Cyber security system : An approach that address a severe problem in Cyber Security System.

Abstract : Cyber-security systems, which protect networks and computers against cyber attacks, are becoming common due to increasing threats and government regulation. At the same time, the enormous amount of data gathered by cyber-security systems poses a serious threat to the privacy of the people protected by those systems.

Introduction : Nowadays, nobody has clear idea that how deep they depended on computer networks. For everything directly or indirectly people are depending on computer, computer networks. Most of the services : simple services like Pizza ordering, online hotel reservation to complicated services like Medication, Teaching learning , Banking are provided through internet. Most of Government and Private sectors organisations are using emerging technologies to provide sophisticated services to people and customers.

In recent years, governments and corporations have increasingly relied on cyber-security systems to protect against increasing threats on networks, devices, and organizational and personal information. These systems prevent adversaries from breaking into networks and devices, from sabotaging digital activity, and from accessing private information. At the same time, by monitoring networks and computing devices, cyber-security systems ultimately affect individuals’ privacy. Systems in domains such as intrusion detection, malware detection, data leakage prevention, and phishing identification regularly monitor network traffic, device use, and personal communications. In many cases, the monitoring system can trace the identities of users and access sensitive information. For instance, many enterprise cyber-security systems monitor IP addresses that can be easily traced back to a particular individual. Moreover, the user’s device identification on mobile devices is often accessed by cyber-security applications. Therefore, while cyber-security mechanisms protect individuals from attacks from hackers and other third-party adversaries, they also create new vulnerabilities for privacy violation from the entity that runs the cyber-security system. These vulnerabilities can be realized if the security systems themselves are compromised, 1 if insiders make use of this information, or if the personal data are used contrary to the expectations of end users. 2 The increasing threat of computer attacks and the intrusiveness of cyber-security mechanisms present policymakers and technology developers with the difficult challenge of balancing security risks against privacy and civil liberties concerns (Tene 2014; Landau 2014). The fact that many national cyber-security policies require the sharing of the detailed information of attack logs and other types of information necessitates an urgent understanding of the privacy risks related to cyber-security (Sales 2013; Nolan 2015). Privacy concerns are among the reasons why employees switch to their personal devices (e.g., smartphones and portable computers) to perform workrelated activities (Pfleeger et al. 2014) and home-users turn away from some anti-virus applications (Warkentin and Willison 2009). Therefore, understanding and solving privacy threats is crucial, as those threats can reduce the acceptance and usage of cyber-security systems by organizations and individuals, leading to increased number of threats for everybody.

Methodology: To ground this threat, I studied common and novel cyber-security technologies and analyze them according to the potential for privacy invasion. I studied a taxonomy for privacy risks assessment of information security technologies, based on the level of data exposure, the level of identification of individual users, the data sensitivity and the user control over the monitoring, and collection and analysis of the data. I study the results in light of the recent technological trends and suggest some new directions for making these mechanisms more privacy-aware.

Bibliography :

Claudio Bettini and Daniele Riboni. 2015. Privacy protection in pervasive systems: State of the art and technical challenges. *Pervas. Mobile Comput.* 17 (2015), 159–174. DOI:http://dx.doi.org/10.1016/j.pmcj.2014.09.010

Giuseppe Bianchi, Simone Teofili, and Matteo Pomposini. 2008. New directions in privacy-preserving anomaly detection for network traffic. In *Proceedings of the 1st ACM Workshop on Network Data Anonymization*. ACM, 11–18.

Canada Privacy Commissioner. 2013. *What an IP Address Can Reveal About You*. Technical Report. Office of the Privacy Commissioner of Canada.

Keywhan Chung, Charles A. Kamhoua, Kevin A. Kwiat, Zbigniew T. Kalbarczyk, and Ravishankar K. Iyer. 2016. Game theory with learning for cyber security monitoring. In *Proceedings of the 2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)*. IEEE, 1–8.