Incentives for and Against Pervasive Monitoring Threats

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.

References

5. Joe St Sauver, PhD, Scientist, Farsight Security,Inc. Senior Technical Advisor, M3AAWG, 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”
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
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
18. S.Kent, BBN technologies, “Opportunistic security as countermeasure to Pervasive
Monitoring”, Network Working Group, April 2014
27. Dr. Glyn Lawson, Dr. Alex Stedmon, Hostile Intent and Counter-terrorism- Human factors Theory and application
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

Index Terms

Computer Science Information Sciences

Keywords

Pervasive, monitoring, threat, necessity, comparison