Bypass102

Introduction to Basic Bypass Remediation

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

Terry Luan
terry@physsec.org
@terryluan12

Intro

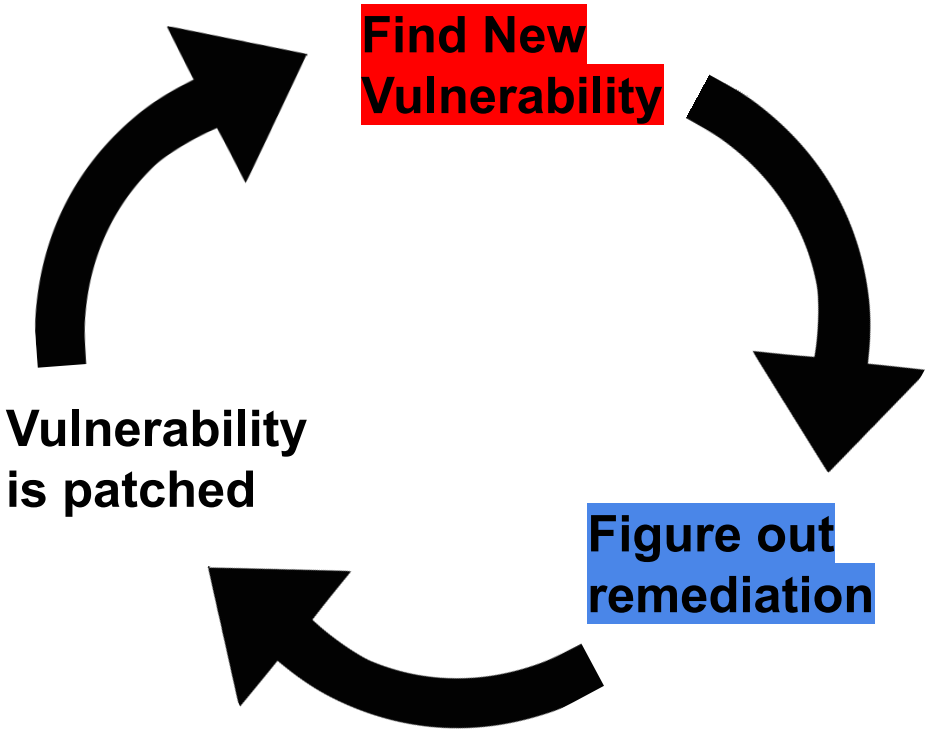
This talk is a followup to Bypass101. It's recommended that you watch that as a prerequisite.

This talk covers remediation and retrofits to secure your facilities from basic bypass methods.

A Constant Game of Cat and Mouse

Finding physical security vulnerabilities and remediations for each bypass method is a constant back and forth between the red and blue team.

A Constant Game of Cat and Mouse



ΦSV

About Lock Bypass

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

These methods are used often in physical hacking, and are simple enough to be used by anyone with the proper knowledge.

Latch-Targeted Bypass

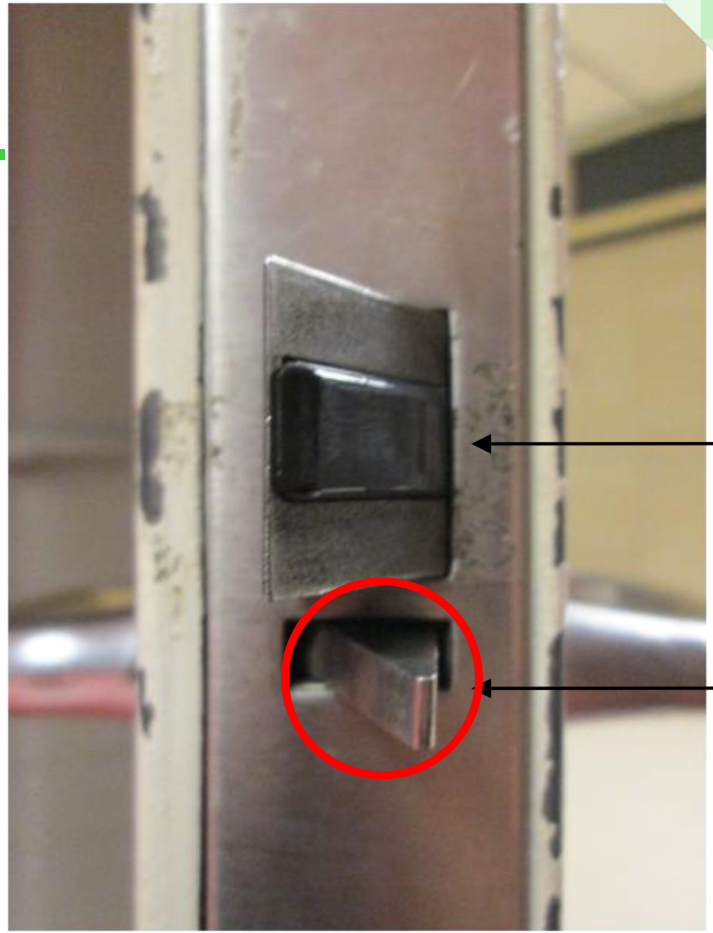
Latch Targeted Bypass - Intro

Carding targets the latches that hold the door closed.

Remediation

The best way to prevent this method of bypass is to install doors properly.

Deadlatches



F
DOREX
SS

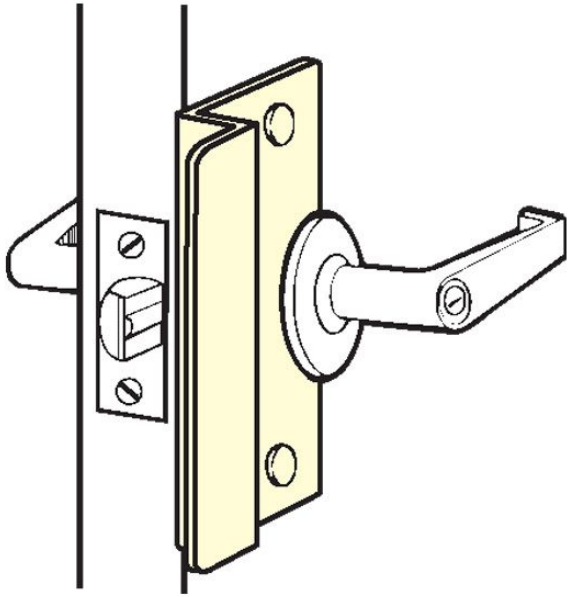
The Deadlatch

The easiest way to prevent latch slipping/pulling is to ensure that

- the deadlatch is actuated when the door is closed
- the strike plate is installed properly
- the door fits the door frame properly

Remediation - Retrofit

For a door that is already installed, there are retrofits, such as latch guards, that can help prevent this bypass method.



Remediation - Retrofit

The latch guard covers the latch from being easily accessed, and makes it harder to bypass.

However, they are imperfect and can still be bypassed using other methods.

Handle-Targeted Bypass

Including door knobs and crashbars

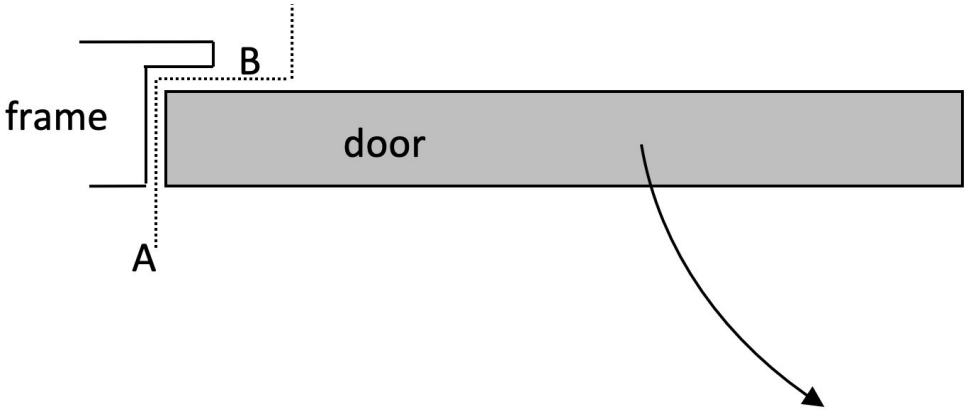
Handle-Targeted Bypass

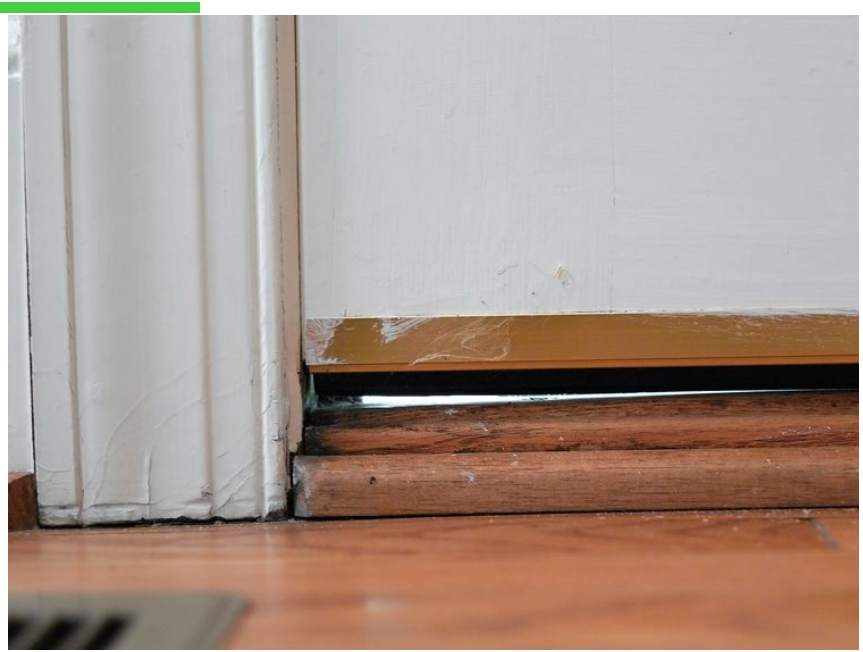
Handle-targeted bypass methods mimic a person exiting through the door from the other side.

This can be done on lever handles using under the door tools, as well as on doorknobs and crashbars.

Remediation

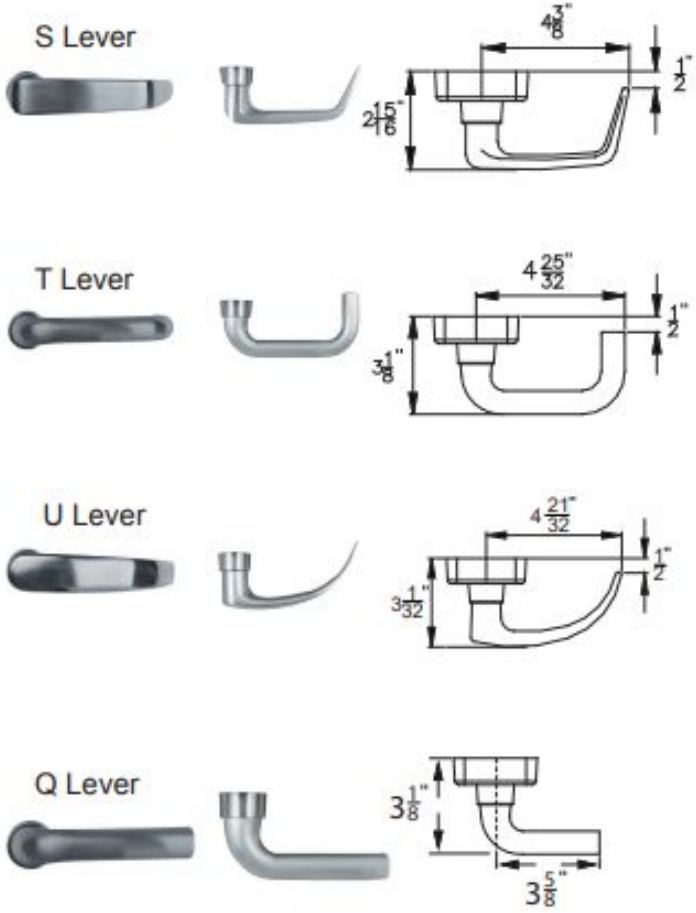
The easiest way to prevent this is to have a properly sized door for the frame, with little to no gap under and beside the door.





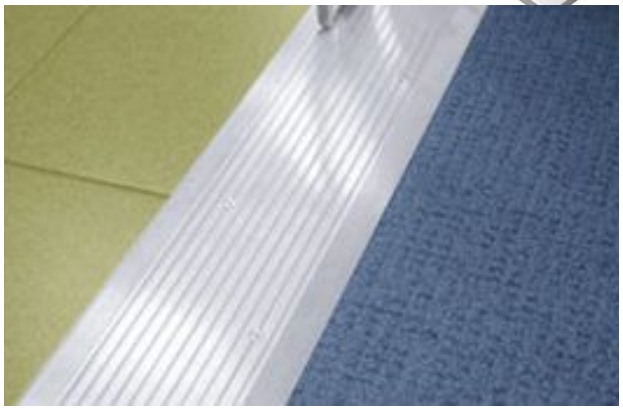
Remediation

In addition, certain lever-types are harder to use under-the-door tools with, and can delay intruders attempting to bypass doors with lever-type handles.



Remediation - Retrofit

A fitted beveled door threshold prevents bypass tools from fitting through the gap underneath the door.



Remediation - Retrofit

Rubber door seals and brush seals can make under-the-door tools harder to use.

Remediation - Retrofit

Windows in or next to your door can make using under the door tools easier.

If possible, cover up these windows.

Remediation - Retrofit

Maglocks can also provide additional security to doors.

However, these can also be bypassed.

Deadbolts

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.

Double Sided Deadbolts

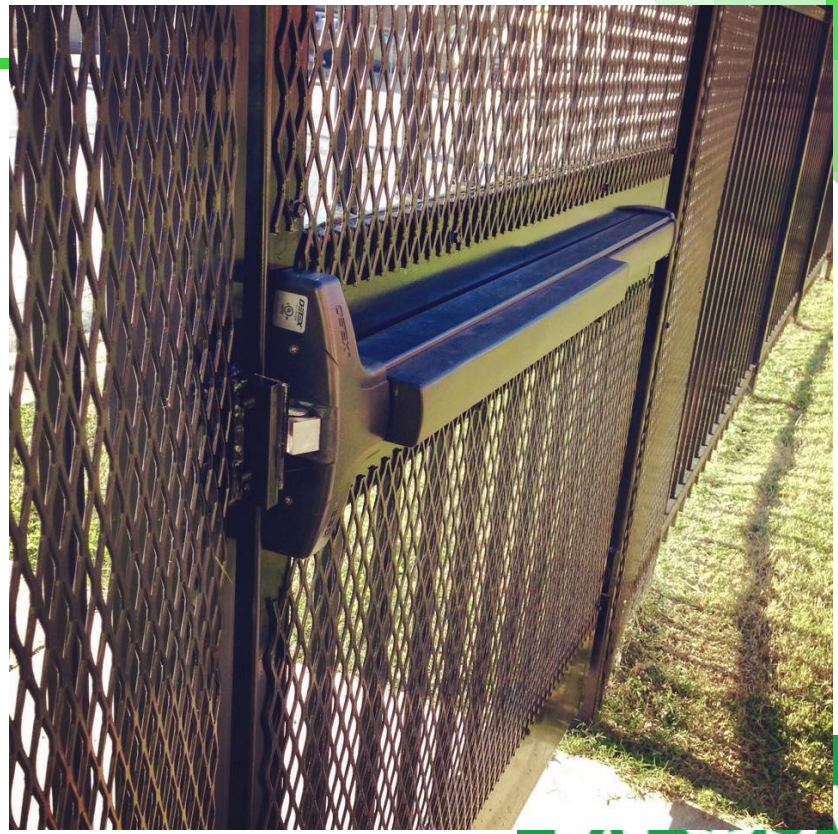
Double sided deadbolts are more secure than thumbturn deadbolts – J tools can’t be used to bypass them.

Pushbars

Remediation

Don’t have holes or gaps in your door if possible.

Use a pushbar with deadlatches (or a latch guard) to prevent latch-targeted attacks.



Remediation - Retrofits

Covers/shields can be retrofitted onto pushbar doors to prevent access to the pushbar.

Remediation - Retrofits

Bar guards can also be retrofitted onto pushbar doors to further prevent bypasses.

Removing the Hinges

Remediation

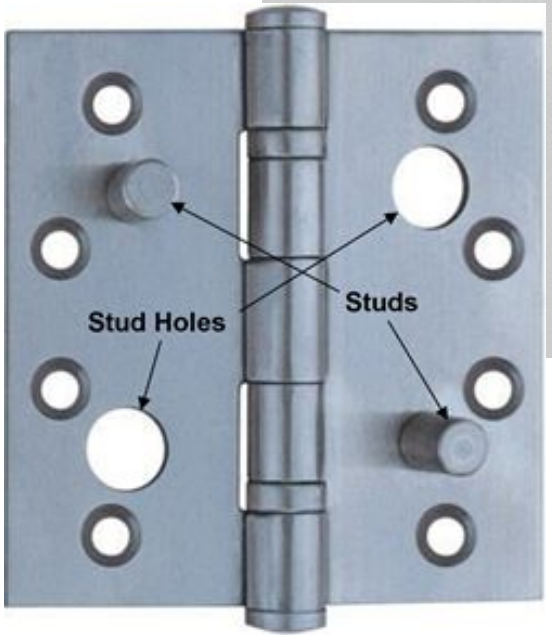
There are hinges available with non-removable hinge pins!

There are also hinges with set screws, which prevent the hinge pin from being removed while the door is closed.

Remediation

Additionally, there are hinges with studs and stud holes that prevent the two parts of the hinge from being slid apart if the hinge pin is removed.

You can also get retrofit hinge security screws that mimic these studs.



Button-Push Combination Locks

Simplex

The default code from the factory is (24)3

CHANGE YOUR COMBINATION

Other Combination Locks

If you suspect that someone unauthorized knows the combination to your button push combination lock

CHANGE YOUR 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.

CHANGE YOUR COMBINATION

Enterphones

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

Once opened, enterphones can easily be jumpered to unlock the door.

Remediation - Retrofits

CHANGE YOUR LOCK

Remediation - Retrofits

Enterphone covers and security bars can be used to prevent enterphones from being opened by key or by force.

ΦSV

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.

Request to Exit Sensors

Most REX sensors rely on passive infrared (PIR).

If someone can trick the sensor into thinking there is someone on the inside, exiting the building, then it will allow them access.

Remediation

Interlogix ~~makes~~ made a REX sensor that uses both PIR and radar to detect if someone was actually moving towards the door.

ΦSV

Remediation

REX sensors are generally more convenient but less secure – for more secure areas, try using a button* or tap-out system instead.

*Ensure the button can’t easily be pressed from the unsecure side of the door.

Elevators

Elevators - Intro

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 to.

There are many ways to bypass these and get to locked out floors through elevator hacking.

ΦSV

Remediation

CHANGE YOUR LOCKS

You can switch out most common service keyswitches for more secure locks*.

You CANNOT do this to fire recall keyswitches.

This also doesn’t prevent jumpering or hoistway access.

*check your local regulations

ΦSV

Remediation

Don’t rely on elevator floor lockouts for security.

It’s more secure to have additional locked doors past the elevator.

Other Remediations

Remediation - Proper Security Culture

The best way to prevent tailgating and other methods of social engineering is to promote a proper security culture.

Employees that disallow tailgating, and are not afraid to call out people they don’t recognize can help stop bad actors.

Remediation - Alarms and Sensors

Alarms and sensors can be used in combination with retrofits to prevent bypasses from being used without being caught.

However, these are imperfect and can also be bypassed.

Without sensors, anyone can get in with sufficient force!

Remediation - Cameras

Well-placed cameras can also be used to catch bad actors as a part of a complete security plan.

Again, these are also imperfect and can also be bypassed.

Cameras deter, enable response and minimize risk of insurance claims refusal.

Remediation - Timing Analysis

In combination with alarms, sensors, and cameras, timing analysis and security response should be considered to prevent bad actors from taking advantage of bypasses, elevators, and bad security practices.

Questions?

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

Terry Luan
terry@physsec.org
@terryluan12

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

Oh god there's too many social medias

- Check out my other talks on Elevator Hacking and Bypass101
- Enjoy the rest of the Village!
- Check out our Vendor Booth in Caesars Forum!