Hybrid PhySec Tools

Best of Both Worlds or Just Weird?
DEFCON 28 - TOOOL’s LPV
Agenda

Intro - What are PhySec Tools?
Why? - Why are you doing it? Is there a need?
What? - What hasn’t already been made?
::~$ man d1dymu5

- Picking locks for 13 years
- Favorite Pick - Deforrest Offset
- Least Favorite Pick - This?!
- Security Engineer
- Lockpick Enthusiast
- Happily Married, Father of 4
What are PhySec Tools?

PhySec - Physical Security Tools

“Any tools used to test and compromise physical security.” (I made this up)

**Examples**: Lockpicks, bypass tools, drivers, jigglers, shims, etc

**Weird examples**: multitools, wedges, compressed air, film reel

**Awesome examples**: thumb latch tool, under-the-door-tool, etc.

**Works in a pinch**: bobby pins, paper clips, stuff you find, etc.
“Hybrid” tools

More than one tool when traditionally it’s only one tool.

* Hybrid doesn’t always mean better.

“It can do 2 things. Doesn’t mean it can do 2 things well.”

Super specific tool vs More with Less philosophy

Creativity - Someone will like it
Why?

Do more with less.

Some social engineering engagements, can’t bring the whole kit

Custom tools

Creative side

Can lead to better tools overall

But why?
My Inspiration

Spy Stuff

SERE
Improvements examples

Sparrows Dark Shift Expansion
Improvement Use Case

Tag 5 Industries
Hybrid tool examples

@LockNoob1
...or just weird
Where to begin?

What am I trying to solve or improve?

What’s currently out there?

Design and drawing phase.

Prototypes and testing

Repeat
Problems

Lock Pick Wallet Cards

Bogotas

Metallic?
Lock Pick Collar Stays - R&D
Redesigns

Smooth corners
Tweak pick tips
Add serrations to Tension
Testing
Usability

*Disclaimer
Manufacturing and Production

Raw Materials

- McMaster Carr, 301 High Yield Spring Stainless Steel, .020”/.508mm, .031”/.787mm

Production

- DIY vs Pay someone

Shipping

- DIY (Google Forms > PayPal (postage, shipping labels, etc)
A word on crowdfunding...

Pros:

- Good platform, gets word out, showcases your stuff, gets you money to produce

Cons:

- Taxes, percentage of raised funds, platform is not liable, refunds, delays on money (~1-4 weeks depending)

My Advice:

Figure out design, manufacturing & prod first. **DO NOT USE** funds for R&D and figuring out mistakes. Always be responsive. Fulfill commitments.
Success

"LASER."
Current Projects by d1dymu5

Backstory

Bypass tool, jigglers, common keys
Brainstorming

- Bypass tool
- Small Form Factor
- TSA safe/allowed
- Reusable
- Durable
- Versatile
Currently available tools

Mini Jim
CH751
Auto-jigglers
Wafer Picks
TSA007
Shank/decoder
Design - Paper

Sketch out ideas
Design - CAD

Fusion360*

LibreCAD
Prototypes - MK1- “Lock-O-Diles”
Serrations tip

Dull vs Sharp Serrations
Prototyping
What’s next?

Keep improving prototypes

Send out prototypes to trusted friends to give candid feedback

Raw materials and Manufacturing


Distribution
Questions on Discord
@d1dymu5
Thanks