Incentives for and Against Pervasive Monitoring Threats

Sheema Zia
Jamia Hamdard
Jamia Hamdard University
New Delhi-62

Afshar Alam
Jamia Hamdard
Jamia Hamdard University
New Delhi-62

ABSTRACT
Pervasive is defined as 'spreading widely throughout an area or a group of people (Especially of an unwelcome influence or effect'. Pervasive monitoring is simply a case of continuous monitoring of people for the sake of checking conduct or watching over. After the recent Snowdonia occurrence, where Edward Snowden leaked classified information about the ongoing surveillance programs by the NSA of United States, pervasive monitoring became a hot topic of discussion and if it was beneficial for the users or internet or posed as a threat. The objective of the paper is to analyze whether pervasive monitoring is a threat or a necessity and also to compare the benefits and challenges of pervasive monitoring. The comparison between the importance of pervasive monitoring and that of its ill-effect argue that it helps in combating terrorism as it is unbiased and non-targeted. Moreover, it does not collect the meta-data but, only collects it. Besides its importance, it is also essential for network administrators to have plaintext for managing their networks. On the other hand, the STRINT workshop by IETF called it a technical attack same as any attack as it leads to some chilling effects like self censorship etc. If pervasive monitoring is being done by an organisation, it can lead to the database holder or admin to exercise undue influence on the employees of the organisation undergoing the monitoring. Even though it is against the basic human right to privacy but the public does not seem to care too much about it. The pervasive nature of this monitoring might help the governments but also has adverse affect. The beneficial and destructive effects of pervasive monitoring are tabulated according to different fields pervasive monitoring is done for. This includes the fields of organisation, future, software, law, networking and healthcare. Considering all the researched and analyzed fields, it can be stated that pervasive monitoring should be allowed at some levels as it becomes a necessity and also have some standards and protocols so as not to be misused for personal issues or motives. The standards and policies should be defined for all internet traffic without any bias whatsoever.

General Terms
Security, Pervasive Monitoring, Surveillance, Snowdonia

Keywords
Pervasive, monitoring, threat, necessity, comparison

1. INTRODUCTION
The economics of information security has become a very flourishing and enthralling subject matter. This new field of study not only touches the broader topics of security but also, focuses on the general security questions as what can be considered privacy and how to maintain it.

The common myth surrounding internet is that you are anonymous while using it and nobody will know your identity. In reality though, privacy has become a myth in today times. It would be considered foolish to even expect complete privacy of an individual while using internet. Numerous puzzles have been posed by the steady but gradual erosion of privacy. 'Why is it occurring, and why do people care about it?'

Privacy has to be maintained at all levels and all humans should have the right to it. Keeping this thought in mind, the ongoing scenario of continuous watching-over by certain organisations or government in the name of pervasive monitoring can be thought of as a threat.

The oxford dictionary describes pervasive as 'spreading widely throughout an area or a group of people (Especially of an unwelcome influence or physical effect)'.Therefore, pervasive monitoring is like an unwelcome influence of surveillance on everybody. Pervasive Monitoring is simply a case of non-targeted attempt to catch all traffic or users, which is perpetrated by an organization on government or any other organization.

The year 2013 had brought a series of revelations that have focused the entire Internet community on the topics of privacy and pervasive monitoring. Although some of the vulnerabilities were known and some of the potential was alleged, the depth and scale shocked all.

In June 2013, a computer professional, former CIA agent, copied and leaked classified information from NSA of United States without any authorization. The documents released to the press by Edward Snowden have revealed several operations undertaken by intelligence agencies to exploit Internet communications for intelligence purposes. His disclosures revealed numerous global surveillance programs, many run by the NSA and the Five Eyes Intelligence Alliance with the cooperation of telecommunication companies and European governments. The attacks were striking in their pervasive nature, both in terms of the amount of Internet communications targeted, and in terms of the diversity of attack techniques employed. This 'Snowdonia' re-energized the technical communities to do better on security and privacy in general.

The motivation of this paper has been to understand PM as a threat so that it can evaluate novel solutions for strengthening security and privacy. This is a review paper which focuses on comparing the incentives of pervasive monitoring to analyze whether pervasive monitoring is a threat or a necessity and to assess the benefits and challenges of pervasive monitoring. A table has been maintained to compare and analyze the pros and cons of PM.

2. LITERATURE REVIEW
Specific literary work has been researched upon to examine and consolidate the work by scholars, technical communities and research scientists. The literature reviewed has been split up in two portions as declaring pervasive monitoring a threat or a necessity.

2.1 Pervasive monitoring as a threat

In 2014, a STRINT workshop was held which was attended by 93 experts across the globe. The focus of their meeting was the ongoing issue of pervasive monitoring, its global impact and the reaction about it. The workshop was jointly sponsored by IAB and W3C. They came to a consensus that terminology about pervasive monitoring should be made generic and a threat model depicting pervasive monitoring as a threat should be developed.[1]

In a technical assessment of PM, by IETF community, it was declared to be an attack on the privacy of internet users and organisations. Authors were encouraged to give ways to mitigate these attacks through protocols which would increase the work force of the attack or make it infeasible. It also rejected the notion of PM not being harmful as it is non targeted by concluding that the attackers are indistinguishable in their motives [2].

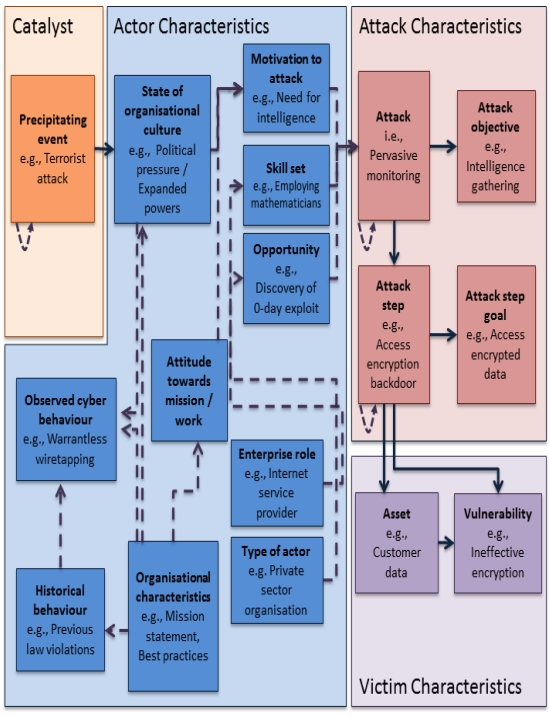
Jari Arrko in a discussion with Netnod magazine emphasized that pervasive monitoring should be considered a threat to the internet and technology should be improved to counter these dangers. [3]

Tim Bray [4] rejects the objections against IETF considering PM as a threat, by giving his own takes on why they can be invalidated. Also M3AAWG's work against Pervasive Monitoring has been formulated [5] for internet privacy.

In her paper, Dana Polatin-Reuben proposes pervasive monitoring to be an insider threat and also examines and adapts PM case studies according to insider threat model by Nurse et al.

Furthermore, PM has been depicted as an insider threat adapting it to Nurse et al. model [6]

Table2.2.1 Adapted insider threat model depicting Pervasive Monitoring as an attack



2.2 Pervasive monitoring as a necessity

However, in a paper by Stephen Farrell from December 2015 [7], he states some differences between traditional attacks and pervasive monitoring by the focal point being the '*modus operandi*' of the attacker. In his paper, he differentiates by saying that PM has no specific targets, other than to collect everything possible.

Two puzzles regarding PM were queried in 2003 [8]:

The first privacy puzzle he posed was that even though the public shows severe concerns about the privacy and security, it is not doing much to avoid it. It can be safely assumed that the public does not care about it. The second puzzle we come across in his paper is, that even though all these concerns about privacy are voiced, the government and organizations are only working towards eroding it and for valid reasons like combating terrorism; tax evasion etc. Even employees are monitored by organizations as a fundamental right.

In accordance with favouring PM, it was concluded that effective employee background checks and vetting are essential. It is further stated that insiders will always be a part of the organisation and a balance should be maintained between privileges and level of control and audit. Even though monitoring staff activity might lead to clash of security controls and human factors, 'employers do have the right to monitor employee activity' [9]. Even though employees in a workplace have the legitimate expectation of privacy, but they consent to monitoring implicitly for the sake of employment relationship.[10]

Cappelli et al.'s definition of insider threats (from comprehensive guide to insider threats) is extensively used to justify pervasive monitoring to be covered in this definition:

'*A malicious insider threat is a current employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems*'. [11]

But this definition implies only for a person enacting harm upon an organization, so it would be inapplicable to consider PM as a threat.

Adding to it PM is described as blanket surveillance and argued with some common reasons for PM necessity as PM helps combating crime and hence saves lives, it also protects against viruses and hackers and also against information leaks [12]. It is suggested that more proactive approach to cyber security should be taken and traditional approaches though increasingly important to maintain, will not be sufficient enough. In favour of PM, it states that cyber threat intelligence should be prioritized and the information gleaned from it allows organisations to identify attackers through log analysis. [13]

Politics has also been cited as a legitimate reason for government to monitor and control communication as threats against national security and intelligence can be accepted as valid concerns. [14]

For the IETF workshop two papers (even though not finished in time) are worth being mentioned: one, by Jari Arrko, "Privacy and Networking Functions" [15]; and another by Johan Pouwelse, "The Shadow Internet: liberation from Surveillance, Censorship and Servers" [Pouwelse] [16].

3. PROPOSED SOLUTION

There are various mechanisms which can be set up in order to address the concerns about pervasive monitoring being considered a threat or attack:

3.1 Encryption

The best technical advice is to be given to service providers to harden their cryptography posture for best configuring crypto-enabled web servers, mail servers etc. Better crypto handbook is available at https://bettercrypto.org/static/applied-crypto-hardening.pdf [5]

Also encryption has been a focus for IETF for countering pervasive monitoring. The newly coined term 'opportunistic encryption' is being frequently used to address new techniques of encryption and even though it is not to be projected as a substitute for authenticated, integrity-protected encryption,[17] but still benefits the applications not having the mandated explicit security mechanisms [18].

It is simply a case of session encryption without a pre arrangement, only having authenticated knowledge about the other party. It is also called anonymous encryption, without breaking the existing systems provides an upgraded path. An example of opportunistic security would be, using TLS with self-signed certificates in the context of browser as well as non-browser. Other tools include IPSec, DNSSec, etc. Crypto-based authentication makes it easier to detect MITM attacks and also assists in the human perceptible delays in session/connection establishment.

3.2 Tools Improvisation

Tools for the operating systems which would protect against a passive eavesdropper and would also allow end point authentication against an active attacker, would enhance the opportunistic security paradigm.

Terminologies regarding connection failures in encrypting, like silent fail, should be improved upon. Experts should be involved in UI and encryption and distinctions should be made between UI, user understanding, and user experience.

Other ways for tools improvisation include: The proposal to introduce TOFU in http headers [19] or WebRTC for peer-to-peer communication and making user aware of XMPP which has authentication, encryption and OTR [20].

3.3 Data Minimization

The metadata in some cases relating to the communication might also be confidential. By distinguishing between explicit and implicit metadata and hiding much of it by passing it through several servers might serve the purpose of maintaining the confidentiality, but would make the communication slow and increasing the traffic (e.g. Tor). 'Aggregation', 'Contraflow' and 'Multipath' are three kinds of measures [21] which increase the cost for the attacker while protecting the metadata. Minimizing the data by making the applications pass less data reduces the redundant metadata. E.g. Anonymous temporary handles in place of permanent identifiers.

3.4 Deployment

MITM attacks might go unnoticed for middle boxes like captive portals, so assistance to a connecting device about login page by applying an extension to DHCP can be provided. Some practical problems with deployment of protocols should be addressed such as captive portals being old and not have been updated [22].

Deployment of secure solutions can be made cheaper and quicker for System administrators and more Ipv6 deployments in mobile networks should be encouraged. [23].

3.5 Better Implementations

Improving the certificate system to achieve certificate transparency (CT), improving the awareness regarding risks, and taking influential decisions which are in compliance to human rights of privacy.

Other solutions to tackle the threat of pervasive monitoring would involve, working collaboratively with the internet technical community towards making the internet communications more private and secure [22].

4. RESULTS AND DISCUSSION

A table has been formulated to condense the two sides of the discussion about Pervasive Monitoring being bane or boon. This table consists of the various reasons why PM can be considered good or bad, hence determining incentives for and against Pervasive Monitoring Threat. The table includes different fields of study including organizations, future, software, law, business, networking and healthcare. The table is as follows:

Incentives in favour of Pervasive Monitoring include the facts that public is indifferent to it since it is unbiased and not specifically targeted. Moreover, in some scenarios it becomes essential to monitor traffic e.g. Network administration for billing, detecting outages, identifying intrusions, spam etc., parents/schools for monitoring minor internet activity, organizations for monitoring employee internet activity, lawful interception for criminal investigation, software for protection against information leaks and malware and healthcare for interoperability and autonomous systems. The internet of Things is one of the technologies for the future which use pervasive monitoring.

On the other hand, incentives against Pervasive monitoring include the fact that it can be highly misused by Database holders or lead to self censorship. It can also increase the number of zero day attacks as holes in software of any company or organisation can be easily known and used as per convenience. Some employees might get uncomfortable with the continuous scrutiny and some citizens of a government might feel violated with the surveillance, hindering their privacy.

Table 4.1 Incentives for and against Pervasive Monitoring Threats

Reasons	Incentives for	Incentives against
Organizations	Helps in detection of insider threats	Might make employees uncomfortable
Future-related	It can give rise to new technologies like Internet of Things	Leads to chilling things like Self-Censorship
Lawful Interception	Helps combat terrorism	Leads to violation of human right to privacy
Software	Protects against viruses, hackers and information leaks	Leads to pumping of zero-day attacks, drives-up cost of deploying, managing and using privacy technology

Network Administrators	Essential for billing, detecting outages etc.	The DB holder can exercise undue advantages
Healthcare	Removes location, time and other restraints	Cost issues, security and privacy issues

5. LIMITATIONS AND FUTURE SCOPE

The preceding section posed some arguments and based on them we can propose that even though the stance taken by IETF by declaring PM as a threat is in the right direction, but it cannot be said for sure that the steps taken to prevent it might be effective. For example, in an instance if IETF develops a new standard to make IP's more secure against pervasive monitoring, the cyber security agencies (e.g. NSA) might pressurize the governments to simply outlaw it.

Since time immemorial, the police have been using the old trick as pretext to capture 'people of interest' by following them in a car until they inevitably commit a traffic infringement. Continual surveillance might be seen in the same light as it serves the same purpose.

For criminal Law Enforcement, some limitations are as follows:

1. Only a proportion of offences are significant
2. Only 30 days are allocated for intercept orders
3. Specific targets for surveillance have to be identified

The scope of this article includes the possibility of adapting other threat models to pervasive monitoring or design a new model for it. Also, a new model can be designed for making clear distinctions based on motives (modus operandi) of pervasive monitoring and characterizing them as a threat or a necessity.

6. CONCLUSIONS

The incentives for and against pervasive monitoring threats were analyzed and the benefits and challenges of doing it were determined. It can also be seen that Pervasive monitoring in some scenarios is necessary while being a threat in other situations. It is vital to distinguish between pervasive monitoring as a crime, and pervasive monitoring as a requisite. A model can also be designed in the future for categorizing PM according to motives and enforcing criminal law according to it. Moreover appropriate action should be taken to protect users by M3AAWG members

7. ACKNOWLEDGMENTS

I am sincerely grateful to the support and guidance of my mentor Mr. Afshar Alam, and my friends and family.

8. REFERENCES

[1] Stephen Farrell "Report from the Strengthening the Internet (STRINT) Workshop", rfc7687, December 2015

[2] S. Farrell, IETF, BCP188, May 2014, https://tools.ietf.org/html/rfc7258

[3] Discussion with Jari Arrko: IETF and Pervasive monitoring, Netnod News Magazine, spring 2014

[4] Tim Bray, amazon employee, http://www.tbray.org/ongoing/When/201x/2014/05/13/Pervasive-Monitoring-is-an-Attack

[5] Joe St Sauver, PhD, Scientist, Farsight Security,Inc. Senior Technical Advisor, M^{3}AAWG, SECURECOMM, Dallas TX; "What must we do? Industry reactions to Pervasive Monitoring Programs

[6] Dana Polatin-Reuben "Pervasive Monitoring as an Insider Threat An Adapted Model"

[7] Karen O'Donoghue, STRINT workshop focuses on pervasive monitoring, IETF Journal July 2014

[8] Andrew Odlyzko, Privacy, Economics, and Price Discrimination on the Internet, Revised version, July 27, 2003

[9] Carl Colwill, "Human factors in information security: The insider threat Who can you trust these days" information security technical report 14 (2 0 0 9) 1 8 6 e1 9

[10] Judith Symonds, Ubiquitous and Pervasive Computing: Concepts, Methodologies, Tools and Applications, Auckland University of Technology, New Zealand

[11] Cappelli, D., Moore, A., and Trzeciak, R., 2012. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).* Upper Saddle River, NJ: Pearson Education, Inc.

[12] Dave Thaler, November 6, 2013, summary of recent pervasive monitoring threats

[13] Cyber Threat Intelligence-how to get ahead of cybercrime by Ernst and Young Ltd. from November 2014

[14] Jeremy Martin, Beginner's Guide to the Internet Underground, 31 may 2015

[15] Arkko, J., "Privacy and Networking Functions", March 2014,http://www.arkko.com/ietf/strint/draft-arkko-strint-networking-functions.txt

[16] Pouwelse, J., "The Shadow Internet: liberation from Surveillance, Censorship and Servers", Work in Progress, draft-pouwelse-perpass-shadow-internet-00, February 2014.

[17] Melinda Shore, Karen O'Donoghue, Trust problems in pervasive monitoring, https://www.w3.org/2014/strint/papers/58.pdf

[18] S.Kent, BBN technologies, "Opportunistic security as countermeasure to Pervasive Monitoring", Network Working Group, April 2014

[19] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Authentication Protocol", RFC 4252, DOI 10.17487/RFC4252, January 2006, http://www.rfc-editor.org/info/rfc4252

[20] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <http://www.rfc-editor.org/info/rfc6120>.

[21] Hardie,T., "Flows and Pervasive Monitoring", STRINT Workshop, 2014, <https://www.w3.org/2014/strint/papers/4.pdf>.

[22] Wikipedia, "Captive portal", October 2015,<https://en.wikipedia.org/w/index.php?title=Captive_portal&oldid=685621201>.

[23] Olaf Kolkman, Chief ITO, Internet Society, http://www.internetsociety.org/blog/tech-matters/2015/02/talking-encryption-routing-security-ipv6-and-more-mobile-world-congress

[24] Ryan Gallagher, Operation Auroragold, Dewayne Net Archives, December 2014

[25] Tech Desk, 'WhatsApp end-to-end encryption: How it works and what it means for users', April 2016

[26] Asheeta Regidi, 'WhatsApp end-to-end encryption is legal in India, but not for long', April 2016

[27] Dr. Glyn Lawson, Dr. Alex Stedmon, Hostile Intent and Counter-terrorism- Human factors Theory and application

[28] Melinda Shore, Karen O'Donoghue, Trust problems in pervasive monitoring, https://www.w3.org/2014/strint/papers/58.pdf

[29] Richardson, M. and D. Redelmeier, "Opportunistic Encryption using the Internet Key Exchange (IKE)", RFC4322, December 2005

[30] David Meyer, "how the internet engineers are fighting mass surveillance", December 30, 2014