OpSec for All

Dr Rob Hegarty

Overview

- OpSec – Operational Security
- Security and Privacy
- Privacy – Arguments For and Against
- Threats to Security & Privacy
- Strava Case Study
- Improving Your OpSec
- IoT Security Research – Data footprints everywhere!

OpSec for All

- Operation Security – Originally a military concept
- Goal – Deny an adversary access to information that would compromise the security of a mission

- Who are your adversaries?
  - Hold that thought!

Security

- Use of controls (Technical, Policy, Education) to preserve :

- Confidentiality
- Integrity
- Availability

Privacy

- “Right to private; Thought, Communication, etc”
- “Freedom from unwanted intrusion”
- “Being free from public attention”

- “Right to have control over how information is; Gathered, Stored, Processed, Used”

Privacy & Perspective

- Nothing to hide argument – Often used by proponents of state / government surveillance.

- “Nothing to hide, you have nothing to fear” – Joseph Goebbels (Nazi Party)

- "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place” – Eric Schmidt (Google CEO)

Privacy & Perspective

- Wanting privacy is not equal to having something to hide.
- If we have nothing to hide, why are we under surveillance?
- “Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.” – Edward Snowdon
- Human Rights Act – Respect for private life and correspondence
  - Emails, letters, telephone calls
- “Nothing to hide” Encourages **complete trust in the state** / judiciary, Provides false reassurance – Open Rights Group

Potential Adversaries

- Consider the following pieces of information, and your likely adversaries:
- Full name
- Location
- NI Number
- Date of Birth
- Social Media Posts
- Bank Sort Code and Account Number
- Credit Card and Card Verification Code

Threats to Privacy

- Data leaks – Businesses, Governments, etc
- Online Social Networks
- Smart Phones, Tracking, Malware
- Wearables
- CCTV
- IoT Devices

Case Study – Fitness Tracking

- **The Fitness Tracking Model**
- Wearable devices gather GPS tracks of users.
- Services aggregate, process, visualise and share fitness data (Inc GPS Tracks)
- Users compete with each other via these fitnes social networks.
- https://tinyurl.com/yas6b6qx

Case Study Fitness Tracking

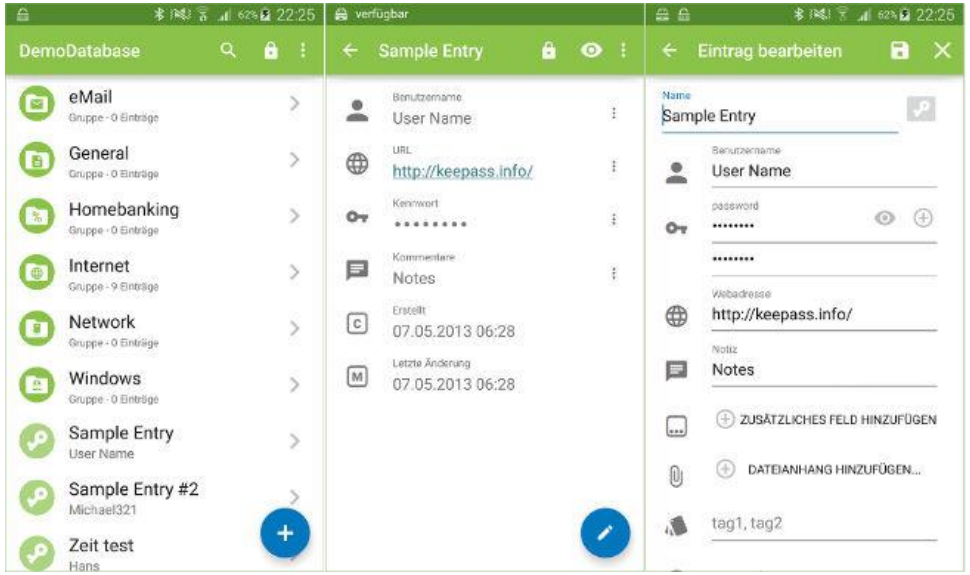
- OpSec of military personal is degraded.
- Who is to blame?
- What are possible solutions?

Other Fitness Tracker Case Studies

- Bike Theft - https://tinyurl.com/yb9vhhq8
- Private night time activity- https://tinyurl.com/y9rt9tjt
- Less scandalous:
  - Your potential employer may view your activity logs
  - You may value your right to privacy!

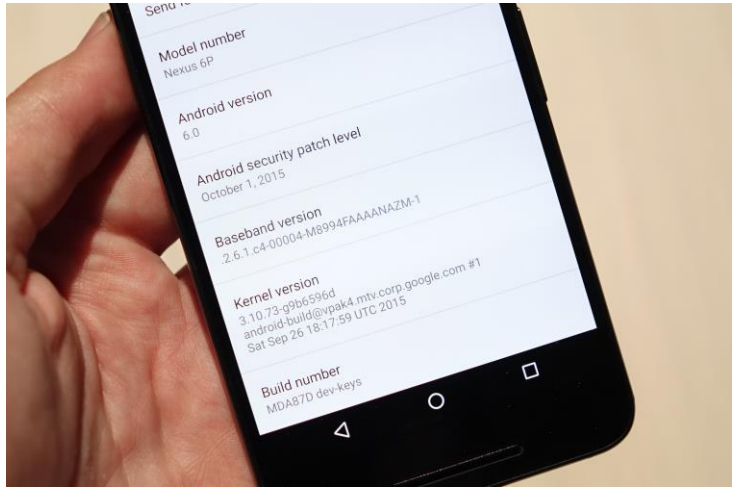
Improving Your OpSec - Authentication

- Enable 2FA
- Use a decentralised password manager (e.g. KeePass).
- Check Website and App recovery mechanism (Server Side Password Storage)



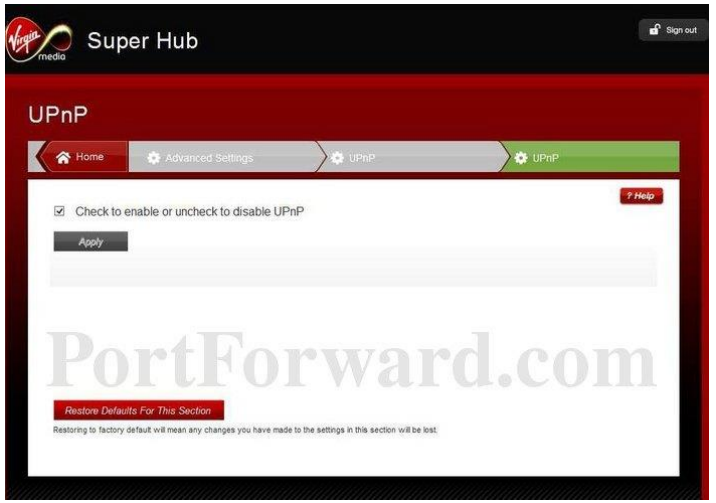
Improving Your OpSec – Devices

- Don’t:
  - Delay OS updates.
  - Use your computer with admin rights
  - Install apps from untrusted sources
- Consider mobile OS update frequency when purchasing your next smart phone.
- Setup and use a VPN for web browsing over public Wi-Fi hotspots (tip use TCP over 443)
- Remember to turn on Full Volume Encryption (Have a backup solution in place)



Improving Your OpSec – IoT & Cloud

- Treat IoT devices as if they are Internet Reachable
- Consider the implications of your home network being compromised
- Turn off UPNP if you have untrusted devices on your network.
- Review the privacy setting of apps and services.
- Remember if you aren't paying for a service, you are the product!
- Consider the privacy convenience trade off of new devices (Alexa, Google Home, etc)



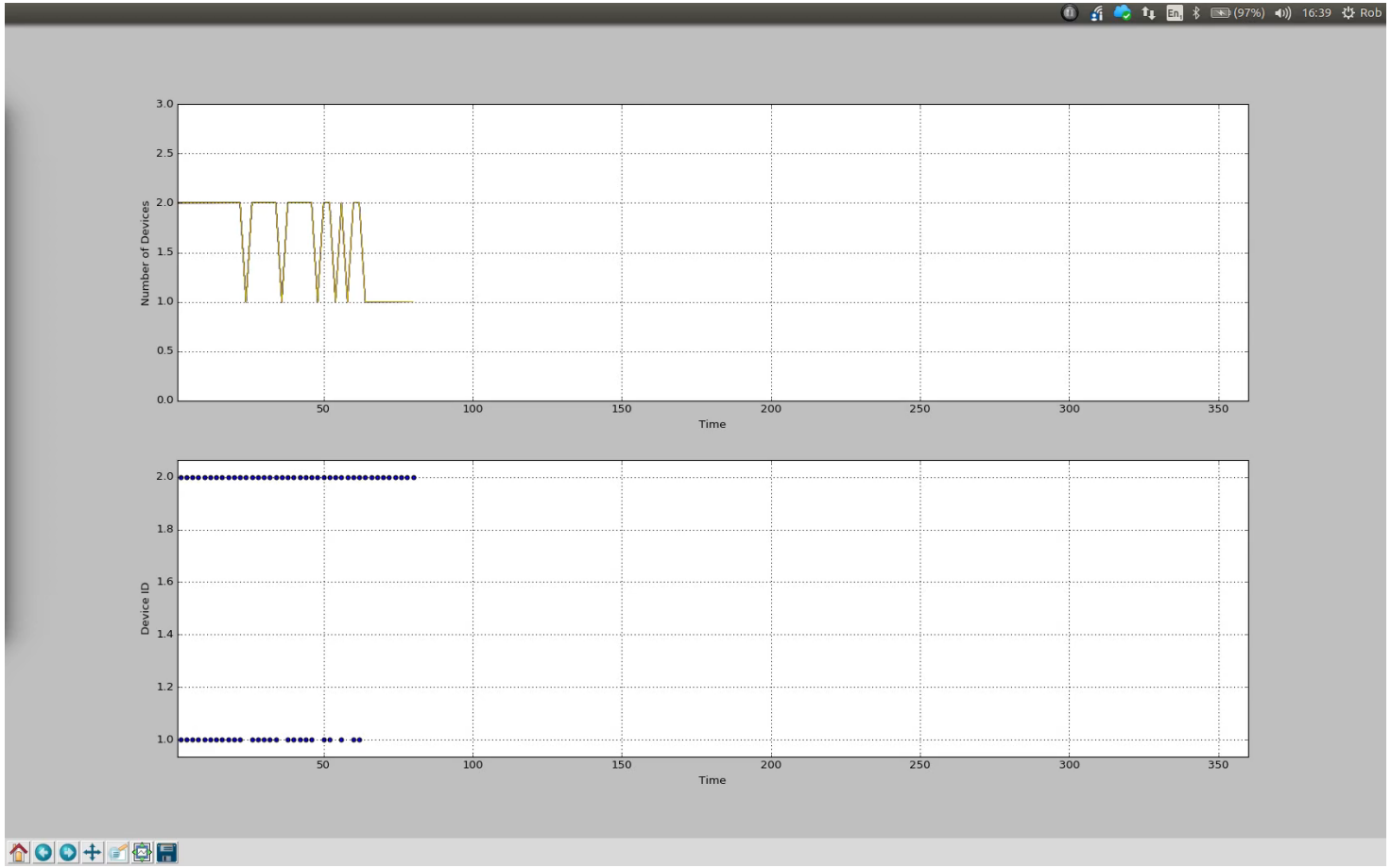
Improving Your OpSec – General Practice

- Consider what data your browser is giving away.
- Log off and turn off machines.
- Remember the (Legally Challenged) Investigatory Powers Act required ISPs log every website your visit/
- https://tinyurl.com/ya2lnhth

IoT Research

- Bluetooth vs Bluetooth Low Energy
- Prevalence of devices
- Advertising packets
- Poor anonymity implementations on wearables
- Data aggregation across public locations
- Hidden data

IoT Video


(97%) 16:39 Rob
Number of Devices
3.0
2.5
2.0
1.5
1.0
0.5
0.0
50
100
150
200
250
300
350
Time
Device ID
2.0
1.8
1.6
1.4
1.2
1.0
50
100
150
200
250
300
350
Time

BLE Apps

- Android RaMBLE - https://tinyurl.com/yb6cnz2f
- Android Eddystone - https://tinyurl.com/ybjvwt2r
- IOS LightBlue - https://tinyurl.com/yccvlnd7

Summary

- OpSec is everyone's responsibility
- Technology enhances our existence however, if you value your privacy, review your security practice, consider the benefits and drawbacks of emerging technology
- Shape our future
- Be privacy aware
- Express your views on privacy, discuss, debate, vote

Questions, Observations, Thoughts?