UNIVERSITY OF Southampton

# Pervasive Monitoring: From Bad to Worse


By Dr. Nawfal Fadhel


Academic Centre of Excellence

# Question

What is pervasive Monitoring?

# Pervasive Monitoring

From RFC7258/BCP188:

"*Pervasive Monitoring is an Attack*"

Pervasive Monitoring (PM) is widespread (and often covert) surveillance through intrusive gathering of protocol artefacts, including application content, or protocol meta-data such as headers.

# Pervasive Monitoring

*"its political violence"*

"Remember, remember, the Fifth of November
Gunpowder treason and plot
I see no reason why gunpowder treason
Should ever be forgot"

*"driven by beliefs"*

"A penny loaf to feed the Pope
A farthing o' cheese to choke him
A pint of beer to rinse it down
A faggot of sticks to burn him
Burn him in a tub of tar
Burn him like a blazing star
Burn his body from his head
Then we'll say ol' Pope is dead.
Hip hip hoorah!"

# Recipe for Pervasive Monitoring

*1 tea spoon of terrorism*

*2 tables spoon of fear mongering*

*½ tea spoon trespass on civil liberties*

*3 or 4 politicians*

*2 pounds of the press*

*And*

*Sprinkle a small dash of public apprroval*

# Question

Is Pervasive Monitoring a Man in the Middle attack?

# Motivation for Pervasive Monitoring

- The scale arguably makes this an example of a new pervasive monitoring threat model that is neither purely passive nor a classic Man-in-the-Middle and that we have not normally considered in protocol design, implementation or deployment
- A purely technical response will not "solve the problem" but we should treat an attack as we usually do and try mitigate it

# Example: Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ

Britain's surveillance agency GCHQ, with aid from the US National Security Agency, intercepted and stored the webcam images of millions of internet users not suspected of wrongdoing

GCHQ files dating between 2008 and 2010 explicitly state that a surveillance program codenamed Optic Nerve collected still images of Yahoo webcam chats in bulk and saved them to agency databases, regardless of whether individual users were an intelligence target or not.

# Example: GCHQ faces new Belgacom hack allegations

New leaks from NSA whistle-blower Edward Snowden reveal that the alleged GCHQ cyber-attack on Belgacom used Regin malware and was undiscovered for two years before it was detected. Plus, there are now concerns that the clean-up operation was not successful.

In September 2013, Snowden revealed that Belgacom, the largest telecommunications company in Belgium, had been hit by an advanced persistent threat (APT) attack which - he says - was the work of the UK's GCHQ (Government Communications Headquarters) intelligence agency.

# Example: State Funded Firmware Hack “Sonic Screwdriver & LoJax”

WikiLeaks’ Vault 7 files showed that the CIA apparently developed an implant for Apple's computers that used the Extensible Firmware Interface (the predecessor of UEFI) but required physical access to the targeted computer and a malicious Thunderbolt Ethernet adapter (called the “Sonic Screwdriver”).

LoJax is an entirely different animal—it was built to be deployed remotely, using malware tools that can read and overwrite parts of the UEFI firmware’s flash memory.

# Pervasive Monitoring

- Pervasive Monitoring is not every type of attack although they could be use as part of the attack.
- Pervasive Monitoring is far from the only security or privacy issue on which we need to work such as Spam, malware, DDoS, ...
- But mitigations for Pervasive Monitoring can also help a lot with other problems.

# Hypothesis

If we work to address Pervasive Monitoring , and prioritise services and mechanisms that mitigate PM and that are also effective against other attacks then we will be doing the “right thing”

# Active VS. Passive Pervasive Monitoring

From RFC7258/BCP188:

"*Pervasive Monitoring is an Attack*"

Active or passive wiretaps and traffic analysis, (e.g., correlation, timing or measuring packet sizes), or subverting the cryptographic keys used to secure protocols can also be used as part of pervasive monitoring.

Pervasive monitoring is distinguished by being indiscriminate and very large-scale, rather than by introducing new types of technical compromise.

# Motivation for Pervasive Monitoring

- The '5-Eyes': The US, the UK, Canada, New Zealand and Australia
- The '9-Eyes': The '5-Eyes' group plus Denmark, Norway, the Netherlands and France
- The '14-Eyes': The two above groups plus Germany, Sweden, Belgium, Spain, and Italy
- The intelligence shared
  - Signals intelligence (SIGINT) and often involves
  - Defence intelligence (DEFINT)
  - Human intelligence (HUMINT)
  - Geospatial intelligence (GEOINT)
- These actions are not unique

# Pervasive Monitoring Vs Targeted Monitoring

- Most people are against pervasive monitoring, but all right with targeted surveillance (e.g. under warrant wiretap),
  often called ”lawful interception”.
- Lawful interception can be, and have been, used for pervasive monitoring.

# Pervasive Monitoring Vs Pervasive Advertising

- Data driven advertising is opposite to privacy and will always be, its worse as it coerce even the educated users.
- Data driven advertising will collect more data than government agencies.
- Government agencies can convince or coerce companies into collaborating.
- Google's core business is around advertising so how can we convince internet business not to use ad-trackers?
- How to balance toxicity of data vs. data-mining benefits?

# Pervasive Monitoring and data mining

The problem that we face today is not data, or how to acquire it. The Problem is what it means.

The Facebook–**Cambridge Analytica** data scandal was a major political scandal in early 2018 when it was revealed that **Cambridge Analytica** had harvested the personal data of millions of peoples' Facebook profiles without their consent and used it for political advertising purposes.

# Pervasive Monitoring Scope

- Pervasive monitoring targets a everyone and at a massive scale.
- If there is more than one way to do pervasive monitor. They will try all of them.
- Data is collected even offensively.

# Pervasive Monitoring Defense

- RFC 7258/BCP 188 states that all IETF work will consider pervasive monitoring as an attack for all protocol development to be mitigated as part of our normal design processes.
- RFC 7258/BCP 188 states that the IETF will work on introducing new protocols and revising existing ones to mitigate pervasive monitoring by design. (e.g : Certificate Transparency).
- RFC 7435 defines "Opportunistic Security" to do security by default which may lead to some harsh practices on the users.
- IAB: Recommends to
  - Design for confidentially by default (Encrypt everything).
  - Creating a pervasive monitoring threat model document (Draft).
- DNS Privacy: The (DNSSEC), contrary to what its name might imply, does not encrypt the payload of the DNS query or response, but rather, provides a method of validating the authenticity of the information.

- RFC: Request For Comment
- BCP: Best Current Practices
- IAB: Internet Architecture Board
- IETF: Internet Engineering Task Force
- DNSSEC: Domain Name System Security Extensions

# Pervasive Monitoring Defense - Continued

Non technical solutions are:

I. User education.
II. Free and open-source software.
III. Legislation. (e.g GDPR)
IV. Cleverer cryptography. (e.g Transparent Certificates)

# Why Pervasive Monitoring will never go away

- Government or cooperate espionage is not going a way.
- Privacy invasive commerce (legitimate and not) is very lucrative.
- Lack of legal accountability mechanisms (courts of various kinds)
- Its not well understood so it keeps getting worse which leads to badly-informed decision makers.
- Slow Government regulation of business (e.g. Data Protection Agencies)
- Slow Commercial reaction to user privacy requirements
- Low attention to NGOs working to enhance privacy.
- Technical privacy enhancing/enforcement mechanisms are still in their infancy.

# Pervasive Monitoring Consequences

- Tighter export control on information.
  - News blackout on revolution
- Censorship
  - Arrests and assignations of activists
- More power to authoritarian regimes.
  - Corruption and wasted public funds
- Network Neutrality
  - Block VOIP application like Whatsup and Viber. Sometimes internet altogether.
- Hate Speech
  - There are plenty of that going around

The Question remains

# Summary

- IETF has consensus pervasive monitoring is an attack (RFC7258) and is working that problem, as are others.
- We all should consider how we can work to make pervasive monitoring harder, since those doing it will not just stop.
- When/if societies do decide that pervasive monitoring is as bad as it is, then the technical community should have in place the tools to effect that decision.

# References


- https://arstechnica.com/information-technology/2018/10/first-uefi-malware-discovered-in-wild-is-laptop-security-software-hijacked-by-russians/
- https://tools.ietf.org/id/draft-barnes-pervasive-problem-00.html
- https://tools.ietf.org/html/rfc6962
- https://tools.ietf.org/html/bcp188
- https://tools.ietf.org/html/rfc7435
- http://cphpost.dk/news/international/denmark-is-one-of-the-nsas-9-eyes.html
- https://www.bbc.co.uk/news/technology-25085592
- https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo