Bypass101

An Introduction to Basic Bypass Methods

Karen Ng
k.ng@ggrsecurity.com
@kng.bsky.social
@hwenab

Sam Mayers
S@clearsear.ch
@mac0s
@XProtectSzn

INTRO/WHAT IS BYPASS?

When people think of physical hacking, they often think of showier methods such as lockpicking.

However, there are plenty of other methods that can allow people to access locked-out locations known collectively as “Lock Bypass”.

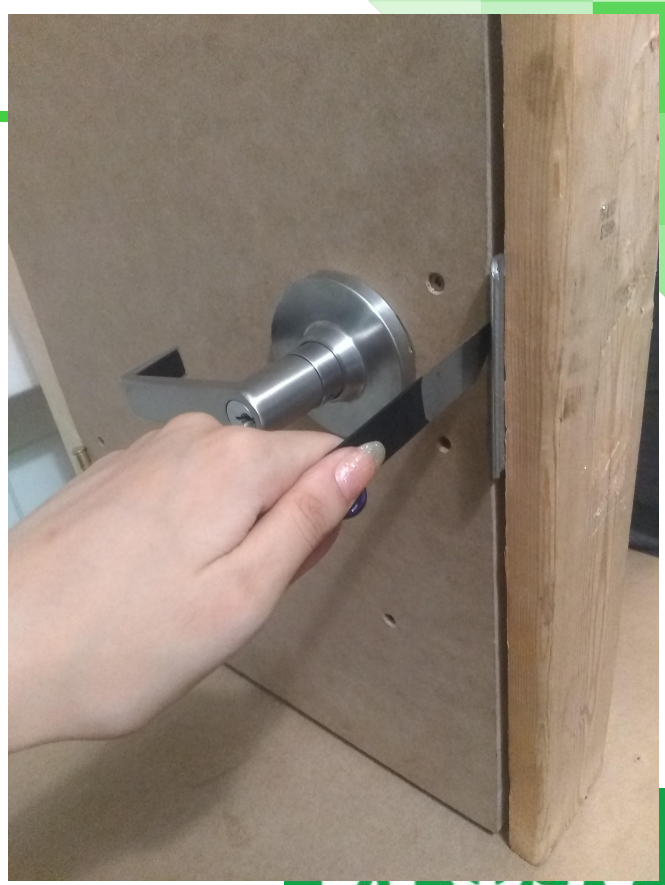
twitter.com/Cyber_Cox

ΦSV

MORE INTRO/WHY BYPASS?

Lock Bypass involves ignoring the lock altogether and finding alternative ways to open a door or avoid having to use a door altogether.

Lock Bypass methods are often much faster and more reliable than lockpicking, and is used more often in physical hacking.



tiktok.com/ryansadusky

AGENDA/TYPES OF BYPASS

- Latch Pulling/Shoving
- Under-the-door tool
- Doorknobs
- Crashbars
- Pushbars
- Pulling Really Hard
- Hinges
- Padlock shims
- Button-Push Combination Boxes
- Enterphones
- Wheelchair Buttons
- Elevators
- Alarm Basics
- Contact Sensors
- PIR Sensors
- Unlocked/Improperly Locked Doors
- Getting around it — Ceilings/Windows/Etc

ΦSV

Latch-Targeted Bypass

Latch Targeted Bypass - Intro

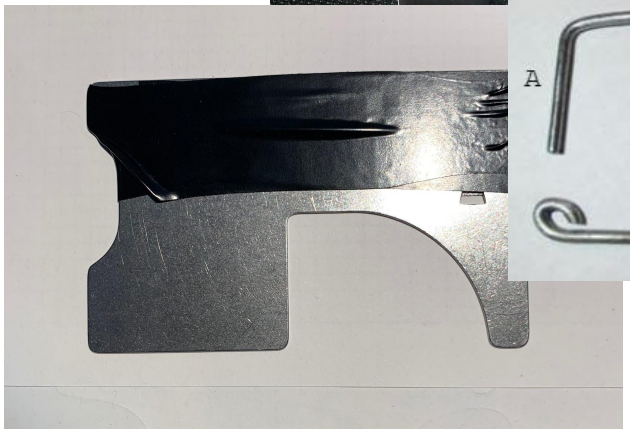
Carding targets the latches that hold the door closed.

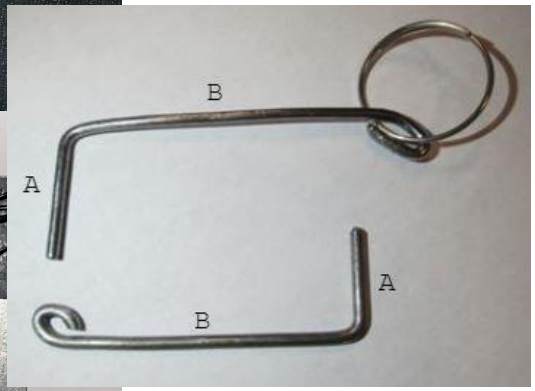
Depending on the orientation of the latch, one is able to either “shove” or “pull” the latch.

THE TOOL

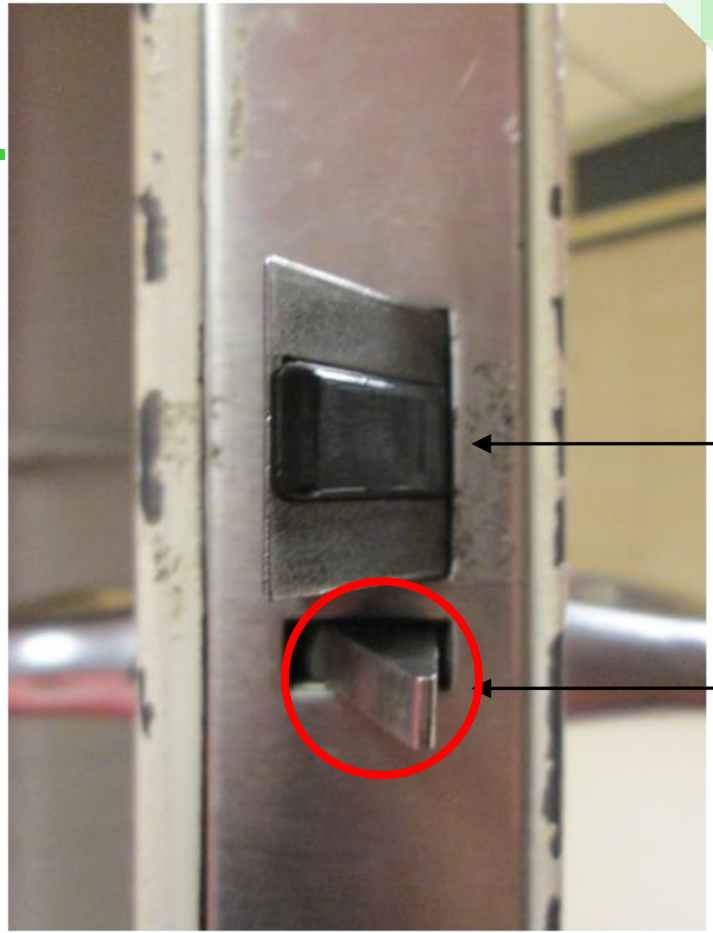
There’s a variety of tools you can use for carding. Most commonly:

- latch slips/travelers hooks
- plastic cards
- A well bent piece of wire





REQUIREMENTS




F
DOREX
SS

De-actuating the Deadlatch

Sometimes, the door is installed in such a way that the deadlatch is already in a hole in the strikeplate.

Other times, the deadlatch is installed almost properly.

DEADBOLTS

This is a deadbolt. They are different from deadlatches, and often have a thumb turn on the other side.

These prevent you from being able to use latch-targeted bypass techniques, as well as the under-the-door tool.

INSTRUCTIONS FOR USE (PULLING)

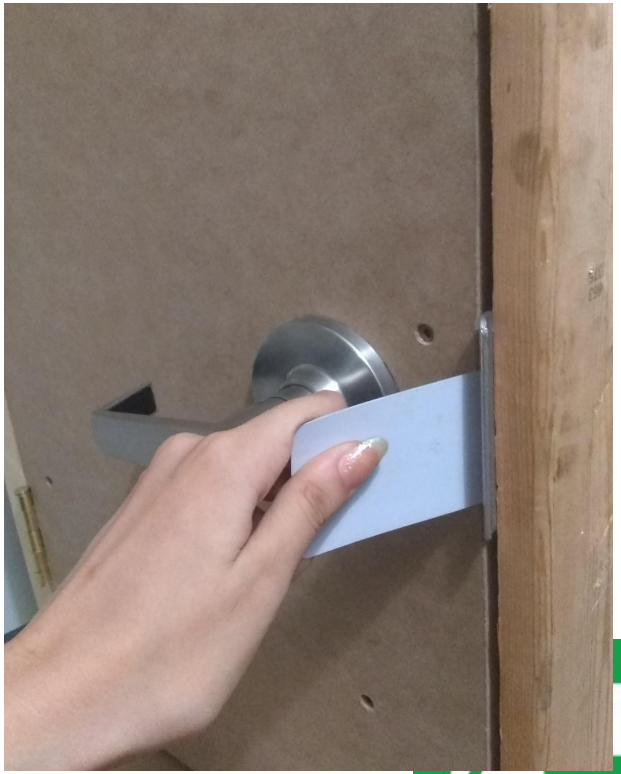
After ensuring that the deadlatch is not actuated:

1. Place the latch slip tool behind the latch. Wiggle the latch slip to move the latch into the door.
2. Without removing the tool from holding in the latch, pull the door open.

INSTRUCTIONS FOR USE (SHOVING)

After ensuring that the deadlatch is not actuated:

1. Shove the shoving tool between the latch and the strikeplate.
2. Without removing the tool from holding in the latch, pull the door open.



ΦSV

Handle-Targeted Bypass

Handle-Targeted Bypass - Intro

Sometimes, the deadlatch is actuated and the door cannot be carded. All is not lost!

There exists Lock Bypass methods that target the handle of the door instead of the latch.

This method mimics a person exiting through the door from the other side.

HANDLE-TARGETED BYPASS - INTRO

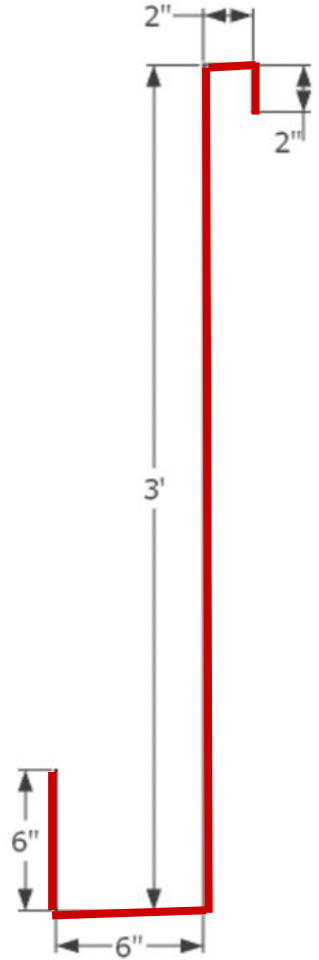
The under-the-door tool allows us access to areas with properly functioning deadlatches.

This Bypass method targets doors with lever-type handles.

THE TOOL

Thick wire about 5ft long, with string tied to the end.

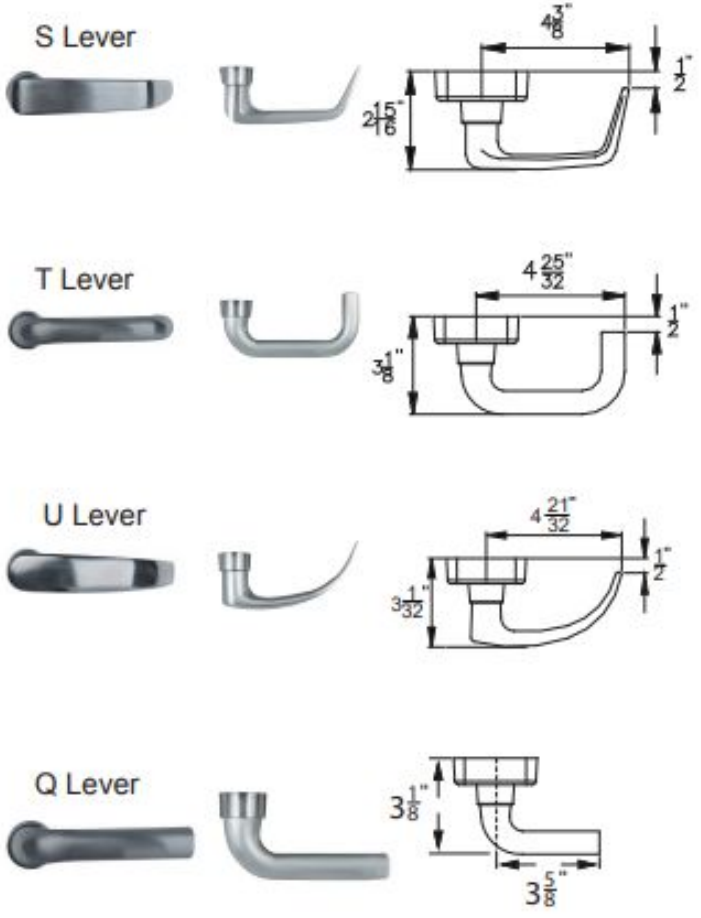
The tool is measured against the door handle and is bent into a hook-shape at the top.



REQUIREMENTS

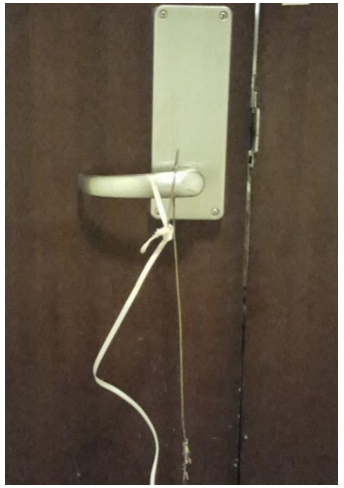
As mentioned before, this Bypass Method targets doors with lever-type handles.

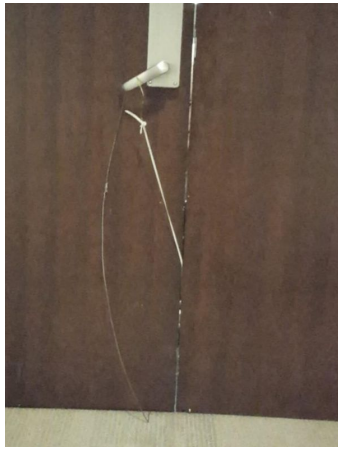
In addition to this, you will also need enough room under or beside the door to fit the tool.



INSTRUCTIONS FOR USE

1. Insert the tool under the door
2. Maneuver the tool until the top hook rests behind the door handle.
3. Move the tool to the end of the handle.
4. Pull on the string, actuating the lever.



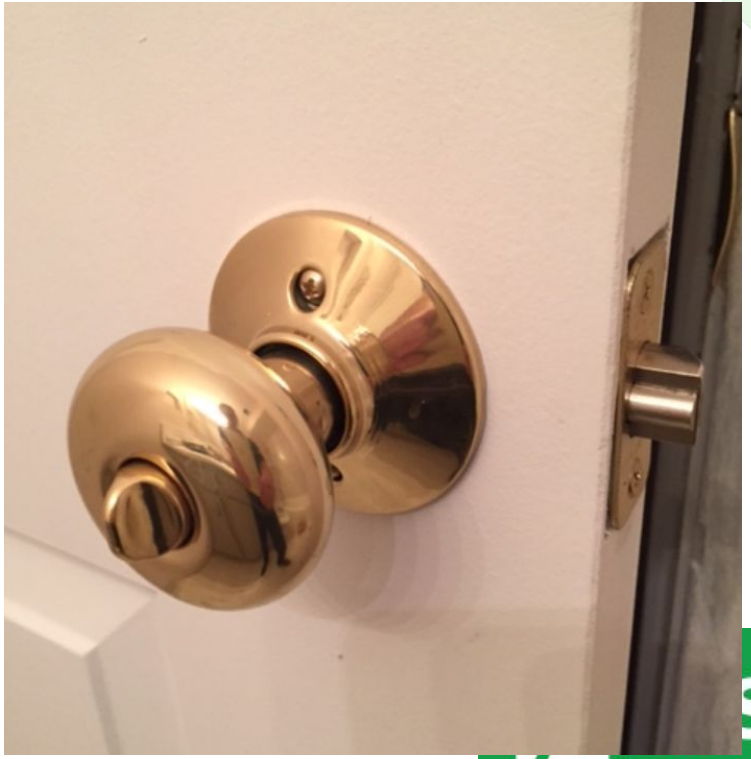


Door Knobs

DOOR KNOBS - INTRO

Doorknobs are often difficult to bypass. Thankfully, they are slowly being phased out of use.

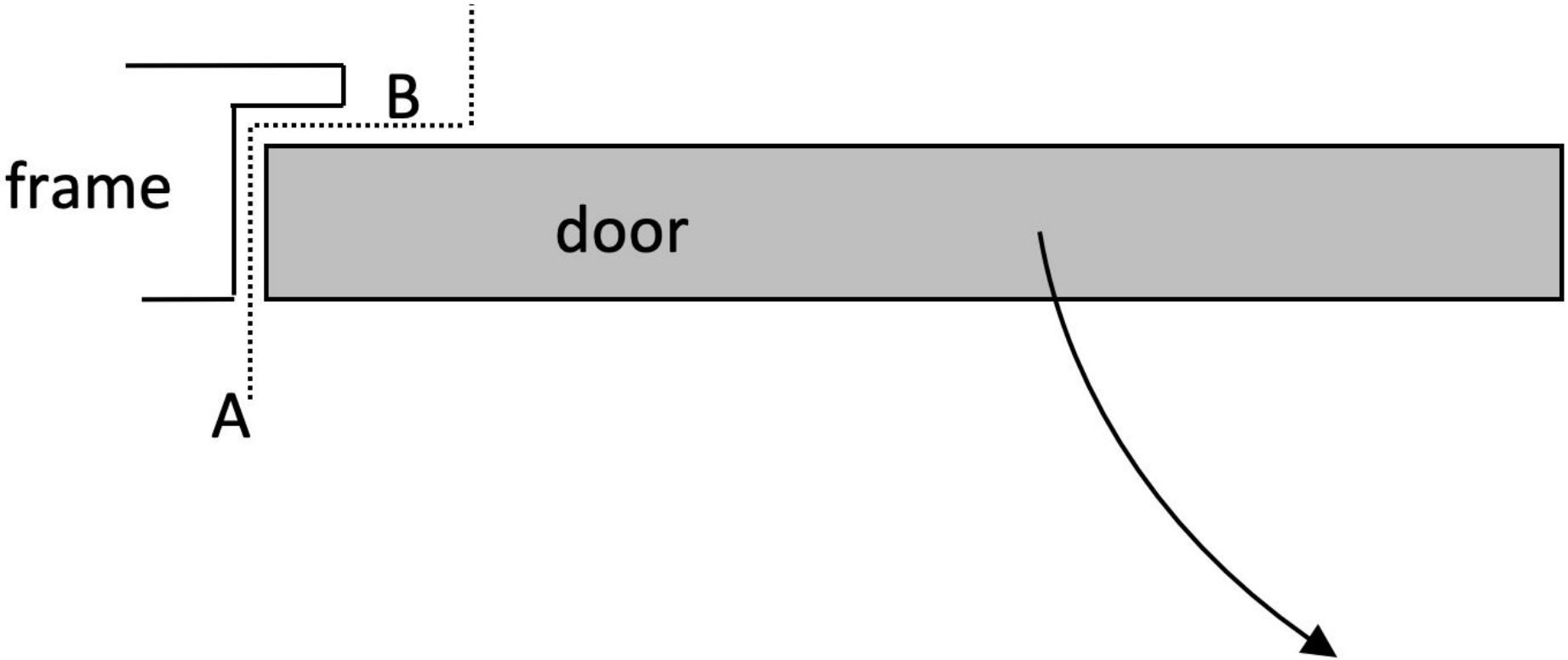
You may still encounter some of them in the wild.



THE TOOL

A bent piece of wire, used to deposit a piece of string onto the knob.

Tape, rubber, or other materials can be added to the string to increase friction on the doorknob.


B
frame
door
A

REQUIREMENTS

A doorknob.

In addition to this, you will also need enough room under or beside the door to fit the tool.

INSTRUCTIONS FOR USE

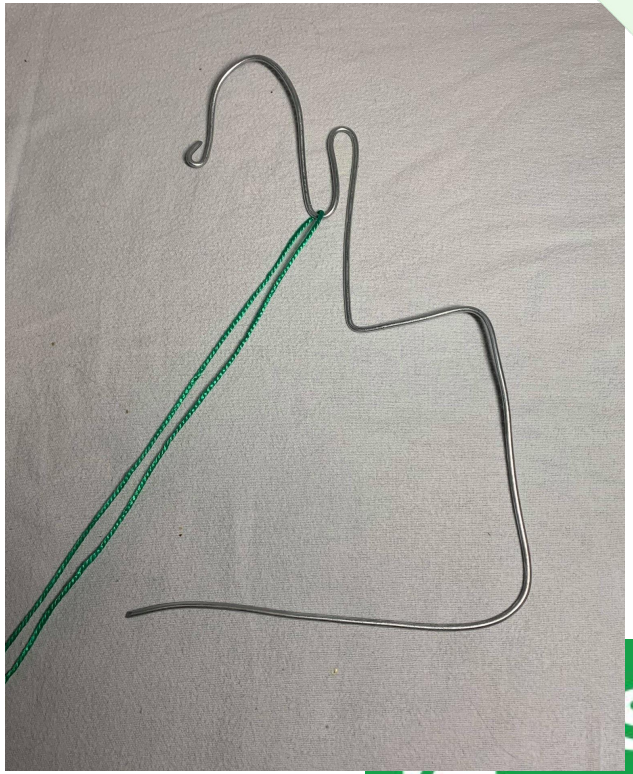
Crashbars

CRASHBARS - INTRO

Crashbars, not to be confused with pushbars, are relatively simple in concept. The bar across the crashbar pushes down and unlocks the door.

THE TOOL

Similar to the under-the-door tool, the crashbar tool uses cleverly bent wire and some string to actuate the crashbar and unlock the door.

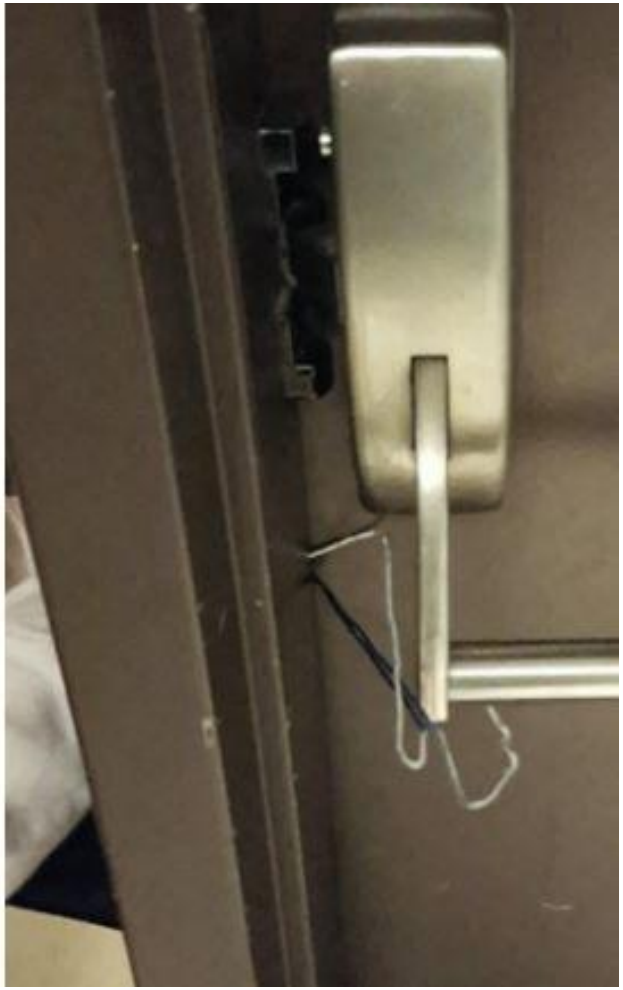


REQUIREMENTS

All you need is to have a crashbar on the other side of the door, and to ensure there is enough room beside the door to fit the tool.

INSTRUCTIONS FOR USE

1. Insert the tool through the side of the door (or start at the bottom and move up).
2. Rotate the tool until the hook lands on the crashbar.
3. Pull down the string, pulling the crashbar towards the door and unlocking it from the inside.



Pushbars

PUSHBARS - INTRO

Pushbar-targeted bypasses tend to be more difficult due to there being less things to hook onto. Often, the best bypass for a pushbar is a latch-targeting one.

ΦSV

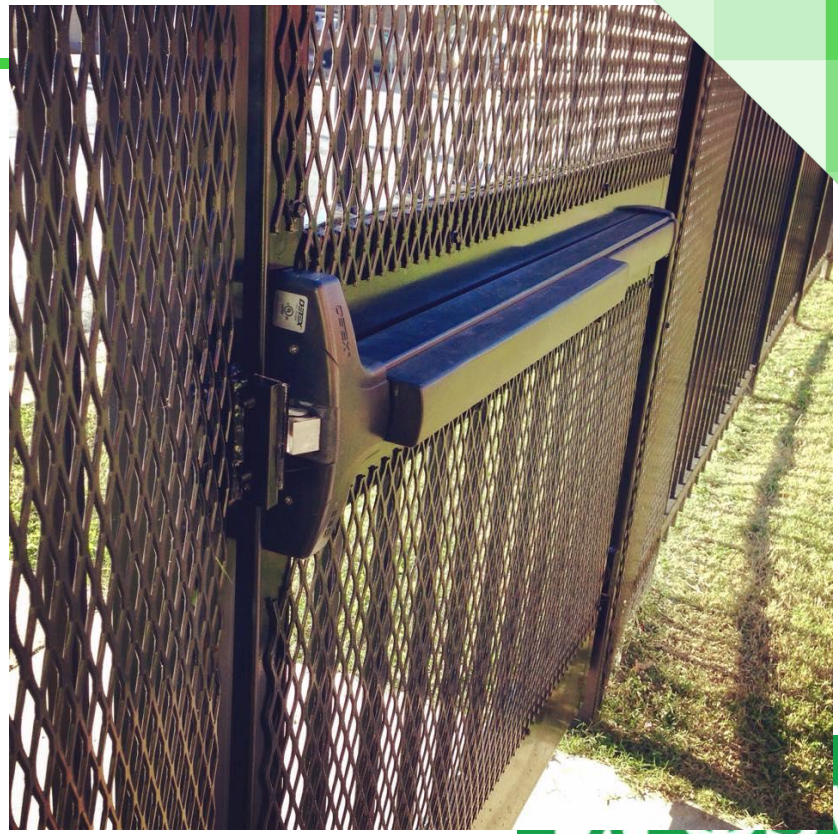
THE TOOL

A piece of string

Optional: Stiff wire or sticks for positioning the string, ideally in a hook or L-shape

REQUIREMENTS

For this Bypass Method to work, the pushbar must be either on a door with holes, or with room above and below the door.



INSTRUCTIONS FOR USE

1. Feed the piece of string through the top of the door or through a hole above the pushbar.
2. Use the wire pieces to finesse the string over the pushbar and through the bottom of the door or through a hole below the pushbar.
3. Grab both ends of the string, and pull.

Pulling Really Hard

PULLING REALLY HARD - INTRO

“Pulling really hard” is a longstanding tradition of physical hackers. Many doors are loose in the frame and can be pulled open with a strong enough arm.

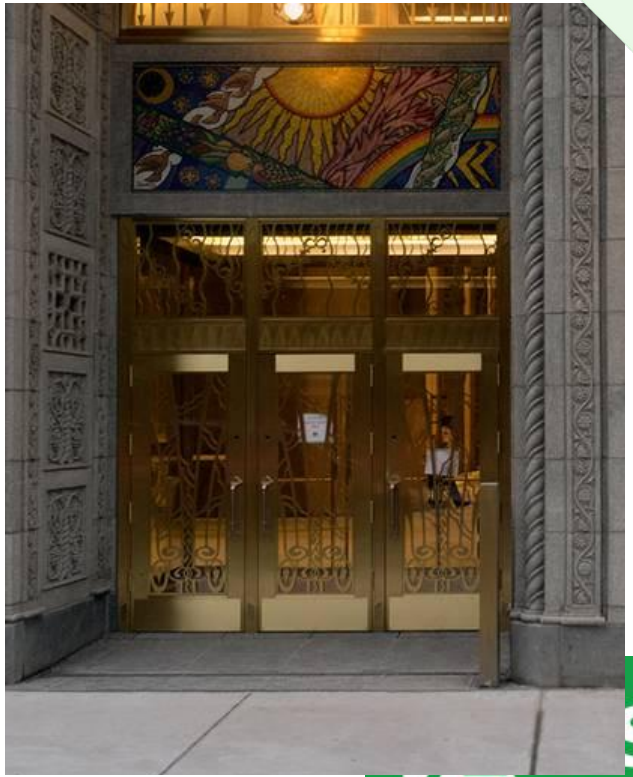
THE TOOL

Probably the easiest bypass method to pack for, all you need is a strong pair of arms

REQUIREMENTS

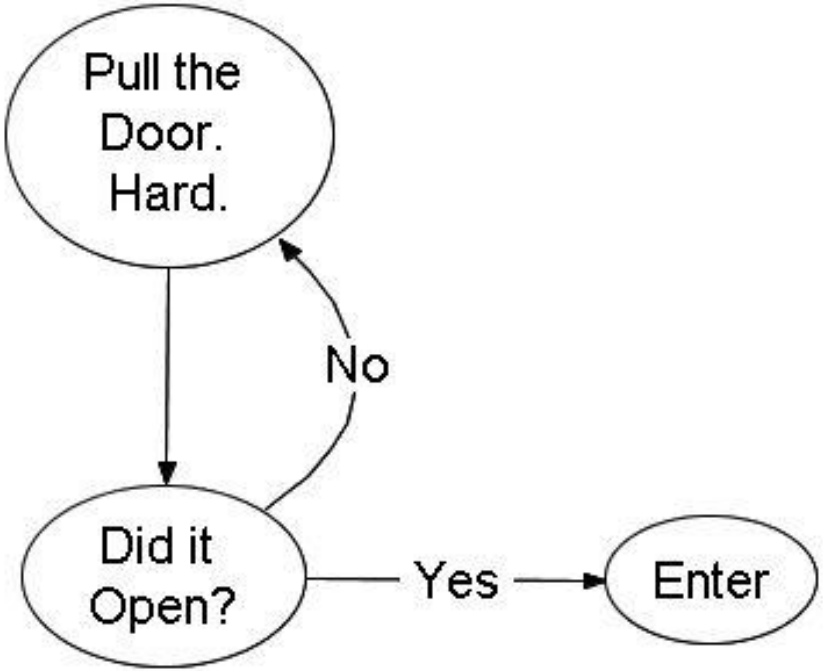
Not all doors are pullable, but a surprising number of them can be opened this way.

Look for “Springy, loose in the frame” that have some amount of flex. Multibank doors are often pullable.



INSTRUCTIONS FOR USE

Pull.



Removing the Hinges

REMOVING THE HINGES - INTRO

Sometimes, the easiest way to unlock a door is to not unlock it at all.

Some doors are installed with the hinges backwards, which allow you to unscrew the door from the frame and take the door off the hinges.

THE TOOL

A screwdriver.

REQUIREMENTS

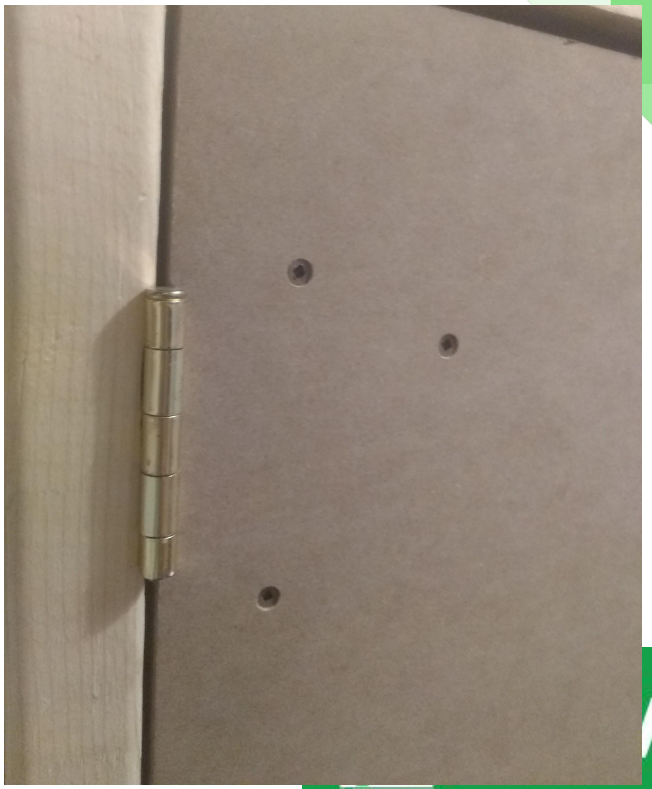
The screws of the door hinges must be exposed and accessible.

INSTRUCTIONS FOR USE

1. Unscrew the hinges.
2. Remove the door.
3. Enter.

REMOVING THE HINGES 2 - INTRO

Often, doors will have the pin of the hinge exposed. The pin can be removed and allow the door to come off the frame.



THE TOOL

- A screwdriver (or nail)
- A hammer
- Vice Grips (optional)

REQUIREMENTS

The door must be an outward swinging door, with exposed hinges.

In addition, this will not work on security hinges, such as setscrew or stud hinges.

INSTRUCTIONS FOR USE

1. Remove the bottom cap (if there is one) with the screwdriver and hammer.
2. Place the screwdriver under the hinge, with the point touching the bottom of the hinge pin.
3. Gently tap on the screwdriver with the hammer until the pin can be pulled out.
4. Repeat with the other hinge.
5. Remove the door.

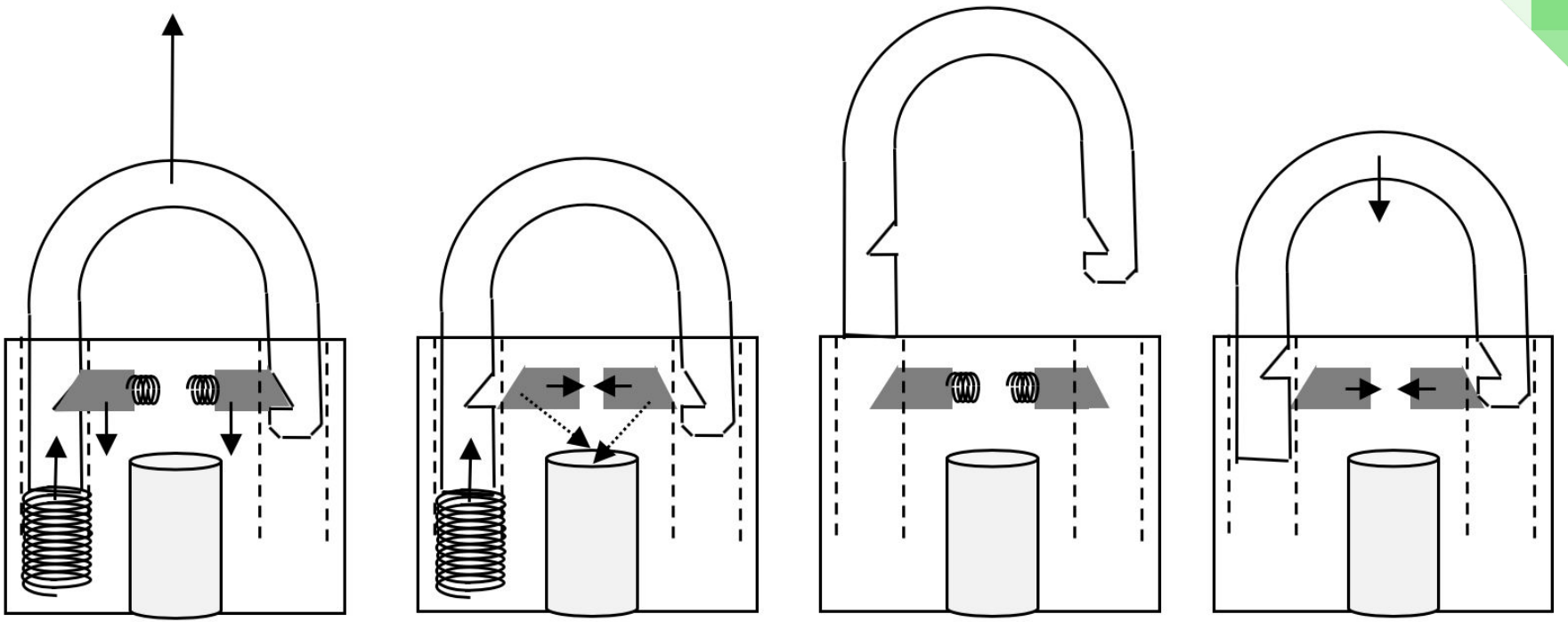
Padlock Shims

THE TOOL

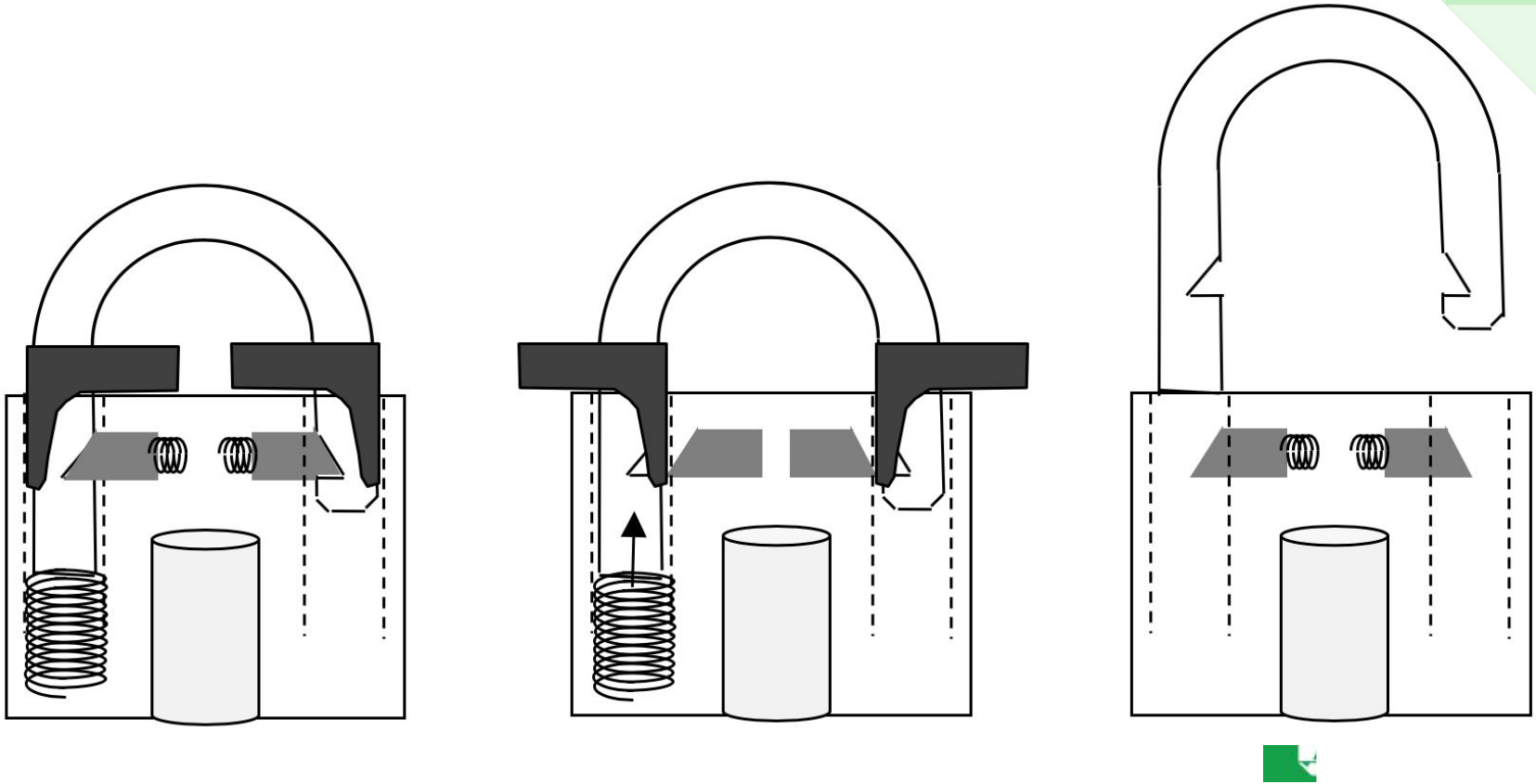
Padlock shims!

- These can be bought online in plastic or metal versions
- Or just DIY them

INSTRUCTIONS FOR USE



INSTRUCTIONS FOR USE



Button-Push Combination Locks

COMBINATION LOCKS - INTRO

Button-Push combination locks allow access without needing to have a physical key.

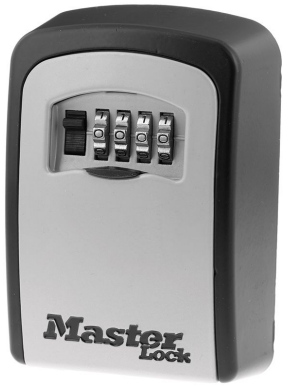
There are also boxes that can contain keys inside of them.

ΦSV


Master Lock
WARD


Master
Master
ΦSV

Fob Cloning


Master Lock

+


LF_ANT_500UH
Portable ANT V3.0
Center Freq:125k
ELECHOUSE

=

Using UV Ink/Powder

UV ink or powder can be applied to the buttons to figure out which are being used to unlock the door.

With a uv light and some patience, you can reduce the number of possible combinations enough to brute force.

Instructions

1. Apply uv ink or powder to all the buttons on the lock.
2. Wait for the lock to be used a few times. As it is used, the ink will rub off of the buttons.
3. Return with a UV light. The buttons used to unlock the box will have less ink on them than the others.
4. Try all possible combinations with the inkless buttons.

Bonus Fun Fact

Depending on the UV ink or powder you use, it’s possible for pigment to transfer from one button to another when someone is unlocking the lock.

You can use this to figure out the combination order without brute forcing the combination.

Any Guesses?

Sometimes, you don’t even need to use UV to figure out the combination.

SIMPLEX

Simplex Locks:

The default code from the factory is (24)3

Often, people will not bother to set a new combination.

Enterphones

ENTERPHONES - INTRO

Enterphones are devices used to let people into buildings, commonly apartments, condos, and other high-rises.

They allow visitors to contact someone in the building who can remotely unlock the door to let them in.

ENTERPHONES

The master code allows for you to configure the enterphone–from adding residents to adding entry codes.

Default master codes can easily be found online from manufacturers.

Again, people will often not bother to set a new combination.

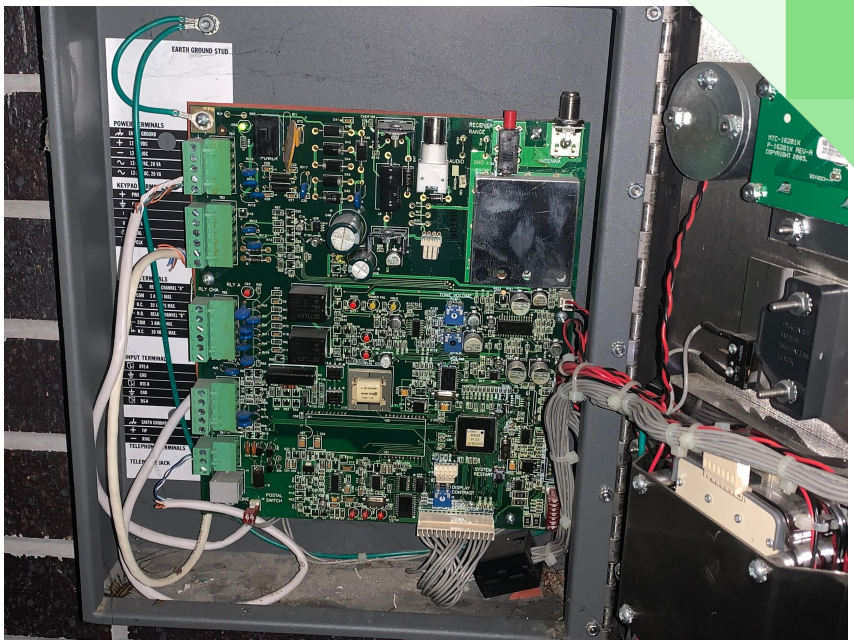
ENTERPHONES

There’s several major companies that make enterphones--Doorking, Door Guard, Linear, Mircom.

Enterphones are usually keyed-alike, meaning that one key can open enterphones made by the same company.

Instructions

1. Open the enterphone panel with the corresponding key.
2. Find the unlocking mechanism.
3. Use something conductive to jumper the mechanism.
4. The door should unlock, as if someone buzzed you in.



ΦSV

Wheelchair Buttons

WHEELCHAIR BUTTONS

Wheelchair buttons allow the door to open automatically when the button is pushed.

Sometimes, the button is installed so it will unlock and open the door, regardless of if the door should be locked otherwise.

Elevators

ELEVATORS

Elevators are everywhere in modern buildings. Often, there will be floors in buildings and high rises that are locked out, often requiring a keycard or fob to get into, whether that's in the stairway or the elevator.

Luckily, there are many ways to bypass these and get to locked out floors through elevator hacking. Check out the Elevator Hacking talk for more!

ΦSV

Alarm Basics

Circuits

Electronics run off of signals representing:

a) Open/Off/0

b) Shorted/On/1

In cheaper alarm systems without mechanisms to detect tampering, you can trick the circuit very easily to think the door is not open.

More Circuits

Disconnect the panel (unscrew, crowbar, etc.)

Identify the state of the mechanism. If the mechanism is normally open (NO), short the mechanism. If the mechanism is normally closed (NC), disconnect the wires.

a) (short): Short the mechanism by using something conductive (wire, keys, etc...) to connect both terminals.

b) (open): Disconnect the leads or snip the wires.

Contact Sensors

Magnets

Contact sensors often use magnets! There's a magnet in/on the door, and a sensor in/on the door frame.

You can use a magnetic probe to determine the location and the polarity of the magnet!

You can use a proxy magnet of the right polarity and strength to substitute the magnet in the door and open it without the alarm going off.

Passive Infrared (PIR) Request to Exit Sensors

REQUEST TO EXIT SENSORS

Some Request-to-Exit (REX) sensors are set up so they unlock and allow the person inside to leave the building, others prevent the door forced alarm from going off..

If you can trick the sensor into thinking there is someone on the inside, exiting the building, then it will unlock itself, allowing access.


Maxxtro
SPRAYDUSTER
DRUCKGAS-REINIGER
BOMBE DÉPOUSSIÉRANTE
ARIA COMPRESSA
SPRAY DUSTER

https://www.youtube.com/channel/UC8Jj_TMTI2kxO2yEgRhnKWg

Unlocked/Improperly Locked Doors

INTRO

You would be surprised at the number of doors that are left unlocked or completely open!

There’s plenty of times you can access an area just by pulling on some doors and seeing which ones are unlocked.

REASONS DOORS WON'T BE LOCKED

Human Error

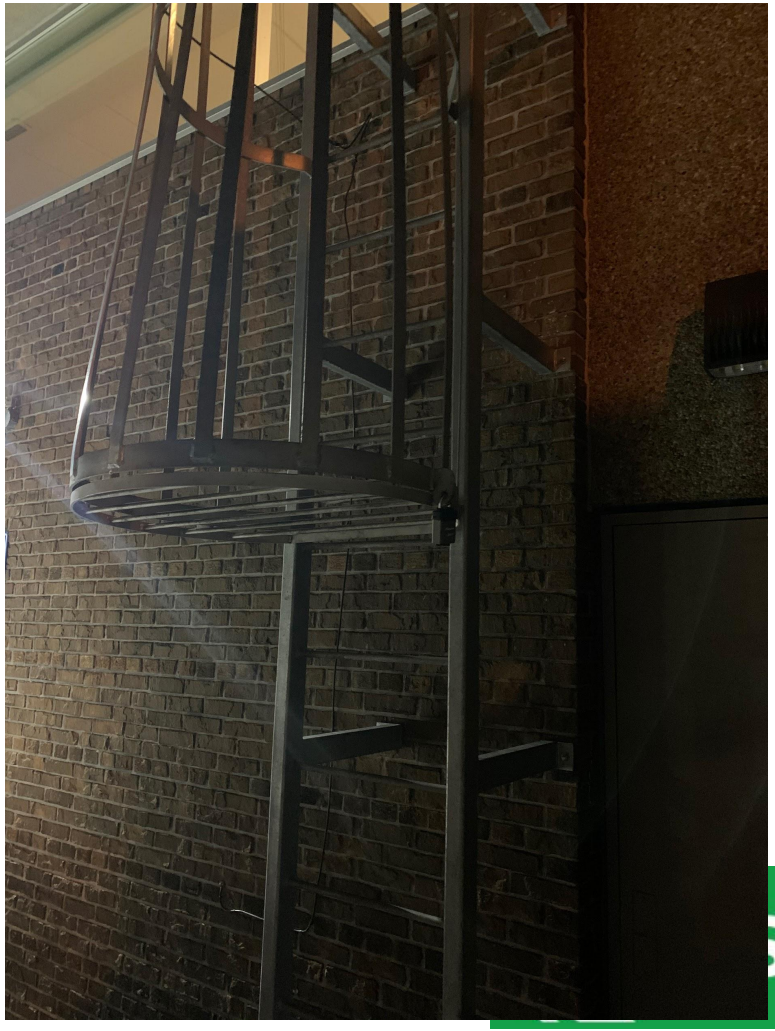
- A worker propped it open and forgot to unprop it
- You came when the building was open and propped it
- Someone left clutter by the door that held it open
- The security guard or closing staff forgot to lock it

Environmental

- Air pressure difference
- Warped door frame
- Poorly installed door or lock
- The door closer isn't working properly
- The lock is broken
- There is no lock there


255
NOTICE
KEEP
THIS DOOR
CLOSED
Fresh!
255

Ceilings and Windows, and Going Around




WMUR.com
AID PHARMACY
LIVE
ADAM SEXTON
WMUR News 9

ΦSV

Questions?

Karen Ng
k.ng@ggrsecurity.com
@hwenab
@kng.bsky.social

Sam Mayers
S@clearsear.ch
@XProtectSzn
@mac0s

@physsec
@physsec.bsky.social
@physsec@defcon.social

Oh god there's too many social medias

- Check out my other talks on Elevator Hacking and Bypass102: Basic Bypass Remediation!
- Enjoy the rest of the Village!
- Check out our Vendor Booth in Caesars Forum!

Special Thanks to:
Sunny Liu, Ege Feyzioglu, Bobby Graydon, Bill Graydon, Paul Robichaud