OWASP

Open Web Application Security Project

Going ~~Dark~~ Grey

How to be pretty anonymous online

Prior art

- @thegrugq
  - OPSEC for freedom fighters
    - this.lightVersion("hands-on")
    - Focus on Gothenburg, Sweden, today
      - on my way here
      - *TIL: never redecorate the house, arrange two OWASP meetups, be presenter on one of them and give another presentation for a customer and start a new assignment on the same week*

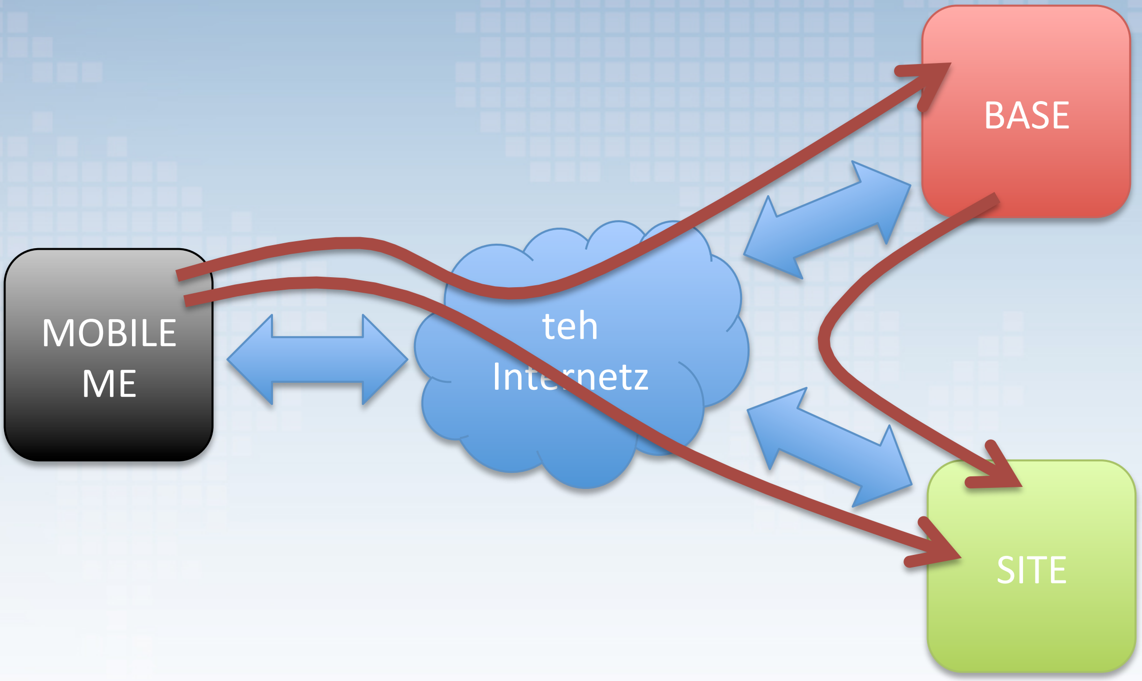
Why?

- The plumbing is boring and hard to get right
  - practice makes perfect
  - you never know when you are going to need it
- 45 yo, father of 2, living in the suburbs, driving a Volvo…
  - not much 1337
- Responsible disclosure
  - currently seams to be responsible only one way

Some of the commandments

- Never operate from your house
- Keep personal life and freedom fighting separated
  - don’t contaminate
- STFU ← FAIL

Architecture



Challenges

- TOR and/or VPN?
- Hardware?
- How to buy stuff?

Tor

- Provides anonymity
- Anonymity protects you
  - Data leaving Tor through exit node is not protected.
  - Correlation of entry and exit?
  - Not foolproof, but pretty ok unless you have nation states as adversaries

VPN

- Provides privacy
- Privacy protects your data
  - Tunnel endpoint IP can be detected
  - VPN provider can have logs
  - Traffic correlation?

Tor and/or VPN

- “TOR -> VPN – OK”
  - Anonymous person within the Tor cloud connects to a VPN-exit on the internet.
    - Or directly to your persistence-platform
    - Looks like HTTPS locally?
- “VPN -> TOR – GOTO JAIL”
  - An IP connected to a person and/or geolocation connects to the Tor cloud. Communications from Tor to Internet/target/platform are monitored.
    - Can you VPN to Tor? Through your own server?
    - Running Tor through a VPN tunnel?

Too much work

Tor and/or VPN

- Prepaid mobile broadband
  - Not from home, not connected to me
  - Can of course be tracked to a location
- VPN
  - An extra step to keep ISP eyes away

Hardware

- Mobile broadband
  - – Prepaid starter kit
- Amazon platform
  - – Probably monitored, but will not leave trace on your..
- Mobile unit
  - – Buy a laptop or use your old one
- Personal Onion Router To Avoid Leo
  - – Fail close and a fun project – Raspberry 2?

Money

- Purchase VPN over TOR with bitcoins
  - Anonymous but, can be traced
    - don’t mix wallets
    - use mixers
- Light
  - Prepaid credit cards
    - Tied to physical location
    - CCTV
    - Purchases are monitored

Case study for lazy and moderately evil ha><><0rz

- Walk into 7Eleven or Pressbyrån
  - – Buy a prepaid credit card
  - – Buy a mobile broadband modem
    - ISP starter pack, from 199:-
    - Kjell&Co 399:-
  - – Use cash and your favorite hoodie
- Use credit card to order a VPN
  - – and create an amazon account
    - Email, cell phone no
- Done

Oh, and you need at least one persona and a couple of hacker nicks as well

OWASP
Open Web Application
Security Project