
TOR Accessible
Raspberry Pi
Motion Capture Camera
(how to DIY)
Djilpmh Pi

TOR Accessible Raspberry Pi Motion Capture Camera (How To DIY)

Build your own remote video monitoring camera with motion trigger and scheduled time lapse image capture accessed through TOR.

djilpmh pi

This book is for sale at http://leanpub.com/torpicam

This version was published on 2021-04-03

This is a Leanpub book. Leanpub empowers authors and publishers with the Lean Publishing process. Lean Publishing is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

Also By djilpmh pi

Shadow IT

You Can Use The Dark Web For Good

This effort is dedicated to all of you who have not given up and want to claw back some bit of privacy into our lives. I know you can do it, and I will help you.

Contents

Disclaimer

Do not use the information in this ebook to commit a crime or perform unethical / immoral activities. If I have information that you intend to do so I will personally report it to the appropriate authorities.

The information provided is for ordinary people to protect what little privacy we have left, in as secure a way as I can recommend. I use these methods myself to run my cameras, so I am fairly confident that they are unlikely to be compromised: see the chapter on "Is TOR Secure?" for my interpretation and reasoning - you make up your own mind whether the rationale is sound or defective. If you find a defect in the thinking, please feel free to let me know so I can correct it, and modify these recommendations.

You are responsible for your own actions. I am not a lawyer, I am not trained in legal aspects of information use and abuse. I can only tell you what I find by means of free resources on the public internet. I am not trying to convince you of anything here. Take it or leave it.

The information in this ebook does not claim to provide security. Besides, all software being defective in some way, any of the components I describe will have a vulnerability revealed some day and the entire house of cards can collapse, so it is important to keep aware of known vulnerabilities. If TOR or SSH have publicized vulnerabilities, or if you break discipline and do something stupid, nothing in this ebook will help you.

If a product is mentioned in the discussion, it is only as an example. I neither endorse nor does listing such an item suggest that I have used or tested such an item. Obtain your parts and software from reputable and reliable sources.

P.S.
This book and any references mentioned here, are meant solely for the confusion of the intended recipients. It may contain confidential and/or privileged information and you should feel privileged to have received it. The contents of this book are intended to give the impression that the author is being helpful while providing no actual value. If you are not the intended recipient of this book, you are prohibited from reading, printing, duplicating, disseminating or otherwise using this information. If you are the intended recipient, the same goes for you. If you have received this book, do not forward or distribute it to others. Instead, shred any copies you may have printed and/or its attachments and then burn the shredded remains. Any similarity between the content of this book and any reality, true or imagined, is purely unintentional. No animals were harmed during the production of this book.

Introduction

What is this book about? Who should care?

TL:DR
This book will show you in detail how to build and operate a video camera attached to a Raspberry Pi computer. It will run the "motion" package that can detect motion and trigger a video recording, and take regular snapshots to create time lapse/ stop motion at the interval you choose. The best feature is it is very securely accessed by TOR as a hidden service on a 56 alphanumeric character ".onion" address that is very hard to guess or find by scanning the address space.

If you prefer I can show you how to build the entire system from the parts up, to a fully functional setup. Or, if you just want to buy one, we will reconfigure it so only you know how to access it (change passwords and TOR address). See end of this chapter for more information.

What is this book about?

There are several parts, each :

1. Get and set up a basic Raspberry Pi single board computer (SBC) hardware, with a standard operating system.
2. Install OS and enable SSH and Camera.
3. Get a Raspberry Pi compatible camera or USB camera.
4. Install the motion package and configure it.
5. Install and configure TOR, and create a hidden service.
6. Install and configure 2FA using TOTP to protect SSH command line access.

Who should care?

When I gave a talk at a local university to the student chapter of a security organization, one of the points I made is this:

> "In the Age of the Empire, each Jedi knight must know how to build and repair their own light saber."

In the age of the Empire, there are powerful forces which want to control everything you have, see, know, or own. This is not Star Wars fiction; today most consumers are caught up in the net of data collection performed by: Google, Apple, Amazon, Facebook, Microsoft, Experian and Credit rating entities, Credit Card companies, and these are only the legal ones. Criminal hackers of all stripes hack into security software and unwitting customers install the updates along with malware/viruses. See events in 2020 related to "Solarwinds" and "Mimecast":

+ https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12
+ https://www.reuters.com/article/us-global-cyber-mimecast/email-security-firm-mimecast-says-hackers-hijacked-its-products-to-spy-on-customers-idUSKBN29H22K

If you have something private that you want to keep private to yourself and key people you trust, using TOR to communicate is one of the better methods.

If you configure the tools yourself, you don't have to rely on other people's promises. You control the passwords, the TOTP (time based one time password), and you configure and update the TOR hidden service address. You can build your own light saber.

Why not just buy the Empire's light saber? Because the storm troopers can shut yours off whenever they want. You, Jedi, have an obligation to build and repair your own - in this case, your own private system to communicate over public, untrusted networks.

Other related topics from security talk

The necessity of each Jedi knight making and repairing their own light saber, was one of three topics I covered when I spoke to the university students who were interested in security. The other two topics were

Do the best you can, make your light saber durable and resistant to abusive misuse or unintended outcomes.

For your own sake, don't be lazy and sloppy about your work. Make it durable and fit for its purpose. Test it and check for ways it might be misused. What if it were available to malicious actors?

Think through and consider the ethical /moral implications of what you do.

This is a hard one. While privacy is important to democracy and justice, it can also be abused by criminals and bad actors. As with free speech, it is more important to protect free speech even if it is abused by hate groups: privacy is, I've concluded, more important than allowing evildoers to use it also.

Put simply, privacy and private communications are necessary to the Second Amendment to the Constitution, which is regularly interpreted to allow citizens to resist an unjust government. The "well regulated milita" and right to bear arms is rather apt: cryptography was classified as a munition and it was, until the 1990's, a Federal crime to export such munitions (strong cryptography) outside the US borders. See Phil Zimmerman's story where the course of history changed: https://en.wikipedia.org/wiki/Phil_Zimmermann.

On a more general level, it is important to think about and balance the potential harm of the work you accomplish. Robert Oppenheimer, the leader of the project that created the first atomic bombs (Hiroshima and Nagasaki), was certain that he was doing his duty all the while he knew the bomb's killing power. It's not so clear that DNA collection and analysis promoted as family history research is protected against abuse: https://www.cnbc.com/2018/06/16/5-biggest-risks-of-sharing-dna-with-consumer-genetic-testing-companies.html.

Ownership of the DNA data should be more clearly disclosed, but too late for some people, whose information is being purchased by private equity firms: https://www.cbsnews.com/news/blackstone-private-equity-ancestry-com-dna/. The phrase comes to mind: "ripe for abuse."

Want to learn how?

In my role as privacy advocate, I feel that the more people know how to use the available technology to protect some portion of their privacy, the better. If you are serious about this, I will set aside a day (how much of it we use will depend on how much or little you already know) and we will take the necessary parts and build a fully working video monitoring system accessible with good security over TOR, on a Raspberry Pi Zero W and camera. The fee for this is negotiable and depends on what you already know, how many pieces of peripheral hardware you don't already have, and whether you need a "computer, networking, linux, and security bootcamp" to establish basic knowledge. The fee for the bootcamp is also negotiable. Contact me at djilpmh@protonmail.com to discuss.

Want to just buy one?

If you don't wish to get into the technical details, but want a secure camera, a fully assembled and operational device can be provided.

However, you really should learn how to keep the software updated and patched, move the files to clear space, update passwords, and maintain a minimum security and privacy discipline. If that seems like a lot of extra work you would not be interested in doing, it's simpler to just buy a commercial camera and pay for the vendor's cloud storage and alerting system: many are easy to use and have good functionality. I use blinkforhome, outside the house only though. See the following section for some reasons to make the system your own and take on the responsibility for supporting and fixing it.

Additional reasons why you should make your own system

One: When you purchase a commercial service, you rely on their promise to keep your data safe. Maybe the breach will be with their supplier or cloud storage provider, not even their own software or site. Either way, your data can be at risk due to failure to do perform due diligence at many parts of the service supply chain.

Two: Who owns the rights to the video of the party in your living room? https://www.reddit.com/r/Ring/comments/cwmrsa/who_owns_the_copyright_to_ring_doorbell_video/

> from Ring terms of service: "*You hereby grant Ring and its licensees an unlimited, irrevocable, fully paid and royalty-free, perpetual, worldwide right to re-use, distribute, store, delete, translate, copy, modify, display, sell, create derivative works from and otherwise exploit such Shared Content for any purpose and in any media*

> *formats in any media channels without compensation to you.*"

In short, you are not the exclusive owner of the video clips, and your private party can be used in the vendor's advertising; you have already given them permission.

Let's get going

Let's get going!

If you have any questions contact me at djilpmh@protonmail.com.

Raspberry Pi

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Which One Should I Get?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Parts, or Kit

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Parts for Configuration

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Alternate Parts for Configuration

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Install OS and Enable SSH and Camera

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

OS Installation

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Insert the microSD card and check installation

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Plug in components and power up!

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

System configuration

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Network configuration

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Other characteristics of TOR

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Get a Pi Camera or USB Camera

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Install the Motion Package and Configure it

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Install

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Configure

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Check and test

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Notes on Sensing Motion

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

motion.conf

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Daemon

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Logfile

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Rotation

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Width and Height

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Image File Output

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Snapshot

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Target Base Directory

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Snapshot filename

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

HTTP Video Stream Port

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Video Stream Authentication

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Install and Configure TOR, and Create a Hidden Service

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Editing /etc/tor/torrc

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Once you have configured a hidden service, you can look at the

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Restart TOR

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Find the hidden service host address

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

How will this information be use?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Test and Verify

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Bookmark the URLs

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Set up script for SSH

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Install and Configure 2FA Using TOTP

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Miscellaneous Privacy Topics

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Privacy is Not a Single Product

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Is the access using TOR secure?

Here we will look at several factors that make the access via TOR to this device hard to attack. These factors include the observation that

1. it's hard to find within the huge address space,
2. the published service is open at a high port - among the over 65,500 available service ports,
3. the camera will require username+password authentication to access it
4. the SSH service port (also moved to nonstandard high port) can be configured to require 2FA (two factor authentication), also known as TOTP (time based one time passwords).

TOR address space is Huger Than Huge

A TOR "hidden service" is almost impossible to find in its very large address space.

Let's do a little math here so I can make a point about TOR.

IPv4 address space

The full conventional IPv4 Internet address space is 32 bits long. So the entire address space is 2^{32} (base 2 raised to the 32 power), which is about 4.3 billion IP addresses. Some are reserved, so the usable space is a bit less than that.

IPv6 address space

IPv6 expanded the address space to 128 bits. 2^{128} is much bigger. That's 3.4 x 10^{38}, or thirty-eight zeros.

To give you an idea how much space there is, it was considered unproductive to scan IPv6 subnets for potential devices (as we used to do with IPv4) because it would take too long to check the addresses within even a small subnet.

TOR address space

TOR addresses, including the ones for creating hidden services, are 56 alphanumeric characters followed by the ".onion" suffix.

36^{56} = 1.4 x10^{87}, or eighty-seven zeros.

Such a large address space where hidden service addresses are calculated cryptographically, makes it futile for someone to look for you in in TOR. Even if they accidentally find the TOR hidden service address, other layers of protection come into play.

High port

If we think of any single IP address or TOR address as a building, there are 2^16, or 65,536 doorways or service ports that can be used to enter that building. Ordinarily a service port is TCP port 80 or 443 for web traffic, HTTP and HTTPS, and the standard service port for SSH is TCP port 22.

In this implementation we obfuscate the service port to a "high port", so the webcam access by using the TOR browser can be configured to listen on port 58765. SSH server can listen on port 56922 instead of the standard port. This simply makes it harder to

find since many system scanners only check the standard ports and would walk right past.

We can access it because we know where the hidden service's high port is configured.

Camera access: Username + Password

The live view of the camera using the TOR browser will be configured to use a Username + Password combination. Without them, a visitor will be looking at a closed and locked door.

SSH access: TOTP

SSH access by default will use a Username + Password combination, just as with any SSH implementation. If desired, a key pair can be generated to be used as the authentication mechanism instead of username and password.

A second level of protection can also be implemented, using 2FA / TOTP (two factor authentication, or time based one time passwords).

TOR client authorization feature

For a stronger level of security, TOR has a feature called Client Authorization, described in https://community.torproject.org/onion-services/advanced/client-auth/. In short, the service port is invisible to TOR clients (browsers or SSH, or other), even if the real '.onion' address is known, unless each authorized client has the client key

included in the client's torrc configuration file. This feature can be thought of an "invisibility cloak." While this is a very high level of privacy and security, it is also a lot more work for both the server and every client to generate the keys, distribute them securely, and configuring every authorized client to add the key to their 'torrc' file.

Administrative artifact: KYC

System and server administrators have an obligation to know who is using their system as an ethical and moral imperative. You can't just say "we are open to all visitors and everyone can use the system as they wish," as much as that is a lovely universal open access principle. Rather, administrators have a duty to review who is using their system for what; including criminals and others using the system to attack others, for example. Generally the concept comes from the KYC, or Know Your Customer requirements applied to most financial institutions, to at least make a show of verifying that the money being deposited or invested, does not come from drug, human, or arms trafficking, or theft from ethnic cleansing. It seems that some multinational corporations who make a lot of money providing social media platforms, have more responsibility to enforce bans against hate and false statements made on their platforms.

As an administrator, if someone makes a connection to you via TOR, you lose the ability to see the source IP address of the remote client. For example, using the 'w' command, the FROM column usually reports the IP address of the remote client and what command they are running. Using TOR, the source IP address is the internal loopback 127.0.0.1 – if you are a TOR advocate, this is good, because your real location is being protected. But as an administrator, you are now blind.

```
$ w
```

```
15:03:24 up 15:03, 2 users, load average: 2.06, 1.77, 1.35
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
pi pts/0 127.0.0.1 15:00 1:48 7.10s 4.81s ssh -l
pi pts/1 127.0.0.1 15:03 3.00s 0.82s 0.04s w
```

What does this mean? The loss of this information doesn't mean the administrator should just give up, it means you need to do a bit more diligence in your part as the admin when user accounts are issued: are they legitimate individuals and can they prove their status to you in other ways using other channels? For your personal home system you're only going to have a single user, yourself. But in general, if you give out accounts for others to use, you have additional work to do to KYC since one of the tools you used to have (to identify the user's IP address and location) is now gone.

Generating a new TOR hidden service address

If you believe your 56 alphanumeric character ".onion" address has been compromised or leaked by someone, (perhaps your friend got hacked), generating a new one is as easy as deleting the hostname from its folder, usually found in:

```
/var/lib/tor/hidden_service/
```

But before you do, leave that one alone until you activate your backup TOR address. Edit your /etc/tor/torrc file to enable a second hidden service to the same machine (remember to remove the `#` at the beginning of the lines to "uncomment" and activate those lines in the configuration. Restart TOR to create a new hostname in

```
/var/lib/tor/other_hidden_service
```

That way you can maintain administrative access through the process of generating a new TOR address. To remove a TOR address, just edit the

`/etc/tor/torrc`

file and remove the section you wish to remove, and restart TOR. It's probably also best to delete those files since they cannot be used any more anyway.

Make It Your Own

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Change TOR address

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Change the password

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

Change the livestream user:password

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.

When you're done

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/torpicam.