How To Make Friends
&
Influence Lock Manufacturers

Schuyler Towne & Jon King
DEFCON 16, 2008

Reviewing this on the DEFCON 16 DVD? Be sure to check ndemag.com/DC16 for updates. Much of the material covered in this talk is on-going. This document has been prepared more than a month prior to publication. Any omissions or inaccuracies in this version will have to be forgiven. Please consult the current version for accurate information. Thank you.

LOCK-AND-KEY:

n. The distinguishing device of civilization and enlightenment.

– Ambrose Bierce

Let's Talk

- RoboKey System:
  - Developed with the locksport community
- Kwikset / Weiser's Smartkey
  - Responded to bumping with complete redesign
- ABUS Plus
  - Fixed flaw found by lockpicker & issued new challenge
- Medeco
  - Worked with Jon King to mutually release exploit
- Q&A / Super-secret announcement

The RoboKey System



John Laughlin with Barry Wels of TOOOL

Background

- John & Bob Laughlin
  - John was a communications engineer
  - Bob was a retired lock engineer
  - When telcom bust John started working with his father
- Inspiration
  - Both have a healthy interest in security
  - World more interested in security than ever before
  - Opportunity to address a lot of areas that hadn't received the scrutiny they were due
  - How can we secure containers that have to change hands multiple times / survive tough environments

Basic Operation

- Disc-Detainer type mechanism
  - Looks like an Abloy style cylinder
  - Has flies like a combo lock
  - Extremely rugged for environmental conditions
- Automatic dialer
  - Operator does not need to know combo, just has to be a valid user
  - Various potential forms of authentication – password, RFID, embedded dialer in cell phone, matched pair, etc.
- Manual dialer
  - Physical lock can still be operated manually

Community Scrutiny

- First Introductions
  - Bob Laughlin met Han Fey via eBay/both avid collectors
  - Met in Holland in early 2006 to see RKS
  - Han invited John to the Dutch Open
- Dutch Open
  - “The people were very generous with their knowledge”
  - Panel on viable attacks & applications
- ALOA
  - Attended ALOA with Han & Barry
  - Showcased RKS & other products
  - Article in Locksmith Ledger as a result

Open Source Future

- Open source developer kits
  - Looking to license their product
  - Wanted to get the ball rolling while seeking a deal
  - Open source software and microcontroller
  - Add whatever functionality you want
  - Aiming to get total package, lock & dialer kit for ~$300
- Would love to hear from you
  - John has always kept in touch with folks in the locksport community
  - Answering questions and fielding commentary about the NDE article at lockpickology.com

Smartkey

"At least one lock maker says the hobbyists can help companies..."

–Wall Street Journal



Photo courtesy Mike Brewerton

Bump In The Night

- How blind were we?
  - Walt Strader told the WSJ he heard of bumping via locksport groups
  - Told them this in 2006
- Smartkey is launched
  - Lock is 100% bump proof
  - Rekeyable (NOT U-Change)
  - Subdued marketing campaign – no initial mention of bumping
  - Rigorous testing process

How Does It Work?



Sidebar assembly housing fully assembled

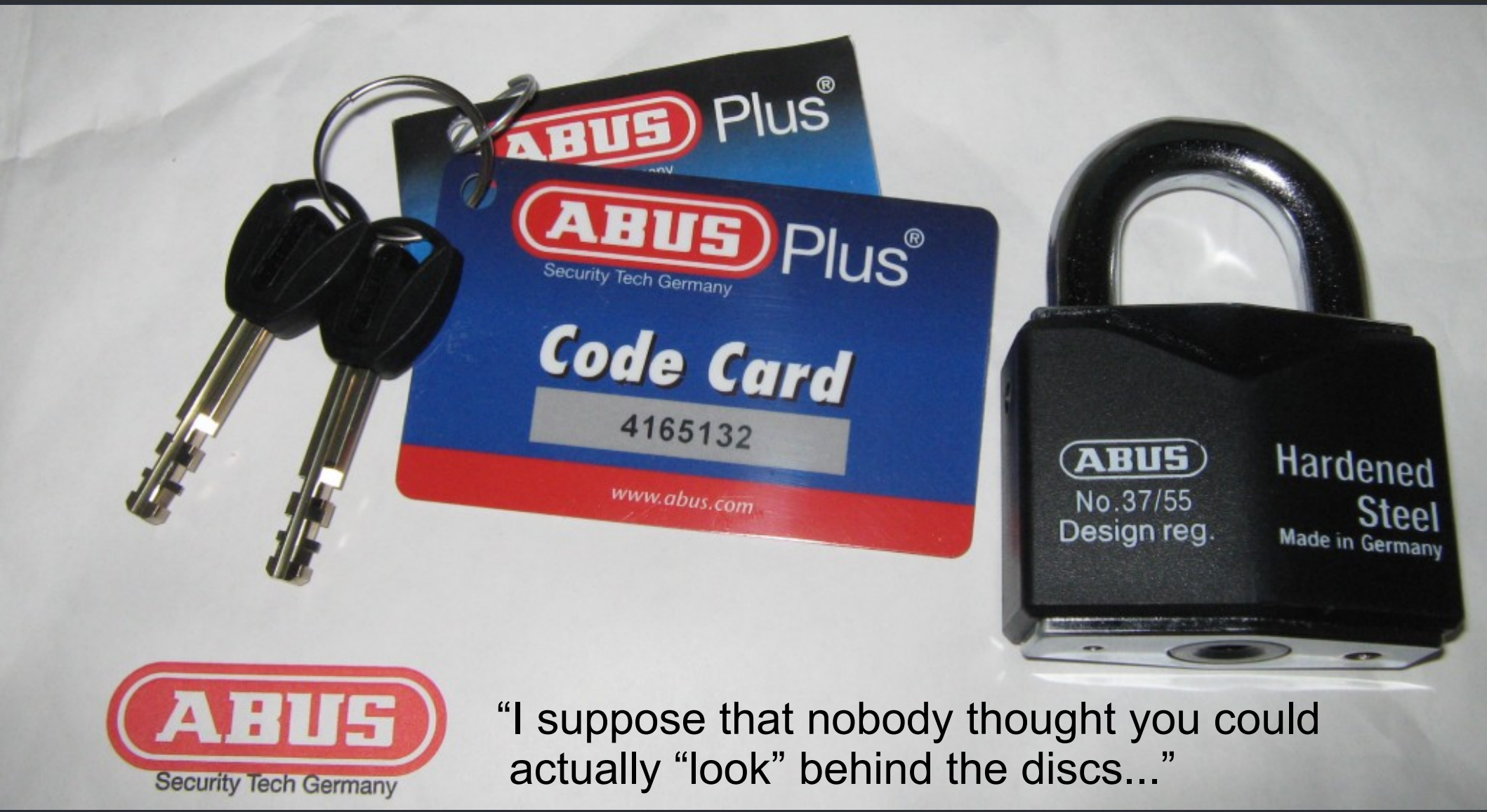
Testing

- 2006 Dutch Open
  - Prototype from an unnamed company
  - Arthurmeister!
  - Definite challenge
- Japan
  - Different culture of entry
  - Interesting methods of testing
  - Passed the 15 minute attacks with flying colors

Smartkey 2

- The new generation
  - Updated materials for destructive entry (DE) concerns
  - Similarly subdued roll-out to first generation
  - Out now!
- What does the future hold?
  - Black and Decker employees now keep an active eye on the locksport community
  - Led to current advances & additional free feedback
  - Excited for future collaboration

ABUS Plus System



ABUS
Security Tech Germany

"I suppose that nobody thought you could actually "look" behind the discs..."

Photo & Quote by Jaakko Fagerlund

The Exploit

- Background
  - Zeke's Contest
  - Everyone missed the flaw – forest for the trees
  - Created proof of concept
- How it works:

Photos Courtesy Jaakko Fagerlund

Simplification

- The goal
  - Build the simplest version of Jaakko's tool possible
  - Build the least expensive version possible
- The tool
  - At the advice of a fellow lockpicker we used the filed down head of a nail
  - Many impressioning mediums were tried before we settled on white glue

Alerting ABUS

- First Contact
  - Arranged by an LP101 member “mh”
  - Initial response was polite, but non-commital
  - Proof is in the pudding - Jaakko's PDF got attention
- The Response
  - A brief silence
  - Updated all current production
  - Challenged Jaakko to defeat the new mixed cylinder
  - Jaakko could only get the keys to the lock if he uncovered the bitting

Current Events

- Jaakko's ABUS Plus Pick
  - A brief silence
  - Community funded
  - Successfully picked the challenge lock!

Medecoder



"Who is Jon King
and what is he
doing with our locks?"
–Peter Field, Medeco

Photo & Quote by Jaakko Fagerlund

Who is this guy?

- Jon King
  - JK_the_CJer, JK, etc.
  - Navy
  - Locksport Hobbiest
  - Security Geek
- I am NOT
  - Speaking on behalf of the Navy
  - Speaking on behalf of Medeco

My Obsession

- Why Medeco?
  - Holy Grail of pin tumblers
  - Pins must lift and rotate
  - Lots of attempts by the community
- OK – Show me...in one picture

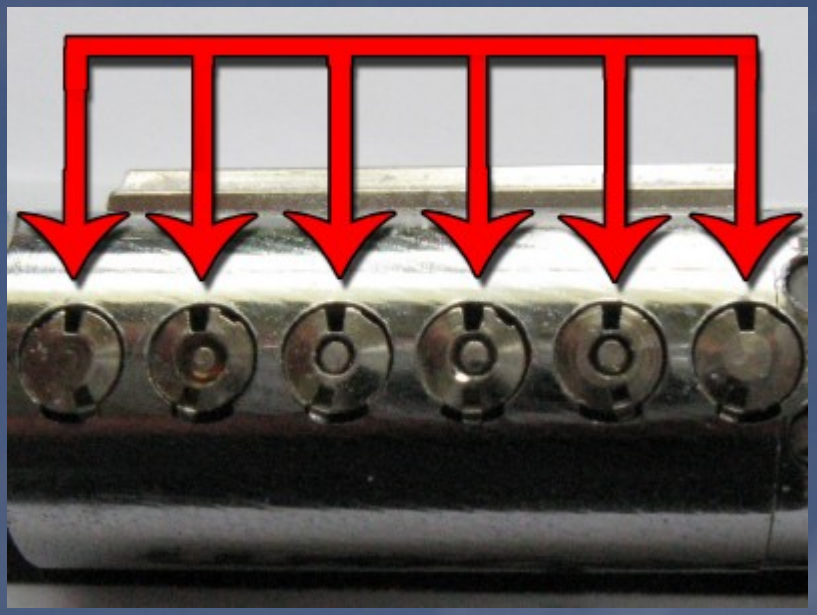
The Problems

- Open Grooves

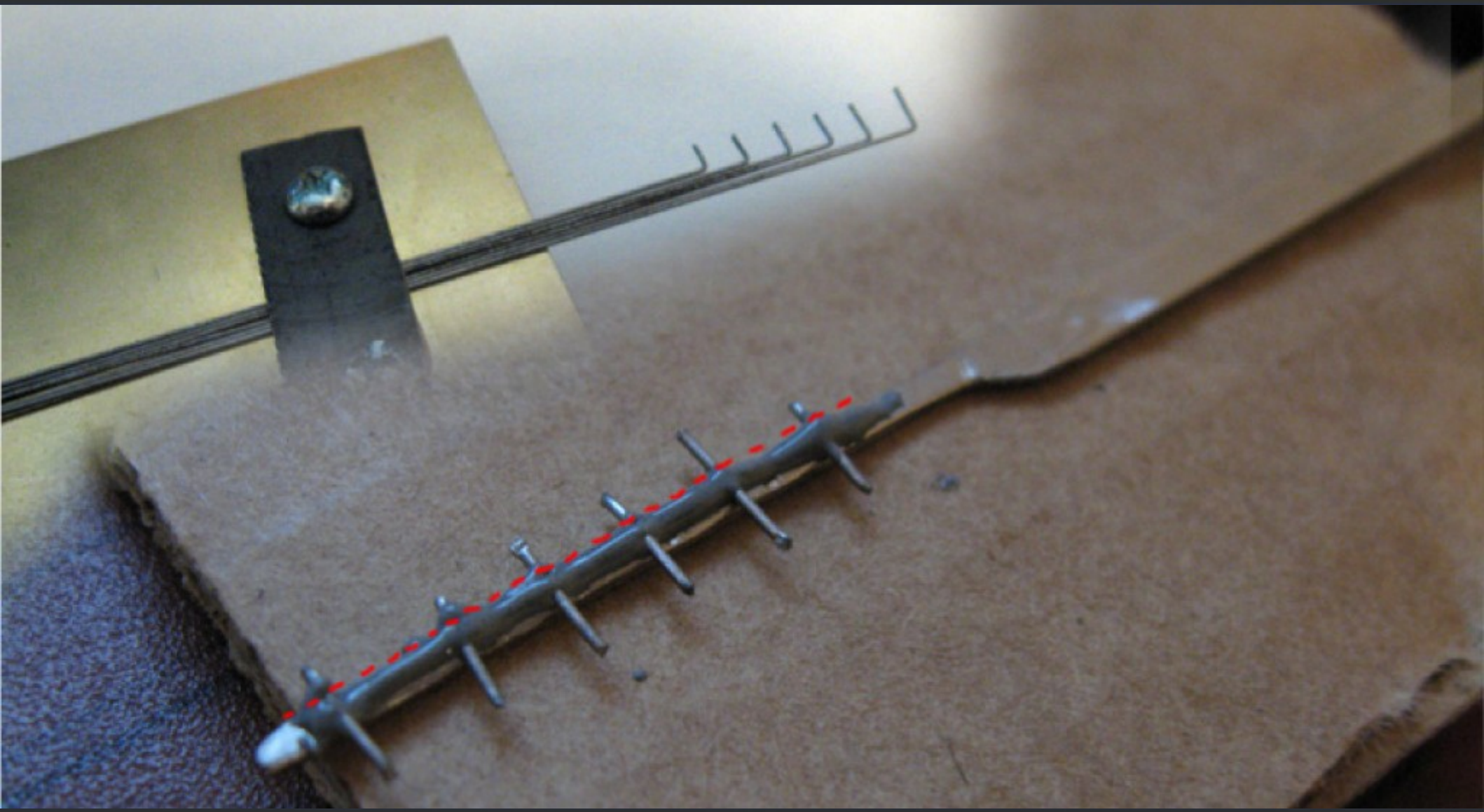


OMG Wire!

- Even Spacing

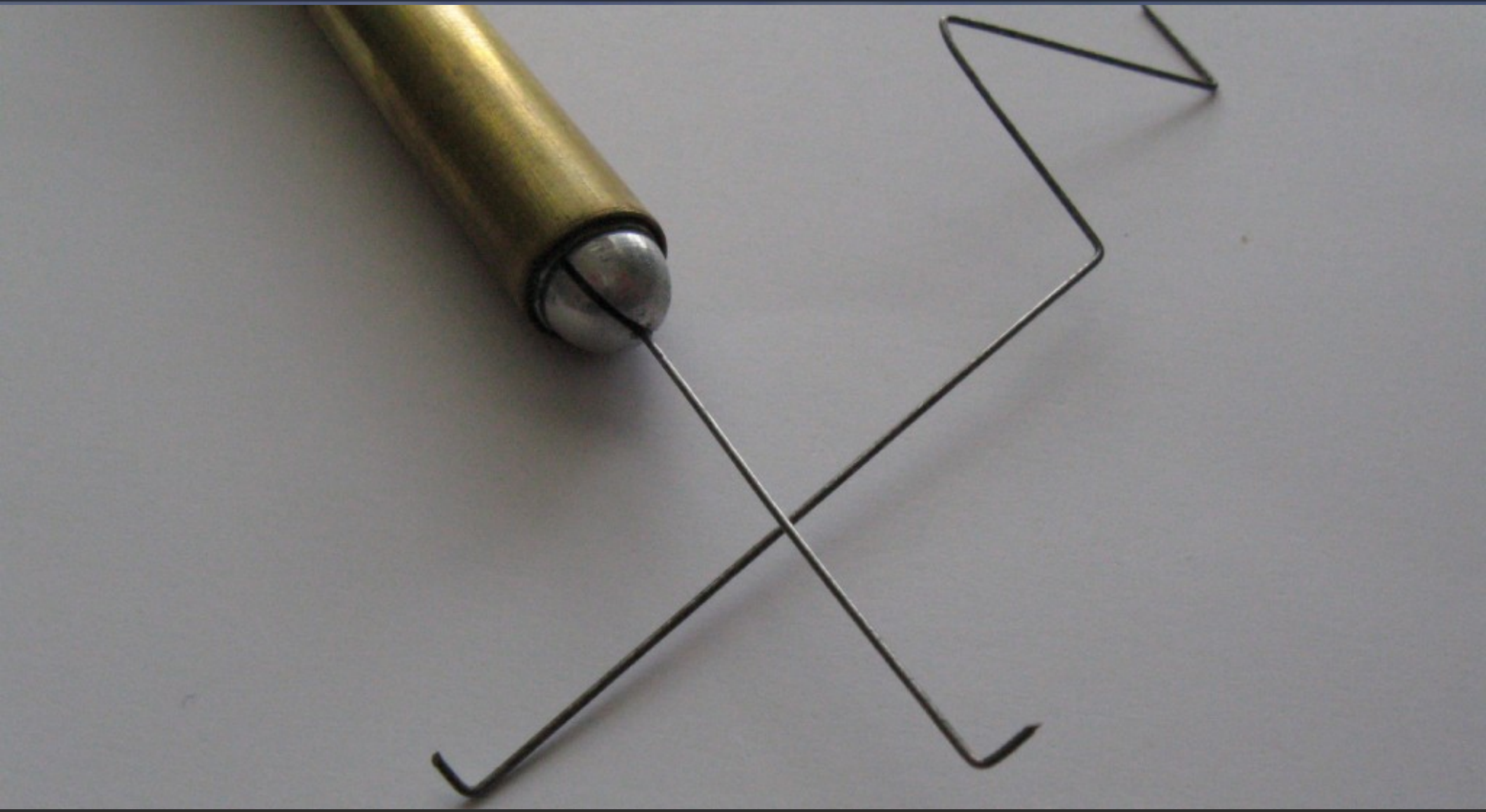


Humble Beginnings



Early tool designs aimed at rotating all of the pins at once

Let's Simplify



Maybe I'll try hooking into one pin first

The Early Tools



Purdy



The Community

- Lockpicking101.com
  - Schuyler Towne
  - Doug Farre
  - Mitch Capper
  - Everyone else...
- Public release & NDE
  - Wanted to publicly release via NDE Magazine
  - “Let's get a manufacturer reaction”

Quite A Reaction

- Peter Field
  - Head of R&D at Medeco drove to my house
  - Lock talk, history, other exploits, etc.
- Closed Grooves
  - Medeco reimplements the ARX closed groove pins



The Future

- Keep going! Nothing is impossible!
- Think before disclosure!
- Don't get wrapped up, have fun!

Final Thoughts

- Please help
  - We're getting our feet in the door
  - Our communities are merging
  - Physical security disclosure is DIFFERENT than digital security disclosure
  - Want to help?

schuyler@ndemag.com

And finally, that super-secret announcement...

The NDE Grant

- Misson

  Our goal is to help get tools and supplies into the hands of hobbyists who are doing legitimate lock research.

  Once an exploit is discovered and verified we work with the researcher(s) to communicate with the manufacturer.

  I have privately funded a few research projects, but this is not sustainable for me financially, so I'm opening the funding up to public donations.

  For more details, please visit: ndemag.com/grant

Thank You!

- And thanks to:
  - Zeke79
  - Raimundo & DB
  - Mike Brewerton
  - Lockpickology.com & LP101
  - Jon King
  - Peter Fields
  - Walt Strader
  - John Laughlin
  - Jaakko Fagerlund
  - ABUS

FOR LOCKSPORT!