"The ABUS Story"

Great Moments In Locksport

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

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

The Exploit

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

Jaakko's Notes

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

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

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

The Fix Is In

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

A New Direction

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

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

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

The Challenge Lock

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

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

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

And we were proud to be there.

—NDE MAGAZINE

NDE Magazine

For Locksport!

Timeline ...

From Discovery to Disclosure

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

‹ 2007 | 2008 ›