Expedient Digital Defense



A Primer on Secure Digital Travel

This briefing is UNCLASSIFIED

Who Is This?



Grey Fox (more grey than fox these days)

- Former Air Force (retired)
- Language, Signals, and Digital Network Intelligence Analyst
- Digital forensics and pentesting on the side
- Obsessed with RF and wireless tech
- Long walks on the sidewalk (not a beach guy)

UNCLASSIFIED

What Is This?



- A Primer with foundations
- Threat modeling and biggest threats
- Digital and mobile security best practices

—”if you only had a half hour, what would you recommend for regular people?...”

What This Isn't...



- Comprehensive – just foundations
- An ad for privacy apps
- Meant to scare you – keep your phone and Facebook account, but let's get better at using them

Threat Models



Threat Profile

- Your adversaries
- Their intent
- Capabilities

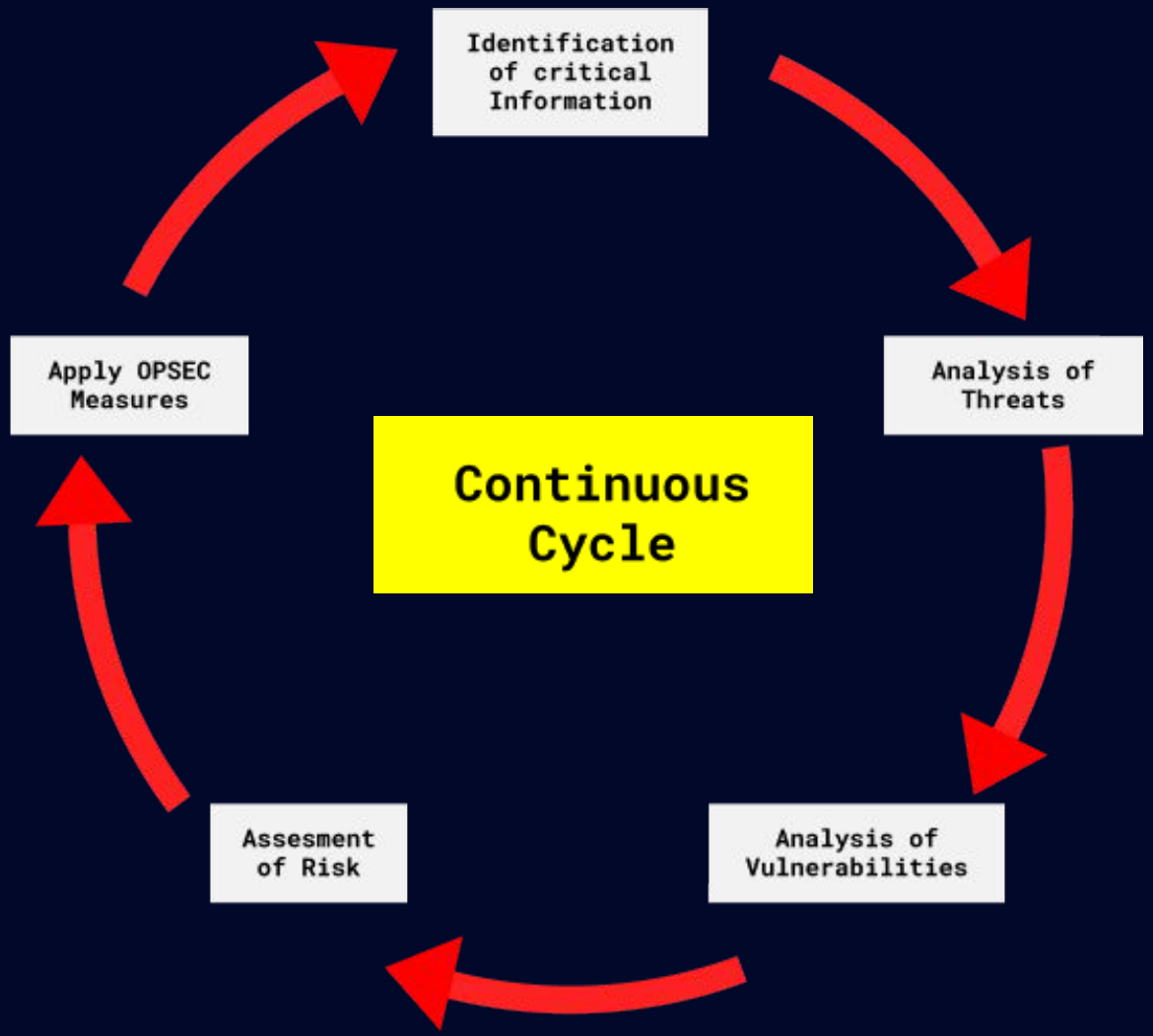
+

Attack Surface

- Devices, apps, services
- Patterns of life, travel
- Patterns of communication

UNCLASSIFIED

Operations Security (OPSEC)



Continuous change

Continuous analysis

Continuous inquisition

"What if I see this in someone's feed tomorrow?"

OPSEC is risk analysis

See from the adversary perspective

UNCLASSIFIED

Attack Surface Management – A Start...



- Multi-factor Authentication (MFA)
- Long, complicated, and unique passwords and/or passphrases
- Everything gets a PIN
- Password managers
- Backups – at least 2 (on site and off site/cloud)

You just defeated ~95% of attacks

Locking Down Social Media



- Photos – what do they reveal?
- Locations – check-ins, tags, posts, friends' activity
  - Post-event posting – don't tell until you've already left
- True names, numbers, and emails – reuse can connect dots
- Profile filler – education, employment, memberships, hobbies…
- Friends/Contacts – social network analysis made easy

Remember: OPSEC is risk analysis

See from the adversary perspective

“OSINT” Yourself



Part of the OPSEC cycle - Open Source Intelligence (OSINT) to detect vulnerabilities and test mitigations:

- Google, Bing (don’t forget images)
- HaveIBeenPwnd: https://haveibeenpwned.com/
- Search.0t.rocks: https://search.0t.rocks/
- Advanced Background Checks: https://www.advancedbackgroundchecks.com/
- Judy Records: https://www.judyrecords.com/
- Many, many people finder sites (Spokeo, Whitepages, Intelius, BeenVerified, Acxiom, Lexis Nexis, TruePeopleSearch)

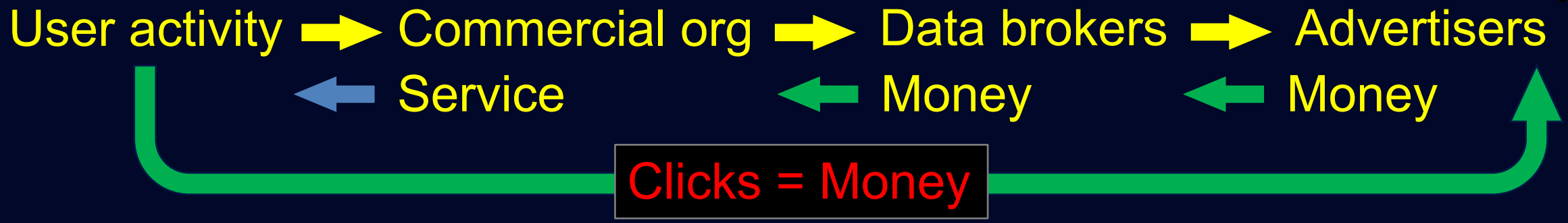
There are many, many more, but these are a start.



- Biggest attack surface
- At least 5 antenna chains
- 3rd party apps
- OS, ISP, Telco
- Location
- Location!
- LOCATION!!!!

https://spectrum.ieee.org/telecom/wireless/building-smartphone-antennas-that-play-nice-together

Apps and Advertising

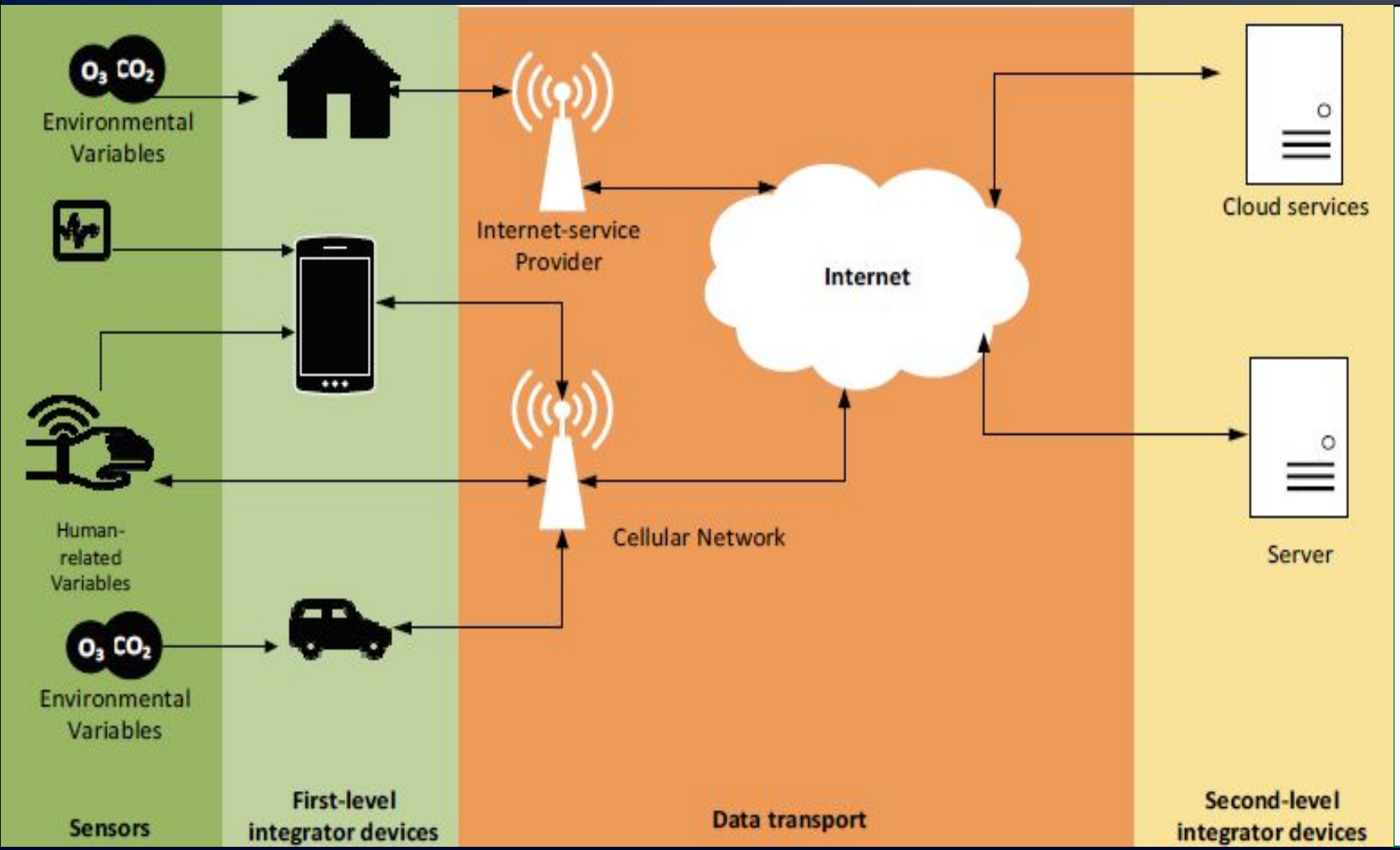


- Users get served ads
- Tailored ads mean more clicks
- Data brokers collect and organise user data for this purpose
- Businesses make huge profits selling user data to brokers
- Brokers make huge profits selling to advertisers

We call this ***Surveillance Capitalism***
Adversaries call this ***A Gold Mine***

UNCLASSIFIED

Ubiquitous Technical Surveillance-"**Smart Cities**"



5 Threat Vectors:

- Online
- Visual/Physical
- Travel
- Electronic
- Financial

First Steps in a Smart City



Online:
- App location discipline
- Encrypted chat/VoIP apps
- Social Media discipline

Visual/physical:
- Face covering
- Gait alteration
  - not necessarily 100% effective

Electronic:
- Wi-Fi, NFC, and Bluetooth discipline

Financial:
- Prepaid cards, cash

Travel:
- Location/GPS discipline
- Avoid vehicle tethering

The main takeaway is awareness

- UTS is very hard to secure or keep anonymised
- Low-tech tactics and device isolation

UNCLASSIFIED

Denying the Spies



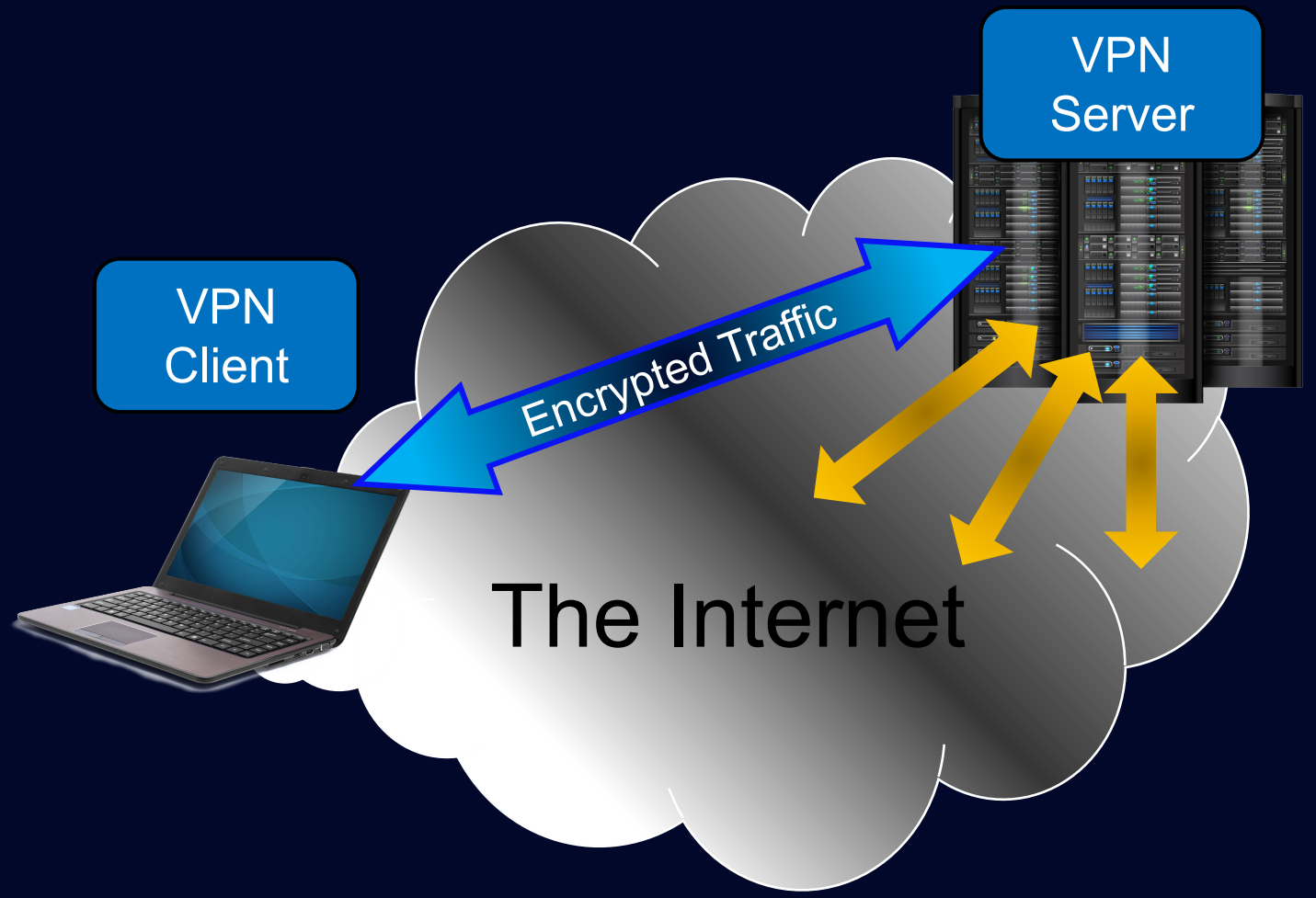
Mobile Device:

- Ad ID: GAID or IDFA can be disabled
- App settings/permissions: control what is accessed and collected
- Disable apps: enable only when needed
- RF Discipline: Wi-Fi, BT, NFC, GPS/Location only when needed

Web Browser:

- Ad blockers: uBlock Origin, Privacy Badger
- Strict cookie settings: **it WILL break websites, but not as many as you think
- DNS over HTTPS: anything but Google

Virtual Private Networks (VPN)



Airports and Checkpoints - Basics



Risks: device loss, theft, seizure/confiscation, infection

Basics:

- Avoid biometric device access
- Log out and/or enable app-specific pins/passwords
- Power off at security checkpoints
- No airport Wi-Fi - use mobile data
- Keep it on you, not in a bag

Extreme:

- Fully remove apps that reveal sensitive details
- Remote work and virtual machines - “shell devices”
- Avoid “dummy phones”

Putting It All Together



- Physical Security -
  - No location/signals = no pattern of travel
  - Locked and off for you = locked and off for them
- Online Security -
  - Sanitized SocMed = no intelligence dossier
  - Hardened browser = much less tracking potential
- Communications Security -
  - Less apps/app access = less data breach value
  - Encryption/secure comms = less content value, more location security

UNCLASSIFIED

Questions? - greyfox@wcassembly.com

Further Learning:

Books to start:

- Parker, Carey. **Firewalls Don't Stop Dragons:** A Step-by-Step Guide to Computer Security and Privacy for Non-Techies
- Hypponen, Mikko. **If It's Smart, It's Vulnerable**
- Bazzell, Michael. **Extreme Privacy:** What It Takes to Disappear
- Tau, Byron. **Means of Control**: How the Hidden Alliance of Tech & Government Is Creating a New Surveillance State

Websites:

- Privacy4cars: https://privacy4cars.com/
- The New Oil: https://thenewoil.org/
- Privacy Guides: https://www.privacyguides.org/
- Techlore: https://techlore.tech/
- Naomi Brockwell on VPNs: https://www.youtube.com/watch?v=8MHBMdTBlok

UNCLASSIFIED