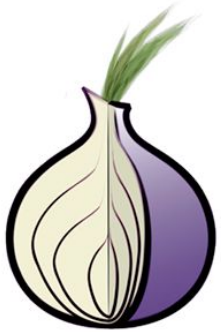
The Internet of  Things

@n8fr8 @guardianproject @torproject

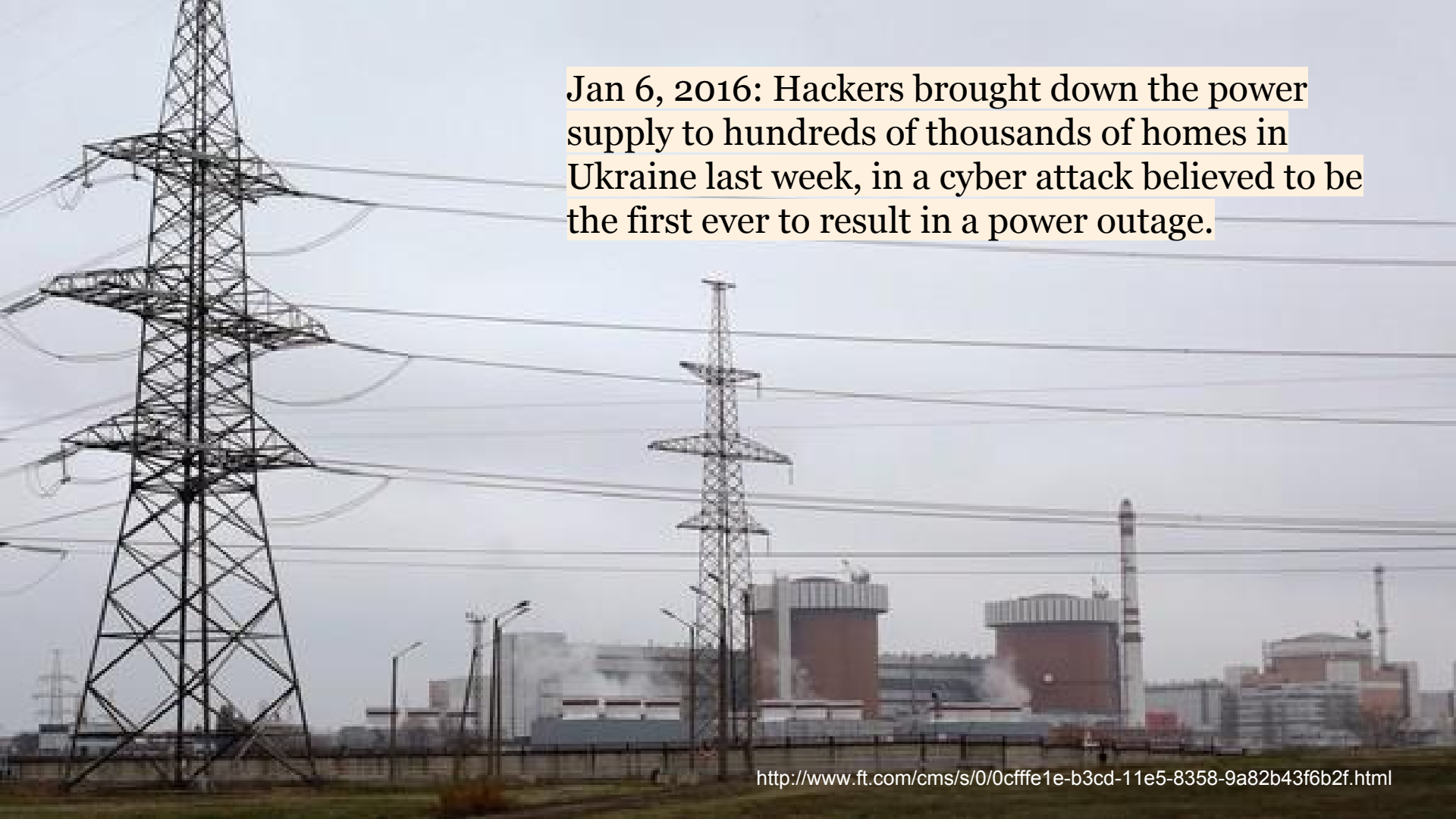
“Networked sensors and the Internet of Things are projected to grow substantially, and this has the potential to drastically change surveillance. The still images, video, and audio captured by these devices may enable real-time intercept and recording with after-the-fact access. Thus an inability to 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.

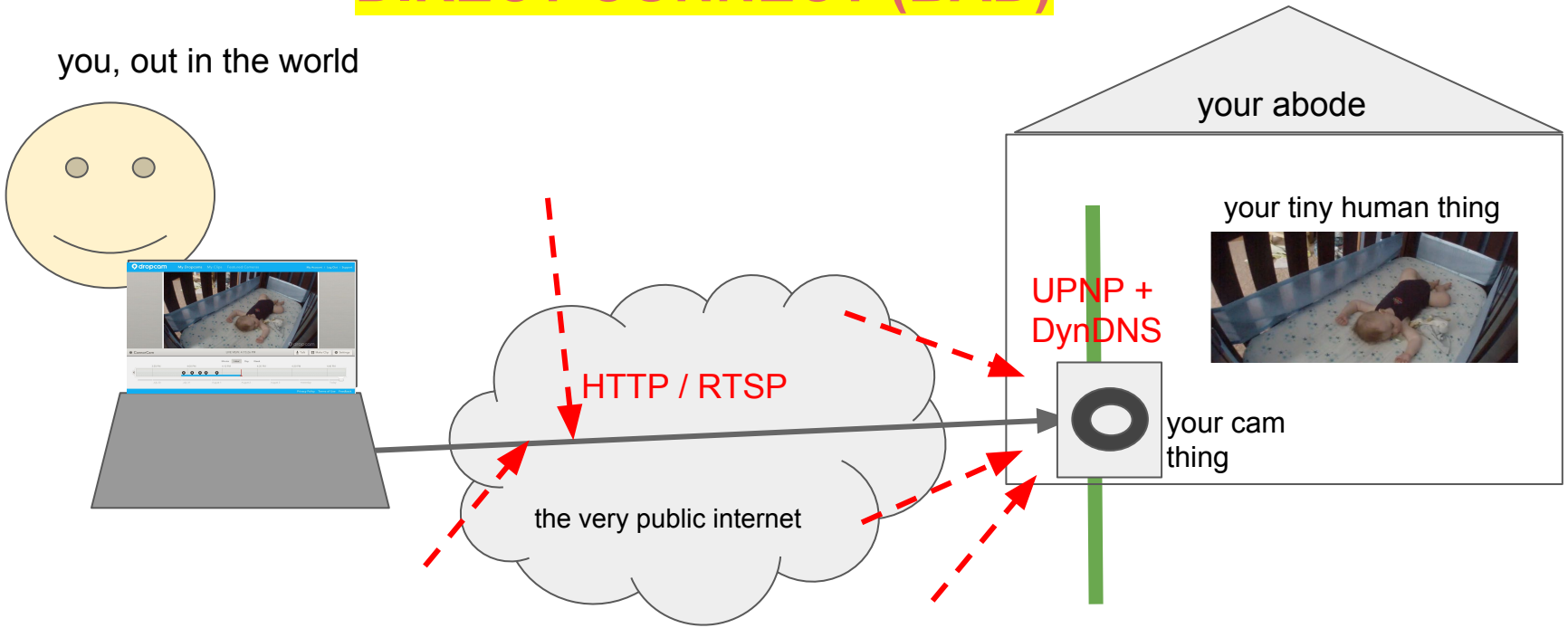
http://www.ft.com/cms/s/0/0cfffe1e-b3cd-11e5-8358-9a82b43f6b2f.html

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

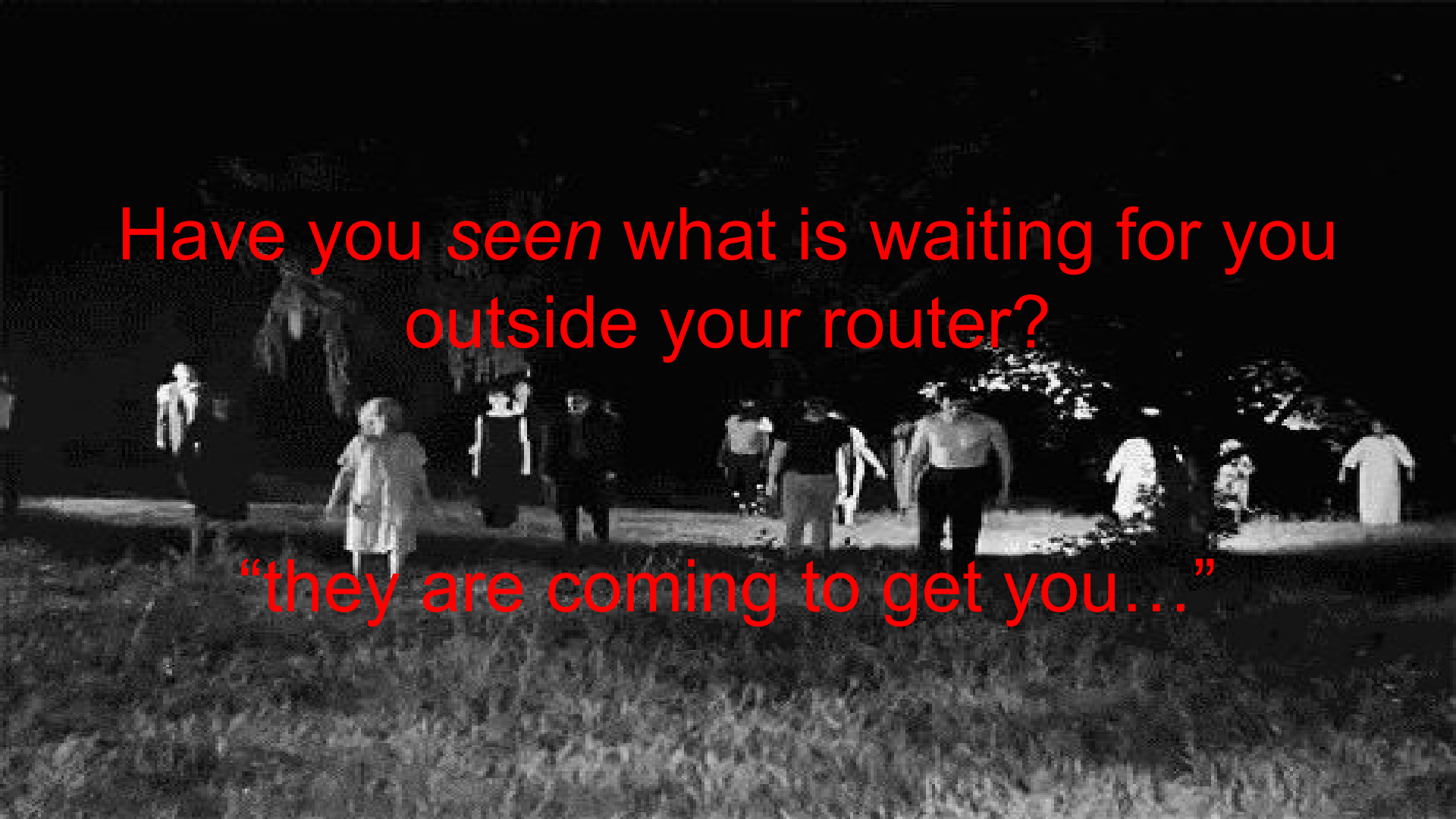
There are more “Things” every day.

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

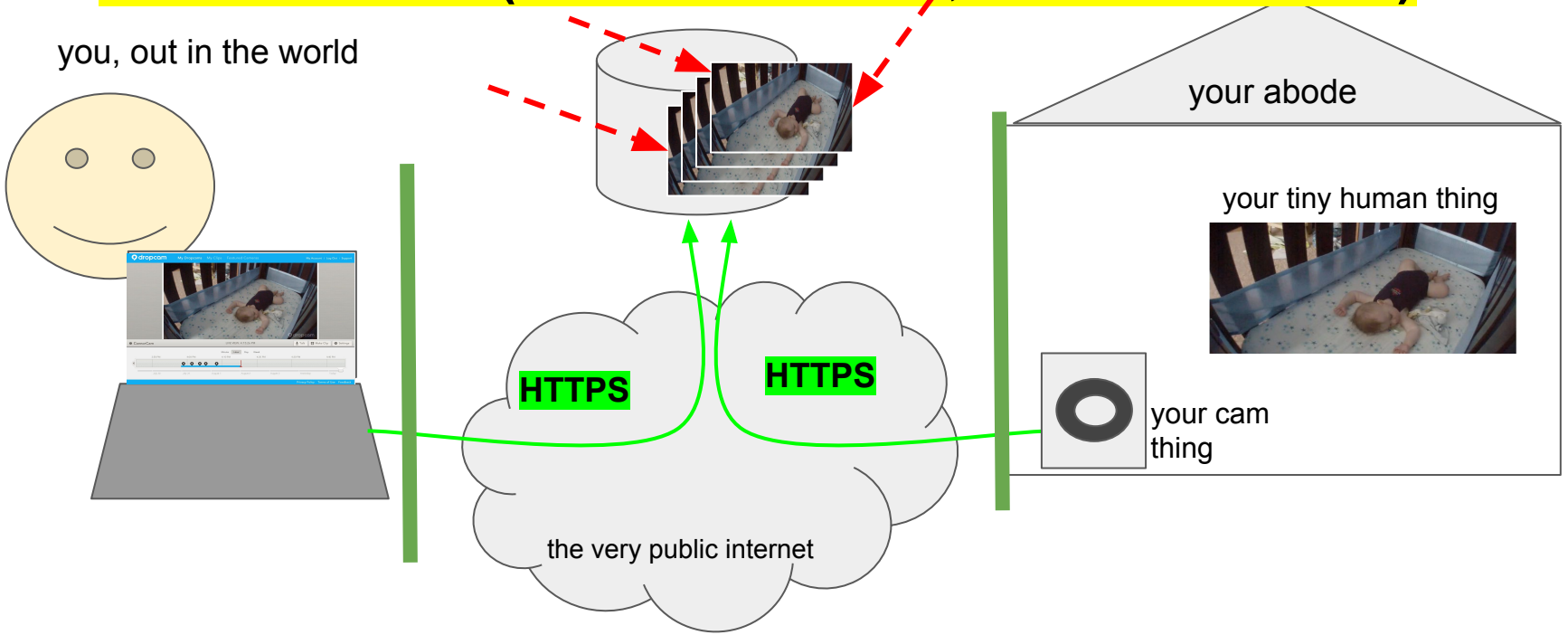
DIRECT CONNECT (BAD)



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…”

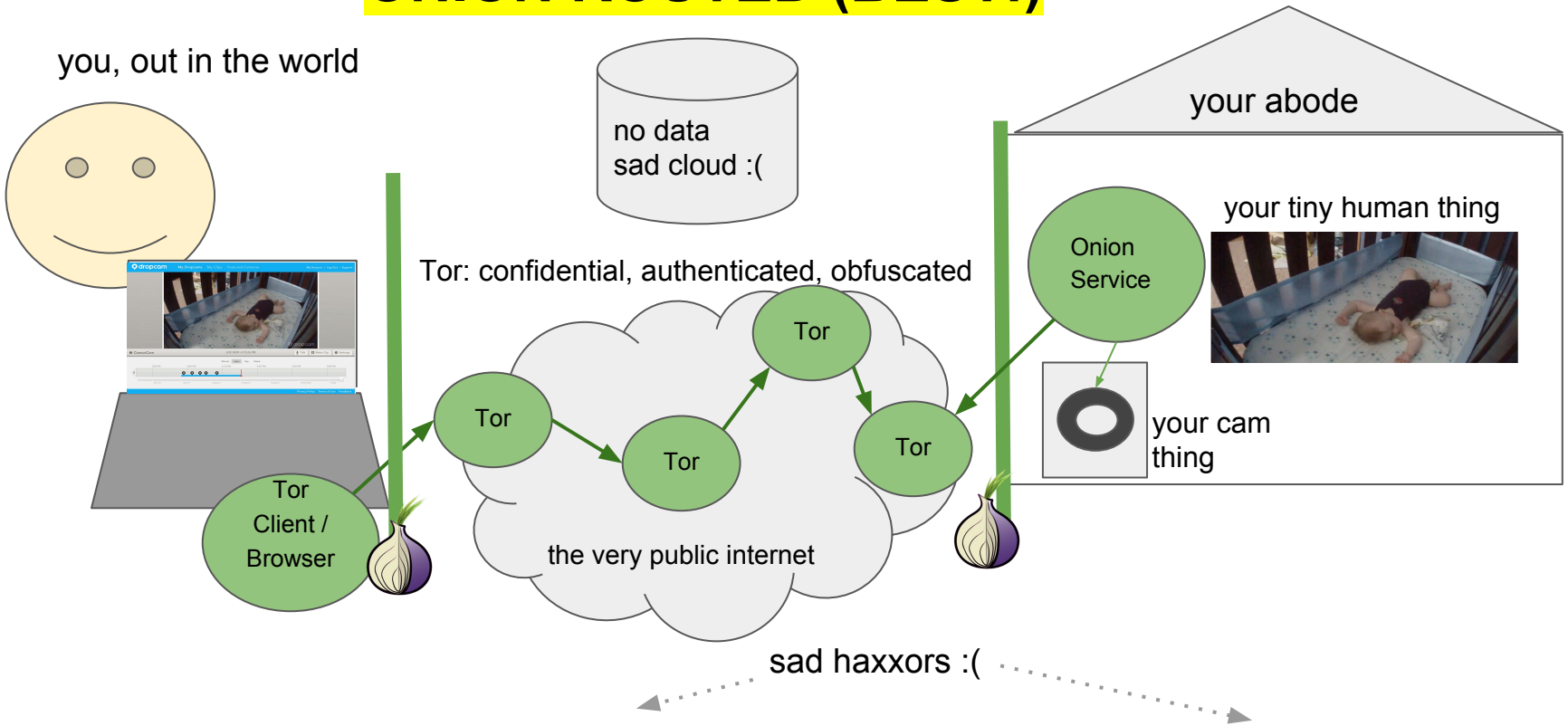
CLOUD SYNC (MORE SECURE, LESS PRIVATE)



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

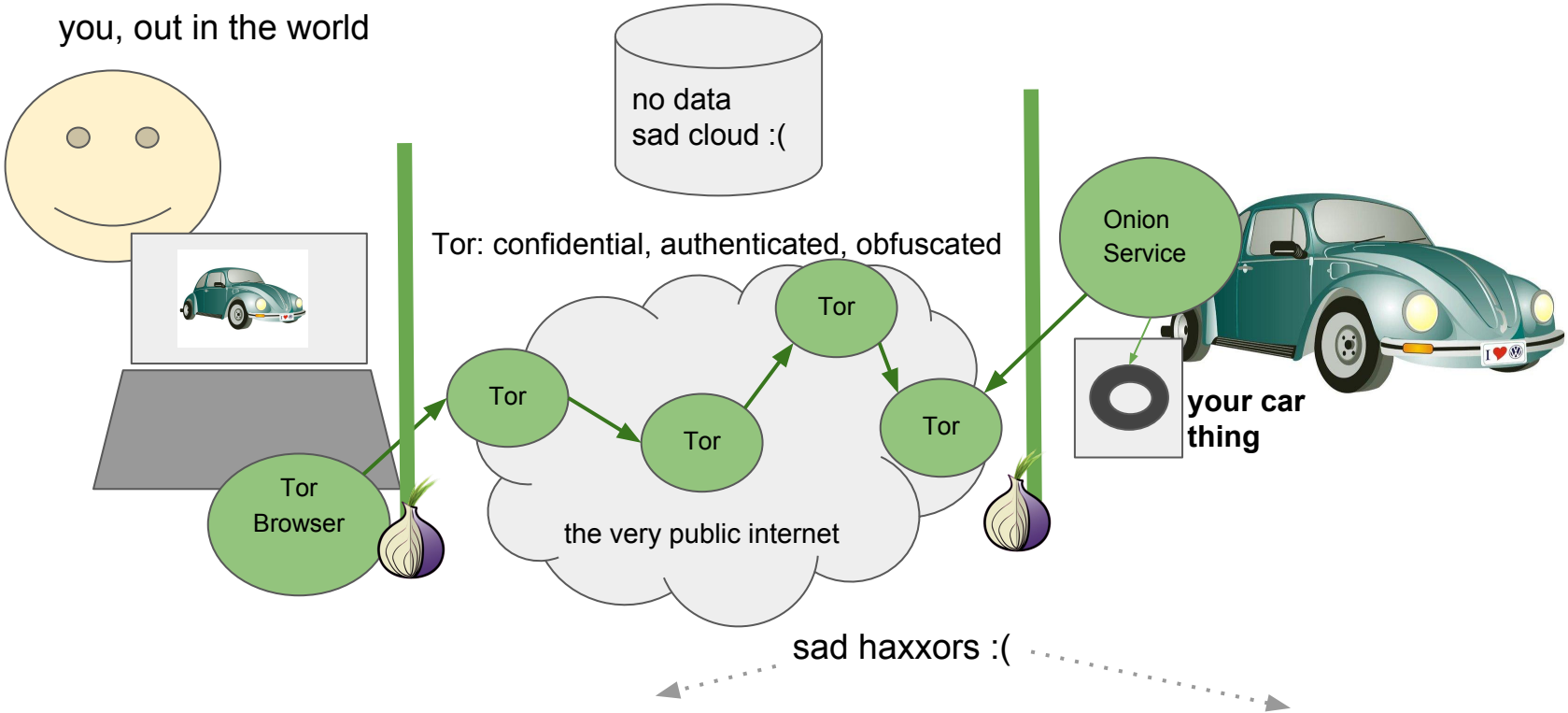
Why continue to rely on the flawed models and implementations of TLS and Certificate Authorities, when the shift to Things means we can do more?

ONION ROUTED (BEST!)

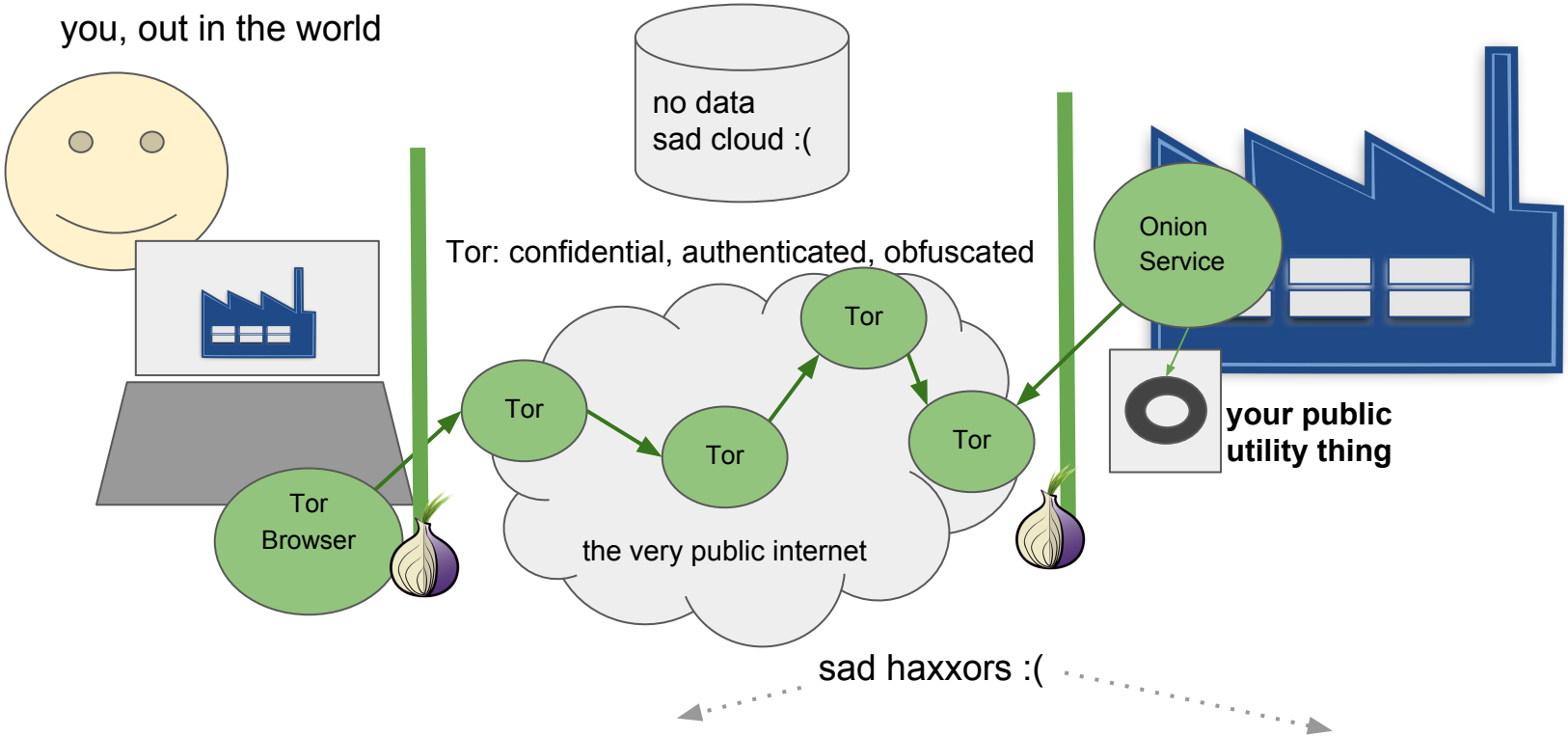


You connect to Your Thing through Tor as an Onion Service
(nobody knows who you are connecting to or what you are seeing except you)

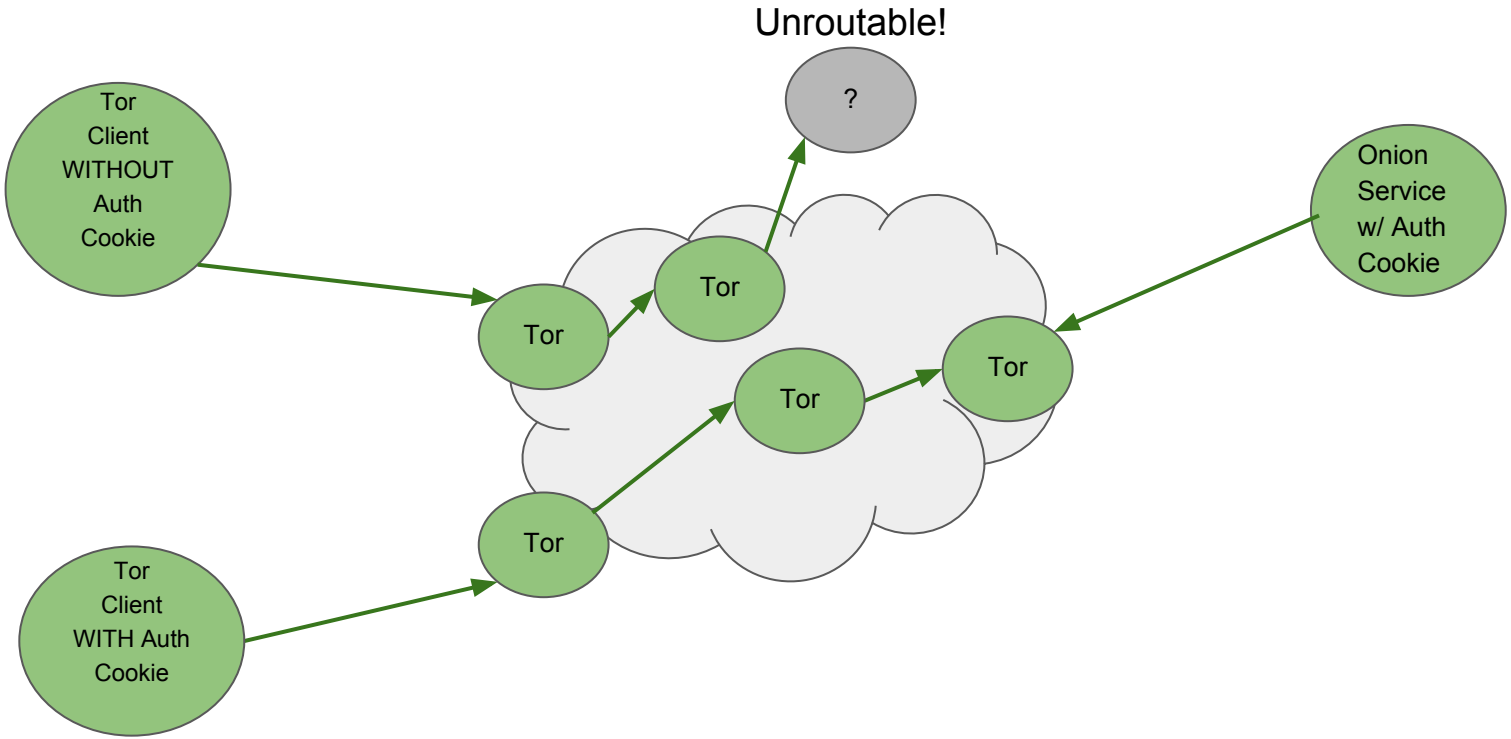
Tor can safely “poke holes” in firewalls to connect you to peers, but does so with a very complicated and real threat model in mind



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)

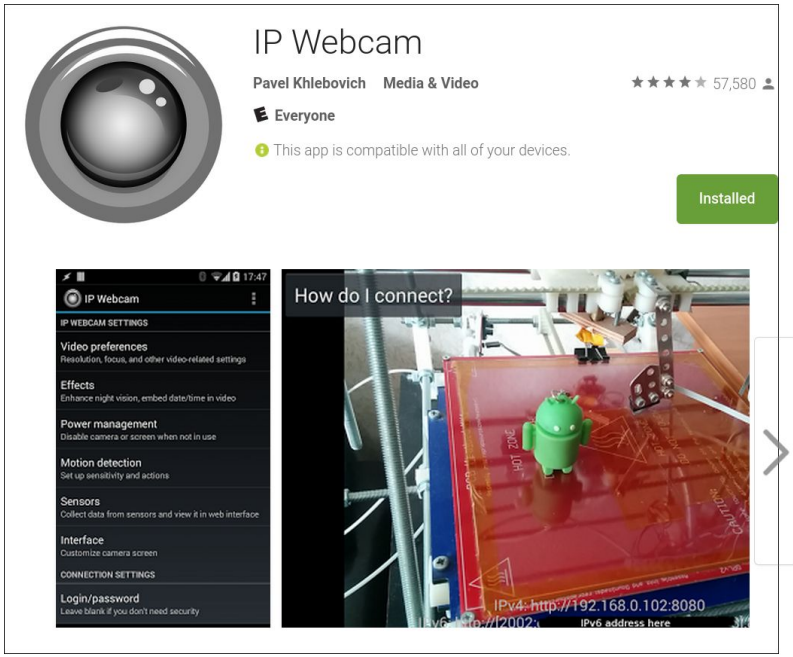


You connect to Your Thing through Tor as an Onion Service
(nobody knows who you are connecting to or what you are seeing except you)

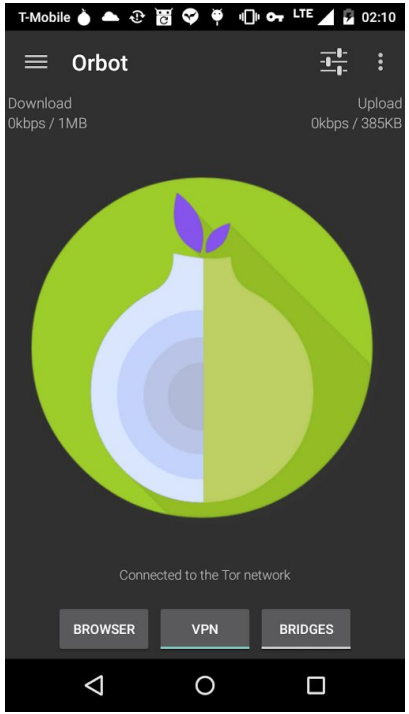


Onion (or “Hidden”) Services can even hide the fact they exist at all, if you don’t know the necessary cookie. With Onion Authentication, you can’t crawl or probe.

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



+



= OnionCam for Android!

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

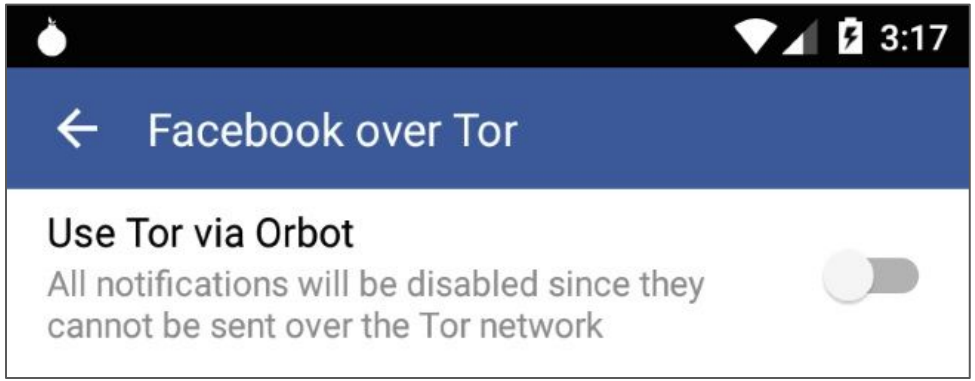
OnionCam: Quick How To

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
    a) Optional: enable VLC to work over Tor and open network stream: http://yourdotonion:8080/video

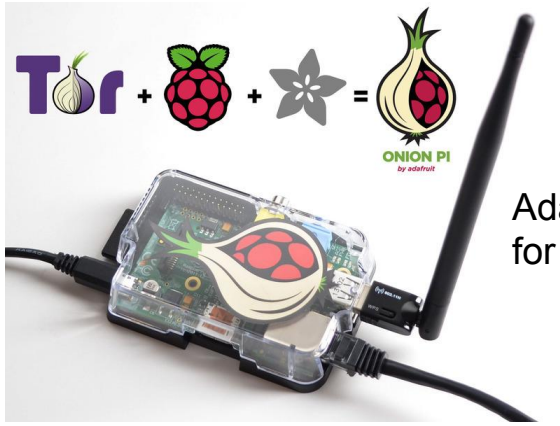
OnionCam in my Kitchen… everything is safe and sound!
Access via Tor Browser at http://<myprivateaddress>.onion:8080
or via VLC RTSP video streaming via rtsp://myprivateaddress.onion:8080/video

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.

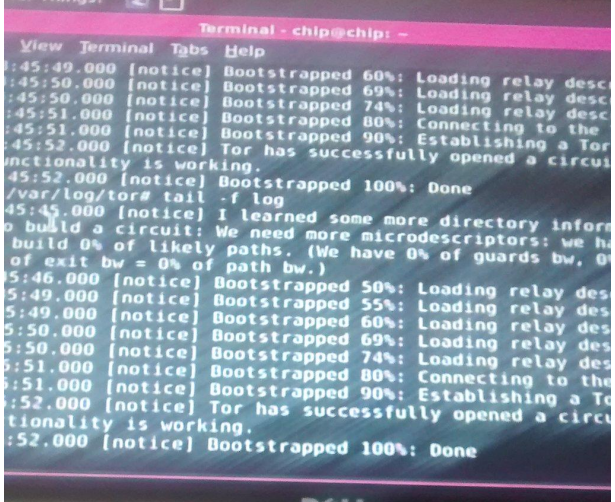
This is what Facebook did to add Tor support into their Android app:



https://guardianproject.info/code/netcipher



AdaFruit OnionPi
for $59



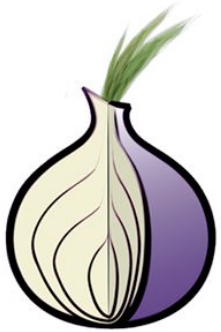
Tor can run on, and be built into, really cheap Things! It just requires some form of Linux and an ARM chip.

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