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, jiggles, 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

Coud’ve said “Multitool” but I didn’t want to confuse it with actual multitools.

Creativity - It might be super weird, but someone will like it. Don’t be afraid to ask for feedback.
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

PhySec tools can be fairly small to begin with.
If you had to conceal something or could only bring a limited number of items, but you didn’t know what you’d come up against, wouldn’t you want a tool that is good for multiple types of locks and doors?

During business hours, on-site engagements, you have to look the part. A big, 5.11 tactical Molle backpack will stick out.

You’re “silly” idea might be the tool locksmiths and locksport enthusiasts have been wanting, but you didn’t know. Some examples shortly.
My Inspiration

Spy Stuff

SERE

https://www.instructables.com/id/Gerber-Multi-Tool-Covert-Entry-Mod/
https://www.spygadgets.com/titanium-escape-ring/
Intl Spy Museum, early lockpick pen and jackknife
Survival, Evasion, Resistance, and Escape (SERE)
Improvements examples

Sparrows Mini Jim, Shank, Wafer Picks/jigglers

Sparrows Dark Shift Expansion

Slim down Mini Jim, skeleton-ize it
Shank tool - shorter, broader handle
Wafer picks - 2 sided, much less metal, less weight. SILENT
Rake/Hook pick called the “Quick Strike” - only available in Dark Shift Expansion set.
Hook AND a rake
Finger grooves
Thinned out handle on Jim
Designed by government covert entry specialist. Designed for field work and holding differently. I recommend these.
Also, featured in the International Spy Museum display
https://tag5industries.com/shop/ols/categories/pickset
Three collaborations with LockNoob and Sparrows. I think he has 6-7, but these are the “hybrid” tools I wanted to mention.
Gut Wrench - Example of a locksmithing tool that everyone needed, but had 5+ tools for various sizes instead.
Goat Wrench - Tubular tensioning
Medusa (Balisong) - Rake and Hook in one

Check out his site. He explains his designs and inventions much better than I do. Check out and subscribe to his YouTube. Good content, never dull or boring.
...or just weird

James Bond 1999 - The World Is Not Enough
Rake/Snake hybrid

Sherlock Holmes - Various Warded tryout keys.
Let's break down LockNoob's process. Again, check out his videos. He'll do a much better job explaining it that I ever could. Took sketches, thought about uses, designs, flaws, etc. Then moved to prototypes. Repeat until perfect. Mass production and collaboration with Sparrows.

Also, laser etching is cool.
Where to begin?

What am I trying to solve or improve?
What’s currently out there?
Design and drawing phase.
Prototypes and testing
Repeat
Slim, reusable, high quality.
TOOOL's is nice. Some aren't.
Lock Pick Collar Stays - R&D
Redesigns

Smooth corners
Tweak pick tips
Add serrations to Tension
Testing
Usability

*Disclaimer

Disclaimer: This will never be as good as full, single-purpose lockpicks.
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))

Did a Kickstarter. Handles shipping, payment, communications, etc.

Google Forms/Sites, PayPal button. PayPal does labels, postage, 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.

Yes, you basically pay all R&D out-of-pocket, but then it’s ready do go once you get funded.
Success

When in doubt: Laser
Check local trophy shops. Ask if they do laser etching AND on reflective surfaces
Current Projects by d1dymu5

Backstory

Bypass tool, jigglers, common keys

Backstory: New house. All the internal doors locked, didn’t leave any keys/screwdrivers/push-button tools
Carried Mini Jim around 24/7 (because my kids would lock them all)
Also, Travelers hooks are not comfortable in pockets.
What am I trying to solve or improve?
- Bypass Tool. Small Form Factor, multiple tools in one.
Current Mini Jims have extra material
What’s currently out there?
  Sparrows Mini Jim. Wafer Picks. Warded Picks. Common keys
Design and drawing phase.
Prototypes and testing
Repeat
Currently available tools

Mini Jim
CH751
Auto-jigglers
Wafer Picks
TSA007
Shank/decoder
Pro tip: Designing on paper is easier because you can trace out existing tools
Get dimensions
Usability
Functionality

**Tracing in CAD:** Take a picture. Make it black and white. Import it in and trace it in the CAD program. Delete the picture layer.

Examples:
Less handle, ergonomics
Dull Serrations
Keyring hole?

Fusion360 - Education License, Startup License, Free Trial, Subscription-based
I designed 4 tools.
I added some finger wells for better ergonomics. On the underside, I included DULL serrations for better gripping.
Added a hole for paracord or keychain.

Look like Crocodiles. Hey, I'm not a marketing guy. Don't care.
Lined-half circles

Dark Shift Serrations aren't as bad because they don't come to a point. They come to a plane.
CH751 - Pretty restricted on what you can change
Wafer Picks - one smooth, curved side, one linear
Auto Jigglers, various designs and things you can do

TSA007 - Scrapped idea. At .031”, Z-shaped wards and keyway,
not ideal for flat steel
Shank/Decoder - Not TSA permitted

Next steps - standardize jim dimensions across all.
Fix weird half-circle cutout on the wafer pick
Change profile of wafer pick. There is a high point that needs to be lower.
Deeper, more pronounced serrations
info@sparrows.com is a good point of contact.
I reached out about my lock pick collar stays and they were interested.

I hire a metal shop to laser cut my stuff. I send the CAD files, they calculate cost my material, thickness, and machine run time.
Questions on Discord
@d1dymu5
Thanks