakes in the way I handled NDE, but I was sure that passing it off to him was one of the best decisions I could have made.

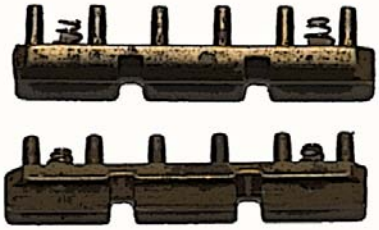
It's strange though. I wonder if this is what it's like to watch your child go to their first day of school. Seeing NDE in someone else's hands. No matter how capable they are, no matter how poor a job you've done up until that point, it's still hard to take that leap of faith and trust someone else to take care of your baby.

I think he'll do it though. He has John, too, who was always champing at the bit for more material from me. Always ready to take a new leap with the website and line up more content. And Mike, who has been wanting on board since it became obvious I was letting the ship sink months ago. I'm glad he was patient enough to join us now.

I'm proud of what they've created in this second offering from NDE and shocked at what is on the horizon. Readers, you are in good hands.

- Schuyler Towne

An Introduction to:



BiLocks

- By James Laird (a.k.a. JHL)

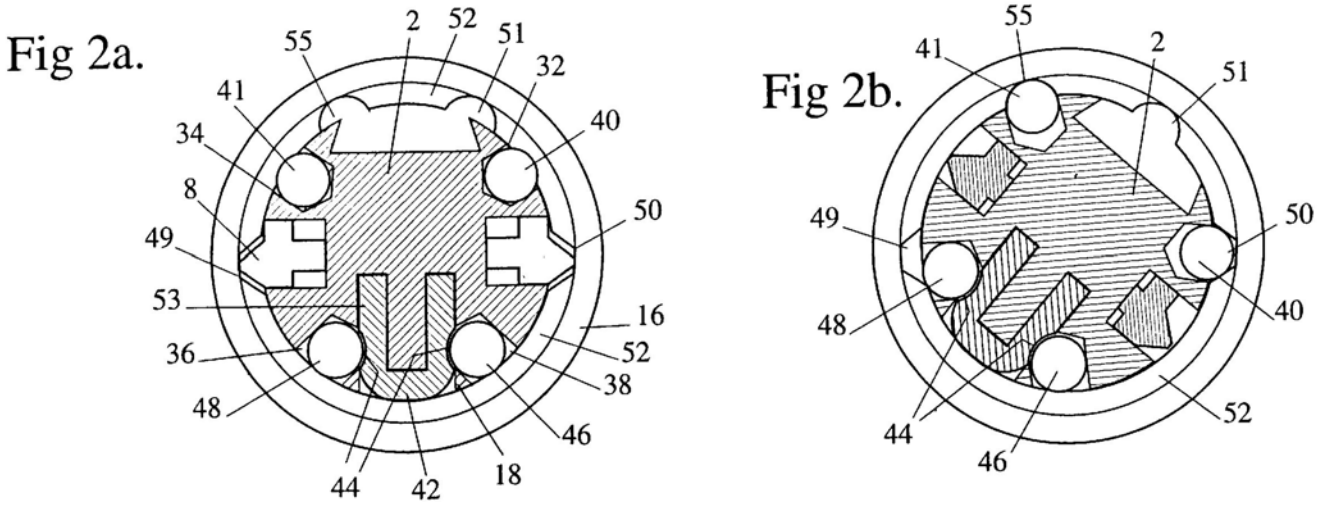
The BiLock Maximum Security Locking System was invented by Australian locksmith Brian Preddey and first patented in 1982. [FN: 4,478,061] This unusual sidebar lock has since become widely used, and has a reputation for being impossible to pick. It is especially popular in Australian institutional, vending and commercial markets.

The first thing you might notice is BiLock's distinctive U-shaped key. They're also pretty bulky, given that normal BiLocks are six pins deep, for a total of twelve pins. However, this is not just a two-row traditional pin tumbler; there is no shear line in this lock. Instead, each side of the plug holds a beveled sidebar. These protrude into matching grooves in the shell when locked, and are held outwards by spring tension. Each sidebar has six fingers that extend through the plug to the pin chambers. All the pins are the same height; what makes them differ is that each has a small hole drilled into its side at one of four different levels. When the key is inserted, all of the pins are lifted to various heights. The correct key lifts the pins so the hole in each pin is level with the sidebar fingers. Then, when the key is turned, the sidebars are able to move inwards as all the fingers enter the holes in the pins, allowing the sidebars to retract and the plug to turn. If any pin is at the wrong height, the corresponding finger will have no hole to move into, and the sidebar will not retract and will block rotation.

So what, you say? The design sounds complex, but easy to pick. It should be easy to feel those holes as you move pins, right? Well, it is, and that's where the main security measure comes in: false holes. Every pin (ignoring mastering for now) has a second, shallow hole drilled in it. This hole is deep enough to allow the pin to set, under sidebar pressure; however, it is far too shallow to allow the sidebar finger to fully enter the pin, and the lock will not turn. These are roughly equivalent to false gates on Abloy locks or the false sidebar grooves found on some Medeco pins.

BiLock pins may be masterkeyed by making two full-depth holes, and these master pins do not have false holes. The blank originally comes in an L shape, and is bent to a U after cutting. Naturally, lots of custom keyway profiles are available, and interchangeable face plates are present on many BiLocks.

A rather clever innovation is the BiLock QCC, or Quick Change Core. This differs from most other quick-change systems in that the plug and sidebars form the entire core; there is no separate shell. The sidebars are retained with punched edges, and four ball bearings are added to the design, protruding from the plug and into the shell. Two of these are fixed, at roughly 50 degrees to the left and right of the top of the plug. Two are movable, next to the keyway at the bottom. They are pushed outwards if a regular key is inserted into the keyway; a correctly dimpled key will allow them to be pushed fully into the plug. These bearings run in a circular groove in the shell, near the front. In normal operation they all simply run in the groove, and prevent the plug from coming out. However, when a quick-change dimpled key is inserted, the bottom bearings are able to enter the plug. At that point, rotating the key 40 degrees to the left or right then aligns the two top bearings, one with a sidebar groove and one with a special removal groove, allowing the plug to be simply pulled out. This is somewhat weak from a security perspective, as any key that opens the lock may be easily modified to



QCC core unlocking using a key with QCC cuts. (US Patent 6,076,386)

remove the core by drilling two dimples in the appropriate location.

QCC locks have the disadvantage that they are hard to disassemble and re-pin without a key. Without picking the lock, one viable method is to shim them: inserting a fairly thick metal shim (such as a cut and filed junior hacksaw blade) down the sidebar grooves from the back allows picking from back to front, with fairly good feedback about false and true holes. Some QCC locks may need drilling to reach the sidebar grooves as there may be blockers on the back preventing shim entry; although drilling in this way does not compromise the security of the lock in normal use.

As to the future of BiLock, in 2003 Brian Preddey filed a patent application for a tubular lock operating on similar principles to the BiLock, although no such locks have reached the marketplace. Another recent change in BiLock is the "Next Generation" key and 13th pin. This feature appears to add little to security, and acts mainly as an extension of patent protection for key duplication. It consists of a 13th pin, located at the centre front of the keyway, which must be pushed upwards to release the plug. A moving lever element in the key performs this task as it is pushed against the front of the plug. This extra pin does not appear to come in different sizes.

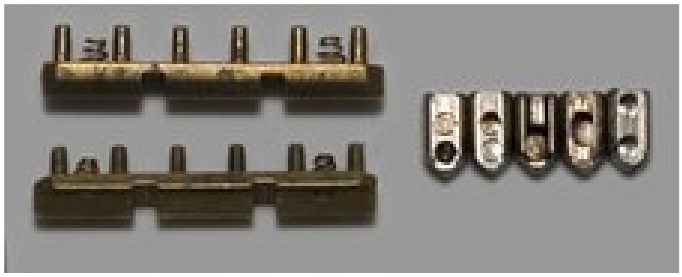
No lock is 100% secure, and BiLock is no exception. John Falle makes a decoder and make-up key system for these locks. The sidebar system certainly makes picking difficult, but not impossible. Despite the aforementioned weaknesses, overall the BiLock system offers a good level of security. BiLock keys are available only to registered dealers, who maintain their own keying systems and often their own profiles. Due to their mechanism, bumping them is impossible. The Falle decoder is only available to select government agencies so many do not feel it is a significant risk.

One final item I'd like to mention is also one of the reasons I wrote this article. I feel that a weakness exists in the design of this lock that may allow it to be decoded, picked and impressioned more easily than previously thought. It is not a major weakness, and although these locks will still be very difficult to bypass even with this knowledge, I have mixed feelings as to whether to publish this information in a future article. I'm curious as to how readers feel on this issue. Should I publicly release this information so people can be aware of the weaknesses in security equipment they buy? Or should I inform the manufacturer and allow them time to respond first? What do you think?

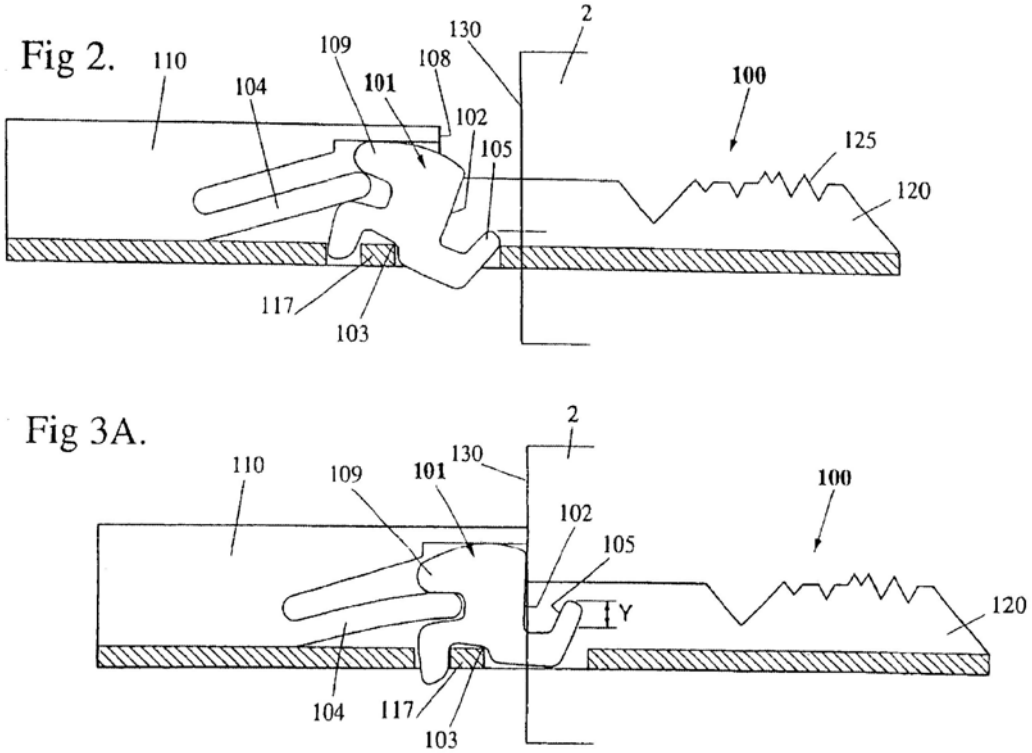
Regular (left) and QCC (right) Bilock plugs/cores.

Pictures Explained

QCC shell, showing the retaining and removal grooves



Sidebars and some pins. Right three pins are mastered.



Next Gen key, showing how it lifts a special pin on insertion. (US Patent 6,681,609).

Tell Us Your Thoughts!

Log onto www.NDEmag.com and tell us your thoughts. Post in the comments, or participate in our online polls. Do you have experience with this lock? Share your experiences, and contribute to NDE, we are always looking for new writers.

Next Month's Issue

Late April - Early May

- Interview with Chris, Ryan and Luke of TruTV's Tiger Team!

- An interesting new breakthough in Medeco locks.

- Jaakko Fagerlund releases his Abus Disk Exploit to the public.

- Longhorn Lockpickers tell their stories.

- Updates on big plans at Defcon and HOPE for this summer, start practicing now.

-And more!

We're Back