*2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*
*Amity University, Noida, India. June 4-5, 2020*

# Security & Privacy Model for Work from Home Paradigm

Laxmi Ahuja
Amity Institue of Information Technology,
Amity University Sector – 125 Noida,
Uttar Pradesh India
lahuja@amity.edu

Ajay Rana
Amity Institue of Information Technology,
Amity University Sector – 125 Noida,
Uttar Pradesh India

Siddharth Gupta
Amity Institue of Information Technology,
Amity University Sector – 125 Noida,
Uttar Pradesh India
siddharth.gupta12@student.amity.edu

*Abstract* - **The outbreak of novel corona-virus pandemic has caused the entire world to initiate a total lockdown and thus, affecting the businesses and other economic activities thus, as a work around several organizations are now capitalizing the work from home paradigm that allows them to continue with their economic activities with certain limitations. However, such a widespread use of the above mentioned paradigm has risked the privacy and security of the underlying computer resources even more. Work from home (WFH) is indeed the need of the hour but is full of loopholes which can be exploited further by those having malicious intentions and when a huge population of the world is following such a paradigm then the threat becomes even more serious. The underlying project aims propose a cyber security model for the work from home paradigm to make it relatively secure. Just like the Biba and Bell-LaPadula models which have been used as a basis for many security practices in general, this project proposes a similar model but specifically meant for the WFH practice as following this paradigm doesn't generally involve a lot of people as compared to the traditional on-site working but the risk surprisingly is more as individuals tend to avoid security practices whilst following *'at home'* ideology. The model suggests various practices and steps to be taken in order to ensure the confidentiality, integrity and availability of the data with a focus on cyber hygiene.**

***Keywords: Cyber Security, Work From Home, Privacy, Cyber vulnerability, Cyber Threat***

## I. INTRODUCTION

The novel corona-virus pandemic has caused the nations to undergo lockdowns. As a direct outcome the economic activities are impacted severely and thus, for ensuring public safety and to follow the guidelines of social distancing suggested by authorities like CDC and WHO, the work from home paradigm was adopted so that the employees of an organization can continue to contribute towards economic activities. Considering the use of personal devices for commercial and related purposes and general user habits, this paper highlights common threats and vulnerabilities users may subject themselves to while pursuing work from home. Section 2 of this study marks the literature review in which a few such threats and related cause of concerns have been described which are generally unavoidable due to a prolonged cyber habit being adopted by the users. Section 3 talks about a few popular security architectures like SSE CMM, BLP and BIBA model, describing the imperatives of a security structure, section 4 is the core of this paper, which describes practices that can be adopted to ensure immunity against the threats and vulnerabilities whilst WFH. Section 5 concludes the paper and discusses the future prospects of this study.

## II. LITERATURE REVIEW

The use of personal devices for official purposes and the unhealthy environment with (cyber) unhealthy habits. The paragraph below describes various such habits which are completely unhygienic from a cyber security perspective. Although an obvious question rises that whether or not we need strictness for security while following this paradigm as many argue that if they're by themselves then devices are immune to unauthorized access and other threats but that's not true at all. Kaspersky Lab [1], a multi-national cyber security firm better known for its Antimalware product classifies these threats to be the most pertinent for personal devices and thus adversely affecting the WFH ideology.

Considering the exhaustive usage of mobile and other devices of similar nature leaves a constant threat of the following:

- **Rouge Wi-Fi Broadcast:** Devices like Pineapple [2], are capable of broadcasting rogue wifi signals over a range and the attacker then could receive all of the traffic from the connected users and in this case, if they happen to use e-payments then their credit card information for instance, can be leaked.
- **Faulty Anti-Malware Software:** A majority of the anti-malware software which are incapable of detecting various attack vectors. Plus, on personal devices, people often deliberately disable their anti-malware services. Other than that there are many un-trustworthy antimalware software within the market
- **Smishing & Phishing Attacks:** SMS phishing and spear phishing attacks are quite common attacks that individuals working from home can encounter and thus jeopardize lot of information.
- **Privacy Threats:** The most common and the most dangerous threat for individuals working from home. Privacy is not restricted to the physical access of your device there are various other sections in it. [3]

The Bell-LaPadula Model especially meant for government and military applications in order to enforce access control. The reasons for such models to exist are simple i.e. laying down a well defined structure for ensuring security and privacy among a hierarchy. Then, whilst following the WFH there is no such hierarchy but there are threats and vulnerabilities that must be taken care of. Accessibility is an important aspect to ensure security. It

**978-1-7281-7016-9/20/$31.00 ©2020 IEEE**

wouldn't be wrong to state that in order to ensure security in the digital realm has a lot to do with information privacy more so than physical privacy and this has always been the concern for many users this is quite evident from [4] in which a research was conducted that raised concerns for many popular websites collecting lots of personal information covertly and thus caused anxiety and panic in lots of users.

While working from home the employees do get physical privacy and security however, information privacy is always at a threat due to various cyber habits. For instance from [5] we can decipher how modern trends and advancements in technology like data mining and machine learning has jeopardized a user's existence on the internet especially in terms of data and its underlying analysis for sake of providing better services or recommendations and that being applicable on other sectors as well and not just on medical data. Then at the most basic level, ensuring security of the employees is a challenge because their psychological well being has to be considered too. In order to do so, there is indeed an excising concept of anonymity however, in pursuing a professional life anonymity cannot be completely afforded. The concept is still a matter of debate. Also, it is subjective i.e. it is not the same for everyone. The attack vectors mentioned above continue to pose an imminent threat to the users following the work from home (WFH) paradigm. Below are some cases to provide an overview of the same:

- **Covert Triggering of Microphones & Cameras in Smartphone:** As fictitious as it may sound, but yes there is evidence concerning the cameras and microphones in these smart devices are capable of eavesdropping on costumers, evident from [6] when Vizio a television set manufacturing company was accused of snooping on FTC owners. The former had to agree upon paying a penalty to latter of worth $ 2.2 Million
- **Snooping by various Voice Agents like Cortana, Bing, Siri, Google, etc:** Accidental triggering of such agents on the computers and cell phones and their transition into an active listening state clearly raises questions as they too are capable of communicating with various servers for sharing that information.
- **Operating Systems are Spying on Users:** The Dutch Data Protection Authority (DPAA) has accused Microsoft for its worldwide popular operating system, Windows 10 of not clearly specifying its users of the data collection which is enabled by default. DPAA has also mentioned that Microsoft also has not specified the kind of data they collect from users and its underlying purpose. [7]
- **Mobile Applications are on the list:** Various mobile applications need your live location in order to perform their functioning well. For instance, Google always keeps a track of its user's locations. Not only that, the searches made via Google search engine stay on Google servers for several years for one obvious reason i.e. analytics.[8]

Privacy and anonymity are always in a jeopardy regardless of the whereabouts of the employees. Mentioned above are just few examples of what is really a long list. Many people these days also make extensive use of wearable technology like activity trackers, heart-rate monitors for instance, Pentagon USA, examined the wearable activity trackers of the US military and that too revealed way too much about the fitness routines of these officer, their locations, where they go for cycling and jogging, which obviously is harmful for an organizations like the military. Although WFH is not that serious but, is also liable to certain breaches due to the tools and technology being used for availing working facilities. Software like Microsoft Teams, Zoom Communication's Zoom, Skype, etc. During the lockdown period these tools have become a tradition, but recently it was noted that Zoom has a security breach. Some of the highlighted flaws are: [10]

- it allows anyone to join meetings and share objectionable content
- Accused of selling private user data
- Leakage of email addresses.

With these few reasons alone it is quite evident that following the WFH paradigm for long times is indeed a challenge

## III. RELATED WORK

This section examines a few concepts and ideas of security, privacy and anonymity. Examining from an historic perspective, the ideation used today for WFH is indeed a part of what is known as the (Group Decision Support System) [11] which is further a subset of widely adopted paradigm that rose with the ease of access to the internet, Computer Mediated Communication [13]. The need for cyber anonymity also attracted attention due to a political architecture known as *democracy*. However, a little lower aspect. Privacy as the theme of this entire study is built around strengthening it. Implementation of cyber security is a crucial task because of the settings it advises to follow. Often it is not easy to merely do exactly as a model specifies and due to human errors data or security breach happen. To introduce the reader to a few applications of the security models, a briefing of widely adopted models is provided below:

- Software Security Engineering Capacity Maturity Model provides assurances to those applying it regarding the security practices being adopted by an organization in the security domain. The entire SSE CMM comprises of a couple of components such as, a model for processing of security techniques and projects of organization, along with the assessment methodologies to know the maturity of the model [14] following are the levels of maturity in the SSE CMM model
    - **Level – 0:** All the basic practices (security) have not been implemented
    - **Level – 1:** The basic security practices have been performed but without any standardized documentation
    - **Level – 2:** Appropriate planning and tracking of activities

- **Level – 3**: The processes are properly laid down and are being followed according to a set standard and definition.
- **Level – 4:** Constant observation of the process through quantitative measures
- **Level - 5:** Adaptable to changes and constant improvement in the processes

- Bell – LaPadula Model : is one of the most well known security model, designed for ensuring the confidentiality of the information. However, it is considered way too rigid to be used in commercial applications for the fact that it was designed for military applications. But, with certain modifications it can be adopted to commercial environments. The pillars of this model are mentioned below:
- **Mandatory Access Control:** defines permissions regarding operations on a resource in accordance with defined attributes such that the rights of one subject are not to be exercised with others. There are two principles, namely a subject and an object and MAC defines the practices that a subject can do on the underlying object.

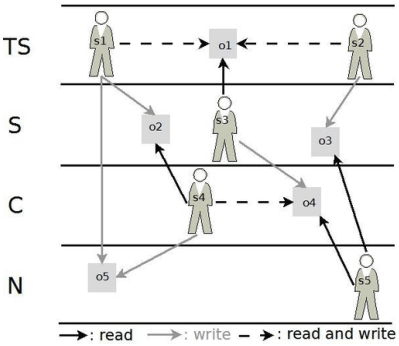
The BLP policy defines various security practices along with discretionary access control. To be appropriate, the Bell-LaPadula model comprises of the following structure:

- There exists a set of subjects S, a set of objects O and a set K of security levels for a given system
- A dominance relation with respect to security policies K.
- ($f_s$ $f_o$ $f_c$) a set of triplets, where the first two elements are functions mapped to subjects with their maximum and at-present security levels.
- A set of access methods P = {e ,r, a, w} conveying sending, reading, appending, executing and writing
- A set which is a proper subset of sets S, O , P which defines the access rights available to users along with a discretionary access control set

**The Biba Model** overcomes the flaw of the aforementioned BLP model i.e. the latter takes no consideration of data integrity and only data confidentiality. That being mentioned the biba model stands fit in a commercial application than the BLP model, comprising of two major rules given by its founder Kenneth J. Biba namely:

- **Simple Integrity Rule:** The subjects (users) are divided into various classifications with each being designated a set of rights. Keeping that in view, a particular subject residing in a particular classification cannot access/read the data (or object) of a lower classification thus ensuring *no read down* [15]
- **Integrity Rule:** Just like the simple integrity rule, the integrity rule ensures that a subject at a particular level should not be able to write the object to a higher level classification lying beyond their permission. Doing so ensures that no erroneous information is passed to the higher levels. [16]

The diagram explains the depiction and idea of the Biba model, showing the classifications with arrows and the table adjacent to it shows access rights with respect to the objects or resources within an organization. Clearly, following the architecture ensures data integrity as not all the subjects are able to access all the objects.




| | o1 | o2 | o3 | o4 | o5 |
|---|---|---|---|---|---|
| s1 | read write | write | | | write |
| s2 | read write | | write | | |
| s3 | read | | | write | |
| s4 | | read | | read write | write |
| s5 | | | read | read | |

Fig. 1. The Biba Model

## IV. PROPOSED WORK

While following the work from home paradigm, although users can ensure physical privacy concerning the physical access of their devices. There are however various risks involved as lots of commercial activities go on through personal devices. Due to faulty cyber hygiene and other erroneous digital habits, the WFH paradigm is risky. This section provides a framework comprising of certain steps and practices to strengthen the WFH experience. But, first below is a glimpse of some widely adopted cyber habits that are common to almost every device.

- **Microsoft Windows 10 as primary operating system:** Based on a user's browsing habits windows 10 generates an advertising ID which in turn not only track your browsing habits but also the activities done via windows apps.
- **The Location Tracking Feature:** Generally, when moving with Windows 10 installed portable devices, the operating system tracks the user's location to enable various features like temperature, places nearby, etc
- **Cortana:** The Windows 10 digital assistant, that can automate a few mundane tasks, has a trade-off i.e. it constantly keeps an eye on the device and often communicates with the Microsoft servers. Not only that the accidental triggering i.e. activation of Cortana client even when the trigger word hasn't been spoken raises questions.
- **Habits with Antivirus software:** A majority of windows users often disable anti-virus their software due to various reasons, like false alarms/warnings, antivirus interfering with applications, etc. however, doing so invites an obvious risk in terms of security.

It is also important to note that there are numerous kinds of privacy related threats and vulnerabilities coming from various other sources. The diagram below depicts the threat and vulnerability structure in context of Windows 10 default settings. U1 is simply a user liable to the shown happenings. With the advent of WFH paradigm, the devices may contain sensitive data and as depicted below, it is risky in terms of the Confidentiality, Integrity and Availability of the data.

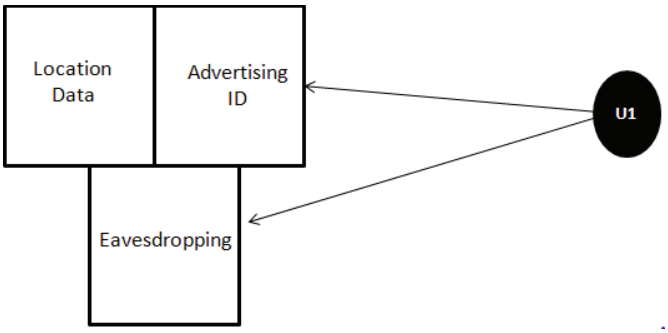



Fig. 2. User & Threat Relationship

In order to provide strength to privacy and CIA triad of the information, the only thing that has to be done, is to be able to break or weaken the link between the user U1 and the threats depicted. In order to further strengthen user's privacy to ensure CIA triad of user data following steps are proposed:

- **Making use of Duck-duck-go search engine for online privacy:** Duck-duck-go is one of the several alternatives to Google search engine, which is more secure and doesn't track user searches. Google on the other hand, gathers loads of information from its users, like emails, search-history, etc. Its counterpart duck-duck-go, follows the privacy motto. It also enables various other features like, random password generation, website status check, etc. [9]
- **Woes of Windows:** A major problem with windows is that it is the most popular choice for personal computers and so, tons of malicious programs exist to cause harm to it. Also, one reason why malwares are so vicious on a windows system is because of the system administrator account. Thus, a program has the most of the privileges making windows more vulnerable to threats.[12]
- **Windows Registry & Shell-bags:** Windows registry is a hierarchical database that stores all the information a running version of operating system needs like timestamps, meta-data of hardware devices, operating system settings and meta-data of installed programs. Shell-bags provide information regarding what files and folders were accessed, while they prove to be an important forensic artifact, they do jeopardize user privacy.

The primary aim is to break the link between the user U1 and the threats. Breaking the link requires some new habits and knowledge which may appear cumbersome at first from an UX perspective. The use of Linux for personal computing would aid in breaking the link due to the following factors:

- **Variety of Linux distributions:** Numerous Linux distributions are available for free, users can choose the one which fits their needs.
- **Majority of viruses and malicious software are designed to target windows**: Linux operating systems stay unaffected from such malwares, considering their immunity they're the primary choice for forensic and malware analysis procedures
- **No administrator at all times:** unlike windows operating systems, in any Linux distribution, the user account does not have all the privileges even though they're system administrator accounts but, the core of Linux user management lies with the root user, which has to be enabled first, so the programs do not have all the privileges.
- **Open source technology:** Linux is flexible as compared to windows operating systems. It works according to the needs of the user. For instance, windows forces users to install updates but it is not the case with Linux.

## V. CONCLUSION & FUTURE SCOPE

The objective of this study was to propose a framework for the work from home paradigm which has become a practice during these hard times of a worldwide pandemic, the briefing of well known threats and vulnerabilities and a small idea that'd enhance user privacy, the diagram above depicts a relation between the users and the threats and vulnerabilities they expose themselves to. The small proposed framework attempts to break this link. The future scope of this study revolves around examining the security structure of Linux and other related open source resources.

## ACKNOWLEDGEMENT

Presenting the uttermost gratitude to the Amity Institute of Information and Technology that provided the opportunity to conduct this study, sincere thanks goes to Dr. Ajay Rana, Director of the department who is always inspiring and supporting us for conducting new studies.

## REFERENCES

[1] Remote working safety and security, Leonid Grustniy, March 2020 https://www.kaspersky.com/blog/remote-work-security/34258/.

[2] Hak5 Pineapple, https://shop.hak5.org/products/wifi-pineapple

[3] Gomez, J., Pinnick, T., and Soltani, A. 2009. "KnowPrivacy: The Current State of Web Privacy, Data Collection, and Information Sharing," School of Information, University of California, Berkeley (http://www.knowprivacy.org/).

[4] Atoum, Issa & Otoom, Ahmed. (2017). A Classification Scheme for Cybersecurity Models. International Journal of Security and Its Applications. 11. 109-120.

[5] International Journal of Mechanical Engineering and Technology (IJMET) Volume 8, Issue 11, November 2017, pp. 964–976, Article ID: IJMET_08_11_098 Available online at http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=8&IType=11 ISSN Print: 0976-6340 and ISSN Online: 0976-6359

[6] How To Stop Your Smart TV From Spying on You - Brian Barret (2017) https://www.wired.com/2017/02/smart-tv-spying-vizio-settlement/

[7] Microsoft's response to privacy concerns in Netherlands, Marisa Rogers https://pulse.microsoft.com/nl-nl/technology-lifestyle-nl-nl/na/fa1-microsofts-response-privacy-concerns-netherlands/

[8] Nikkhah, Hamid Reza & Balapour, Ali & Sabherwal, Rajiv. (2018). Mobile Applications Security: Role of Privacy.

[9] Everything You Need to Know About the Security of Voice-Activated Smart Speakers – Candid Wueest, December 2017, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/security-voice-activated-smart-speakers

[10] Use Zoom at your own risk: Privacy concerns around this viral video conferencing app, April 6 2020

[11] DeSanctis, G. L., & Gallupe, B. (1987). A foundation for the study of group decision support systems.Management Science, 33, 589–609.

[12] Christopherson, Kimberly. (2007). The positive and negative implications of anonymity in Internet social interactions: "On the Internet, Nobody Knows You're a Dog". Computers in Human Behavior. 23. 3038-3056. 10.1016/j.chb.2006.09.001.

[13] DeSanctis, G., & Poole, M. S. (1994). Capturing complexity in advanced technology use: adaptive structuration theory. Organization Science, 5(2), 121–147.

[14] Kurniawan, Endang & Riadi, Imam. (2018). Security level analysis of academic information systems based on standard ISO 27002:2003 using SSE-CMM. International Journal of Computer Science and Information Security,. 16. 139-147. 10.13140/RG.2.2.20925.15840.

[15] Information Gathering Craig Wright, in The IT Regulatory and Standards Compliance Handbook, 2008

[16] Eric Conrad, ... Joshua Feldman, in CISSP Study Guide (Third Edition), 2016

[17] E. Kashyap, A. Rana, "A Comparative Study of S-shape and Concave Software Reliability Growth Models", in Proceedings - 2015 International Conference on Computational Intelligence and Communication Networks, CICN 2015, pp 1452-1455 (2016).

[18] P. Chawla, I. Chana, A. Rana, "Cloud-based automatic test data generation framework", in Journal of Computer and System Sciences, Vol.82, Isuue 5, pp 712-738 (2016).

[19] N. Agarwal N, A. Rana, J. P. Pandey, "Proxy signatures for secured data sharing", in Proceedings of the 2016 6th International Conference - Cloud System and Big Data Engineering, Confluence, pp 255 -258 (2016).

[20] M. K. Shukla, A. Rana, H. Banka, "Classification of the Bangla script document using SVM", in 2016 3rd International Conference on Recent Advances in Information Technology, RAIT 2016, pp 182-185 (2016).

[21] M. Bhardwaj, A. Rana, "Key software metrics and its impact on each other for software development projects", in International Journal of Electrical and Computer Engineering, Vol. 6, Isuue 1, pp 242-248 (2016).

[22] B. D. Chauhan, A. Rana, "Software projects tracking-evolving a new method for software project tracking", in Journal of Software Engineering, Vol. 10, Isuue 1, pp 78-88 (2016).

[23] G. Dubey, A. Rana, J. Ranjan, "A research study of sentiment analysis and various techniques of sentiment classification", in International Journal of Data Analysis Techniques and Strategies, Vol. 8, Issue 2, pp 122-142 (2016).

[24] P. Chawla, I. Chana, A. Rana, "A novel strategy for automatic test data generation using soft computing technique", in Frontiers of Computer Science, Vol. 9, Issue 3, pp 346-363 (2015).