INFORMATION SECURITY

Disabling/Destroying CCTV/IP Cameras with Lasers?

Asked 10 years, 6 months ago Modified 10 years ago Viewed 111k times

35

@D3C4FF has asked a great question and I would like to follow up on that. Basically he had asked whether "[...] *an attacker can identify if a CCTV camera is on/operational without direct physical access to the cable/camera*[.]".

I was highly impressed by @TildalWave 's answer, and particularly about disabling cameras: "[...] *all you need is a decent pocket/torch size green laser (532 nm) directed for a few seconds directly into their CCD/CMOS sensor.*".

I remember some 10 years ago kids in my neighborhood had found out that you could 'DoS' the street lights using the same technique (by pointing the laser to a point near the back of the light bulb). I figured out that this was because those posts light automatically when it gets dark (meaning lack of light) and as soon as it gets bright (meaning light went inside its sensors) the light would turn off.

So I would like to ask:

1 - How does this laser attack apply to cameras?

2 - For which types of cameras does the laser pen attack work against (CCTV Vs. IP)?

3 - Is the laser pen attack the only vector against those devices (apart from obvious things like fire, TNT, acid, shooting, etc)?

4 - Why are cameras still vulnerable to it, if at all?

5 - Finally, how can I prevent those type of attacks against my cameras (they are all IP-based)?

Just a quick edit for those who (like me) was not sure whether this question was appropriate for the site, I have posted a question on Meta.

physical cctv

Share Improve this question Follow edited Mar 17, 2017 at 13:14 asked Jun 19, 2013 at 10:58

Community Bot
1

Lex
4,257 5 20 27

2 Related to the other side of the question is avoiding detection by cameras. See cvdazzle.com for experiments on using makeup as camouflage to hide from automated facial recognition software. – John Deters Jul 10, 2013 at 17:50

2 Can someone clarify if the laser method is a temporary measure or if it can permanently disable an IP camera? – user35908 Dec 18, 2013 at 22:11

2 Answers

Sorted by: Highest score (default)

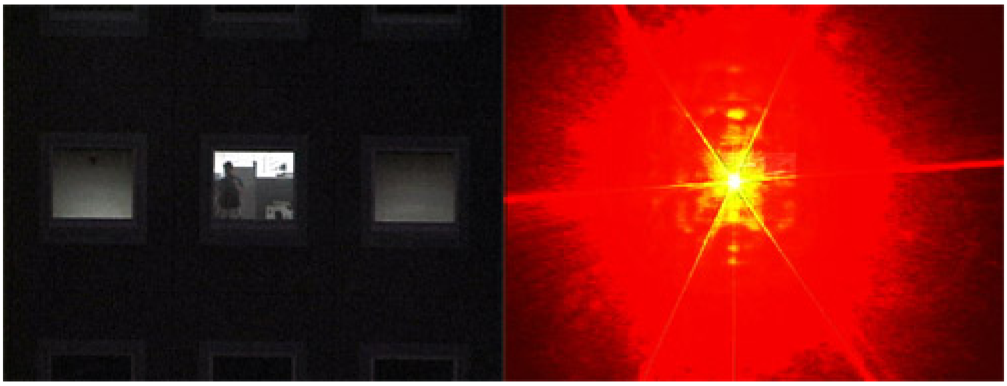
47

I've experimented with this attack previously.

It depends on a few variables. First, the strength in mW of the laser you are using. Second the quality of the camera you are trying to disable.

1 - How does this laser attack apply to cameras?

- A laser creates a super bright and focused spot on the CCD (camera sensor). This spot can be bright enough to blind the camera, or strong enough to physically damage the CCD/CMOS sensor of the camera (melting, overloading the circuitry etc). This is the type of image you'll see when a lazer is pointed at your camera:



2 - For which types of cameras does the laser pen attack work against (CCTV Vs. IP)?

- It doesn't matter. It will work on ALL visible light imaging technologies. This includes film cameras, CCD, CMOS sensors etc. I've tested this with 'prosumer' point and shoot cameras and a wide variety of CCTV cameras. Being IP/CCTV doesn't change the fact that your overloading the light sensing components of the imaging sensor.

3 - Is the laser pen attack the only vector against those devices (apart from obvious things like fire, TNT, acid, shooting, etc)?

- NO! Another clever one that i've used to success is wearable Infrared LED clothes (usually on a hat). This is essentially the same as using a bright light to obscure you from view, you will show up on the screen, but if you use bright enough LED's, it'll make you un-identifiable.

4 - Why are cameras still vulnerable to it, if at all?

- Because cameras sense light, if you throw enough light at them, they won't be able to process the weaker reflected ambient light.

5 - Finally, how can I prevent those type of attacks against my cameras (they are all IP-based)?

- You can't really. Its part of the design of the cameras. The best thing to do would be to identify cameras that may be vulnerable and perhaps install hidden cameras in the area so that if someone disables an overt camera, they'll hopefully miss the covert one.

For more information on this type of attack, check this guy's site, there have been a few projects like this around but this is well written up and contains lots of good example shots.

Share Improve this answer Follow

answered Jun 19, 2013 at 11:11
NULLZ
11.5k 19 80 111

4 +1 for installing two cameras in the same area. Each camera has a blind spot, some times someone could sneak behind it and cut the wires or somehow tamper with it. It's good to have to buddies one watches over the other. – Adi Jun 19, 2013 at 11:58

@Adnan Yeah, exactly! But having a covert camera to watch (especially on important choke/entry/exit points in buildings) is much better than just having a second one pointing at the first. – NULLZ Jun 19, 2013 at 12:16

Oh, perhaps I wasn't clear. I didn't mean having another camera especially to watch the first. I meant setting up the cameras in away that each one falls in the other's visual filed. – Adi Jun 19, 2013 at 12:18

2 @stephen IR may be filtered before it hits the sensor in some cases. Especially in indoors only cameras. Night cameras, esp with IR components are probs most succeptible to IR lasers. Not tested though afaik. – NULLZ Jun 19, 2013 at 13:55

5 For indoor use I'd expect most cameras to have IR/UV filters. General purpose cameras all have them because the sensors respond to light beyond the visible range; and not doing so result in weird color balance. – Dan Is Fiddling By Firelight Jun 19, 2013 at 19:44

15

To add to D3C4FF's answer:

1. Security camera's are often used to direct security staff. It's sufficient to know that a camera is under attack. Real-world security camera's have tamper sensors and self-diagnostics for the same reason: to detect physical attack as opposed to internal failure.
2. Obviously, have physical security staff. Camera's are not a full replacement, they just allow you to deploy people where it is actually necessary.

The same logic actually applies to those wearable IR leds suggested. Camera's don't need to detect precisely *what* is unusual, it is sufficient to detect *that* something is unusual. From that point you get a human involved.

Share Improve this answer Follow

answered Jun 19, 2013 at 14:38
MSalters
2,679 1 16 16

2 Quite right. The only time attacks against CCTV is if a) they are recording and not viewing them or b) if they are viewing them, that you knock out as many as you can as quickly as possible and come back later before they can be replaced. Depends on the environment of course but yeah. :) – NULLZ Jun 20, 2013 at 10:11

Highly active question. Earn 10 reputation (not counting the association bonus) in order to answer this question. The reputation requirement helps protect this question from spam and non-answer activity.