The Internet of Things

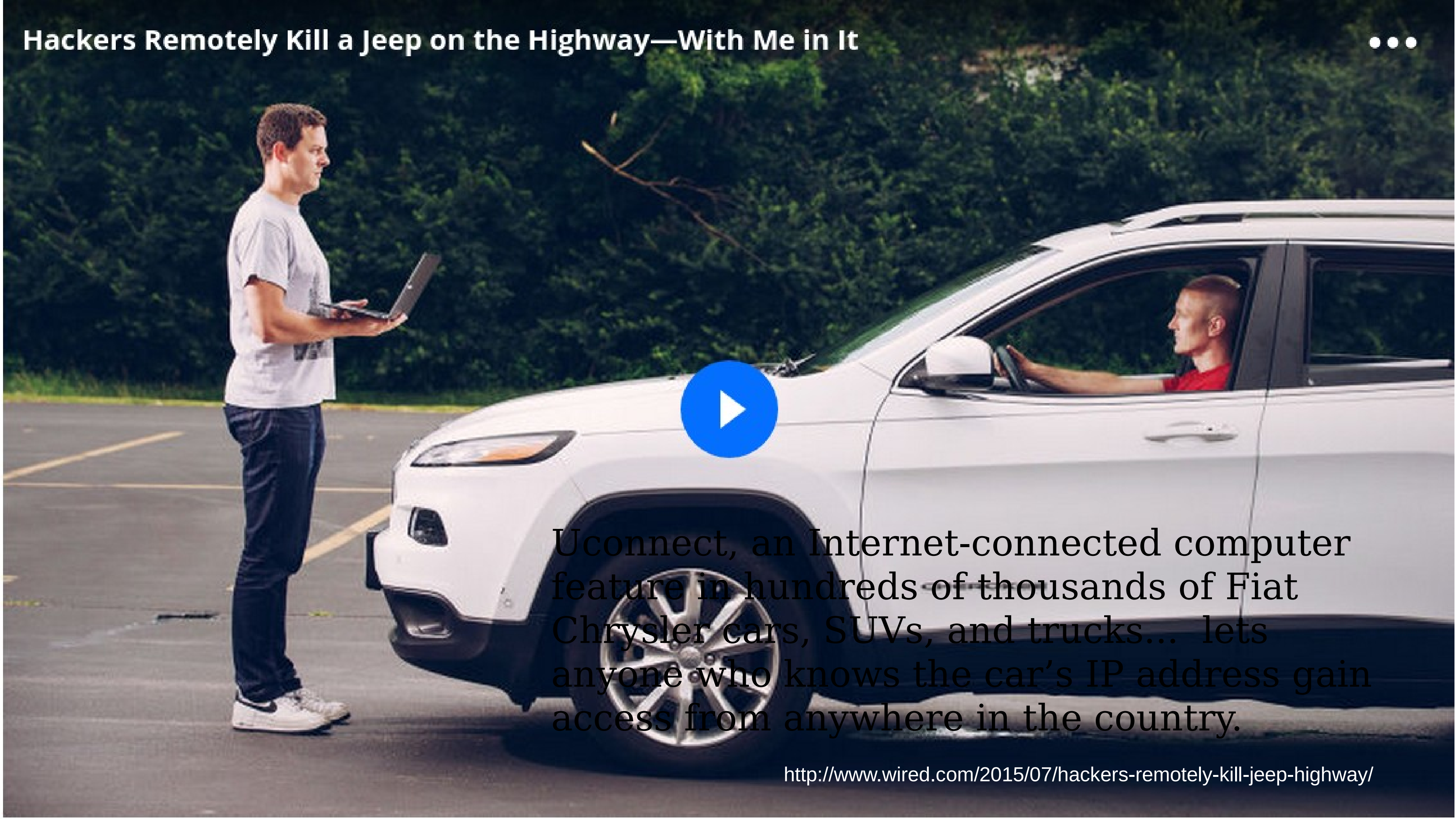
@n8fr8 @guardianproject @torproject

“Networked sensors and the Internet of Things are projected to grow substantially, and this has the potential to drastically change surveillance. The still images, video, and audio captured by these devices may enable real-time intercept and recording with after-the-fact access. Thus an inability to monitor an encrypted channel could be mitigated by the ability to monitor from afar a person through a different channel.“

BERKMAN CENTER REPORT **|** FEB. 01, 2016 "DON'T PANIC"
https://cyber.law.harvard.edu/pubrelease/dont-panic/

The Crazy Things A Savvy Shodan Searcher Can Find Exposed On The Internet

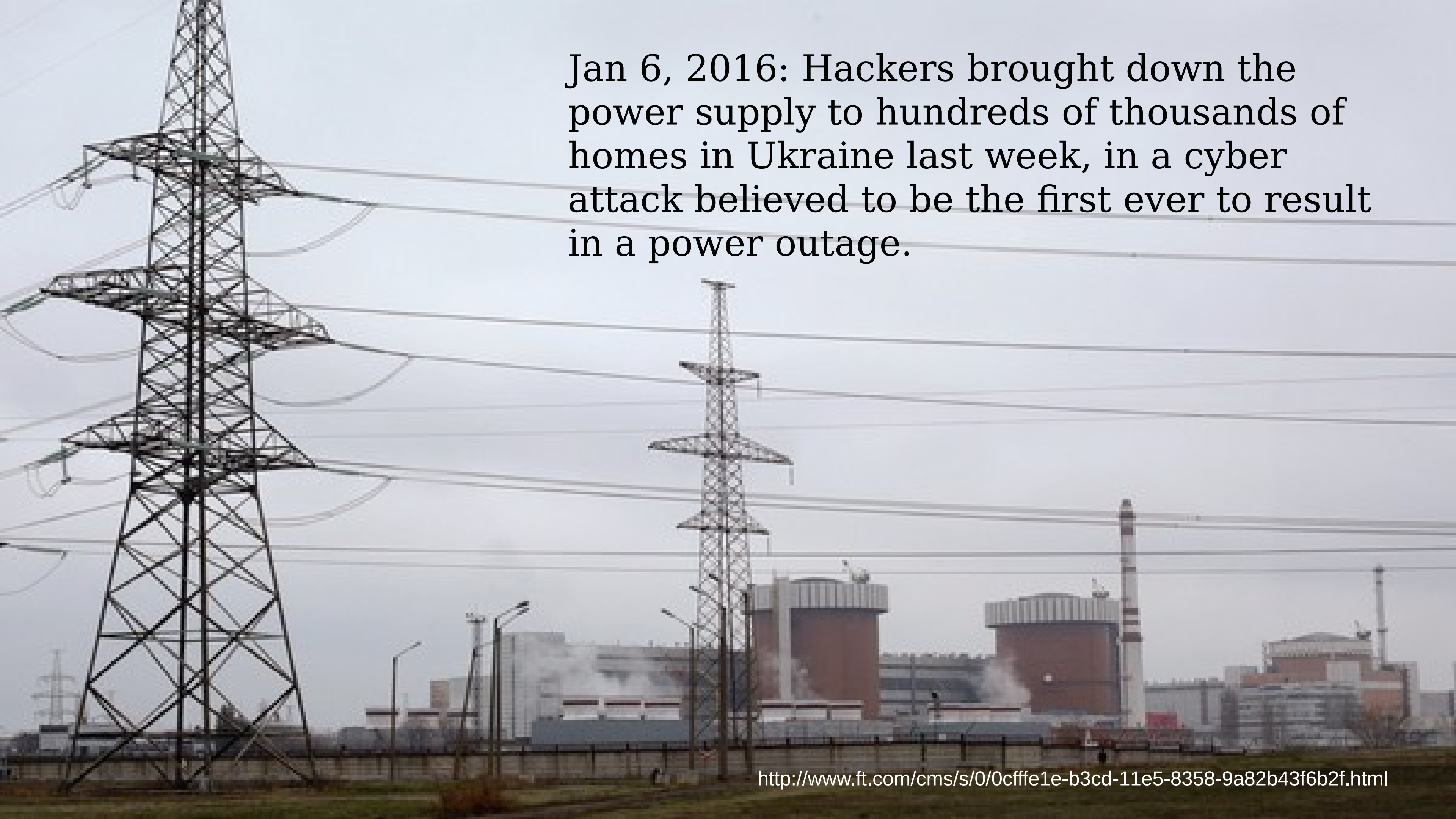
https://www.shodan.io/
http://www.chip.de/news/Shodan-Suchmaschine-findet-Sicherheitsluecken_61471130.html
http://www.forbes.com/sites/kashmirhill/2013/09/05/the-crazy-things-a-savvy-shodan-searcher-can-find-exposed-on-the-internet/#856386b1f240



Hackers Remotely Kill a Jeep on the Highway—With Me in It

Uconnect, an Internet-connected computer feature in hundreds of thousands of Fiat Chrysler cars, SUVs, and trucks… lets anyone who knows the car's IP address gain access from anywhere in the country.

http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/



Jan 6, 2016: Hackers brought down the power supply to hundreds of thousands of homes in Ukraine last week, in a cyber attack believed to be the first ever to result in a power outage.

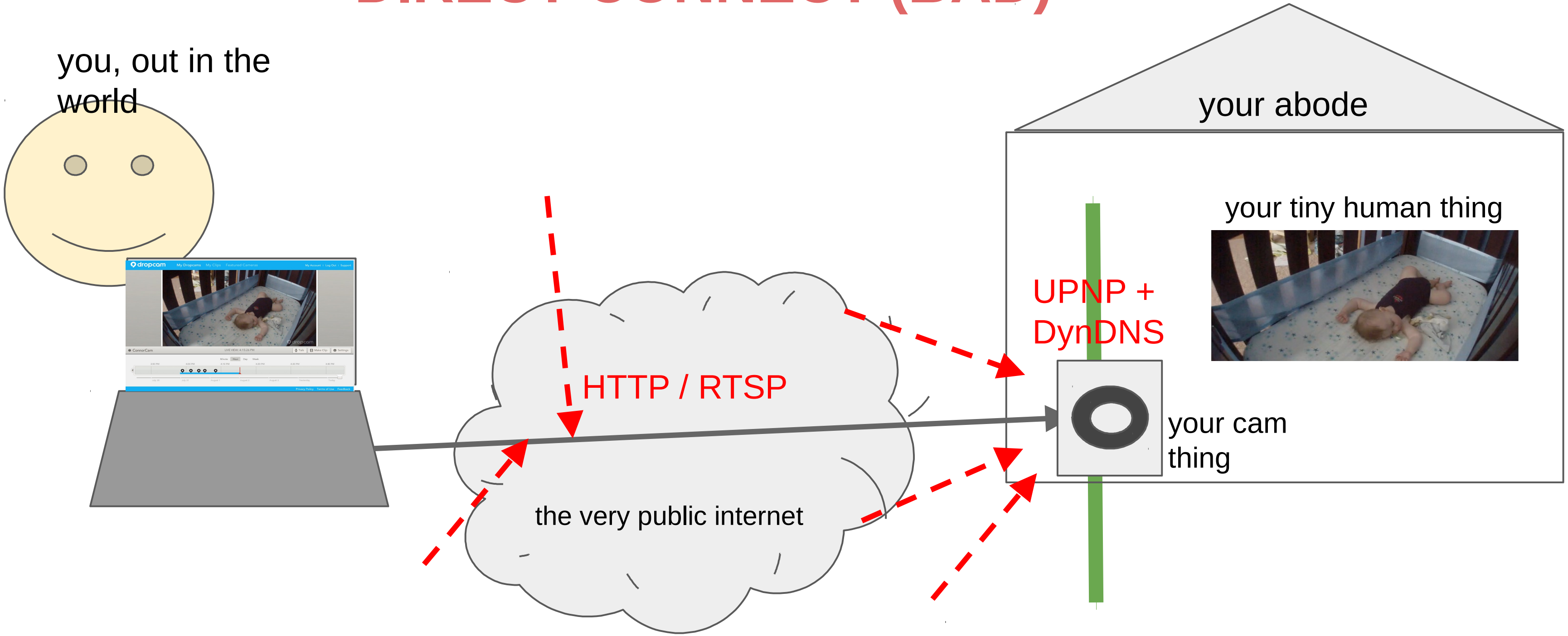
http://www.ft.com/cms/s/0/0cfffe1e-b3cd-11e5-8358-9a82b43f6b2f.html

Too many “Things” are exposed to the public Internet without the ability to provide strongly confidential and authenticated remote access

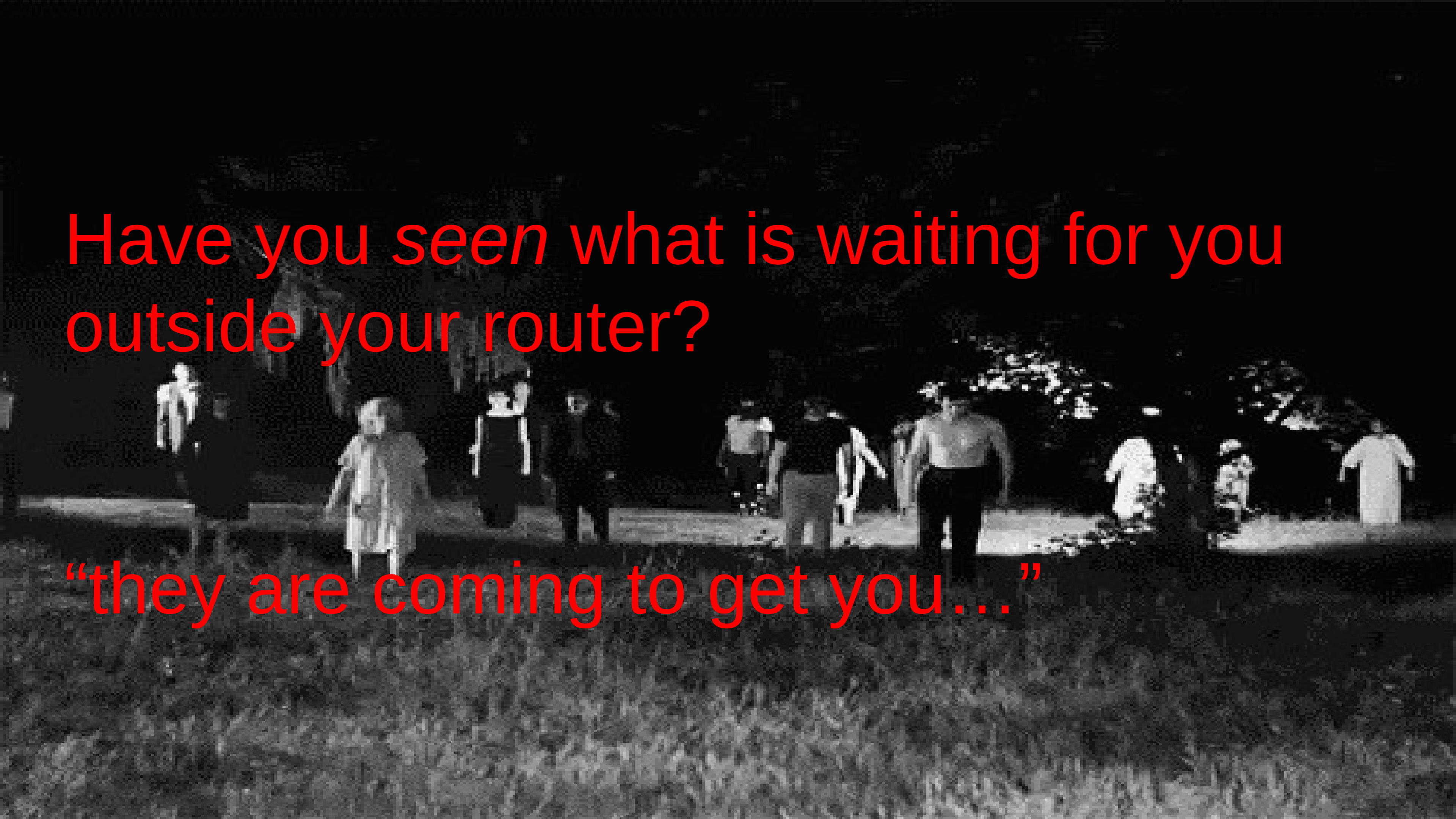
There are more “Things” every day.

We must do something ***now*** to fundamentally change the way they are being connected to the Internet.

DIRECT CONNECT (BAD)



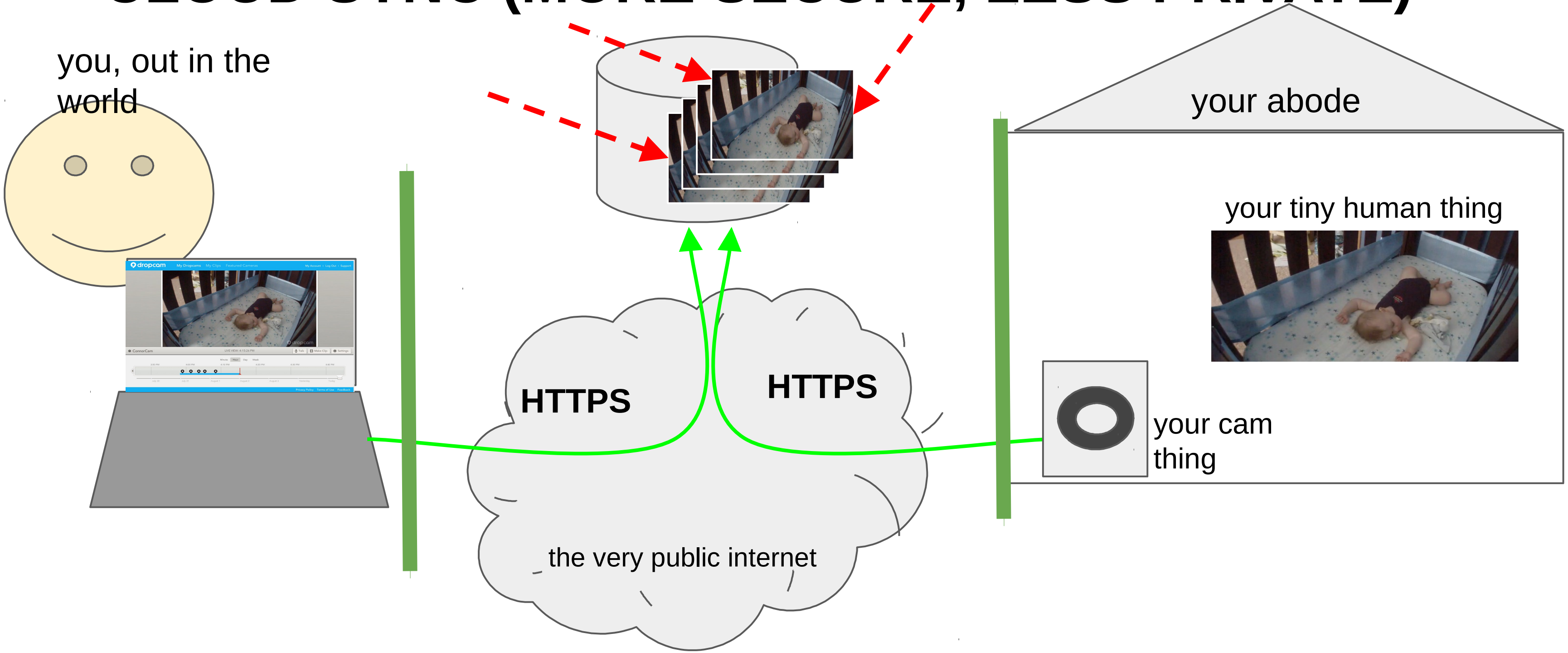
You connect to Your Thing via Direct Internet Address Through Open Firewall Port (usually without encryption and often with default passwords)



Have you *seen* what is waiting for you outside your router?

“they are coming to get you…”

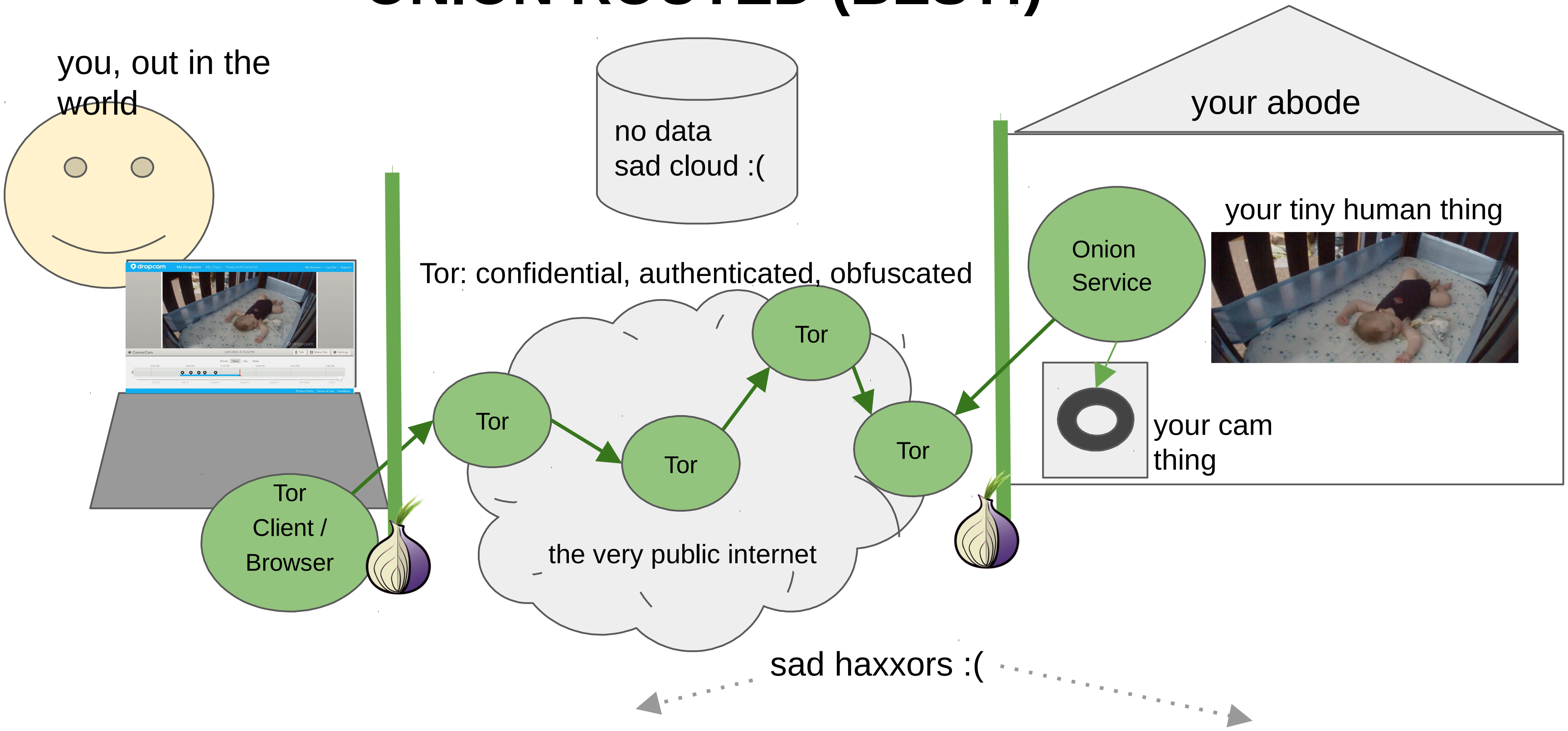
CLOUD SYNC (MORE SECURE, LESS PRIVATE)



You connect to Your Thing through a Cloud Service
(which then knows all, remembers all, and happily shares and/or monetizes all)

Why continue to rely on the flawed models and implementations of TLS and Certificate Authorities, when the shift to Things means we can do more?

ONION ROUTED (BEST!)



you, out in the world

no data
sad cloud :(

your abode

your tiny human thing

Tor: confidential, authenticated, obfuscated

Onion Service

Tor

Tor

Tor

Tor

Tor Client / Browser

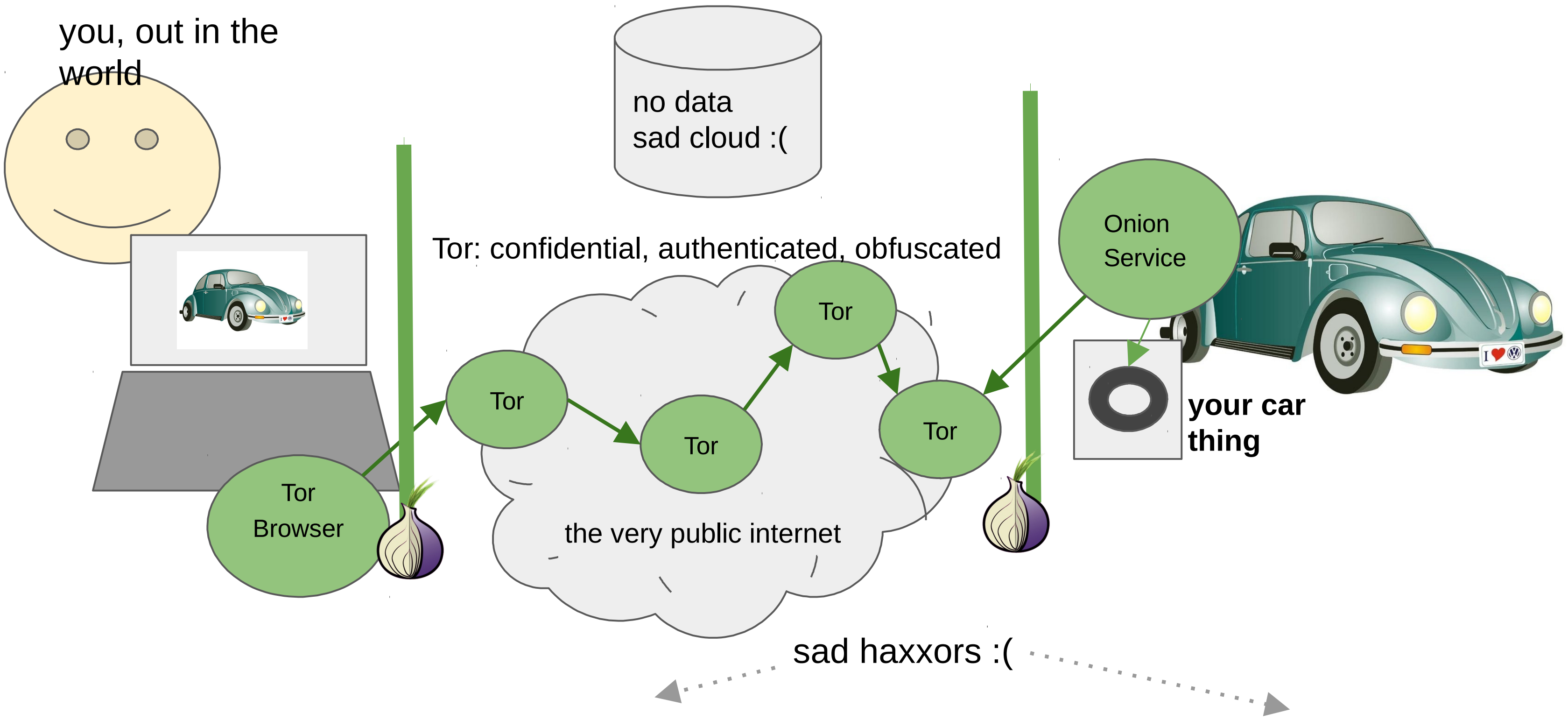
your cam thing

the very public internet

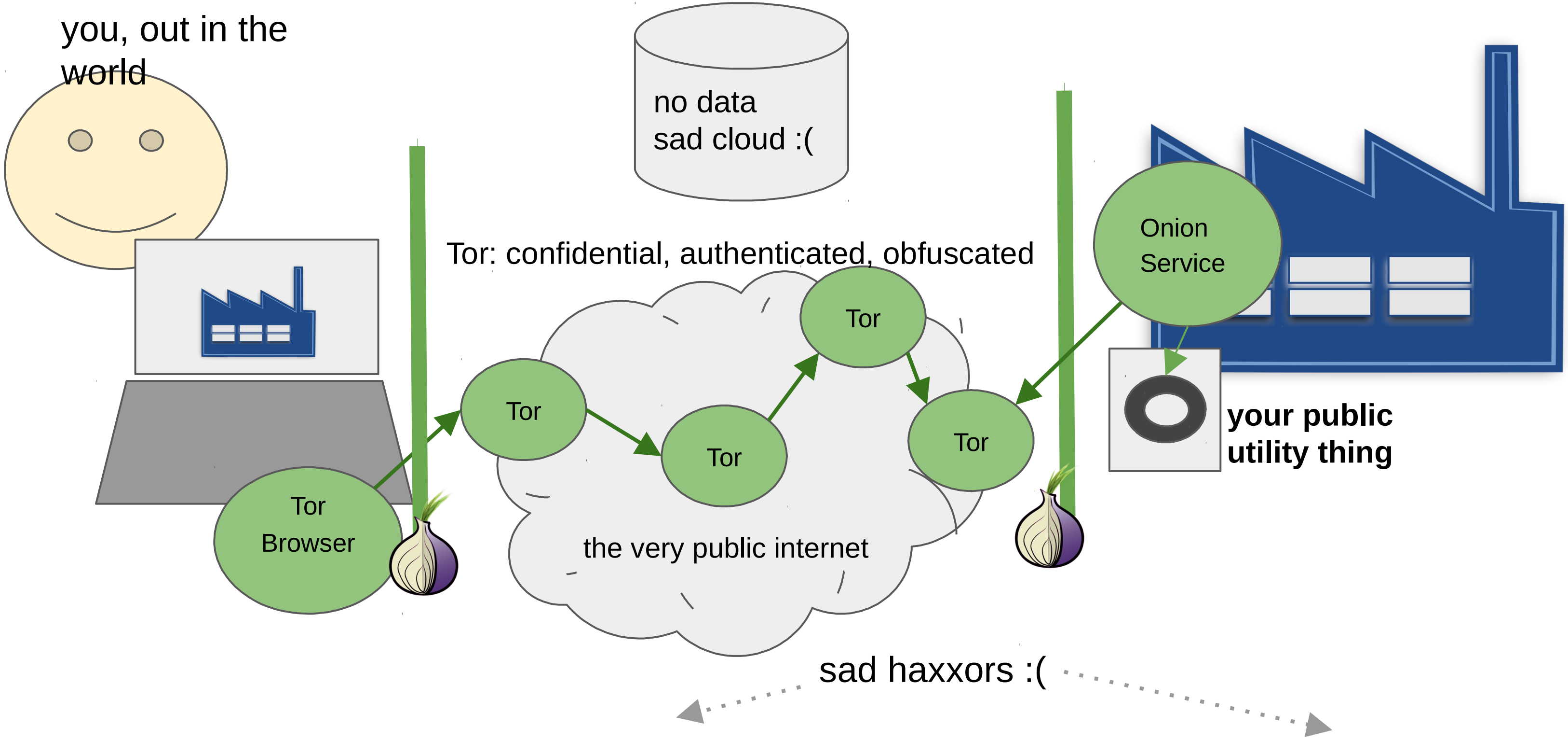
sad haxxors :(

You connect to Your Thing through Tor as an Onion Service
(nobody knows who you are connecting to or what you are seeing except you)

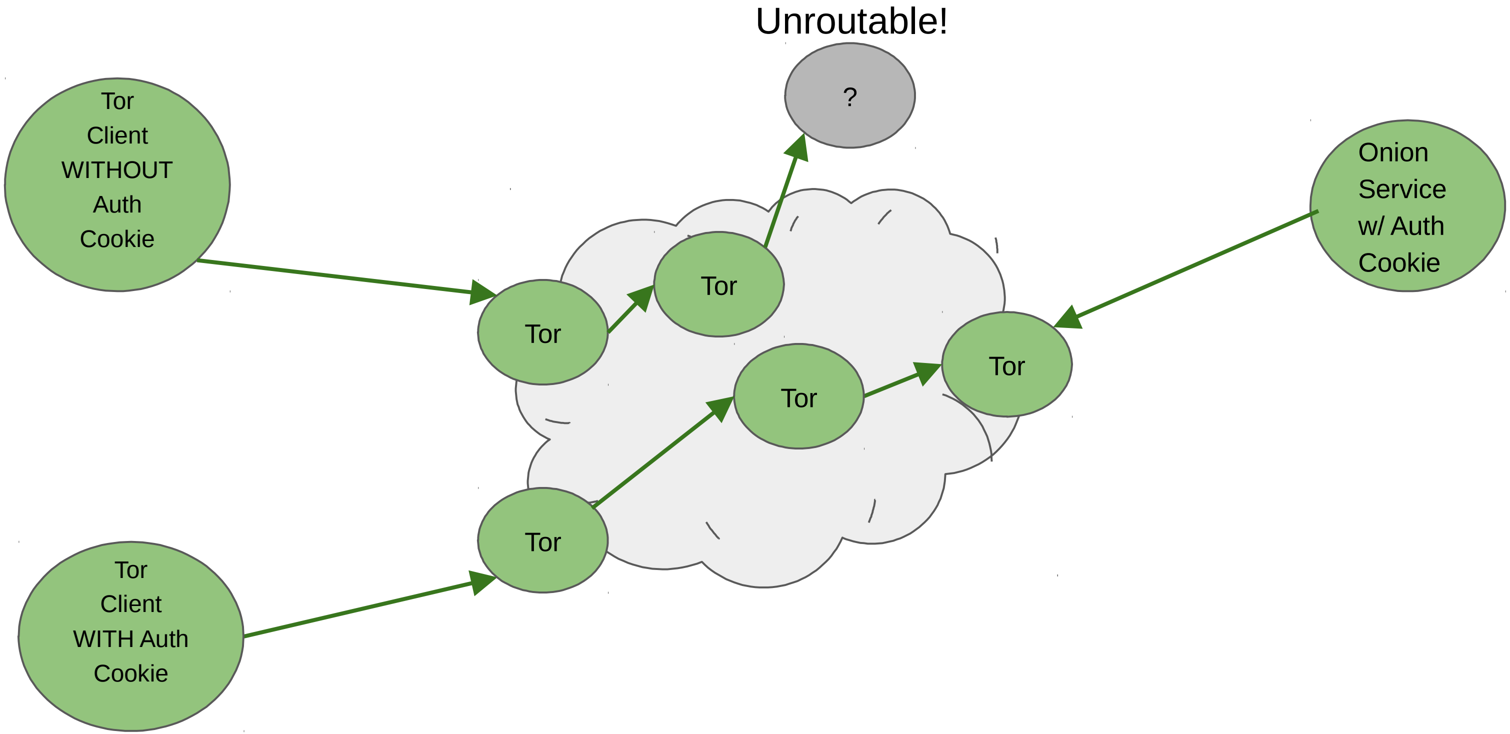
Tor can safely connect you to your devices at home, and does so with a very realistic and complex threat model in mind



You connect to Your Thing through Tor as an Onion Service
(nobody knows who you are connecting to or what you are seeing except you)

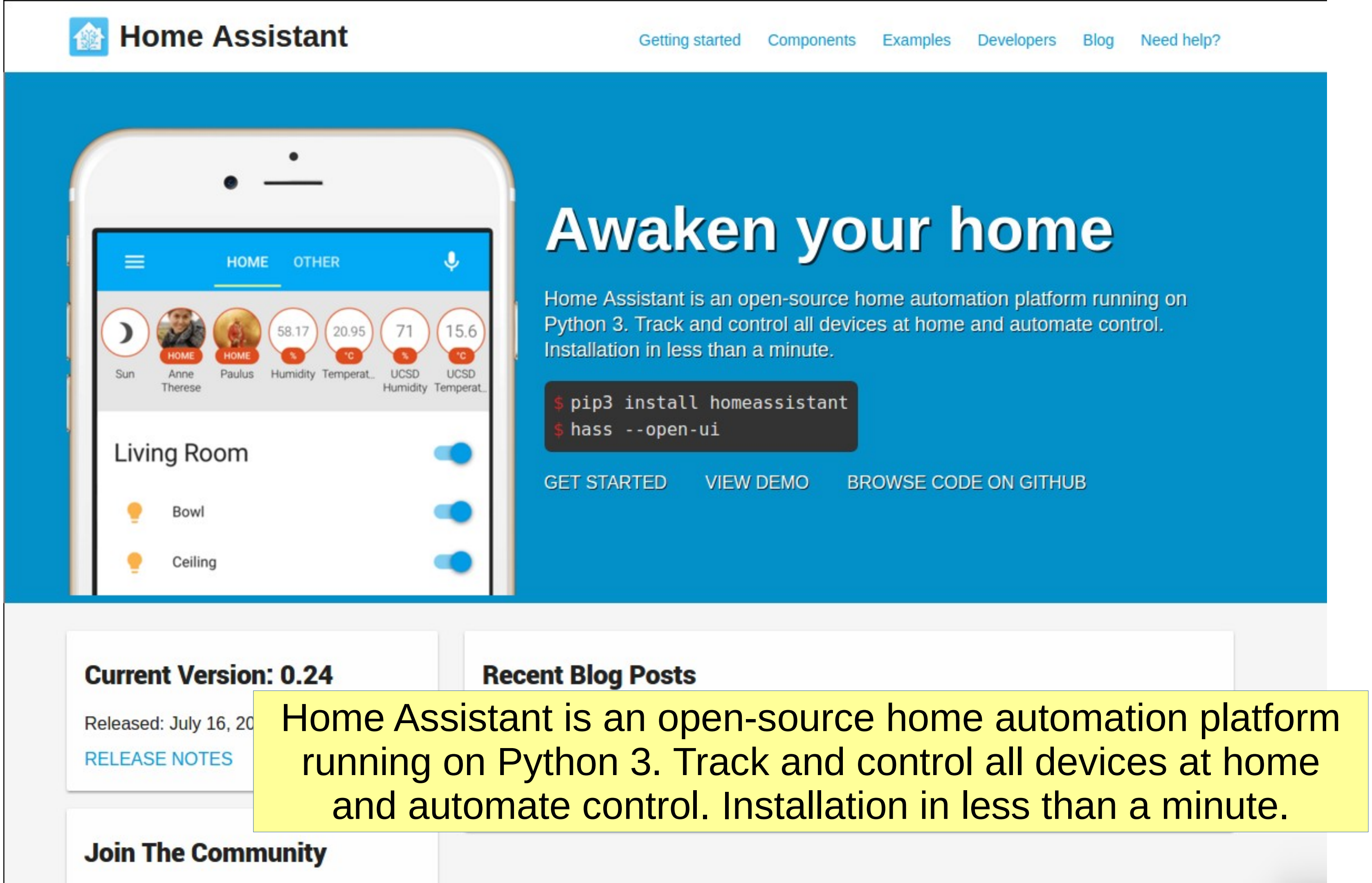


You connect to Your Thing through Tor as an Onion Service
(nobody knows who you are connecting to or what you are seeing except you)


Unroutable!
?
Tor Client WITHOUT Auth Cookie
Tor
Tor
Onion Service w/ Auth Cookie
Tor
Tor
Tor
Tor Client WITH Auth Cookie

Onion (or “Hidden”) Services can even hide the fact they exist at all, if you don’t know the necessary cookie. With Onion Authentication, you can’t crawl or probe.

What can we do now with existing, off the shelf solutions?



Awaken your home

Home Assistant is an open-source home automation platform running on Python 3. Track and control all devices at home and automate control. Installation in less than a minute.

```
$ pip3 install homeassistant
$ hass --open-ui
```

GET STARTED VIEW DEMO BROWSE CODE ON GITHUB

Current Version: 0.24

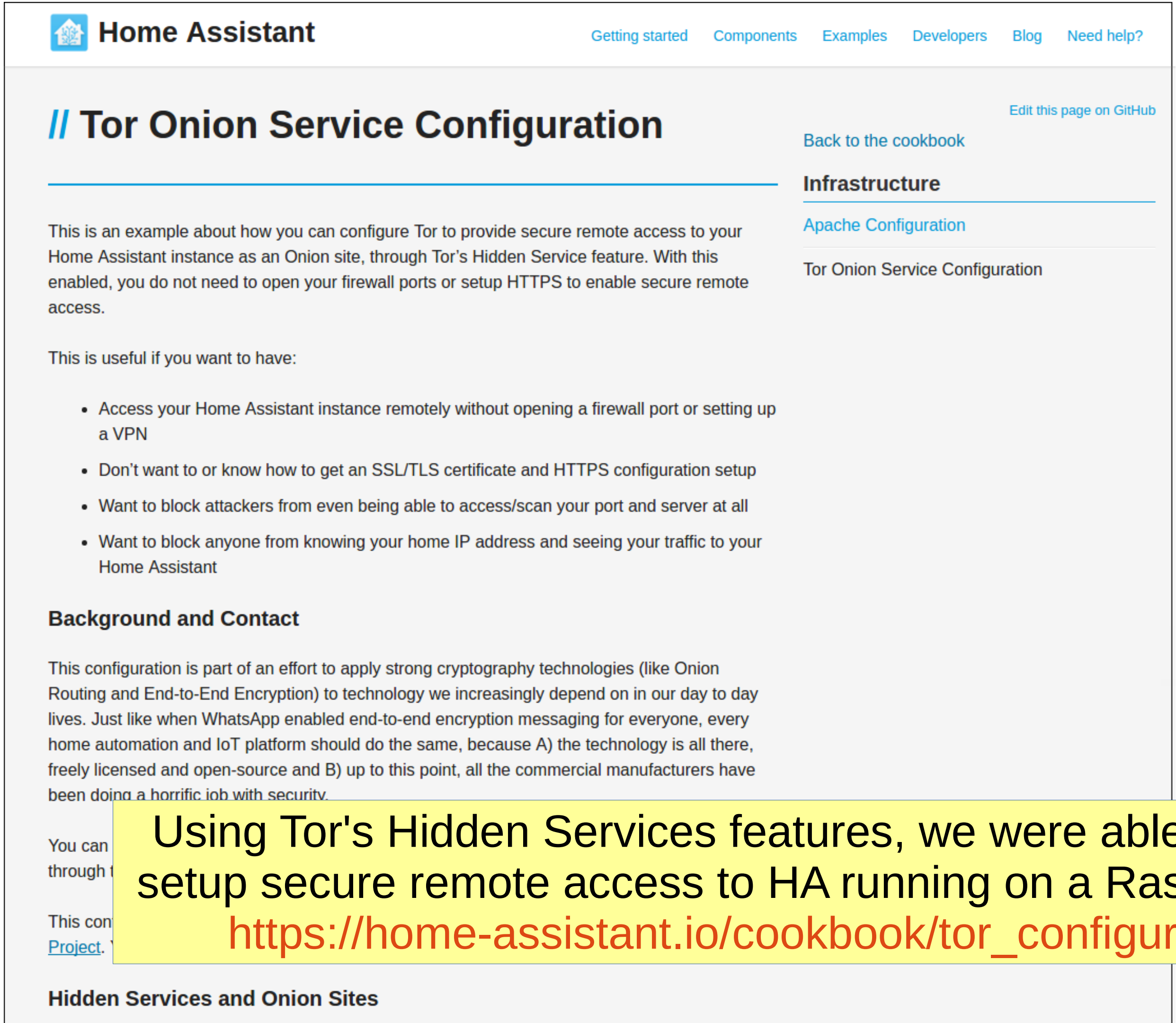
Released: July 16, 20

RELEASE NOTES

Recent Blog Posts

Join The Community

Home Assistant is an open-source home automation platform running on Python 3. Track and control all devices at home and automate control. Installation in less than a minute.



Home Assistant

Getting started Components Examples Developers Blog Need help?

// Tor Onion Service Configuration

Edit this page on GitHub

Back to the cookbook

Infrastructure

Apache Configuration

Tor Onion Service Configuration

This is an example about how you can configure Tor to provide secure remote access to your Home Assistant instance as an Onion site, through Tor's Hidden Service feature. With this enabled, you do not need to open your firewall ports or setup HTTPS to enable secure remote access.

This is useful if you want to have:

- Access your Home Assistant instance remotely without opening a firewall port or setting up a VPN
- Don't want to or know how to get an SSL/TLS certificate and HTTPS configuration setup
- Want to block attackers from even being able to access/scan your port and server at all
- Want to block anyone from knowing your home IP address and seeing your traffic to your Home Assistant

Background and Contact

This configuration is part of an effort to apply strong cryptography technologies (like Onion Routing and End-to-End Encryption) to technology we increasingly depend on in our day to day lives. Just like when WhatsApp enabled end-to-end encryption messaging for everyone, every home automation and IoT platform should do the same, because A) the technology is all there, freely licensed and open-source and B) up to this point, all the commercial manufacturers have been doing a horrific job with security.

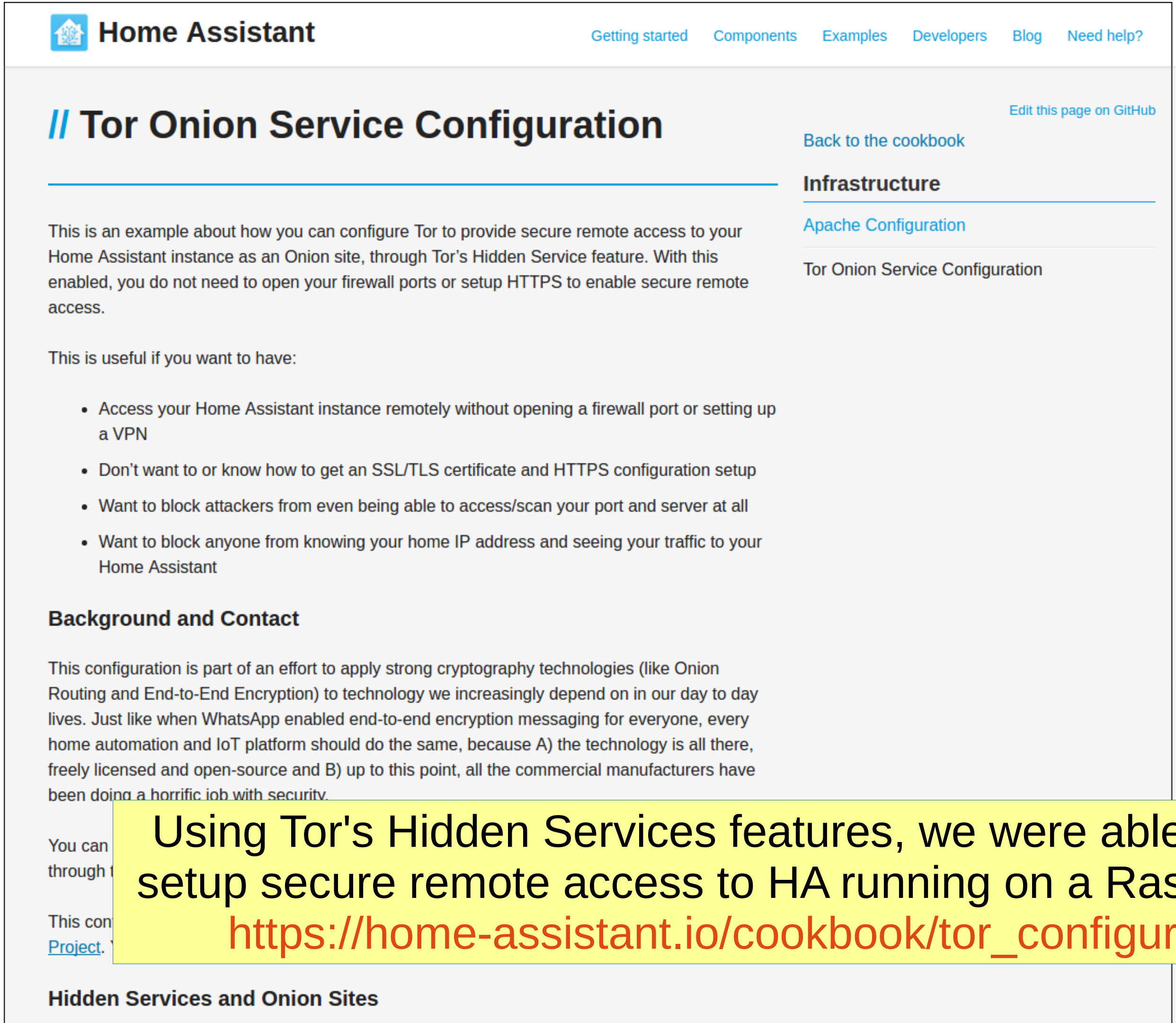
You can
through t

This con
Project. \

Hidden Services and Onion Sites

Using Tor's Hidden Services features, we were able to easily setup secure remote access to HA running on a Raspberry Pi: https://home-assistant.io/cookbook/tor_configuration/

Includes the
Fastest Pi Ever!
Raspberry Pi™ 3 Model B
✓Broadcom® BCM2837 64bit 1.2GHz Quad Core Processor
✓Onboard BCM43143 WiFi
✓Onboard Bluetooth (BLE)
✓1GB RAM
✓4 USB 2.0 Ports
✓40 Pin Extended GPIO
✓Full-Size HDMI
INCLUDES USER GUIDE DOWNLOAD
Raspberry Pi
User Guide
Tor
TorProject.org



// Tor Onion Service Configuration

This is an example about how you can configure Tor to provide secure remote access to your Home Assistant instance as an Onion site, through Tor's Hidden Service feature. With this enabled, you do not need to open your firewall ports or setup HTTPS to enable secure remote access.

This is useful if you want to have:

- Access your Home Assistant instance remotely without opening a firewall port or setting up a VPN
- Don't want to or know how to get an SSL/TLS certificate and HTTPS configuration setup
- Want to block attackers from even being able to access/scan your port and server at all
- Want to block anyone from knowing your home IP address and seeing your traffic to your Home Assistant

Background and Contact

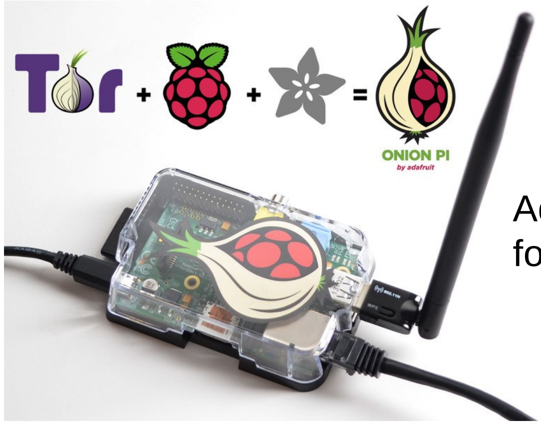
This configuration is part of an effort to apply strong cryptography technologies (like Onion Routing and End-to-End Encryption) to technology we increasingly depend on in our day to day lives. Just like when WhatsApp enabled end-to-end encryption messaging for everyone, every home automation and IoT platform should do the same, because A) the technology is all there, freely licensed and open-source and B) up to this point, all the commercial manufacturers have been doing a horrific job with security.

You can
through t

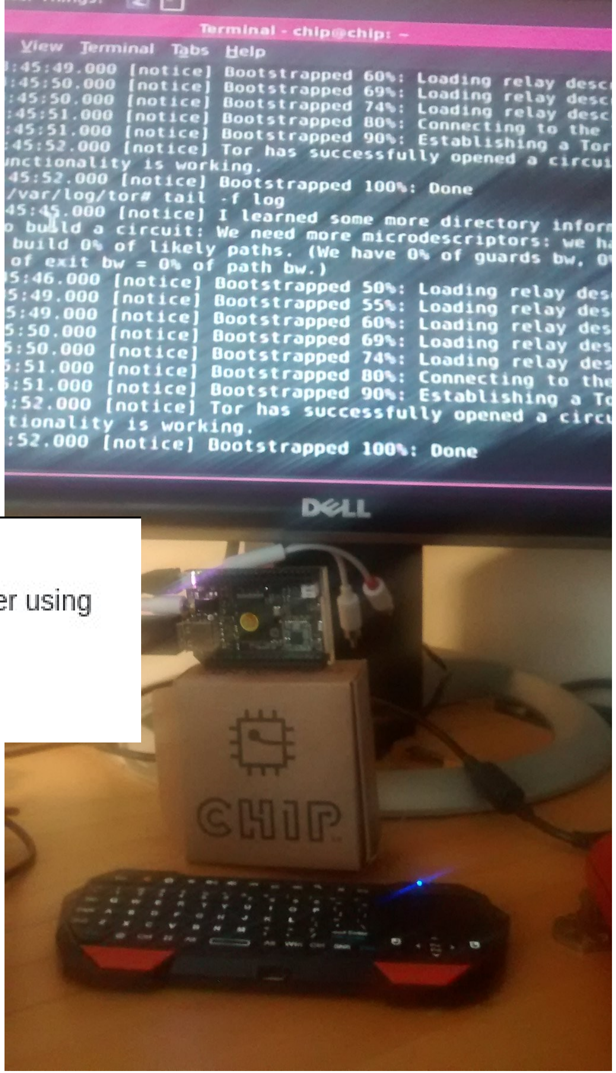
This con
Project. '

Hidden Services and Onion Sites

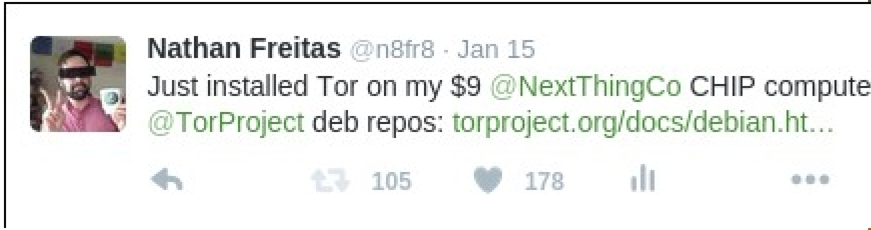
Using Tor's Hidden Services features, we were able to easily setup secure remote access to HA running on a Raspberry Pi: https://home-assistant.io/cookbook/tor_configuration/



AdaFruit OnionPi
for $59



```
:45:49.000 [notice] Bootstrapped 60%: Loading relay desc
:45:50.000 [notice] Bootstrapped 69%: Loading relay desc
:45:50.000 [notice] Bootstrapped 74%: Loading relay desc
:45:51.000 [notice] Bootstrapped 80%: Connecting to the
:45:51.000 [notice] Bootstrapped 90%: Establishing a Tor
:45:52.000 [notice] Tor has successfully opened a circui
nctionality is working.
45:52.000 [notice] Bootstrapped 100%: Done
/var/log/tor# tail -f log
45:45.000 [notice] I learned some more directory infor
o build a circuit: We need more microdescriptors: we ha
 build 0% of likely paths. (We have 0% of guards bw, 0
 of exit bw = 0% of path bw.)
5:46.000 [notice] Bootstrapped 50%: Loading relay des
5:49.000 [notice] Bootstrapped 55%: Loading relay des
5:49.000 [notice] Bootstrapped 60%: Loading relay des
5:50.000 [notice] Bootstrapped 69%: Loading relay des
5:50.000 [notice] Bootstrapped 74%: Loading relay des
5:51.000 [notice] Bootstrapped 80%: Connecting to the
5:51.000 [notice] Bootstrapped 90%: Establishing a To
:52.000 [notice] Tor has successfully opened a circu
tionality is working.
:52.000 [notice] Bootstrapped 100%: Done
```



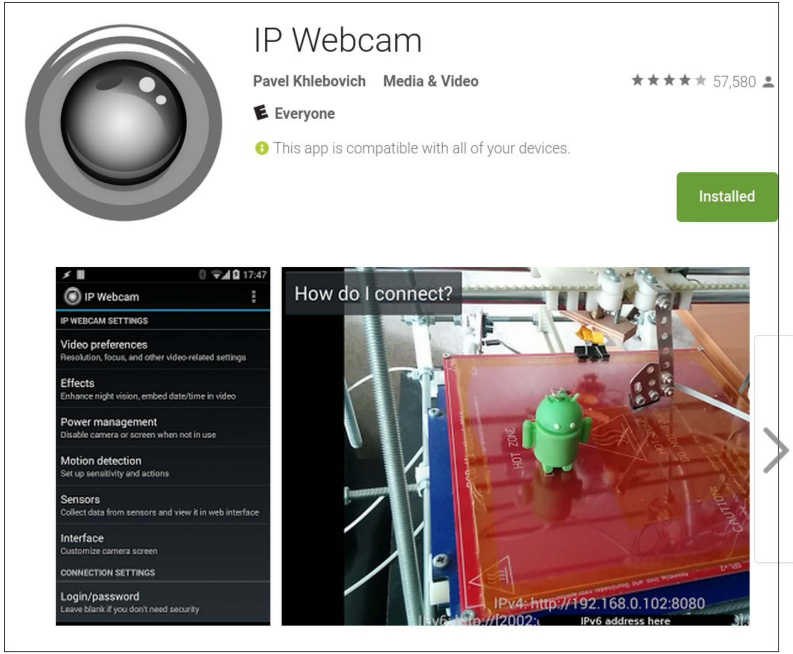
Nathan Freitas @n8fr8 · Jan 15

Just installed Tor on my $9 @NextThingCo CHIP computer using @TorProject deb repos: torproject.org/docs/debian.ht...

105 178

Tor can run on, and be built into, really cheap Things! It just requires some form of Linux and an ARM chip.

What if we built an Onion-secure home webcam or baby monitor device?



IP Webcam

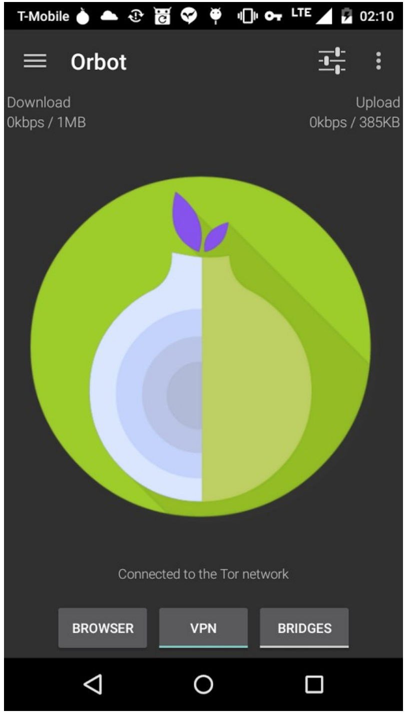
Pavel Khlebovich Media & Video ★★★★☆ 57,580

Everyone

This app is compatible with all of your devices.

Installed
17:47
IP Webcam
IP WEBCAM SETTINGS
Video preferences
Resolution, focus, and other video-related settings
Effects
Enhance night vision, embed date/time in video
Power management
Disable camera or screen when not in use
Motion detection
Set up sensitivity and actions
Sensors
Collect data from sensors and view it in web interface
Interface
Customize camera screen
CONNECTION SETTINGS
Login/password
Leave blank if you don't need security
How do I connect?
IPv4: http://192.168.0.102:8080
IPv6 address here

+



Download
0kbps / 1MB

Upload
0kbps / 385KB

Connected to the Tor network

= OnionCam for Android!

(available now with just a few steps of setup!)

OnionCam: Quick How To

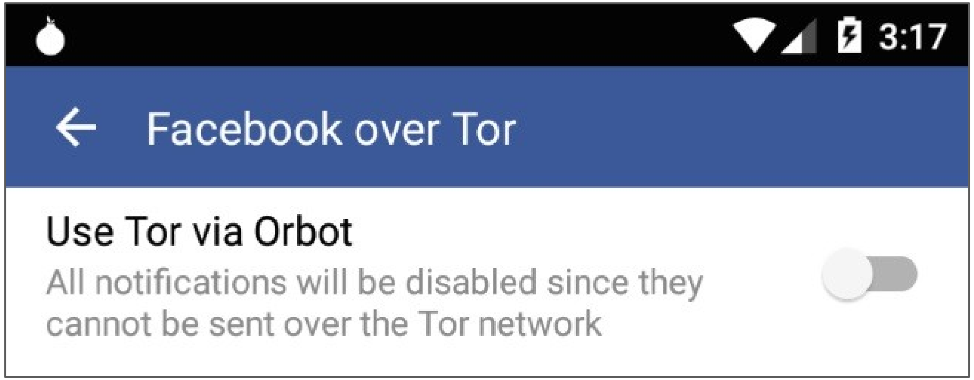
1) Install Orbot
2) Enable Orbot Settings->Hidden Service Hosting
3) Enter “8080” into Orbot Settings->Hidden Service Ports
4) Start/Restart Orbot
5) Find your new Onion hostname in Orbot Settings->.Onion Hostname
6) Install IP Webcam app (Free or Pro)
    a) Set a username/password for the IP Webcam server!
7) Start IP WebCam
8) Go to http://yourdotonion:8080 in Tor Browser

02/09/16 11:54:33 59%
IP Webcam Free Video Recording
Remove this message by going Pro:
http://goo.gl/QgJnKe
BELLA
BREAD

OnionCam in my Kitchen… everything is safe and sound!
Access via Tor Browser at http://<myprivateaddress>.onion:8080
or via VLC RTSP video streaming via rtsp://myprivateaddress.onion:8080/video

Using the NetCipher Library for Android, anyone can build in Onion Service support right into apps like IP WebCam and WebCam viewer apps to make the OnionCam a reality today.

This is what Facebook did to add Tor support into their Android app:



Facebook over Tor

Use Tor via Orbot

All notifications will be disabled since they cannot be sent over the Tor network

https://guardianproject.info/code/netcipher

Tor Onion Services addresses both the needs and threats of IoT

It provides direct connectivity between you and your things, or things and other things, without sacrificing confidentiality and authentication, or compromising your broader network security

It has built-in resistance to unauthenticated probing and access, and decouples specific Internet address from specific devices or services

It is 100% free and open-source, scrupulously engineered,designed to withstand the threat of nation state grade actors, and available NOW

The Internet of Things:

Hopefully coming soon to a webcam, baby monitor, car, power plant, thermostat, toaster, television, toilet, drone, health tracker and anyotherkindofthing near you!

@n8fr8 @torproject and more at https://torproject.org