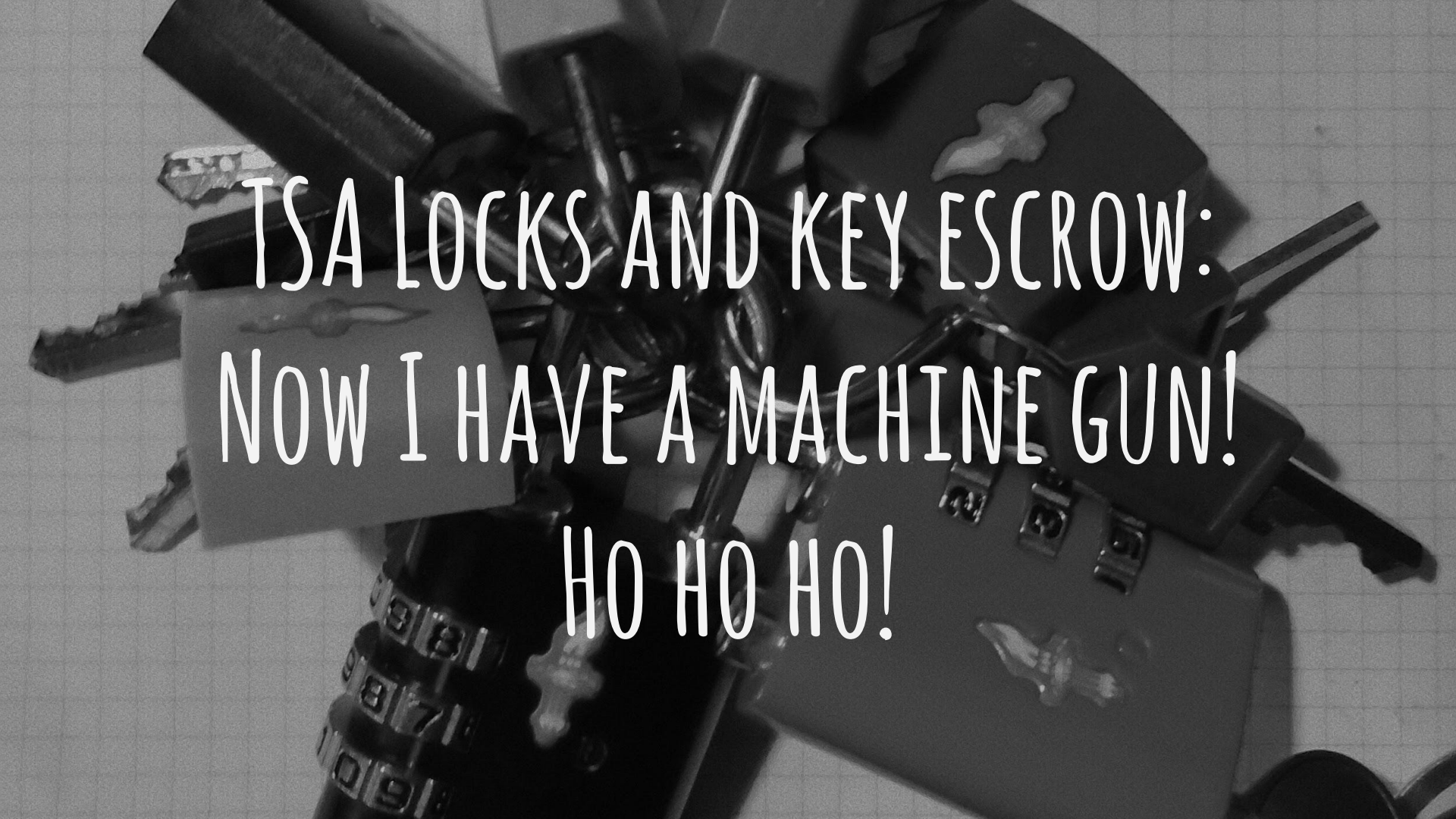

TSA Locks and key escrow:
Now I have a machine gun!
Ho ho ho!

Disclaimers

- This [redacted] presentation [redacted] not endorsed [redacted] has nothing to do [redacted] [redacted] current DHS/TSA, [redacted] or [redacted] [redacted]
- [redacted]
- [redacted] comments [redacted] opinions expressed herein are [redacted] and NOT those of [redacted] or [redacted] or [redacted] [redacted].
- [redacted] WE [redacted] ARE NOT [redacted] [redacted] LAWYERS [redacted]
- Use at your own risk
- Not responsible for death, [redacted] [redacted] lawyers, dismemberment, [redacted] [redacted] [redacted] [redacted] [redacted], acts of war, acts of deities, acts of [redacted] [redacted] in warzones, [redacted] [redacted], loss of [redacted] [redacted], dry mouth
- Not appropriate for children under 6” tall, small parts present a choking hazard to those lacking object permanence
- We are not responsible for your poor decision making
- Call before you dig
- If Frog begins to emit a 2600 HZ tone, deposit Frog in nearest AT&T phone booth
- Do [redacted] try this at home
- Not affiliated with the University of Florida or any other institution of higher learning
- Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by us or competence by the United States Government
- The user takes full responsibility for everything and anything that could and/or does go wrong resulting in any kind or type of problem, difficulty, embarrassment, loss of money or goods or services or sleep or anything else whatsoever

Yet More Disclaimers (you thought you were free)

- Unless the word absquatulation has been used in its correct context somewhere other than in this warning, it does not have any legal or grammatical use and may be ignored
- No animals were harmed in the creation of this presentation, one of you will accuse us of this regardless
- Those of you with an overwhelming fear of the unknown will be gratified to learn that there is no hidden message revealed by reading this warning backwards
- [redacted] and NOT those of [redacted] or [redacted] or [redacted]
- You are advised that urgent, time sensitive and confidential communications should not be sent by e-mail. You agree that you will not use e-mail correspondence for unlawful purposes or in contravention of Laws on electronic communications
- This presentation is intended for the use of the individual attendees in the audience and may contain information that is confidential, privileged or unsuitable for overly sensitive persons with low self-esteem, no sense of humour or irrational religious beliefs, any dissemination, distribution or copying of this slide deck is [redacted] authorised (either explicitly or implicitly or [redacted]) and constitutes an irritating social faux pas
- [redacted] WE STILL [redacted] ARE NOT [redacted] [redacted] [redacted] [redacted] LAWYERS [redacted]
- We do not endorse any activity or recommend it to any particular person - we simply describe our experiences and opinions; If you choose to engage in these activities it is by your own free will and at your own volition
- Use your brain and common sense when engaging in any activity or making any modifications
- Remember: Safety first, always use common sense; Never do more than you are comfortable with; Always wear safety belts and use all appropriate safety equipment

What are TSA Approved locks?

- Introduced to address TSA policy of destructively opening locked luggage for screening in 2003
- Proprietary systems with little public information for review
- Designed to be opened with one of several “master” keys provided to the TSA, customs, law enforcement, etc (both US and foreign agencies) - a form of key escrow
- May be keyed (owner gets a key that operates the lock) or combination (owner receives no key)
- Two competing standards (Travel Sentry and Safe Skies)

What are TSA Approved locks?

- Travel Sentry sets standards for the override keys and mechanisms then licenses those standards to “hundreds” of manufacturers
- Dominant standard in the consumer market
- Currently offers 7 known override keys numbered as TSA001-TSA007

Travel Sentry ®, an organization that provides security solutions to the travel industry, announced today a new baggage locking system that allows airline passengers to lock their bags without interfering with the Transportation Security Administration's (TSA) need to open bags for inspection.

...

"TSA is ready to work with any industry in developing practical solutions that contribute toward our goal of providing world-class security and world-class customer service," said Ken Lauterstein, Program Manager for Checked Baggage Screening Operations in TSA's Office of Aviation Operations.

12 November 2003 - http://www.travelsentry.org/en/press-release/2003/pr-12-november.php

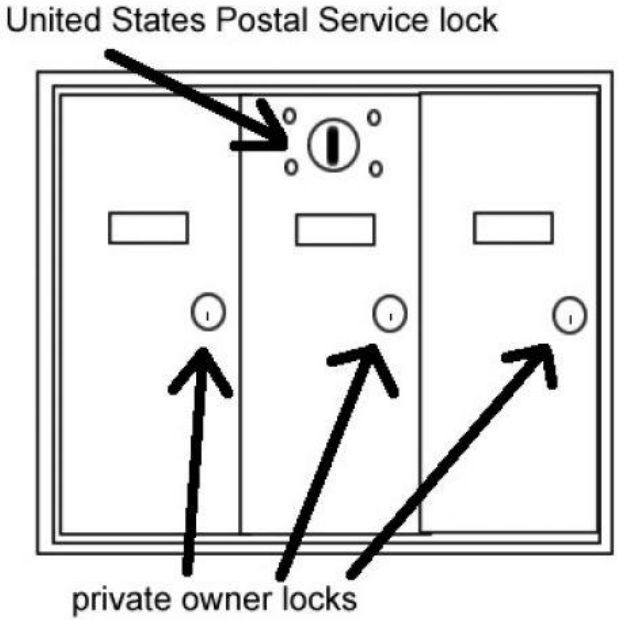
(Remember these quotes for later)

What are TSA Approved locks?

- Safe Skies manufactures locks under their own competing standard
- Only offers a single override key (labeled as TSA Safe Skies)
- Has sued Travel Sentry for patent infringement
- Smaller market share than Travel Sentry
- All available information indicates only one override/master key for their entire system

What is Key Escrow?

- owner/users gets an access token
- 3rd party (typically Gov't) get a separate access token held in 'escrow'
- 3rd party is only allowed to use escrowed token under specific situations
- USPS multi-dwelling unit mailboxes work on this principle
- Proper function requires 3rd party complies with the rules

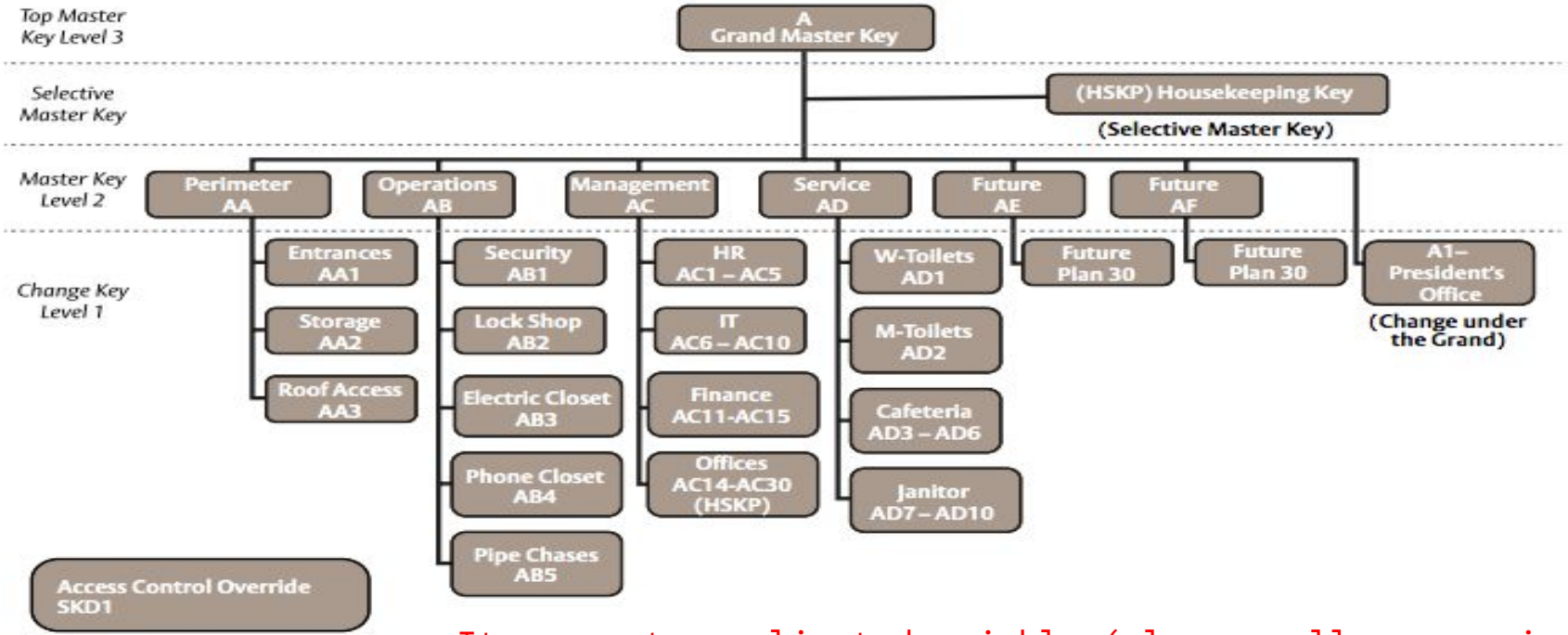


USPS lock gives letter carrier access to all boxes, owner locks give access to individual boxes.

image source: http://hubpages.com/living/USPS-Approved-Mailboxes---FAQ

Master Keys

The following represents a schematic of a level three (GMK) system.
Your system may vary somewhat from this.



It can get complicated quickly (also, really expensive)

The TSA went for something a bit simpler

Less simple, slightly more secure.

We now have 8 master keys to compromise but, a bad (internal) actor can still grab them on a single keyring.

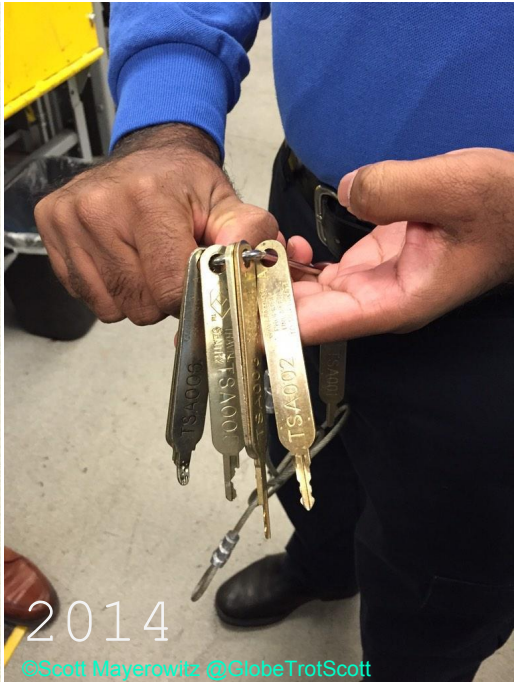
Protected by US Patents 7,021,537 and 7,036,728

Travel Sentry key compromise

Travel Sentry and the TSA are bad at data classification and key escrow security.

Travel Sentry key compromise

Travel Sentry and the TSA are bad at data classification and key escrow security.



Travel Sentry key compromise

Travel Sentry and the TSA are bad at data classification and key escrow security.

Travel Sentry ke

Travel Sentry and classification and key escrow securi

©Ryetronics on Instagram

Guide to Travel Sentry Passkeys - May 1 2008

TSA001 - Version A with black numbers

TSA002 - Original – never changed

TSA003 - Black metal version

TSA004 - Original – never changed

TSA005 - Original – never changed

TSA006 - Version A with black numbers

TSA007 - Original – never changed

Sensitive Information – do not post, copy or disseminate

bags passed through TSA hands during the Thanksgiving

The Washington Post

ys for TSA-approved baggage locks.

One Gas Pump Key Lets Thieves Steal Your ID

The NBC Bay Area Investigative Unit has found a single master key grants access to gas pumps across the state and it s giving easy access to thieves looking to compromise Bay Area drivers credit card information. Vicky Nguyen first aired this story Nov. 8 at 11 p.m.

T:a classification and

1

2

3

4

5

checked bags passed through TSA hands during the Thanksgiving

2014

The Washington Post

master keys for TSA-approved baggage locks.

One Gas Pump Key Lets Thieves Steal

The NBC Bay Area Investigative Unit has found a single master key grants a
to gas pumps across the state and it s giving easy access to thieves looking
compromise Bay Area drivers credit card information. Vicky Nguyen first aire
story Nov. 8 at 11 p.m.

NEW YORK POST

METRO

The $8 key that can open New York City to terrorists

By Susan Edelman

September 20, 2015 | 5:22am

A Post reporter bought this key to the city online -- with no questions asked.

Photo: Anne Wermiel

Travel Sentry key compromise

Travel Sentry and the TSA are bad at data classification and key escrow security.

Real Bad.

And yet you did exactly that.

***** They left it at https://www.travelsentry.org/security/pdf/Guide_to_TravelSentry_Passkeys_1_October_2012-EN.pdf and didn't notice for months. *****

Photos aren't the same as handing out keys, right?

- Oops, nope. Just as bad if not worse. (You can't email a physical object)
- Researchers in academia and the security community have been warning about key duplication from photos for years
- At least two business (Key.me and Keysduplicated.com) offer this as their primary service
- TOOOL.nl and others have even demonstrated using this technique for High Security keys and locks
    - "Showing Keys in Public - What Could Possibly Go Wrong?" Jos Weyers, HOPE X, July 19, 2014
    - "Copying keys from photos is child's play" The Guardian, November 14, 2008 (Sneakey project)
    - "Methods of Copying High Security Keys" Barry Wels and Han Fey, The Last HOPE, July 19, 2008
    - AutoKey3D (formerly PhotoBump) Presented at LockCon 2014 and released on GitHub by Christian Holler (https://github.com/choller/autokey3d)

“Fun” with 3D Printing

The "Fun:"

- @DarkSim905, @Xylit01, MS3FGX, @J0hnnyXm4s
  1. Take images
  2. Raytrace
  3. 3D CAD
  4. 3D print those suckers and test
  5. Refine, reiterate
  6. GitHub!
  7. Refine, reiterate

README.md

3D TSA "Travel Sentry" master keys

Recently, pictures of TSA master baggage keys got leaked by the Washington Post and also PDFs hosted on TravelSentry's Website. This repo is a reproduction attempt

Security researchers have long warned of the dangers of using master-keyed locks

The TSA has issued an official statement making it known that they don't even care that we've done this, as the now-pointless locks affect theft prevention, not airline safety.

> **[!] Important**: These keys have not been widely-tested, though we do have reports that many do work from at least one source. 006 May never work, as we're not sure of the depth of the "dimples," and also consumer-grade 3D printers may not be up to such finely-detailed tasks.
>
> Added the stubby versions of the keys by MS3FGX, which appear to still work fine !

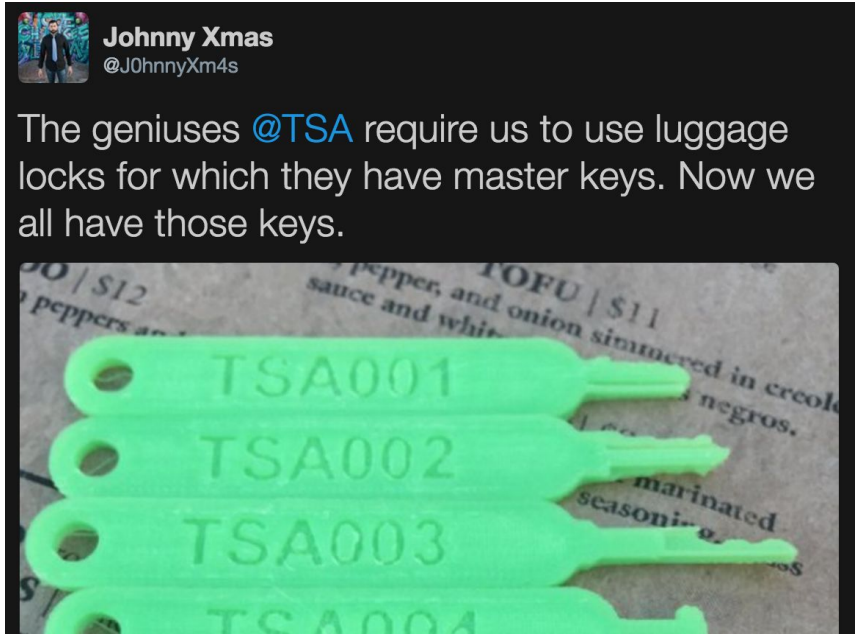
3D Printing keys is a really dumb idea

- Torsion strength of materials is often less than is necessary
  - Even when they do work, you rarely get more than a few uses out of a single key
- Materials expand / contract while cooling, resulting in a final product that can deviate significantly from the design
- Filing our own metal keys is very easy.

Dealing with the Media

DEALING WITH THE MEDIA

- Content is rarely, if ever fact checked.
- Most news outlets:
  - At best are now nothing more than Twitter aggregates
  - At worst, they are news outlet aggregates
- Attempts to contact the “journalists” to have corrections made were almost universally met with radio silence

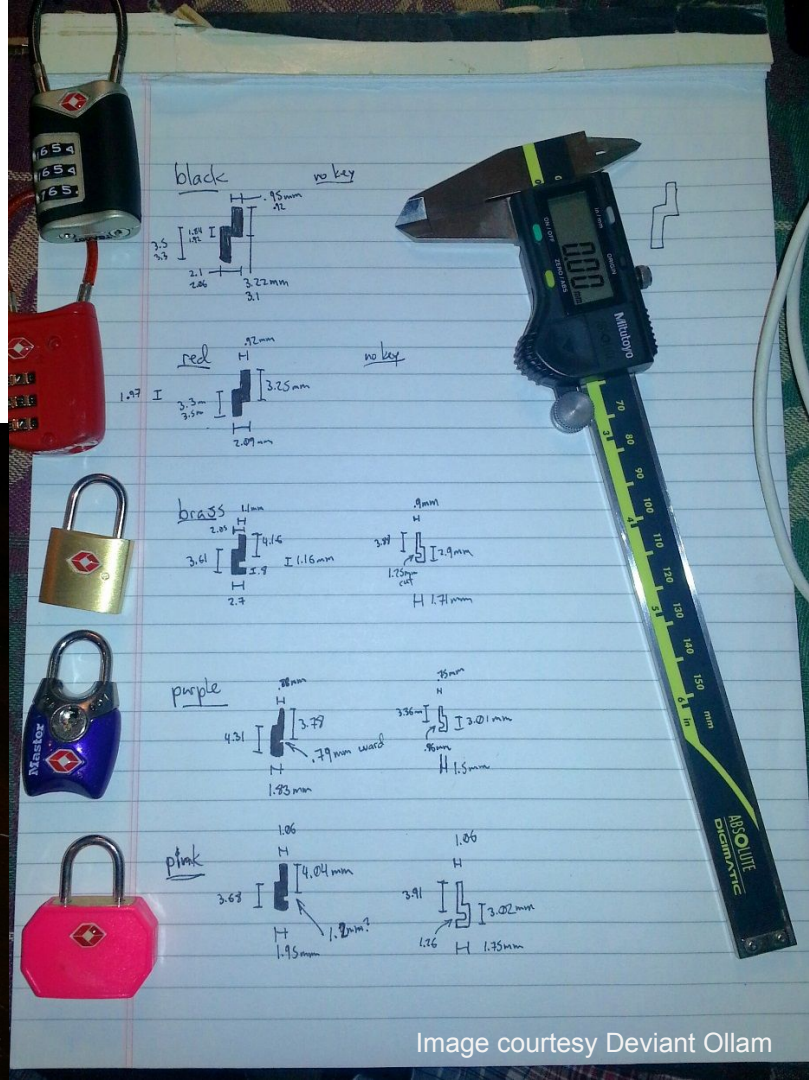


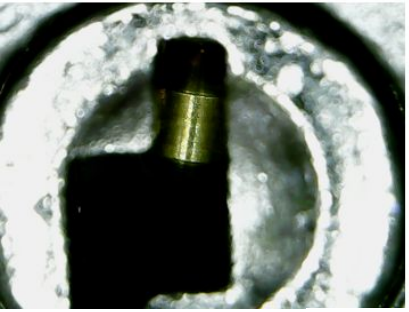
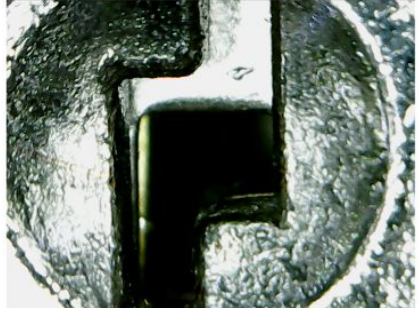
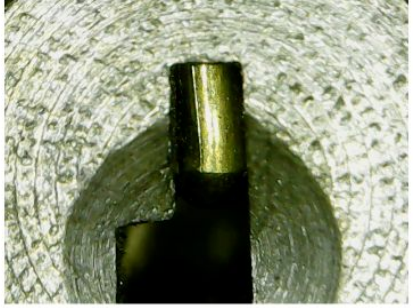
DEALING WITH THE MEDIA

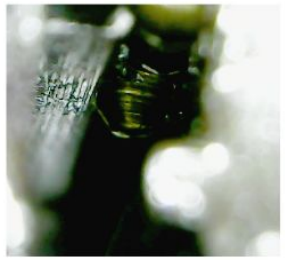
- OK, yes, there are still good journalists who care about presenting a story factually and properly
  - Brian Krebs (Krebs on Security)
  - Jenna McLaughlin (The Intercept)
  - Cory Doctorow (Boing Boing)
  - Jose Pagliery (CNN Money)
  - Andy Greenberg (Wired)
  - Steve Ragan (CSO Online)
  - Bruce Schneier (Schneier on Security)

- Note they’re mostly tech journals, which muggles don’t read :/

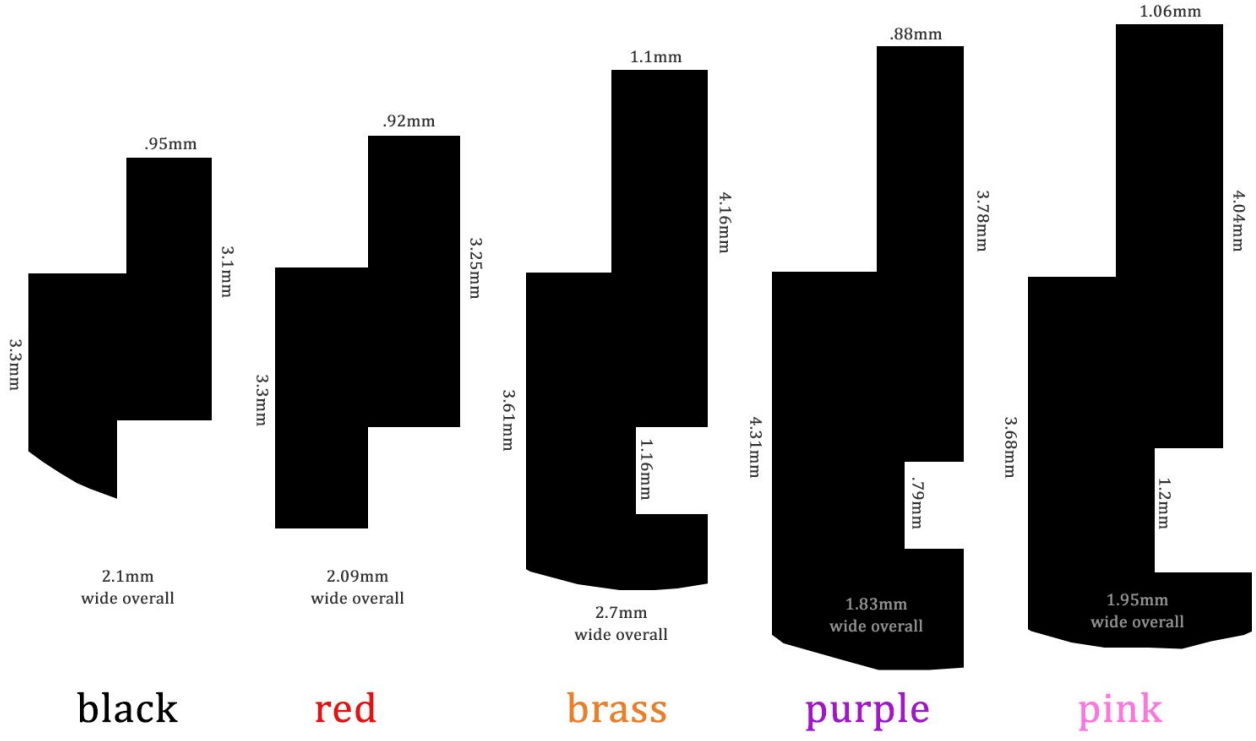
Testing and Refining





A comparison of TSA007 keyways and mechanisms showing the varying dimensions and mechanisms between designs



Images courtesy The CORE Group and Deviant Ollam
See http://enterthecore.net/tsa007/

Rogue Keys, Mock-ups, Impressioning, and Decoding

So, nothing left to do, right?

Not quite. Remember, two competing standards? Only one compromised by leaked images and docs. Also not everyone has a 3D printer or the cash to buy printer time from Shapeways.

So what do we do? Fall back on century old techniques:

1. ID and source compatible blanks (or modify ‘user’ keys)
2. Impression the hell out of some locks
3. Adopt, adapt, improve.

No Safe Skies, you can't feel smug either

First, we need key blanks.

What if we can't find them? We make our own.

The easy way: sheet styrene from a hobby shop and some glue

The hard way: find a blank that is close and introduce it to a Dremel tool

No Safe Skies, you can't feel smug either

Okay we have our blanks but this is going to be a long brute force slog right?

Safe Skies committed the one of the cardinal sins of key security.
They used a single key for both master keyed and non-master keyed locks.

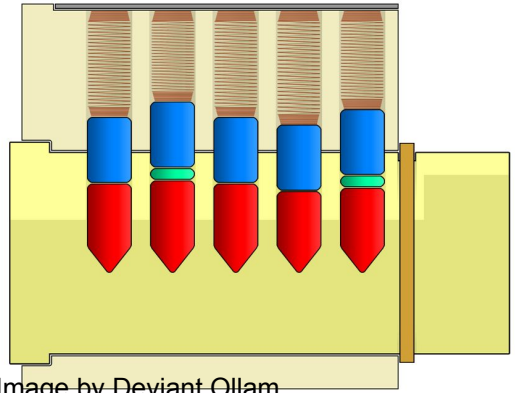


Image by Deviant Ollam

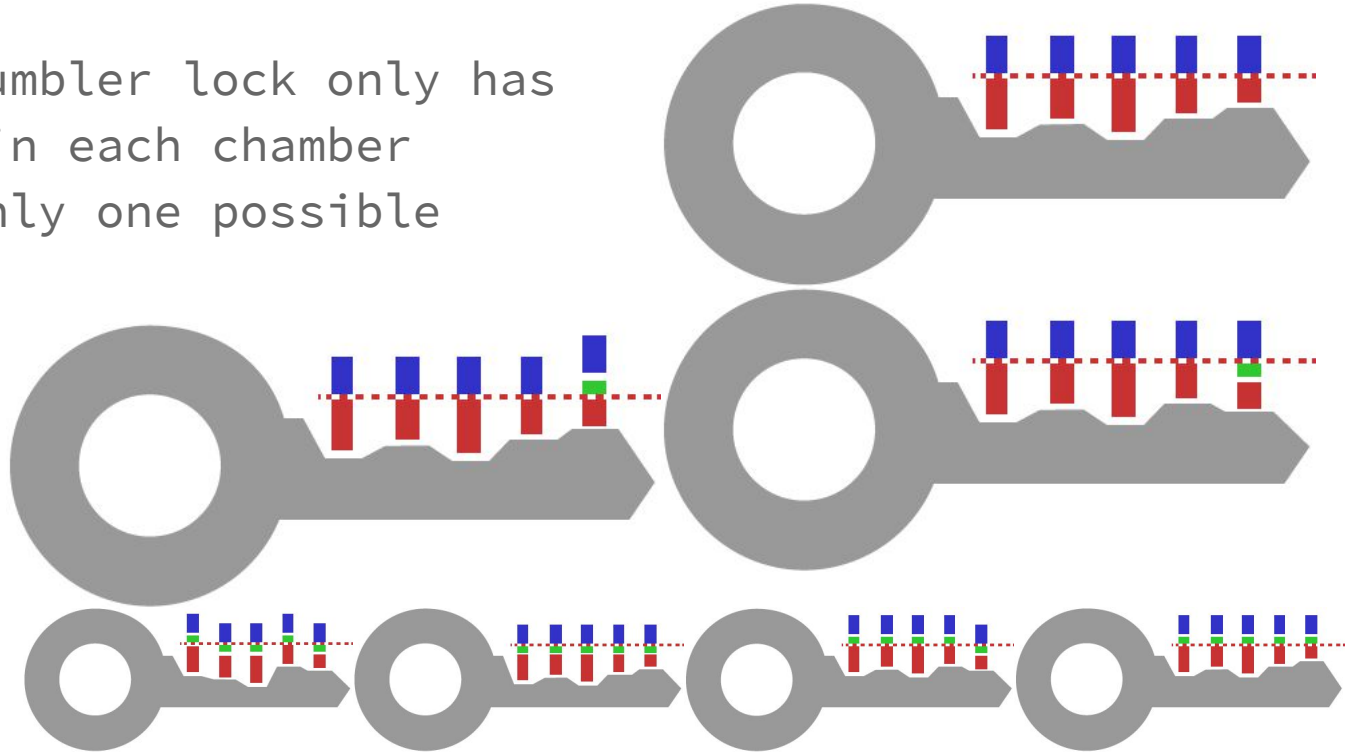
Big difference in complexity

Master Keying

A regular pin-tumbler lock only has a pair of pins in each chamber which creates only one possible key.

Adding more pins to each stack creates extra possible keys.
1 master pin = 2 keys
2 master pins = 4 keys
3 master pins = 8 keys
4 master pins = 16 keys

and so on following the formula of 2^x where x is the number of master pins

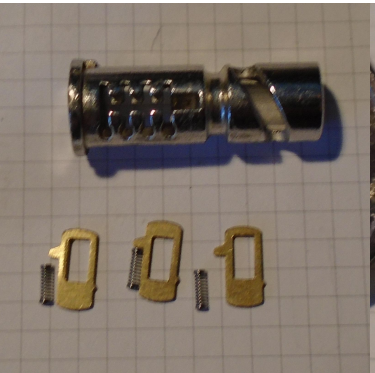


Images courtesy David Knauer

No Safe Skies, you can't feel smug either

Physical access with no monitoring means we can get messy.

1. Take non-mastered lock, introduce a Dremel tool
2. Remove override cylinder
3. Decode and fit homemade blanks
4. ???
5. Exploit!



What does the TSA think?

"The reported ability to create keys for TSA-approved suitcase locks from a digital image does not create a threat to aviation security. These consumer products are "peace of mind" devices, not part of TSA's aviation security regime. Carried and checked bags are subject to the TSA's electronic screening and manual inspection. In addition, the reported availability of keys to unauthorized persons causes no loss of physical security to bags while they are under TSA control. In fact, the vast majority of bags are not locked when checked in prior to flight."

-TSA spokesperson Mike England
https://theintercept.com/2015/09/16/tsa-doesnt-really-care-luggage-locks-hacked/

README.md

3D TSA "Travel Sentry" master keys

Recently, pictures of TSA master baggage keys got leaked by the Washington Post and also PDFs hosted on TravelSentry's Website. This repo is a reproduction attempt

Security researchers have long warned of the dangers of using master-keyed locks

The TSA has issued an official statement making it known that they don't even care that we've done this, as the now-pointless locks affect theft prevention, not airline safety.

> **[!] Important**: These keys have not been widely-tested, though we do have reports that many do work from at least one source. 006 May never work, as we're not sure of the depth of the "dimples," and also consumer-grade 3D printers may not be up to such finely-detailed tasks.
>
> Added the stubby versions of the keys by MS3FGX, which appear to still work fine !

Future Systems (Stanton Concepts Gen 2 proposal)

TSA's Challenge, too many keys:

- "Keys are a BIG pain in the #@%$" Senior Management
  - 450 Airports
  - 4000 Kits
    - Key Ring Contains all TSA Keys:
      - TSA001 – Ningbo et al
      - TSA002 – Sinox et al
      - TSA003 – Fullyear-Brother et al
      - TSA004 – CCL et al
      - TSA005 – Sun Lock et al
      - TSA007 – Yi Feng et al
      - "SAFE SKIES"
    - 8" Side Cutting Electricians Pliers (the grand master key)
    - 24" Bolt Cutters (the supreme grand master key)
- "Would rather just cut the locks off" Senior Management

Future Systems (Stanton Concepts Gen 2 proposal)

SCI recognises why the existing system is bad for the traveling public

The Consumer's Challenge: More for Less

- Existing Products Offer Low Security:
  - 1 Key opens 10's of millions of locks of the same family
  - Locks easily picked:
    - YouTube ~750 videos on bypassing luggage locks
    - Google ~85,000 results from "TSA Lock Picking" query
  - Keys are copied:
    - Instructional videos on the Web
    - Easily duplicated
    - 3D printing
  - No Tamper Indication
    - Current products easy to bypass, and no indication of violation
- Cost

Future Systems (Stanton Concepts Gen 2 proposal)

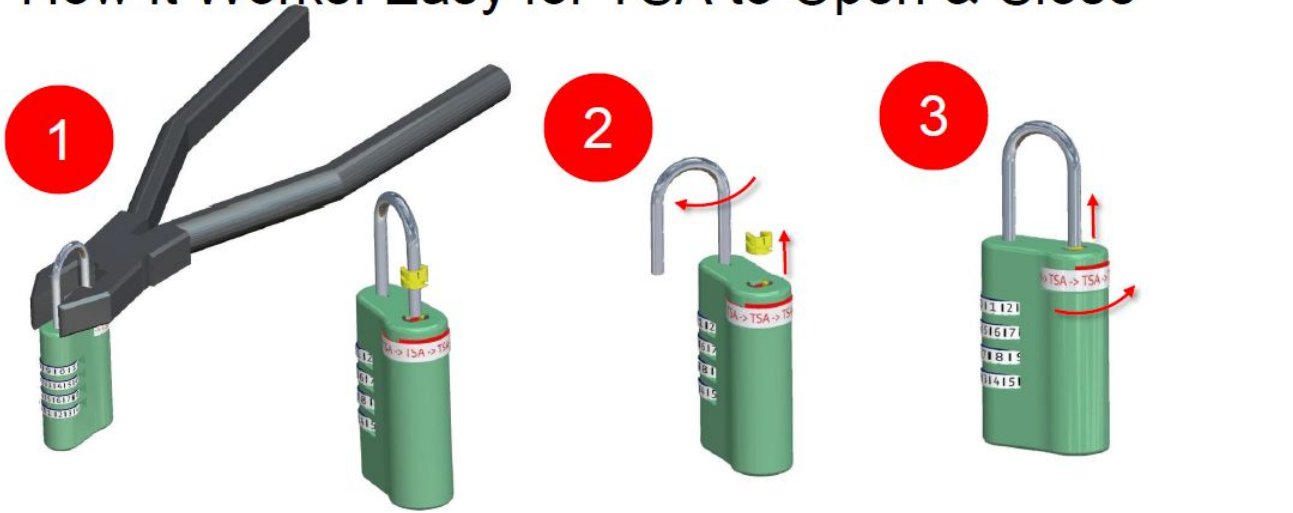
SCI recognises why the existing system is bad for the traveling public

So they make it worse!

SCI's Next Generation Lock:

Patent Pending

How It Works: Easy for TSA to Open & Close



Clip Cup with standard tool (8" Pliers) → Inspect → Advance New Cup

So what now? (for the traveling public)

- TSA Approved locks were never secure to begin with and most luggage isn't either
- Remember criminals have had access to these keys or subtle destructive techniques for years
  - Theft by airline and TSA staff is common and easily hidden
- The only real change is that now YOU know
  - Use tamper evident seals
  - Remember this every time a government official claims to need more access and authority
  - **Avoid valuable or sensitive items in checked bags. This is the only failsafe.**

So what now? (for the security community)

- Use this to explain why Key Escrow crypto systems in government hands are unsafe
- Every security system is only as good as its weakest element
- You need plans to revoke and replace compromised locks and keys just like CA certs and crypto keys
- Don’t trust “black box” security solutions
- We need to apply the same peer review and open source philosophy to analysing physical security
- Hold government, standards bodies, and manufacturers accountable for their screwups

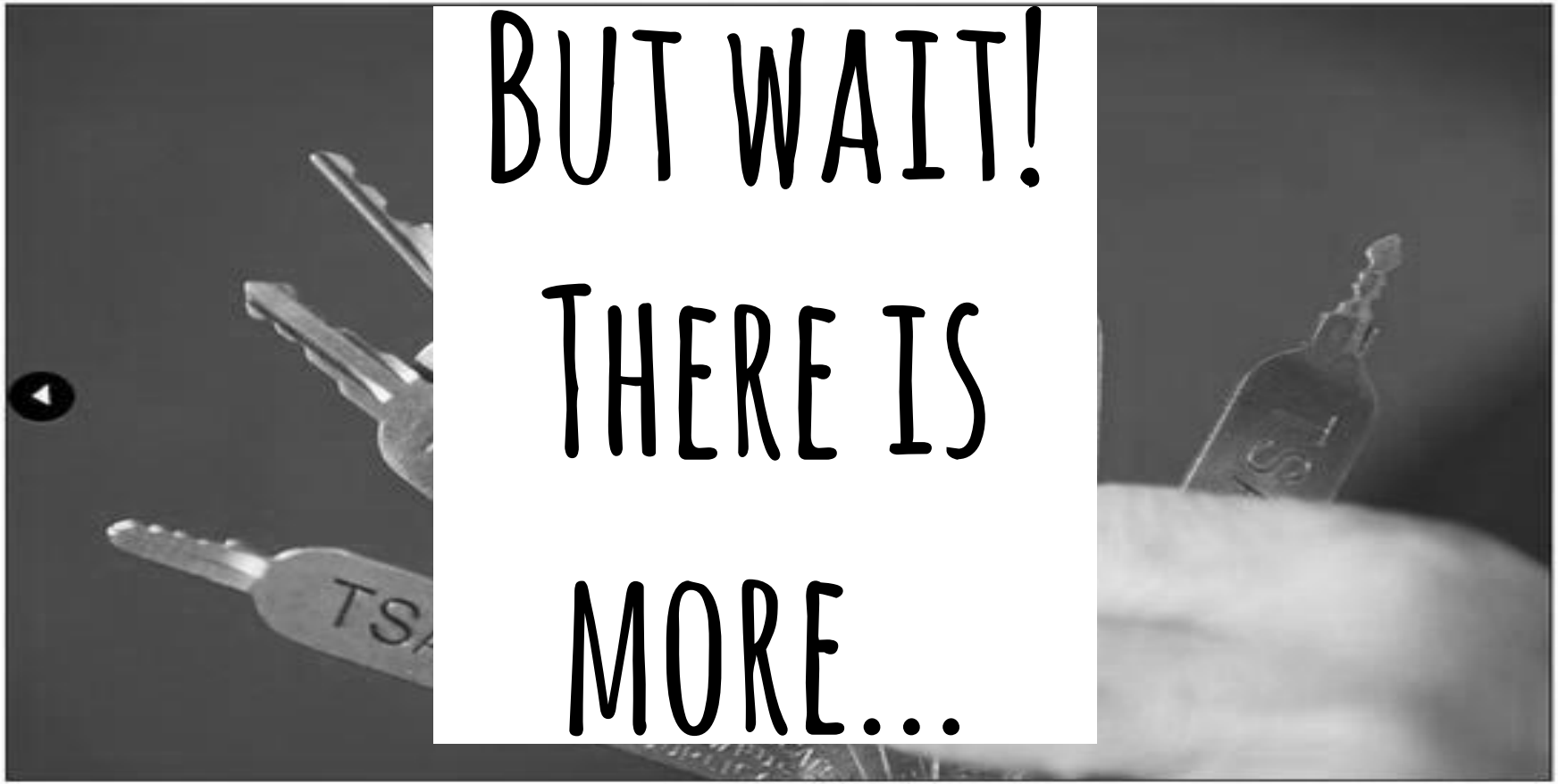
Questions?

(too bad)

@DarkSim905, @J0hnnyXm4s, @nite0wl_2600

With Many thanks to ***Xylit01***, MS3FGX, Irongeek_ADC, Deviant Ollam, David Knauer, PNTinDC, Click, and too many others I can't name.

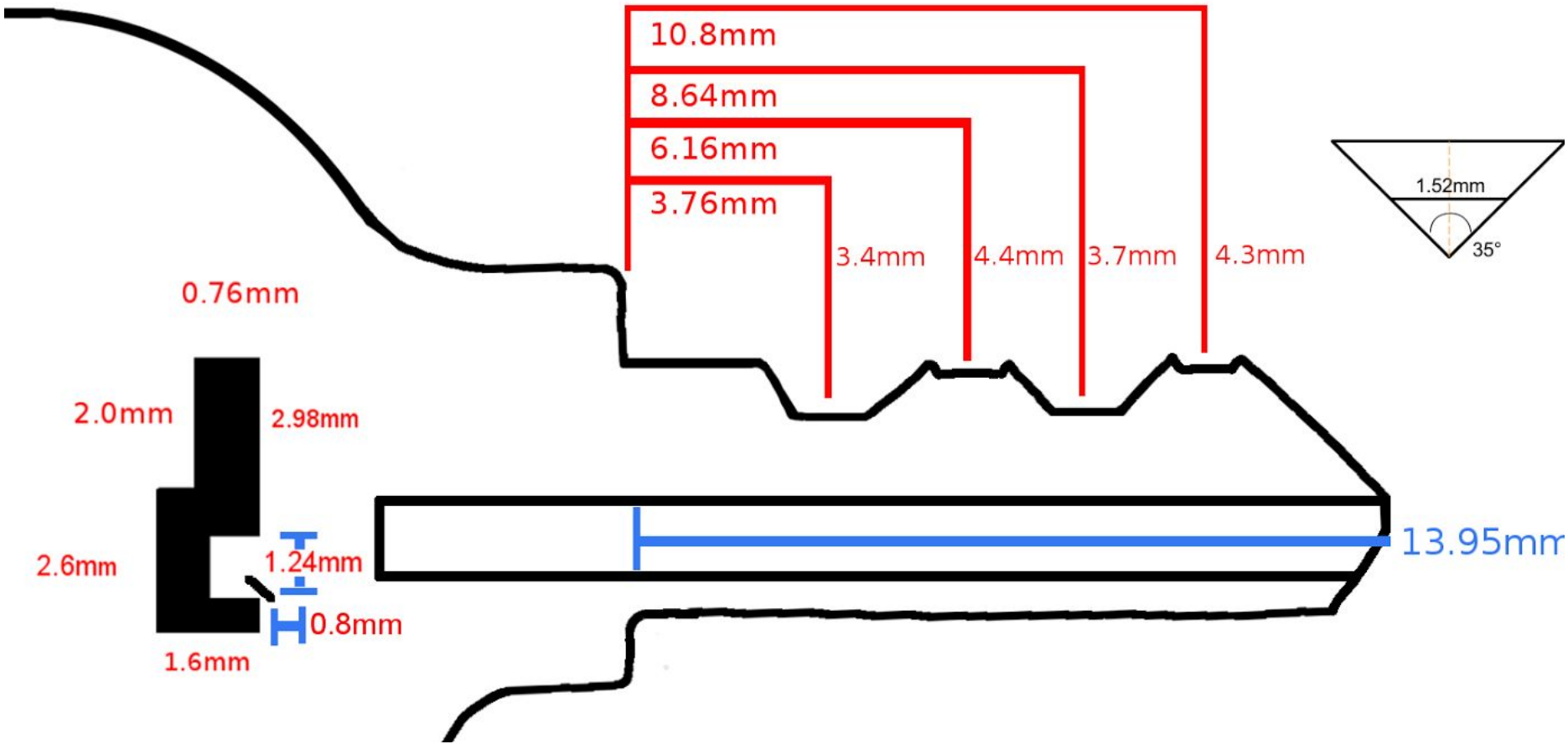
About 14 million checked bags passed through TSA hands during the Thanksgiving holiday weekend.



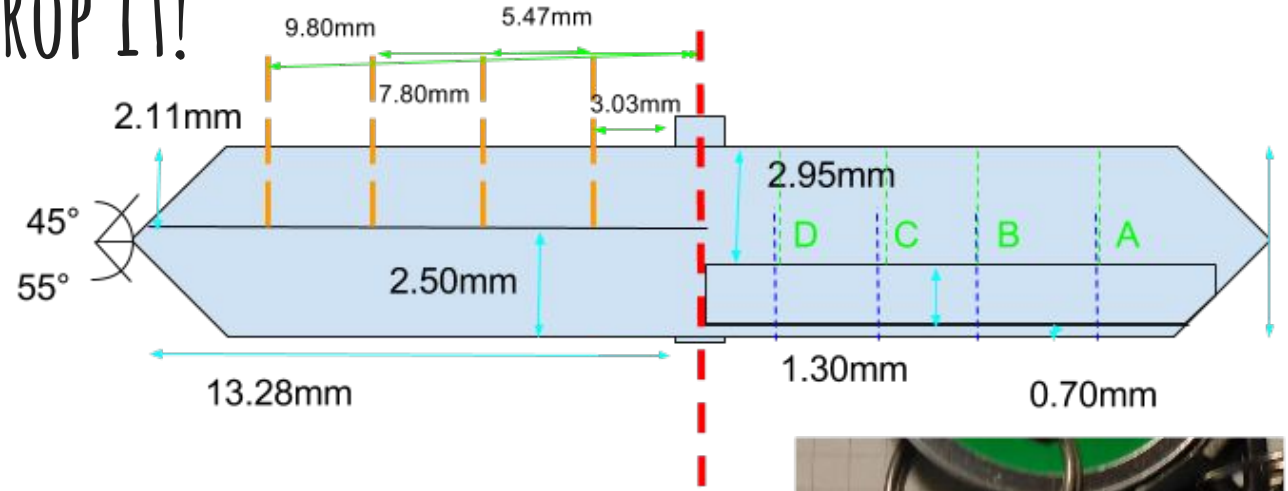
The Washington Post

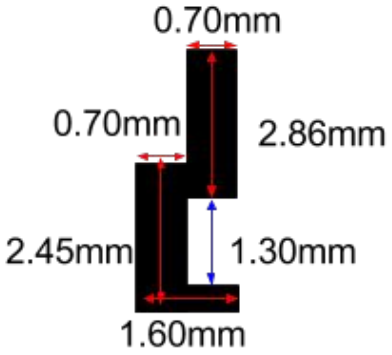
Security officers have master keys for TSA-approved baggage locks.

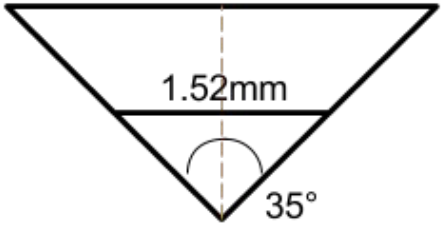
Drop it!


10.8mm
8.64mm
6.16mm
3.76mm
3.4mm
4.4mm
3.7mm
4.3mm
1.52mm
35°
0.76mm
2.0mm
2.98mm
2.6mm
1.24mm
0.8mm
1.6mm
13.95mm

Drop it!







Cut Depths(Green/dark blue):
A: 0.6mm/3.45mm
B: 0.87mm/4.30mm
C: 0.29mm/3.66mm
D: 1.13mm/3.62mm

In the research samples Safe Skies locks are frequently not fully populated and stack 4 is often left un-populated, particularly in keyed pin-tumbler locks.