

#3

Non-Destructive Entry Magazine

Medecoder

ABUS Plus

Ingersoll

Tiger Team

And More!



MAY

FOR LOCKSPORT!

2008

Welcome

For Locksport!

I received a message the other night. It was Amanda, a friend of mine who has recently taken up lockpicking. She was complaining that the challenge lock I left at her house had pricked her with a metal splinter. I told her I was sorry, she simply replied:

“I HAVE BLED FOR LOCKSPORT!”

I have too actually, when I first tried to make my own picks. In fact, in an informal survey I found that 100% of NDE readers who were surveyed have bled for locksport. A staggering percentage! We give our blood to these locks and it's worth remembering what they give to us.

Locks provide us not just with physical safety, but with peace of mind. They are a staple of the civilized world. A lock says “someone owns this, it's not for you.” It's the dividing line between the public and the private. And for the lockpicker? A lock presents a challenge, a never-ending supply of new puzzles and as our hobby grows. Fueled as everything is now, by the internet, we see more collaboration, faster progress and ever more clever solutions to the problems the locks pose. However, there are new challenges that we should have seen coming. Specifically, how to disclose this information.

The trouble is, when we get excited at our discovery and bound off to tell as many people as we can, we are celebrating what a lock means for us, it's been conquered, the puzzle solved, the code deciphered. Unfortunately, in doing so we risk destroying what a lock means to the rest of society. We have the power to redraw the line between public and private.

To those who would contend that the only way to protect those people is to immediately and publicly expose the weaknesses in their locks, I hope this issue of NDE can provide you with some fresh insight. The lock industry is changing for the better. They are opening their doors and welcoming some interesting new perspectives. I am proud to see NDE carry these exciting new stories.

What happens when a lock manufacturer meets a lockpicker? Read on to find out.



Contents



The Tiger Team

by Doug Farre

Page 5



A New Day

by Josh Nekrep

Page 7



The Medecoder

Jon King's homebrewed
Medecoder & the response
from Medeco themselves

Page 9



Centerfold

Photo by Mike Brewerton

Page 18



ABUS Plus Exploit

Our interview with Jaakko
Fagerlund of Finland on his
remarkably simple attack

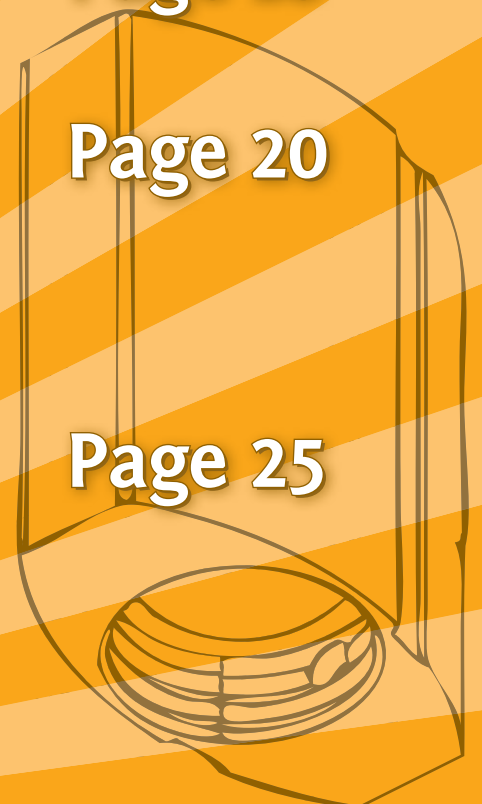
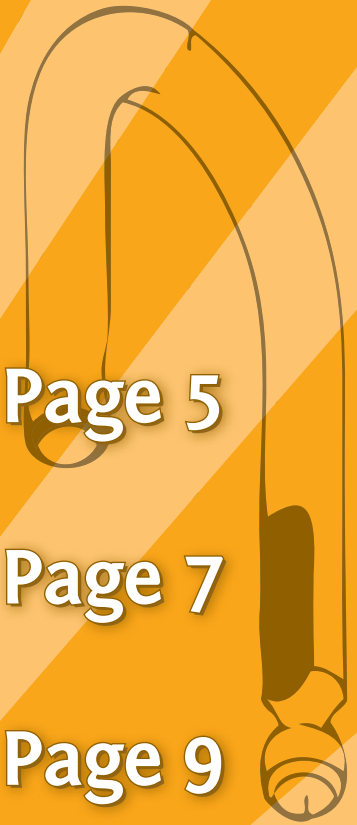
Page 20



Breaking Ingersoll

John Naughton's in-depth
first report on Ingersoll's
lever padlocks

Page 25



NDE Mag

Staff

Executive Editor
Managing Editor
Online Editor
Contributing Editor

Schuyler Towne
Mike Brewerton
John Naughton
Doug Farre

Writers:

Tiger Team
Open Letter
Medecoder
Ingersoll
A New Day
ABUS

Doug Farre
Peter Field
Jon King
John Naughton
Josh Nekrep
Schuyler Towne

Photography:

Tiger Team
Medeco Centerfold
ABUS Plus
Ingersoll

TruTv Promotional Material
Mike Brewerton
Jaakko Fagerlund
Adam Ferguson

Special Thanks:

Creator of this typeface: josbuivenga.demon.nl

Note: This pdf is best viewed in a “facing” page layout. To adjust this setting in Adobe Reader, click the “view” dropdown menu, select “page layout” then make sure that “facing” is checked.

ndemag.com
info@ndemag.com

Insecurity:

An interview with some of the nation's best known security experts.

Being a lock picker as well as a security and technical enthusiast, when I first heard about a new show on truTV (formerly CourtTV) called "Tiger Team" there was no doubt in my mind that this show was going to be awe-inspiring. It promised lock picking, hacking, and social engineering in each episode. Not to mention sneaking around at night, using the latest high tech toys, and recording every second of it for the world to watch. So if you're not excited at this point, you should be. The show is about a team with Chris Nickerson, Luke McOmie, and Ryan Jones, who are hired as Penetration Testers to test the physical, electronic, and procedural security of a target facility. Two episodes of "Tiger Team" aired on truTV December 25, 2007. Over 680,000 viewers tuned in to see the episodes that Christmas night, making it a very successful premier. As promised, the episodes were filled with lock picking, safe cracking, wireless network hacking, elaborate social manipulation scenarios, security system bypass, and tons of other stunts that made you think "Why didn't I think of that?" Personally, I was a bit hesitant at first. I kept thinking "How much of this was staged?" However, after watching the episodes four or five times, I began to realize how professional these guys really were. Chris, Luke, and Ryan are some of the best Penetration Testers out there. These are their stories.

Chris Nickerson (aka "Indi") Chris' story is by no means unique. Like most technology geeks, he started out young, breaking and fixing his parent's computers. As a teenager he began messing with the phone systems and running BBS's out of his house without his parent's knowledge. Sounds familiar, right? Chris went on to college and specialized in virology, although his main interest was partying. It didn't take him long to realize that he didn't like school very much, so he joined the military where he worked in intelligence. This is where it gets a little more exciting. After leaving the U.S. Army, he started to gain most of the major computer defense skills that he uses today. He worked at a law firm that defended the tobacco industry, and got his chops in virtual and physical security, as people constantly tried to hack their way in to gain insider knowledge on the case. After the case was over Chris left the law firm to become a Chief Security Air-Tech at Sprint for seven years, then to KPMD to begin his career as a penetration tester. He currently works at Alternative Technology (who bought out KMPD), in Denver Colorado where he is a Team Leader and a Senior Security Consultant. Chris has a fascinating personality. On the show, there is no doubt that he is the Team Leader. His ability to manipulate any social situation and extract the exact information he needs to accomplish his goal is flawless. He does this without the least bit of sympathy for the emotional tolls his broken promises may inflict upon those involved. An example of this can be seen in the episode "Car Dealership Takedown". Chris promised several employees of the dealership that he intended to purchase a half-million dollar car the following day. Chris explains to NDE, without a quiver of sympathy in his voice, how angry and hurt the salesmen were (and still are) when they discovered he was not really buying a car. Had I been in Chris' shoes I would have felt bad for the guy, but I imagine that as a professional you can't worry about such things.

Ryan (aka "Lizzie Borden") Ryan just might be my personal favorite, and if you've watched the premier episodes then you will understand why. This guy can only be described as a finger-print-dusting, lock picking, and safe cracking machine. He picks through locks under some very stressful conditions without even flinching. Like many others in this field, Ryan first discovered the hobby when he found

the MIT Guide to Lockpicking back in 1992. He described to us the perks of growing up in New Orleans after Mardi Gras, and the abundance of street sweeper bristles left behind that could be used for manufacturing lock picks. Although Ryan argues that his computer skills are also up to par, I had already heard what I wanted to hear. I mean, how often do you get to talk to a guy who gains entry by lock picking, sneaks around places at night, and professionally avoids tripping motion sensors and magnetic door alarms for a living? Although, we did manage to catch the following: Ryan started young, like Chris, with computers, phones, and the early days of the internet. He eventually decided to try college, where he made a semester long attempt to study computer science. He then started his career working for phone companies, and dot-coms, where he developed his interest in security. His next step was IBM where he did penetration testing and risk assessments, similar to what he continues to do today at Alternative Technology.

Luke (aka “Pyro”) Luke’s childhood was very similar to Ryan’s, and Chris’, finding his interest in computers at age 11, and never changing his hobby since. At 16 Luke was already doing hacker work in various groups and eventually began working for the government in addition to security consulting. He later attended college where he studied computer science for over three years, until he found himself expecting two children and was unable to finish. Eventually Luke found himself at KPMD where he met Chris and Ryan. He picked his first lock in August of 2002 at Defcon. He says “Everyone remembers the first lock they pick”, as he recalled the Master Lock cylinder that introduced him to his new hobby. Chris, Ryan, and Luke all joked about how their first marriages failed, due to their constant traveling, late nights, and heavy workloads. Chris and Ryan say they learned from their mistakes, but after Luke broke it off with his first wife, he was the only one to remarry, and it was with his rebound girl. Sorry Luke. Although the team doesn’t like to admit that they are individually better at any one skill, it was quite apparent to us that Luke has a way with computers. He pretty much said it himself when he told us that his favorite types of jobs were network incident response and black hat assessments.

It didn’t seem to upset Chris, Ryan, and Luke too much as they described how truTV has no more plans to continue the series after the premier episodes. I assume it was because of the conflicts they had while producing the episodes. They had nice things to say about truTV itself, but didn’t appreciate all the backroom politics associated with the production company on the project. Although truTV has stopped communicating with the team, other networks have showed interest in the show. In fact they are hoping the show will sell to another network so they can cover a deficiency of \$250,000 in production costs left over from the project. Post production for each episode of Tiger Team costs

around \$285,000. Chris, Ryan, and Luke said that although they had to take a pay cut from their normal jobs at Alternative Technology to do “Tiger Team” it was all worth it. They said they would look forward to doing it again if they had the opportunity.

Doug Farre
Contributing Editor,
NDE Magazine



ON THE JOB: THE CREW OF “TIGER TEAM,” READY TO ROLL OUT.

It's a New Day: Security Through Obscurity & the Locksmith Industry

It seems that everything changes over time, but the physical security industry has changed dramatically and it will never again be the same. For hundreds of years the locksmith trade has been one of precious secrets and knowledge, passed from journeyman to apprentice, from father to son. That was the old paradigm, or what some might even call “the good old days” of locksmithing. Today, anyone with access to the internet can discover “secrets” that were previously possessed by only a select and trusted few. The old paradigm no longer fits and it hasn't for many years. While some may wish to blame locksport, it has been this way for longer than locksport has existed. It is left to the professional locksmiths to grow and adapt to this new world and satisfy the needs of their customers.

In days of old, the “lock smith” was the one who actually made the locks. They worked hard to develop the best possible lock, carefully guarding their secrets. They truly aimed to create security for their customers. Since it was they who crafted the lock, it was they who knew every detail of it, details they certainly didn't want falling into the wrong hands. And so it was for generation after generation, and the system worked reasonably well.

Something changed though, and it wasn't the proliferation of the internet, where secrets are passed around more rapidly than a doobie at a Grateful Dead concert. No, it was much, much earlier than that. What changed? Locksmiths stopped making locks.

Indeed, it was this shift that changed the face of the industry. The role of the locksmith changed forever. They were no longer craftsman, they were knowledgeable experts. They were no longer builders and designers, they were installers and troubleshooters. The locksport community didn't do that to them. It wasn't even conceived of yet. It was the economy of mass production that irreversibly changed their role. It is not to say that locksmiths needed to know less. In fact, one could easily argue that they needed to know more, with the need to know about the wide variety of products and options available to the consumer. Locksmiths continued to serve a vital role in society, but that role had changed.

So what's the problem? The problem was, and in many cases continues to be, that many of the “old ways” remained. Left unchanged was the desire to protect valuable “trade secrets” and other such pieces of information that, at the end of the day, amounts to nothing more than knowledge of vulnerabilities. To some extent, this was done to protect their trade. While it's an understandable position to take, it's not necessarily helpful. Add to this a second influence that came in the form of pressure and expectation from the manufacturers. In some sense, locksmiths have become the salespeople for the lock manufacturers. Locksmiths even invest large sums of money to gain “authorized reseller” status from leading manufacturers. With all this invested, it's easy to understand why they would hold to their old position of security through obscurity.

This does present a serious question to consider: If locksmiths are influenced by pressures to protect their industry and to protect the interests of the manufacturers they represent, then who shall stand as advocate for the consumer? This is the question of the moment in the physical security industry. Before the angry responses begin to fly, it might be worth the effort to note that not all locksmiths can be painted with the same brush because each locksmith may choose to conduct their business as they see fit. There are numerous locksmiths that hold, as the single highest matter of importance, their responsibility to the consumer. With others, the interests of the consumer have been shuffled down on the list of priorities.

The proliferation of the locksport community, though still in its infancy, has emerged from those who simply have an interest in the products they use to secure their person and property, and the limitations inherent within those products. Indeed, few enthusiasts set out to “change the world” in any meaningful way. However, in many cases some have stepped up to become the de facto advocate for consumer awareness. This role would not need to be filled if the locksmith industry at large was fulfilling that need.

It is wise in any industry to consider the needs of the consumer first, because clearly it is the consumer that drives the industry. For far too long they have been left in the dark concerning the vulnerability and risk to which they were subjected. This is made evident by the reaction of average people when they view media stories on the “bumping” technique. Their shock and discomfort serves to show us that the physical security industry has done a poor job of informing the public. Locksmith trade groups claim that the technique has been known to locksmiths for decades. If this is true, why was the public not informed or the vulnerability corrected?

Some argue that it is the public release of information, such as bumping, that creates the vulnerability. The argument is that bumping attacks were uncommon or even unheard of before information on the subject was released widely. There is just enough truth in that argument to make it dangerous. The problem, of course, is that the technique was used. Because bumping leaves little in the way of physical evidence, it is difficult to accurately judge how often it was used. One can't help but wonder if the victims of these crimes would be pleased to know that the locksmith that sold them the lock may have known of the threat, but chose not to inform the consumer. Were those victims better off not knowing of the problem?

The issue of security through obscurity is a dead concept in virtually every area of security, except the locksmith industry. Computer professionals and corporate security advisors have long recognized that security through obscurity can act as one of many layers in a security plan, but left to stand on its own it is disastrous. Anyone doubting this might consider a preview of Kevin Mitnick's *The Art Of Deception*. Despite this, the locksmith industry continues to hold tight to its old ways.

This article is an extrospective look at the locksmith industry. That is to say it is written from an outsider's point of view. The author writes from his own perspective only. Before anyone lines up to state the irrelevance of the author's perspective, it might be worth noting that the author is, himself, a consumer in the physical security industry. If this consumer's perspective is considered invalid, does it not serve to validate the article itself? Food for thought.

Josh Nekrep
President, Locksport International
Administrator, LockPicking101.com

The Medecoder

by
Jon King,
Peter Field
& Schuyler Towne

Prodigal Sons & Responsible Disclosure

I've never spoken directly to this audience about how I entered the world of Locksport. Back in 2006 I was attending the Hackers On Planet Earth (HOPE) conference with some friends. They dragged me along to a talk on lockpicking, a subject which had never held any attraction for me before that time. The talk was two hours long and featured Barry Wels and Marc Tobias. It was incredible. Barry, in particular, amazed me. He was like a very quiet magician on that stage. He spoke to the audience candidly while opening locks casually. Each time a lock popped it was thrilling to me, his relaxed manner, his absolute confidence that the locks would open, and his perpetual half-smile left an indelible impression.

Afterward I approached both men as they sat in the lobby of the Hotel Pennsylvania. I thanked them and asked Barry if he had any clubs in America. I mentioned that some friends of mine and I wanted to start picking locks together. He told me to come see him the next day and he'd give me all of the information I would need. So, at 3pm the next afternoon, on the last day of HOPE #6, I met Barry once again and he introduced me to Omikron, Eric Michaud & Eric Schmiendl. I remember they looked confused to have Barry introducing me. Before I could reflect on it he announced: "You four will be my Board of Directors for The Open Organisation Of Lockpickers, U.S." It was quite a shock. I was thrown in the deep end, just 24 hours after discovering how a lock works.

During the following weeks and months, I learned a lot, I worked hard and started competing. There were people who helped me along and I was lucky to be able to bounce ideas off of some of the best mentors in the world. Now, less than two years later, NDE Magazine is up and running in stable condition. It has found itself planted firmly in the middle of some incredibly talented people, ready to introduce them to one another and tell their stories.

I could not be happier.

I mention all of this because it is absurd to me that one morning in April, I found myself in the kitchen of a sailor in the U.S. Navy, who had worked tirelessly for months to develop a tool to aid in the picking of Medeco locks. Sitting across from us, quiet, curious and unassuming, was the head of Medeco research and development. Which begs the question: "Why was I there?"

The Prodigal Son

At the 2007 Dutch Open, Peter Field, the man from Medeco, was slated to give a four hour talk on lock engineering. It ran for over five. As compelling and comprehensive as the presentation was (and as entertaining as the Frenchman sitting beside me was, whispering as each slide came up: "Ah yes, this lock, let me tell you how we defeat this lock...") what stood out most to me were his opening words:

"Let me just say, in case no one else has, welcome to the industry."

To a room full of lockpickers, he says "Welcome." That is not the reception those of us on this side of the Atlantic are used to. To be clear, in both our private and public lives we have been called criminals, miscreants, thieves and far worse.

To quote the Schlage lock company from an article in the Wall Street Journal “...the company would prefer if the hobbyists ‘acted more like a magic society, where the trade secrets stay in the room.’” The trouble with that statement is that a magician, as amazing as his tricks may be, has never figured out how to enter your home in the middle of the night undetected. It’s a different kind of knowledge we’ve gathered and their response was flippant. So, here is a room full of people, many of whom are used to being insulted, hushed and disregarded, told that they were “Welcome” by a representative of a major American lock manufacturer.

Some who have heard this story secondhand can’t get over one thing, though: there have been problems with Medeco locks for years. So, now that we’re discovering these issues independently, why wait? Why give them time to respond when perhaps this flaw shouldn’t exist in the first place? To these questions, I answer: “Because they are the Prodigal Son.” They have reached out their hand to our community and agreed to treat us with respect, listen to what we’ve learned, and fix the problems we have uncovered. Whatever your feelings are in regard to their past, I hope you can welcome them as Peter welcomed us.

After Peter’s talk I cornered him and thanked him for coming out. I gave him a lock I had brought with me because it sounded like he might not have one in his collection. I wonder now if he wasn’t just being polite when he accepted it on those grounds. It wasn’t a long conversation, but it was mutually friendly and the connection was made.

Responsible Disclosure

At a small conference in Arizona last year, I gave a talk titled “Responsible Disclosure in Physical Security.” Not many people showed up. My friends offered an answer: “Sounds ... exciting.” A line delivered with a sarcastic roll of the eyes. It does sound pretty dull, I can’t deny that. However, those few who attended seemed intrigued by how our community was learning to deal with exposing the flaws we discovered. The talk centered around Jaakko Fagerlund’s ABUS Plus decoding method. It walked through the initial discovery, building the first tool, refining and simplifying the tool, and it talked briefly about how he tried to get in touch with the manufacturer (All of this is discussed in length on page 19, but don’t skip ahead just yet).

That’s the rub, though, isn’t it? How are random, geographically disparate, independent lockpickers supposed to develop the sort of contacts so that they can make a phone call and get ABUS to have lunch with them? As it turns out, via Lockpicking101.com. The disparate lockpicker becomes part of a distributed network of hobbyists, all with their own backgrounds, friends, and occasionally industry contacts. That’s how it worked in Jaakko’s case and that’s how it worked for Jon King, the sailor who put me up for a night in April.

Jon, and my staff at NDE Magazine, have been prepared to publish his story for more than two months. Doug Farre took the helm during Issue 2 and I was largely uninvolved with that issue, until this story crossed my desk. When I made the decision to hold the article, and push back the print date of Issue 2 as a whole, it led to a lot of debate. At issue was whether or not Medeco should be given the opportunity to see the article before it was released. There was a lot of concern that they would somehow try to squelch it. As well as concerns that they could intimidate Jon, or buy him off, or any number of troubling scenarios. Despite this, both my web designer (John Naughton) and myself had met Peter that weekend in Holland and agreed that we could trust him.

More important though, was that he deserved to be let in, because he had let us in first. Most important? There was a chance, slim as we all worried it was, that Medeco might take Jon's work seriously, and potentially even roll out a solution prior to NDE hitting the virtual newsstands.

It may seem anticlimactic to those outside this community, but there is no more exciting headline than "Our exploit is no longer effective!" We defeat, only to be defeated. There is no one I know, who is serious about the research side of this hobby, who doesn't get a thrill thinking about how the manufacturer can repair their lock designs. I would rather wait a few months, work with the manufacturer, and release a story about a new attack and how they fixed the problem so the attack no longer works, before any word of it ever hits the open air.

It's a subject I've spent a lot of time thinking about and discussing with some folks in a field which often overlaps: computer hacking. They have established their means of disclosure and some people think it translates perfectly. Let me lay out the simple differences we have to keep in mind:

Digital security protects your personal information. Physical security protects your person.

The stakes are too high to release without a plan, without trying to get the issue resolved before it goes out the door. Additionally, software manufacturers can fix their broken software by sending a patch directly to your computer. Lock manufactures don't have that luxury. The best they can do is to get the appropriate fix into the hands of locksmiths so they can provide it to their customers. This takes time, and if the manufacturer isn't on board when you release your exploit? It's time that could cost businesses their stock, pay phones their quarters, or families their safety.

We have an ethical duty to take all of this into consideration when we first make a discovery. Happily, the hardest part, being heard, is beginning to get easier. Use each other as a resource to get in touch. Use LP101, use other lockpicking forums and chat rooms, use NDE Magazine, use anyone at your disposal. It is possible that it will fall on deaf ears, but the tide is turning in that regard. From a table in a sailor's kitchen one morning I was proud to witness a clear example of the success of a lockpicker having his exploit considered - and solved.

Schuyler Towne
Executive Editor, NDE Magazine

And now, A word from Medeco...

An open letter to the Sport Lock-Picking Community



Throughout time, people have had a fascination with locks. Locks provide a means of protecting property, so the key to a lock confers an elite status to the person possessing it. Children eagerly await the coming of age when they are allowed to carry a key to their parents' home. As people grow up, they derive satisfaction from having the authority to control the decision about who will have a key to their own property. A lock and its key are powerful symbols of ownership as well as trust.

As architectural details locks are significant in the design of a building. Architects carefully select the style and finishes of the locks for their buildings to reflect a distinct artistic purpose. Collectors of locks admire the wide variety of designs of lock handles, trim plate, padlocks, cylinders, and keys. Antique as well as modern locks are studied, cataloged, traded, photographed, exhibited and purchased by people all over the world.

Locks are unique mechanical puzzles and the solution to their puzzle is their key. To most people, it appears to be impossible to open a lock without the correct key. Locksmiths are experts who are familiar with the internal mechanisms of locks and spend their time understanding the diverse methods used to generate these many different locking puzzles. With their knowledge of the internal cylinder mechanisms they offer a unique service to their community by evaluating threats and recommending solutions to secure property and protect the lives of their customers. Many locksmiths enter the profession because they enjoy the thrill of knowing how to solve the puzzle without the key, but they remain in the industry because they find their customers value their unique knowledge and services. A locksmith who installs some dead bolts in a neighborhood where homes have been burglarized, knows that his work has provided additional safety to the family who lives there. At the end of the day he goes home with the respect and admiration of the community he has served. A locksmith never forgets the gratitude expressed by a woman who has sought help to lock an abusive boyfriend out of her apartment. A lock gives her the ability to resume her life without fear of attack. The new puzzle on her door is more complicated than the boyfriend can decipher.

Lock picking or manipulating the mechanical puzzle of the lock has been of interest to many people, for a long time. Perhaps the most famous of lock pickers is Albert Hobbs, an American, who attended the Great Exhibition in England, in 1851. At this exhibition, Hobbs was able to pick the "unpickable" Chubb Six Lever Detector Lock, in 25 minutes. Then, he undertook a challenge to open the Bramah Lock within 30 days. For 16 days, Hobbs worked under supervision and was able to open the cylinder without damage and the original key still worked. To this day, Hobbs is credited with developing a technique for lock picking that is identified as the "Hobbs' method". To their credit, the lock manufacturers in England learned from Hobbs' techniques and made incremental improvements to their products.

As I was growing up in the Chicago area during the 1950s, I remember hearing about two machinists who hand made prototype lock cylinders and mailed them to each other without the correct key. For years, they challenged each other to decipher the intricate mechanical puzzles without damage to the locks. Most rational people acknowledge that given enough time and resources, anything that can be made by man can eventually be unmade by another man. The thrill is in the sport of figuring out how to do it.

So, if any lock puzzle can be deciphered, how can a consumer decide which lock is best to use? Lock manufacturers and insurance companies from many countries around the world have jointly developed standards to identify and classify the strength, protection levels, and time required to successfully attack locks. Such standards help consumers to identify the differences between the various locks. They use standardized testing of locks against standardized techniques that have been found in the past to successfully compromise locks. They provide a good basis of comparison for the consumer. All standards groups recommend that people wishing additional protection against new and uncommon threats contact locksmiths or other security specialists for supplemental information and guidance.

Within the lock industry there is an unofficial “time-torture” study that tests lock cylinders for uncommon attacks, and gradually improves the security of the locks. As locks are distributed and sold around the world, locksmiths and other interested parties, experiment with them to see if a solution to the mechanical puzzle that does not require the correct key can be found. As these methods are discovered, they are eventually relayed back to the manufacturer. Most all lock manufacturers have a number of documented engineering changes that reflect incremental improvements to their products, due to the solutions uncovered in these unofficial tests. The people who participate in the “time-torture” study of locks have contributed to the improvements of the locks and thus the security of the public. Growing up as a child, I remember that my father always has seat belts in our cars before they were required or furnished by the car manufacturer. As seat belts became mandatory in new cars, the older cars were pointed out as not being safe, and consumers had a good reason to upgrade to a newer vehicle that provided greater safety. Air bags and the side-curtain air bags have further increased passenger safety. In the same way, incremental improvements that are made in the lock industry contribute to the security and safety of the consumer, but they are not as obvious and the consumer is often not aware of these improvements.

Most people grow complacent with things they use every day. While lock models are frequently upgraded, the consumer using a lock is often unaware that improvements have been made, or that the lock on his door is possibly vulnerable to a new attack. People are used to frequently upgrading their cellular phone to a new model at considerable expense. However, there is an expectation that a lock cylinder, which protects both property and personal safety, should last the life of the mortgage of the house, and protect against threats that have not yet been identified.

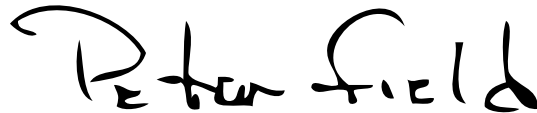
Lock manufacturers are reluctant to publicize potential threats to their products primarily because they do not want to teach criminals how to decipher their mechanical puzzles. While corporations are often stereotyped as uncaring or greedy, it is my experience that most people in the lock industry are genuinely concerned with the security of their customers. We do not want to make information available to persons who would use that information to compromise locks and threaten the security of the consumer. An abusive boyfriend may not be capable of figuring out how to open the mechanical puzzle by himself, but it is possible that he could learn by reading about a technique on the Internet and simply copy what some very talented and dexterous lockpicker has developed. Lock manufacturers are in business to sell new and enhanced products and want the public to be aware of any improvements, but not at the expense of supporting criminals or training new ones. Lock manufacturers are in business to protect people and property, not to compromise their security.

Who is Jon King and what is he doing with our locks? Several months ago, I was contacted by members of the lock-sport community. They told me that, after many months of work and practice, Jon had developed a tool that he was using to open some of our locks. He had made some samples of his tool for the lock-sport community to test and about 20% of the skilled lock pickers who tried his method were able to open our locks. Jon has perfected a technique that he was able to use, and furthermore, was able to teach a few others to do what he was able to do.

I got in touch with Jon and asked if he would show me what he was doing, and allow me to see how his new tool worked. I was interested in evaluating his technique to see what was necessary to counter it, and thus to improve our product. Jon agreed, and we met with Schuyler Towne on a Sunday at Jon's apartment. Schuyler has been involved in the ethics of responsible disclosure and asked to come to our meeting. It was a pleasure to meet with both of these men. We spent hours discussing Jon's work, the lock industry, techniques of solving lock puzzles, and the responsibility of keeping this information away from criminals. I congratulate these men on their ability and on their responsibility to the community. I am most impressed with Jon's fine motor skills, his problem solving ability and his ethical behavior. As editor, Schuyler knew that if NDE published innuendos, fabricated half-truths or resorted to scandal-mongering to garner attention, the reputation of his journal would be reduced to providing entertainment value similar to that of a grocery store tabloid. I am thankful that he wished to publish information that could be used to educate and increase security, rather than endanger property and lives. As a result of our meeting, my company has made additional engineering changes representing incremental improvements in our locking mechanism. Jon and Schuyler have agreed to withhold release or disclosure of their new information for a short time, until we have fully implemented our improvements.

While we have worked with many locksmiths and security specialists in the past to improve our cylinders, this is the first time that we have worked with people in the sport-lock picking community. I am pleased to know that you have as much concern for the security of the public as those of us in the lock industry. Again, I welcome you as representatives of the sport-lock picking community, to the lock industry, and hope that together we can continue to improve the security and safety that locks provide to the world.

Sincerely,

A handwritten signature in black ink that reads "Peter Field". The signature is written in a cursive, slightly slanted style.

Peter Field

**The inventor himself, Jon King,
has our final word, for now...**

Medeco, the Medecoder & Me

Dear Reader,

By now you're likely thinking "Who is this Jon King character and why should I care?" Well, I can't help with the caring part but I can tell you a bit about myself and the events of the last few months. I post on Lockpicking101.com and EZPick.com as JK_the_CJer. This is widely known to be the worst handle on the internet. The first part is a thinly-veiled reference to my name. The second part does not stand for Car Jacker, but instead for Contact Juggler. Give that term a quick Google and you'll discover another hobby of mine (for a good seven years or more). Since the time that I was in middle school (I'm 22 years old now), I remember wanting to try picking locks. I can recall using a hammer to flatten bicycle spokes and grinding them on my back porch's concrete steps. I would then attempt to open my back door lock (Kwikset). Every once in a while I asked my parents for a pick set, but this was declined. I couldn't blame them really. Fast forward a few years to me graduating high school and joining the Navy. I was stationed at a training command for a supplemental electronics school when the curiosity bit me again. I remembered the "MIT Guide to Lockpicking" and started reading. Later that day, I pulled some packing staples out of a discarded case of paper towels and ground them on the concrete outside. I also found a vise in the barracks maintenance closet which helped with bending the hook and tension wrench I had fashioned. After buying a Master #140 padlock, I sat down and started trying to pick. It took four hours straight, but finally..."Open!" I have been a lock picker ever since.

What is Medeco?

Medeco is a brand of high-security locking cylinders used throughout the world to secure very important sites. They have many government contracts and are said to hold 70% of the high-security market in the US. Their popularity came about almost immediately after their invention and production in the early 70's. People saw how revolutionary their design was and pounced on it. They have remained a standard for high-security lock design ever since. I saw Medeco as the holy grail of lockpicking and I believe many others still do. I had it in my head "Maybe one day, I'll pick one once". I even included "Pick a Medeco m3" in my list of long-term goals (along with "Earn a Masters degree in EE") on my Navy paperwork. They have a frightening reputation in the hobby lockpicking world as being one of the hardest locks to open. I read reports of folks saying they had finally opened one and felt their excitement through my laptop's screen. Later, Locknewbie21 developed an ingenious rake-like tool with which he was able to open them on a consistent basis. I remember being so skeptical of just how consistent it was. My doubts were formed from my prejudice against raking and the reputation that Medeco has of being almost impossible to pick. LN21's tool stands out in my mind because it was so much more successful than any of the tools the community had developed up until that point.

The Tool

Eventually I ended up picking my 4-pin + sidebar Medeco Classic Payphone lock. I utilized a combination of single-pin picking and raking. The first time that one of these locks popped open reminded me of that #140 I had picked two years earlier. After only opening it again once or twice like that, I started thinking. I found two simple design elements which held some potential of being leveraged. The first was a method of actually rotating the pins. This is the part that everyone has been racking their brain on over the years. I solved this problem for pretty much every Biaxial, m3, and some Classics. The solution was very simple, but required quite a bit of manual dexterity. Also, the process of rotating the pins was very much like picking a six pin lock with all spool pins by itself. However, it was a vast improvement over my previous technique. On a whim, I made a tool that exploited the second attack vector I had found and combined it with the first. Prior to the implementation, I considered attack #2 to be sort of far-fetched and hard to engineer around. Boy was I wrong, this thing worked! In my opinion, it effectively turns the Medeco locks that it works on (most of them) into 6-pin Schlage locks. Picking the pins to shear becomes the hard part.

Who is Medeco?

After much rejoicing and discussion on both IRC and the advanced forums of Lockpicking101.com, I made the tool look pretty and sold a handful to trusted members. I haven't received much feedback, but I know that at least a couple of them are able to open the locks using it. I am hoping that the others are getting the hang of using it as well. A short time after this, I expressed a desire to release the tool publicly. At the time, NDE magazine was getting started on Issue #2 after a long hiatus. I had released my 3d lockpicking game with them in Issue #1 and decided this publication would be a great way to release. After speaking to a few of the staff folks (especially Schuyler Towne), we decided it would be fun to get Medeco's reaction to the tool. After some social networking, I found myself on the phone with Peter Field (Director of Research at Medeco). He made a very surprising proposal that I was not expecting at all. Peter offered to drive from Medeco HQ (also in Virginia) to my apartment to view the tool and talk about it. We postponed the release in anticipation of this meeting and agreed that Schuyler should be present as well. About a month later, all three of us were sitting in my dining/living room on a Sunday morning. After showing the basic theory of operation, I proceeded to try picking one of my cylinders. I had some initial difficulty related to the shear line picking part and I was nervous. Then the lock opened followed by several others. I picked a Medeco Classic, Biaxial, and m3 in front of a Medeco representative. For the next six hours or so we talked about everything under the sun from destructive entry to disclosure politics.

The Response

Going into the meeting I fully expected Medeco to arrive with a suitcase of cash, a lawsuit, or both. Instead, Peter told us that the company is going to fix the vulnerability in the locks! He merely asked for two months to make the changes to every Medeco cylinder coming off the assembly line. This period will also be used to inform the existing customer base (via Medeco dealers). We are sitting in this two month window right now. Once we have received confirmation that the changes have been fully implemented, the tool itself will be publicly released via this magazine. They are currently closing a vulnerability that has been in the most popular high-security lock in the US for the last 25 years or so. The company is also giving credit for the fix not only to myself, but also to the locksport community as a whole. We made a difference!

Jon King
Inventor, Sailor, Lockpicker





MBI

Jaakko Fagerlund & ABUS Plus

The Exploit

ABUS' Plus system is a disc-detainer style lock. This exploit relies on the fact that the discs contained within happen to be stamped with their individual codes. Now, these codes are stamped on what would be considered the "back" of the disc, the portion not immediately visible from the keyway. However, because they are stamped, a very clear impression can be had by inserting a specialized tool coated with some sort of adhesive and pulling backward gently on the disc.

After the initial proof-of-concept was created there was a new focus on refining the tool to be as simple and affordable as possible. In the end, and with the materials advice of Ray Connors and Josh Nekrep, we were able to reproduce the tool using only a nail, some white glue, and standard hand files. Once the means for attacking a lock can be brought down to such a basic level, an otherwise esoteric exploit becomes an extremely serious issue.



THE STAMPED DISC: THE 4, CLEAR ON THE LEFT.



NOT COVERED: TURNED 90°, THE SPACER & SECOND CODE DISC PROVIDES VERY LITTLE COVER.

This attack was presented at the Dutch Open in the Netherlands and at the University of Advancing Technology in Arizona. The original proof-of-concept is available in the downloads section of ndemag.com.

We had the pleasure of (electronically) sitting down with a couple of the people involved in the development and reporting of the discovery.

NDE: First of all, thanks for meeting with us.

Jaakko: Damn, I'm all sweaty...been all day playing with the lathe. Funny, because I was just making a new pick for the ABUS and the like.

NDE: Hah, excellent. Well, I guess my first question is how long did the whole process take? From approaching the lock the first time, to finding out they had fixed the problem?

Jaakko: About 7 months.

NDE: So how did it start?

Jaakko: I bought the lock a few weeks (don't remember) before I got into advanced on LP101. In the advanced, I saw the contest...

LP101

Lockpicking101.com has two levels of access. When you first join you're entitled to read and post in the public forums, which come with certain limitations. While the function of high security locks can be debated and explained, any picking discussion is disallowed. Similarly any method of destructive entry is off-limits. However, if you display some modicum of competence and stick around for a few months, you can apply to the private, advanced forums where there are no restraints. Many members who are doing research into higher security locks first float their ideas in these friendly waters.

In July of 2007 a contest was started to encourage new material for the advanced end of the site. On offer was a set of automotive tools and, likely more important, bragging rights.

Jaakko: At first I was about to write up about Abloy Classics history, but realized that 5 days ain't gonna cut it...and so it happened that the ABUS was laying all guts out on my table next to me and voila, I saw the flaw. Don't know exactly how the heck did I notice the flaw, but there it was. I was just fiddling with the parts.

NDE: Did you have the lock open for a while before you noticed?

Jaakko: Yeah, like two weeks. It was in parts on the left side of my keyboard as I was thinking of a way to pick it properly.

NDE: And we have to assume that other people have had it open, even in our community, why do you think no one had noticed the problem before?

Jaakko: I suppose that nobody didn't think that you could actually "look" behind the discs, because the looking requires rotating the discs first. Maybe I just got lucky.

NDE: When you noticed the stamped numbers, did you know immediately how to "look" behind the discs?

Jaakko: Not at first. I had in mind to make a some sort of mirror arrangement, but the space was too tight for my budget. Then I thought about impressing somehow. Enter Blu-Tac.

NDE: And you just used the tool you had already made for picking them?

Jaakko: Yes. fit the lock perfectly.

NDE: So - that was your proof of concept, which went on to win the contest, correct?

Jaakko: Well, it was a tie between me and un-something (don't remember the nick).

NDE: Unbreakable!

John Fraser, aka Unbreakable, wrote an excellent, well photographed article on the intricacies of Medeco locks. Medeco has obviously been getting a lot of attention, both here at NDE, in the community at large, and from plenty of folks outside of locksport, as well. John was kind enough to prepare a version of his article for our last issue.

Jaakko: Yeah! I let him keep the prize because the postage would have been tremendous for those automotive tools and I don't have use for those.

NDE: Alright - so your proof of concept is out there, it's valid, other people in the community start playing with the design, did you have any plans after writing about it? Any idea of what to do with your new attack?

Jaakko: 1. ???
2. Profit!
Nah, haha. I had no plans other than to inform ABUS about it and I had/have no idea what to do with the attack.

NDE: And did you have any idea how to go about that?

Jaakko: No, it was at first nick mh [Michael Huebler] who lives in Germany who promised to get in contact with ABUS and he kind of relayed the info. Then a while after that you asked if I would like to hear an opinion from Barry [Wels] and Han [Fey] and not a long time after that Barry called and asked if I would like to come to the Open to explain about it.

Barry Wels is the president and founder of The Open Organisation Of Lockpickers in the Netherlands (and by extension the US division) and has, along with his club members, revolutionized the relationship between lock manufacturers and locksport groups over on the other side of the Atlantic. Han Fey, a TOOOL member himself, is one of the pre-eminent lock collectors in the world and is well known and regarded for his exhaustive articles on high security locking systems regularly posted to the TOOOL.nl website. These two gentlemen have provided a great deal of the inspiration behind this issue of NDE.

NDE: So mh relays the information to ABUS, had you heard back from them before Barry was in contact?

Jaakko: Yes, if my memory doesn't fail.

NDE: So what was the first response you had from ABUS?

Jaakko: mh told me that the customer support said something along the lines "our locks are quality...blah blah...no markings in the keyway...blah blah...all your socks are belong to us" So, mh sent another one, this time with a link to my PDF about the flaw. After a while, some higher up answered that it has been sent to their R&D team and they are looking into it.

Jaakko's Notes:

Sun Jul 08, 2007 20:48

An LP101.com member "mh" from Germany sends me a private message informing me that he has contacted ABUS and made them aware of this problem and promises to keep me posted and to provide a translation of the answer if there is any.

Mon Jul 09, 2007 13:54

I got a new private message from "mh". He suspects that the answer from ABUS came from the first level customer support and to quote: It goes along the lines of "nobody has opened an X-Plus lock without the proper key yet" - "the keyway has no surface markings", either not understanding the problem or trying to avoid confirmation of the problem.

"mh" replied to ABUS by sending the link to my PDF article about the issue and pondered that there might be no answer from ABUS to be heard.

Thu Jul 12, 2007 18:46

I get the third private message from “mh” and it appears to be a translation from the answer of ABUS. To quote the answer from ABUS:

“Thank you very much for your detailed description!

The security level of the ABUS Plus cylinder is - esp. concerning the so-called time resistance - unique in the bike/motorcycle segment. 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!”

Jaakko: So it appears that the PDF article did make a difference in the welcoming and proved a point and the manufacturer presumably responded with some actions. At this point “mh” and I were pretty sure that this was the last thing to be heard from ABUS.

We spoke to Michael Huebler about his involvement as well.

NDE: How did you first find out about Jaakko’s research?

Michael: His post on LP101. Rotating disk locks are very interesting to me, including the German-made ABUS Plus, so this immediately caught my attention. I also wrote a contest entry, it was even about the ABUS X-Plus mechanism, but I failed to realize the significance of the stampings.

NDE: What was your connection to ABUS that allowed you to get in touch with them? Did you just start from the ground floor and hope that someone would listen?

Michael: I had no connection at that time. I just sent an e-mail to their customer support. Meanwhile I know Gerhard Meckbach personally and would contact him directly.

NDE: Were you surprised by their reaction at all?

Michael: The customer support reacted just as you would expect them to - along the lines of ‘our locks are very secure’. It’s professional behavior of customer support people. They did, however, forward the information to the R&D team.

NDE: So – they said R&D was going to look into it, did you hear from them again before you found yourself at the Dutch Open?

Jaakko: Nope.

NDE: Though it was a bit disorganized in it’s setup, I remember that your talk was very well received in Holland.

Jaakko: Yes it was.

NDE: People always seem surprised by this attack, because it’s so easy to understand, but for some reason no one ever thinks to approach the lock in this manner.

Jaakko: Maybe I’m “special”

NDE: Did anything come out of your time at the Open as far as this attack is concerned? Anyone speak with you about it after the talk?

Jaakko: Not exactly, there was a few chit chats about it in the bar, but the “main talk” was with G. Meckbach from ABUS via email. Barry gave me his email address/name.

NDE: So how soon after Holland were you in touch with him?

Jaakko: 10.12.2007 is the date I received the first email from Gerhard Meckbach

NDE: Wait! That was pre-open, if I’m not mistaken

Jaakko: No you silly American! 12.10. for you. 10th of December. Damn your stupid month-first-markings.

NDE: Ah! Sorry! So, what did it say?

Jaakko: He told me he would send me a Padlock with an ABUS Plus Cylinder but without keys. He said I was welcome to find out the key code by “impressioning” and to advise him of the code if I was able to figure it out. He said if I could do this, he would send me the keys to the lock. I haven’t yet picked the padlock he sent me, as I don’t have a pick, yet.

NDE: Did you two speak further?

Jaakko: Yes, well, not exactly, I got CC’s from Barry:

From Barry Wels,

*I take it the lock you will send Jaakko is one from normal production ... right?
Or is it specially modified for this attempt? (or did production change because of the knowledge you have now) I am just asking, I know ABUS is a fair company and does not play games.
Kind regards,
Barry Wels*

Gerhard replied that they had already begun to change the discs in the ABUS Plus Cylinders to a new version without any imprinted numbers on them. The one he had sent along to Jaakko was a mixed cylinder, some original and some updated discs, it would be a new challenge for him and Gerhard made it clear that he was very interested in Jaakko’s results.

NDE: Was there any further communication between you / Barry / Gerhard?

Jaakko: Not that I’m aware of, but I’m sure there is after I get the pick done and (hopefully) the lock open.

NDE: Do you think Jaakko can break the new ABUS Plus system?

Michael: Of course he can. Jaakko has the required machines to make the tool and also the skills. ABUS Plus locks have been picked before, but Jaakko’s method takes the guesswork out of the process. If some disks are now unmarked, he will have to pick them ‘conventionally’ (or decode them in another way), so it will take longer, but I’m sure he will manage.

NDE: What do you think of ABUS reaction to all of this?

Michael: It’s good to know they responded positively. Now that I know more about ABUS, I would expected them to as well. They are a family owned and managed company and seem to have strong ethics, they are the type of people I’d like to do business with.

NDE: Alright - I think that wraps it up. Jaakko, if you have anything you would like to add feel free.

Jaakko: I would like to thank everyone in the LP101 advanced for the advice and help, every listener in the Dutch Open 2007 and of course ABUS who has made a fine example how things should be done.

NDE: Thank you very much for your time, Jaakko, and good luck finishing that lock off!

Jaakko is hard at work on the new pick and the early prototypes look beautiful. I doubt we'll be able to convert this one into a glue and nails operation, but lucky for us he's planning to sell the new model to help offset the costs of traveling to the 2008 Dutch Open. So, if you'd like to help sponsor independent lock research, or just get your hands on a very cool new disc-detainer pick, keep an eye on his progress.

We'd like to thank everyone who spoke to us for this article and a special thank you to the ABUS company for their constant support of the Locksport community.



JAAKKO FAGERLUND'S NEW ABUS PLUS PICK: THE PRODUCTION VERSIONS WILL BE AVAILABLE FOR SALE SOON.

Schuyler Towne
Executive Editor, NDE Magazine

Breaking Ingersoll

Pt. 1: The Breakdown

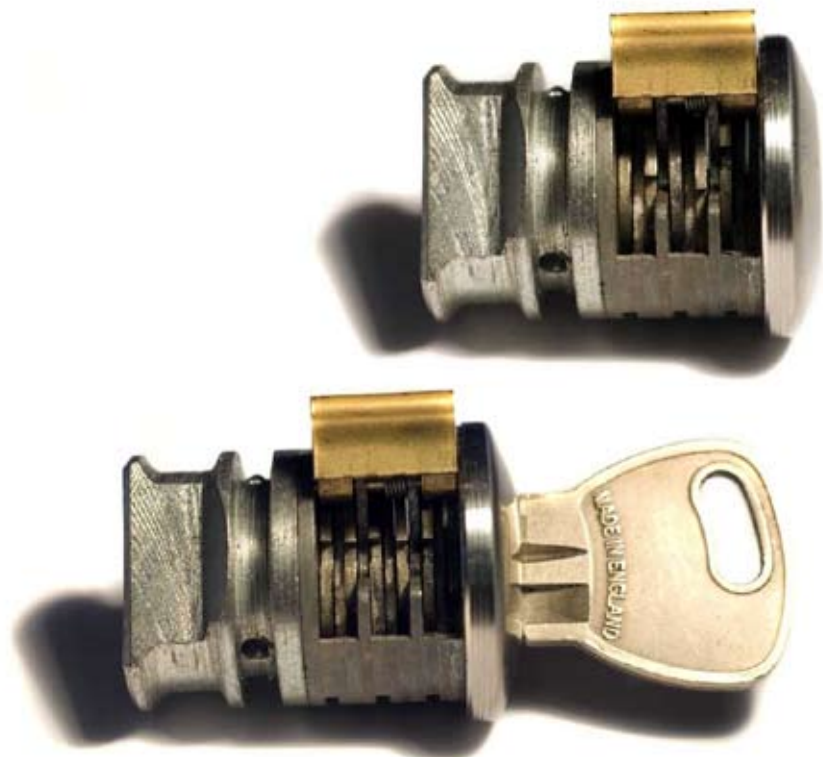


BASIC MECHANISM

The Ingersoll locking mechanism is a very simple but elegant design. It incorporates a double sided key which interacts with equal numbers of levers on each side. 6 lever padlocks will have 3 levers on each side and 10 lever padlocks will have 5 levers on each side.



At rest the with no key inserted the levers will sit in a jumbled fashion with no space for the sidebar. With the correct key inserted the levers will be pushed in to place lining up the gates. When the levers are lined up the sidebar has space to drop in to place.



Disassembling Ingersoll padlocks can be quite challenging. The most common problem people have is removing the shackle from the padlock. This is because there is a small retaining pin pressed into the shackle that is easy to miss. The 600 series padlock was chosen for this article because it is much easier to drill the retaining pin than on the 700 series (10 lever). In the next issue of NDE Magazine there will be an article which will teach you how to pick these locks and so doing it with the easiest to work with seemed like the most sensible choice.

First you will need to drill the retaining pin that sits in the shackle, which stops it from being removed from the body of the padlock:



- 1 – Unlock the padlock.
- 2 – Pull the shackle out as far as it will go.
- 3 – Rotate the shackle 180 .
- 4 – Push the shackle back in to the locked depth.
- 5 – Rotate the shackle back around against the body of the lock (see image).
- 6 – Drill the retaining pin that you can now view through what appears to be a drainage hole.

After you have drilled the retaining pin you can now rotate the shackle back 180 and pull it out completely from the body of the lock. There will be a screw under each side of the shackle which you will need to remove. This will allow you to remove the face plate from the body of the padlock.

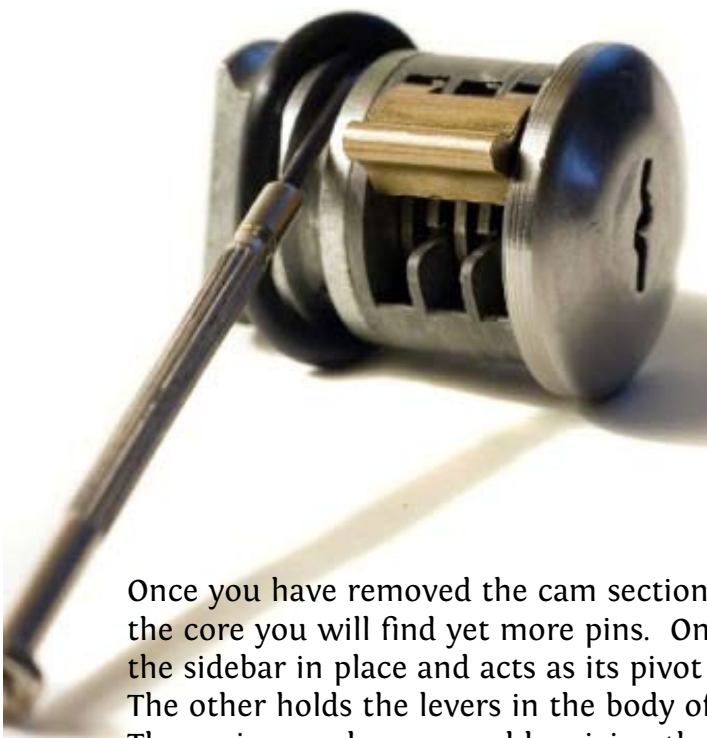
You can now insert the key and twist clockwise 45° to the unlocked position and pull the core out of the body of the padlock. Make sure not to drop or lose the ball bearings that will follow the plug. Set these aside in a safe place.



This is the exposed core of the padlock.

A double sided key interacts with levers on each side of the lock pushing them into place and lining up the gates in the levers. This allows the sidebar, which normally stops rotation of the plug, to drop into place and allow the plug to turn.

To further Disassemble the padlock you will need to locate the rubber washer on the back end of the core and carefully remove, taking care not to damage it. Slipping a small screwdriver along the side and using the body of the core as a fulcrum will give you the safest option.



Underneath this you will find another retaining pin which holds the cam for the double ball mechanism onto the main section of the core. You will need to remove this if you want to remove the levers or sidebar.



Once you have removed the cam section of the core you will find yet more pins. One holds the sidebar in place and acts as its pivot point. The other holds the levers in the body of the lock. These pins can be removed by giving the core of the lock a decent tap on a hard surface. I used the top of the padlock body as it was unlucky enough to still be within reach and was in a less than mint condition already. As soon as the end of the pin is exposed and you can get a grip on it you should remove it completely with a pair of tweezers or needle nose pliers.

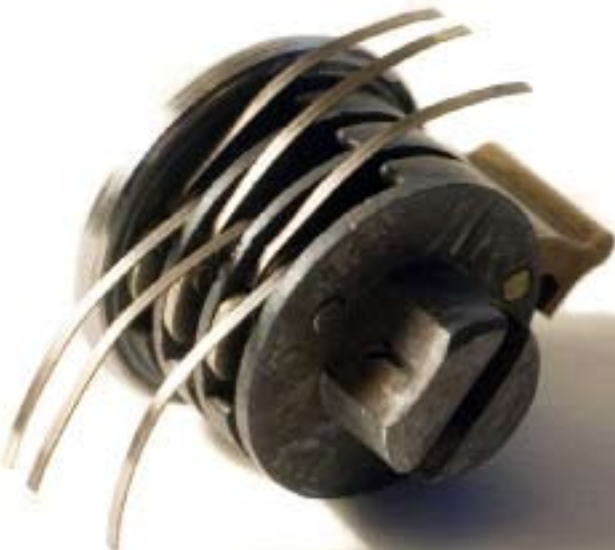


This is the sidebar assembly. If you choose to remove this make sure not to lose the spring. There are 3 pieces to this sidebar assembly, the sidebar, the pivot bar and the spring which pushes the sidebar out so when you lock the padlock it disengages from the levers, allowing you to remove the key. Without the spring the sidebar will simply sit in place because of the binding pressure from the levers and the lock will remain jammed in place.



It is worth mentioning that not all Ingersoll sidebar assemblies use a spring. In some models, such as the SC1 and SC71, the sidebar is lifted out of place by a notch in the back of the lock casing.

To remove the levers first untension the springs. Take a small screwdriver and push from underneath, this will unlatch them and have them point away from the body of the lock as seen in the image below. I recommend using eye protection when untensioning and tensioning springs. I had a lucky escape when a spring snapped at the base of the lever and hit my glasses in the center of the lens.



Now you can remove the final retaining pin followed by the levers. Please be sure to remove them one at a time and keep them in order. Although they are easily identifiable by eye it's easier to just not have to sort them out.



To reassemble this padlock I recommend you fashion a special tool for reinserting the springs into the core. To do this, simply take a small screwdriver and cut a "V" shaped groove in the tip. This can make reassembly much easier and I highly recommend doing it if you plan to follow the picking tutorial in the next issue.

To use the tool insert the levers into the lock and slide the pivot bar in. Then take the tip of the spring and align it with the "V" shaped cut in the screwdriver and press the spring into it's slot. This will make repetitive reassembly of the lock much quicker and easier. And as stated before, some kind of eye protection is recommended.

Congratulations you have now completely disassembled an Ingersoll 600 series padlock.

John Naughton
Online Editor, NDE Magazine



