Mini Review
Volume 13:1, 2023

Journal of Mass Communication & Journalism

ISSN: 2165-7912 Open Access

An Extensive Review of Modern Internet Measurement Methods for Cyber Security

Shujun Li*

Department of Cyber Security for Society, University of Kent, Canterbury, UK

Abstract

Society has become more susceptible to security flaws in the Internet as it has become an essential infrastructure. Cyber security attacks continue to increase in intensity, variety, and impact despite substantial efforts by industry, government, and academia to address many of these vulnerabilities. As a result, it becomes easy to look into the current threats to cyber security, assess the extent to which defenses have been put in place to counter them, and assess the success of risk mitigation efforts. Large-scale empirical data must be collected and analyzed using a variety of Internet measurement methods in order to effectively address these issues. Even though these kinds of measurements can give you accurate and complete insights, they require complicated processes and the creation of new methods to make sure they are accurate and complete. Therefore, it is necessary to carry out a methodical investigation of the most recent Internet measurement approaches for cyber security in order to make it possible to carry out comprehensive studies that make use of a variety of perspectives, correlate a variety of data sources, and possibly make use of successful techniques that have been used in the past for issues that are more recent. Sadly, conducting such an investigation is difficult due to the dispersed nature of the literature. This is largely because each research effort only addresses a small subset of the Internet measurement domain's many components. In addition, we are aware of no studies that have provided an in-depth examination of this important research area in order to encourage advancements in the future. We investigate all relevant aspects of using Internet measurement techniques for cyber security, from threats within specific application domains to threats themselves, in order to fill in these gaps. Taxonomy of two-dimensional Internet measurement studies related to cyber security is provided by us. One dimension is concerned with the numerous vertical layers (and components) of the Internet ecosystem, and the other is concerned with internal normal functions as opposed to the negative effects of external parties on the Internet and the real world. In terms of measurement technique, scope, measurement size, vantage size, and the utilized analysis approach, a comprehensive comparison of the collected studies is also provided. Last but not least, a detailed discussion of the obstacles to effective Internet measurement and potential future research directions is provided.

Keywords: Internet measurement • Cyber security • Large-scale analysis • Security threats

Introduction

The Internet is a dynamic, complex, decentralized system with many parts and features. It is made up of independent networks that use packet switching and the Internet Protocol (IP) to communicate with one another. It is challenging to evaluate any aspect of the Internet on a global scale because of its dispersed structure. The Internet's routing system contained a total of 99,378 distinct autonomous networks at the beginning of 2021. There will be 5.3 billion Internet users (or 66% of the world's population) by 2023, up from 3.9 billion in 2018 (or 51% of the world's population). Additionally, the number of IP-connected devices will exceed three times the global population. In addition, 29.3 billion networked devices are anticipated, a significant increase from the 18.4 billion devices accounted for in 2018. According to Cisco 2020, 14.7 billion Machine-to-Machine (M2M) connections will also have been established. Measurement is the only way to understand many aspects of the operation and use of the Internet, many of which are opaque or constantly changing. In addition, the Internet serves as the foundation and medium of communication for a wide range of services, from mission-critical to online entertainment. Therefore, it is essential to continuously monitor performance metrics and network settings, as well as to carry out a variety of tests, assessments, configurations, and management tasks, in order to ensure dependability, security, and quality of service [1].

Literature Review

Internet measurement is a set of methods for large-scale and in-action (remote) collection of measurable data from the Internet to quantitatively describe the structure (individual systems and protocols), their interaction, and use (the interrelationship between the Internet and the physical world) of the Internet. The empirical foundation, large-scale data collection, and in-the-wild data collection are the three fundamental aspects of Internet measurement research, particularly for cyber security. More specifically, the procedures for gathering data need to be carried out on a sufficiently large scale to generate a sample size that is representative. Because it is impossible to stop or disrupt the normal operation of the Internet for this purpose, the empirical nature of Internet measurement is closely linked to the collection of actual data in the wild [2].

There are three main categories that can be used to effectively classify applications of internet measurement. The first of these categories looks at how the Internet's protocols and services have changed in response to its rapid development. Some important protocols have undergone minor

***Address for Correspondence:** Shujun Li, Department of Cyber Security for Society, University of Kent, Canterbury, UK, E-mail: shujunli@gmail.com*

Received: 02 January 2023, Manuscript No. jmcj-23-90064; **Editor assigned:** 04 January 2023, Pre QC No. P-90064; **Reviewed:** 16 January 2023, QC No. Q-90064; **Revised:** 21 January 2023, Manuscript No. R-90064; **Published:** 28 January 2023, DOI: 10.37421/2165-7912.2023.13.503

revisions since the Internet's widespread adoption in the 1990s to address bugs, improve the quality of various services, enforce policies, or comply with new criteria like privacy and security. HTTP got a few more headers and methods, Transport Layer Security (TLS) got better over time, Transmission Control Protocol (TCP) got better at managing congestion, and Domain Name System (DNS) got new features like Domain Name System Security Extensions (DNSSEC). Due to the ability to modify Internet protocols at any layer and the introduction of network layer independence, the complexity of protocol implementations has also increased. In addition, new standards and protocols, such as Remote Desktop Protocol (RDP) and Virtual Private Networks (VPN), are frequently implemented to add support for a variety of technologies as their demand grows [3].

Discussion

Internet measurement is used to investigate cyberspace security in the second category. This category includes a wide range of applications, many of which focus on examining the security of new protocol implementations. Especially in the early stages of adoption, these new protocol implementations frequently come with vulnerabilities that hackers frequently take advantage of. In addition, it might take a number of years before the full extent of these vulnerabilities is discovered and appropriately patched. For instance, Denial of Service (DoS) attacks can be amplified by several orders of magnitude using protocols and services like Memcached and Network Time Protocol (NTP) that have been in use for a long time but have been insecurely implemented. Additionally, users' privacy can be compromised and data breaches can occur as a result of widespread TLS vulnerabilities. Internet measurement is useful for investigating a wide range of large-scale attacks, such as Denial of Service (DoS), Distributed DoS (DDoS), botnets, ransomware, and phishing, among others, in addition to assessing protocol-related security [4].

Finally, in the third category, the impact of Internet measurement on actual events is evaluated in relation to one another. This is possible because the Internet has become so integral to society and cyberspace that it now permeates every facet of human civilization. As a result, any significant event in one will unavoidably have an effect on the other. Internet measurement, as a result, has the potential to be a useful tool for determining how societal, political, and natural events affect the Internet ecosystem. Measurement of the Internet can also be used to ascertain the Internet's adaptability to unforeseen changes in the real world and the modifications that might need to be implemented as a result. Mention the 2011 Internet blackouts in Egypt and Libya as examples of unanticipated real-world developments as well as instances in which governments have chosen to restrict Internet access [5].

In the end, Internet measurement is very important for analyzing how known vulnerabilities spread, finding new threats, and following the development of attackers' activities. It can also be used to draw people's attention by highlighting the scale of these problems and the shortcomings of their current solutions, despite the fact that these solutions continue to cost more and more. Internet measurement offers a viable means of improving cyber security, which has emerged as a major issue and will remain so for many years to come. This survey will systematically detail the collection, use cases, and research of Internet measurement data in order to promote this enhancement in light of the extensive scope of Internet measurement.

Utilizing robust analytic methods in conjunction with passive and active measurement techniques can provide insight into a subject's security posture in light of the scarcity of real-world data in cyber security research. In addition, the Internet is expanding rapidly in a number of dimensions, including users, threats, protocols, devices, applications, technologies, platforms, and more. Consequently, a number of variables that could alter the measurement are necessary for a system's behavior. Furthermore, the Internet is constantly changing in a number of ways. Without a number of experiments and measurements, it is nearly impossible to make definitive predictions about the Internet's future behavior due to its enormous size and dynamic nature. Because a portion of the data may have changed during transit, little is known about a data stream that a recipient can directly attribute to the suspected source. Internet measurement is frequently compared to astronomy because it involves remote observations to better comprehend a system's operation. Additionally, measurements taken from different vantage points may not always correspond to one another, leading to inconsistent results as a result of Internet-imposed policies like political choices or security measures, such as ISPs blocking Internet Control Message Protocol (ICMP) messages to prevent external scans of their infrastructures [6-10].

Conclusion

In the meantime, a variety of countermeasures to limit information leaks have been implemented as a result of the ongoing focus on the privacy of users and other entities in cyberspace. Although these countermeasures are commendable and necessary, they undoubtedly complicate the process of gathering and evaluating empirical cyber security data. As a result, Internet measurement is frequently challenging and necessitates innovative methods for ensuring its accuracy and completeness. By highlighting a variety of different vantage points that can be leveraged and successful techniques that could be applied to new topics, a systematic review of the developed Internet measurement techniques for cyber security aids researchers in performing a comprehensive analysis. This survey is the first systematic review to our knowledge to examine empirical large-scale Internet data collection for cyber security purposes.

Acknowledgement

None.

Conflict of Interest

None.

References

1. Allix, Kevin, Tegawendé F. Bissyandé, Jacques Klein and Yves Le Traon. "Androzoo: Collecting millions of android apps for the research community." (2016):468-471.
2. Alrawi, Omar, Chaz Lever, Manos Antonakakis and Fabian Monrose. "Sok: Security evaluation of home-based iot deployments." (2019):1362-1380.
3. Bayat, Niloofar, Kunal Mahajan, Sam Denton and Vishal Misra et al. "Down for failure: Active power status monitoring." *Future Gener Comput Syst*. 125 (2021): 629-640.
4. Fadai, Tariq, Sebastian Schrittwieser, Peter Kieseberg and Martin Mulazzani. "Trust me, i'm a root ca! analyzing ssl root cas in modern browsers and operating systems." (2015): 174-179.
5. Fontugne, Romain, Cristel Pelsser, Emile Aben and Randy Bush. "Pinpointing delay and forwarding anomalies using large-scale traceroute measurements." (2017):15-28.
6. Gómez-Boix, Alejandro, Pierre Laperdrix and Benoit Baudry. "Hiding in the crowd: An analysis of the effectiveness of browser fingerprinting at large scale." (2018):309-318.
7. Kolodenker, Eugene, William Koch, Gianluca Stringhini and Manuel Egele. "Paybreak: Defense against cryptographic ransomware." (2017):599-611.
8. Kopp, Daniel, Matthias Wichtlhuber, Ingmar Poese and Jair Santanna, et al. "DDoS hide & seek: On the effectiveness of a booter services takedown." (2019):65-72.
9. Mariconti, Enrico, Jeremiah Onaolapo, Syed Sharique Ahmad and Nicolas Nikiforou, et al. "What's in a Name? understanding profile name reuse on twitter." (2017):1161-1170.
10. Lever, Chaz, Robert Walls, Yacin Nadji and David Dagon, et al. "Domain-z: 28 registrations later measuring the exploitation of residual trust in domains." *IEEE* (2016): 691-706.

How to cite this article: Li, Shujun. "An Extensive Review of Modern Internet Measurement Methods for Cyber Security." *J Mass Communicat Journalism* 13 (2023): 503.