A Router-based Parental Control Tool for Safe Social Network Usage

Aurelio Loris Canino[1][0009−0005−5790−4056], Vincenzo De Angelis[2][0000−0001−9731−3641], and Gianluca Lax[1][0000−0002−5226−0870]

[1] University Mediterranea of Reggio Calabria, Via dell'Universita 25, 89124, Reggio Calabria, Italy
{aurelio.canino,lax}@unirc.it
[2] University of Calabria, Via P.Bucci, 87036, Rende, Italy
vincenzo.deangelis@dimes.unical.it

Abstract. Social networks' explosive growth has changed the way people, especially young people, engage with the digital world. There are many worries about the amount of time kids spend online and the content they are exposed to. Parental control software can be used to monitor and limit Internet usage, but they need to be installed and are easily circumvented. The integration of parental control methods directly into the home router, as proposed in this paper, offers a novel alternative. The router's central location within the home network facilitates monitoring and management of Internet consumption across all connected devices. This method provides granular packet inspection, scalability, and centralized control, allowing for a thorough examination of network traffic, including social network activity. The architecture of the suggested solution consists of modules for social network identification, traffic analysis, and packet capture and inspection.

Keywords: traffic analysis · router · OpenWrt

1 Introduction

The rapid proliferation of social networks has significantly impacted how individuals, particularly young people, interact with the digital world. Platforms like Facebook, Instagram, Twitter, and TikTok have become integral parts of daily life, providing avenues for communication, entertainment, and information sharing [23]. However, this increased usage comes with challenges, especially for parents concerned about the time their children spend online and the content they are exposed to.

Parental control tools have been developed to address these concerns, offering functionalities to monitor and restrict Internet usage [13, 25]. Traditional parental control solutions typically operate on individual devices through dedicated applications. While effective to some extent, these approaches have notable limitations. Device-specific controls require installation and maintenance on every device, which can be cumbersome and easily bypassed by tech-savvy children.

Additionally, these solutions often lack the ability to provide a comprehensive view of Internet usage across multiple devices.

An alternative approach involves DNS filtering, where requests to certain websites are blocked based on a denylist of domains. However, a simple DNS filtering does not offer granular control over specific activities within websites, particularly dynamic and content-rich platforms like social networks [1].

This paper proposes a new solution to these challenges by integrating parental control mechanisms directly into the home router. By leveraging the router's central position in the home network, our system can monitor and manage Internet usage across all connected devices [3]. This approach offers several advantages:

- Centralized Control: All network traffic passes through the router, enabling comprehensive monitoring and management.
- Scalability: New devices connected to the network are automatically subject to the same controls, eliminating the need for individual setup.
- Granularity: Packet inspection allows for detailed analysis of network traffic, including the time and duration of the activities on social networks.

The architecture of the solution includes various modules, whose purposes concern capturing and inspecting network packets, identifying the social networks involved in the activity, analyzing traffic patterns to monitor user activities, and enforcing parental control policies. The proposed solution has been implemented to validate the proposal and a proof of concept is presented.

The rest of the paper is structured as follows. In the next section, we survey the related work. In Section 3, we present the solution proposed to implement a parental control tool. Section 4 describes the implementation of the proposal presented as a proof of concept. Finally, in Section 5, we draw our conclusions.

2 Related Work

Parental control on social networks has emerged as a critical area of research due to the increasing use of these platforms by adolescents and the associated risks. The importance of parental control is underscored in [10], stating that preadolescents, whose parents reported greater control over their child's time on social media, reported better mental health. Reference [8] proposes a framework for the design of parental control. It provides instructions to efficiently integrate parental control tools into digital environments, emphasizing how the aspect of granular access controls can be effective in building parental control systems.

Best practices for building parental control systems are even discussed in [18], which outline how the reviews on the Google Play Store related to parental control applications do not satisfy the requirements needed in such systems.

Numerous studies have explored various strategies and technologies to monitor and manage children's activities online, ensuring their safety while respecting their privacy [17]. In [21], the authors propose a privacy preserving parental control protocol with edge computing that uses Artificial Intelligence techniques to automatically detect harmful content for minors in 5G networks. The aspect of

privacy is also investigated in [27], in which a rule-based expert system is used to emulate human intelligence by using rules and conditions is proposed.

The adoption of blockchain is also proposed to implement parental control in home environments [22]. Traditional approaches that implement parental control are based on machine learning techniques [12, 11, 14, 16, 15].

However, many ML approaches assume the availability of the content of the websites accessed by users. This may limit the applicability of the proposed solutions by requiring the collaboration of the providers.

On the other hand, our proposal aims to implement a parental control mechanism in a home environment, without disclosing the rules or habits of the users to external parties. In particular, our proposal is based on packet inspection [9, 26]. Packet inspection allows for the analysis of data packets transmitted over a network to identify and block harmful content without needing access to the actual content of the websites. This method offers a robust solution for parental control that safeguards user privacy and operates independently of external content providers.

DNS inspection is shown to be effective in blocking children from accessing some platforms [24]. However, simple DNS filtering does not offer granular control over specific activities within social network platforms. Then a more advanced approach that integrates traffic inspection on encrypted traffic [6] and access-based access control to enforce policies [5] without altering flows of messages [4] should be investigated.

3 System Architecture

In this section, we present the design and architecture of the system. The environment we consider in the following paper is depicted in Fig.1. We consider a domestic network where all the users' devices access the Internet through a router. The router enables wireless and wired connections within the environment and provides a multi-device parental control service. The devices can be smartphones, laptops, workstations, and so on, and are used by users to whom parental control policies are applied. Moreover, an admin is considered to establish the policy to apply and the actions to execute when a policy is violated.

The core of the architecture is located in the router, which acts as the main actor for the parental control service. The architecture is composed of six modules that are described in the following and schematized in Figure 2, where the data-flow is presented with reference to a single device (i.e., this workflow is repeated for each device):

1. *Domain Manager* is the module that manages the social network domains to be monitored. Admin can include or remove the domain names that should be monitored by the system.
2. *Policy Manager* is the module that manages the parent control security rules. Admin can include or remove rules for each social network and device.
3. *Domain Name Inspector* intercepts each network packet of the device and searches for DNS queries/responses.

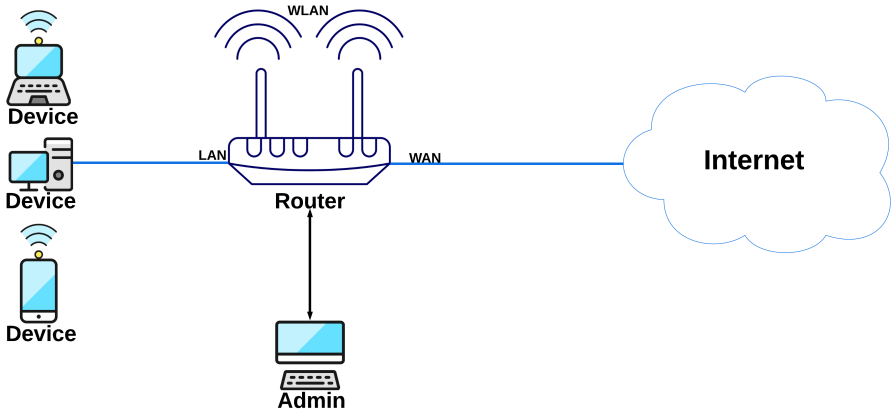

Fig. 1. Environment considered in the paper.

4. *Traffic Inspector* receives a network packet and decides whether this packet should be processed or not.
5. *History Manager* is in charge of storing the traffic of interest to allow for policy compliance checks.
6. *Decider*, the module that eventually decides whether a connection should be processed according to the given policies.

Now, we show how the interactions between the various components work through the following steps:

Step 1. In this step, Admin interacts with both the *Domain Manager* module and the *Policy Manager* module. First, Admin sets within *Domain Manager* the domain names to be monitored. For example, Admin can include `facebook.com` and `tiktok.com` (Step 1a). Next, Admin defines within *Policy Manager* the parental control policies, which can be modified or removed later (Step 1b). For example, Admin may want to prevent connected devices from `tiktok.com` for more than one hour per day, denying future connections, and/or receiving alerts when a device in the network has exceeded the maximum permitted use.

Step 2. Domain Name Inspector intercepts all incoming and outgoing Internet traffic generated by connected devices searching for a DNS query. A DNS query is used to ask for the IP address associated with a domain name. Indeed, to reach a domain it is necessary a request to the DNS servers to get the IP address related to that domain. When a request of a device is directed to a DNS server, *Domain Name Inspector* checks whether the field *domain name* of the DNS request matches any of the domains stored in Domain Manager. In this case, the DNS query is let go to the Internet (step 2a), and the associated DNS response is waited. Once the response is returned, the IP address associated with the DNS query domain is stored in *Domain Manager* together with the associated domain name. The purpose of this module is related to the fact that IP addresses

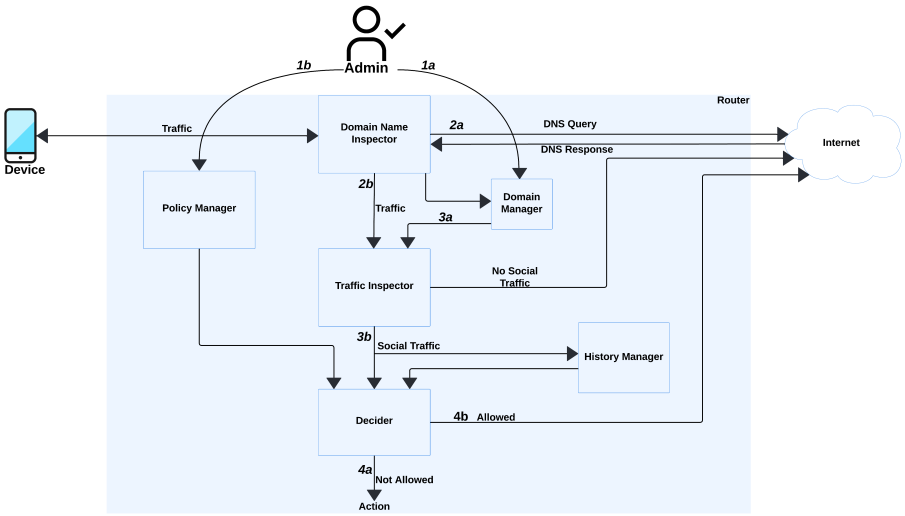

Fig. 2. Example of the architecture considered in the paper.

of social networks can change over time: for example, traffic to a social network can be handled across multiple servers for load-balancing reasons. Again, in case of failure, a server can be replaced by another one with a different IP. In case *Domain Name Inspector* intercepts a DNS query not related to a domain to be monitored, or if the traffic is not a DNS query, then the network packet is forwarded to the *Traffic Inspector* module (Step 2b).

Step 3. Once *Traffic Inspector* receives a network packet from *Domain Name Inspector*, the following actions are done. The destination IP of the packet is extracted and compared with the IPs stored by *Domain Manager* (step 3a). If a match is found (thus, this is a connection to a social network), then the packet is forwarded to the *Decider* module (step 3b), and the packet content is stored in *History Manager* to allow for subsequent statistic analyses (see the next step). If the packet is not a connection to a social network to be monitored, then the packet is let go to the Internet.

Step 4. At this stage, the *Decider* module receives a packet to a social network S and accesses the *Policy Manager* module to extract the policies related to the social network S. For each policy, the condition is extracted and computed by using the data included in *History Manager* (observe that the type of computation done depends on the rules of the policy). If the policy is not satisfied, then the action expected from the policy is carried out (step 4a). For example, consider the policy introduced in Step 1, which prevents connected devices from `tiktok.com` for more than one hour per day. In this case, once a request to Tiktok is intercepted, the *History Manager* is used to compute the total amount of time spent on Tiktok from this device, and if this amount is more than one

hour, the packet is blocked according to the policy. Clearly, if the connection is compliant with the policy, the packet is let go to the Internet (step 4b).

4 Implementation

In this section, we provide a proof of concept of the solution proposed in this paper. We start with the hardware and software used in the implementation.

4.1 Network Infrastructure

We deployed a network infrastructure based on a Netgear R8000 [19] router, on which we installed OpenWrt 22.03.5 [20]. OpenWrt is an open-source firmware based on Linux, designed to be installed on embedded devices, primarily routers. Additionally, it provides a completely writable filesystem with package management, enabling an environment where users can customize the functionalities and features of their devices. To give Internet access to the router, we assigned a public static IP address at its WAN port. Additionally, the router generates a Wireless WiFi network (WWAN) with a private subnet, which is dedicated to host devices to be monitored by our parental control system.

Python 3.10.13 has been installed on the router to enable important functionalities and libraries over traffic monitoring. All Python scripts that constitute our multi-device parental control system are executed in a virtual environment on the router.

The router can be directly accessed using a wired or wireless connection, possibly by remote connection with IPsec IKEv2 Road-Warrior VPN [28].

Finally, to have enough memory to conduct our tests and to store intercepted traffic, we increased the storage capacity of the router to 250GB with an external SSD storage drive [2].

4.2 Modules

We describe now how the six modules of our proposal are implemented.

1. *Domain Manager* module exploits a dictionary as a data structure to store information about domains. Specifically, each key of the dictionary is a string representing a domain name and is associated with a set of IP addresses. The keys of the dictionary are configured by Admin, who can add or remove domain names related to the social networks to be monitored. Such a dictionary is accessible by the *Domain Name Inspector* module.
2. *Policy Manager* module is another dictionary: it associates each domain name with a set of policies.
3. *Domain Name Inspector* and *Traffic Inspector* modules are implemented through the same Python script. This script monitors all Internet traffic generated from the devices through Scapy [7], a Python framework that enables powerful network functionalities such as crafting, sending, receiving,

sniffing, and manipulating network packets. To efficiently process these network packets, our *Domain Name Inspector* captures and analyzes network traffic in real-time. This is achieved by monitoring the network interface (specifically, the WAN interface) and utilizing the sniff function from the Scapy Python library. Multiple instances of sniff run indefinitely and in parallel, facilitated by threading, to ensure comprehensive and concurrent packet capture and analysis. *Domain Name Inspector* intercepts DNS responses and writes the IP addresses of the considered domains in the dictionary of *Domain Manager*.
Traffic Inspector captures packets having an IP address that is stored in the dictionary by *Domain Name Inspector*.

4. *History Manager* module: It is represented by a collection of pcap files stored in a specific directory on the router. Inside the main directory, there are sub-directories, each corresponding to a specific social network. Within these sub-directories, *Traffic Inspector* stores pcap files not only related to the social network but also specific to individual devices.
5. *Decider*: it is implemented through a Python script. It analyses pcap files stored within *History Manager* through Scapy, which allows current Python programs to read pcap files efficiently. Then, *Decider* receives from *Policy Manager* the policies for the specific social network and, based on the result of the analysis, enforces these policies.

5 Conclusion

Digital interactions have changed as a result of the widespread use of social networks, particularly among younger people. Although social media platforms have a number of advantages for contact, amusement, and information exchange, they also present risks associated with overuse and exposure to unsuitable content. Conventional parental control systems, which function on individual devices, provide some safety but have drawbacks in terms of maintenance, installation difficulty, and the inability to give a comprehensive picture of Internet usage across several devices. To address these limitations, this paper proposed a router-based parental control solution. Using the home router's pivotal function in network traffic management, our system our solution enables comprehensive monitoring and control of Internet usage across all devices connected to the home network. Centralized control, automatic scalability with the addition of new devices, and granular traffic analysis capabilities are key advantages of our proposal. Our implementation, validated through a proof of concept, demonstrates the practicality and efficacy of integrating parental control mechanisms into home routers. The ability to capture and inspect network packets, identify social network traffic, analyze usage patterns, and enforce control policies marks a significant advancement in parental control technology.

Future work includes the definition of complex policies to be included in the system to enhance its usability and expand its capabilities to adapt to the evolving landscape of digital interactions.

Acknowledgment

This work is partially funded by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

1. Ali, S., Elgharabawy, M., Duchaussoy, Q., Mannan, M., Youssef, A.: Betrayed by the guardian: Security and privacy risks of parental control solutions. In: Proceedings of the 36th Annual Computer Security Applications Conference. pp. 69–83 (2020)
2. amirhosseinchoghaei: Increase openwrt disk space. https://github.com/amirhosseinchoghaei/Increase-openwrt-disk-space
3. Anselmi, G., Mandalari, A.M., Lazzaro, S., De Angelis, V.: COPSEC: Compliance-Oriented IoT Security and Privacy Evaluation Framework. Association for Computing Machinery, New York, NY, USA (2023), https://doi.org/10.1145/3570361.3615747
4. Buccafurri, F., De Angelis, V., Lazzaro, S.: Mqtt-i: Achieving end-to-end data flow integrity in mqtt. IEEE Transactions on Dependable and Secure Computing pp. 1–18 (2024). https://doi.org/10.1109/TDSC.2024.3358630
5. Buccafurri, F., De Angelis, V., Lazzaro, S., Pugliese, A.: Enforcing security policies on interacting authentication systems. Computers & Security **140**, 103771 (2024). https://doi.org/https://doi.org/10.1016/j.cose.2024.103771, https://www.sciencedirect.com/science/article/pii/S0167404824000725
6. Chen, D., Wang, H., Zhang, N., Nie, X., Dai, H.N., Zhang, K., Choo, K.K.R.: Privacy-preserving encrypted traffic inspection with symmetric cryptographic techniques in iot. IEEE Internet of Things journal **9**(18), 17265–17279 (2022)
7. Creative Commons Attribution-NonCommercial-ShareAlike 2.5: scapy-python. https://scapy.readthedocs.io/en/latest/index.html
8. Dumaru, P., Atashpanjeh, H., Al-Ameen, M.N.: " it's hard for him to make choices sometimes and he needs guidance": Re-orienting parental control for children. Proceedings of the ACM on Human-Computer Interaction **8**(CSCW1), 1–51 (2024)
9. El-Maghraby, R.T., Abd Elazim, N.M., Bahaa-Eldin, A.M.: A survey on deep packet inspection. In: 2017 12th International Conference on Computer Engineering and Systems (ICCES). pp. 188–197. IEEE (2017)
10. Fardouly, J., Magson, N.R., Johnco, C.J., Oar, E.L., Rapee, R.M.: Parental control of the time preadolescents spend on social media: Links with preadolescents' social media appearance comparisons and mental health. Journal of youth and adolescence **47**, 1456–1468 (2018)
11. Fuertes, W., Quimbiulco, K., Galárraga, F., García-Dorado, J.L.: On the development of advanced parental control tools. In: 2015 1st International Conference on Software Security and Assurance (ICSSA). pp. 1–6. IEEE (2015)
12. Fuertes, W., Quimbiulco, K., Galárraga, F., García-Dorado, J.L.: On the development of advanced parental control tools. In: 2015 1st International Conference on Software Security and Assurance (ICSSA). pp. 1–6 (2015). https://doi.org/10.1109/ICSSA.2015.011

13. Ghosh, A.K., Badillo-Urquiola, K., Guha, S., LaViola Jr, J.J., Wisniewski, P.J.: Safety vs. surveillance: what children have to say about mobile apps for parental control. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. pp. 1–14 (2018)
14. Giorgi, G., La Marra, A., Martinelli, F., Mori, P., Saracino, A.: Smart parental advisory: A usage control and deep learning-based framework for dynamic parental control on smart tv. In: Security and Trust Management: 13th International Workshop, STM 2017, Oslo, Norway, September 14–15, 2017, Proceedings 13. pp. 118–133. Springer (2017)
15. Lazzaro, S., De Angelis, V., Mandalari, A.M., Buccafurri, F.: Is your kettle smarter than a hacker? a scalable tool for assessing replay attack vulnerabilities on consumer iot devices. In: 2024 IEEE International Conference on Pervasive Computing and Communications (PerCom). pp. 114–124 (2024), https://doi.org/10.1109/PerCom59722.2024.10494466
16. Leon-Paredes, G.A., Bravo-Quezada, O.G., Bermeo-Aguaysa, P.P., Pelaez-Currillo, M.J., Jimenez-Gonzalez, L.L.: Preventing cyberbullying on social networks with spanish parental control nlp system. International Journal of Advanced Computer Science and Applications **14**(11) (2023). https://doi.org/10.14569/IJACSA.2023.01411141, http://dx.doi.org/10.14569/IJACSA.2023.01411141
17. Li, Y., Li, Y., Yan, Q., Deng, R.H.: Privacy leakage analysis in online social networks. Computers & Security **49**, 239–254 (2015). https://doi.org/https://doi.org/10.1016/j.cose.2014.10.012, https://www.sciencedirect.com/science/article/pii/S0167404814001588
18. Lundberg, J., Marklund, O.: Adolescents in control: Promoting adolescents autonomy in parental control applications (2023)
19. Netgear: Netgear r8000. https://www.netgear.com/home/wifi/routers/r8000/
20. OpenWrt: Openwrt 23.03.5. https://openwrt.org/toh/netgear/r8000
21. Ramezanian, S., Meskanen, T., Niemi, V.: Parental control with edge computing and 5g networks. In: 2021 29th Conference of Open Innovations Association (FRUCT). pp. 290–300 (2021). https://doi.org/10.23919/FRUCT52173.2021.9435552
22. Suchaad, S.A., Mashiko, K., Ismail, N.B., Abidin, M.H.Z.: Blockchain use in home automation for children incentives in parental control. In: Proceedings of the 2018 International Conference on Machine Learning and Machine Intelligence. pp. 50–53 (2018)
23. Swart, J., Peters, C., Broersma, M.: Sharing and discussing news in private social media groups: The social function of news and current affairs in location-based, work-oriented and leisure-focused communities. Digital journalism **7**(2), 187–205 (2019)
24. Trevisan, M., Drago, I., Mellia, M., Munafo, M.M.: Automatic detection of dns manipulations. In: 2017 IEEE International Conference on Big Data (Big Data). pp. 4010–4015. IEEE (2017)
25. Wang, G., Zhao, J., Van Kleek, M., Shadbolt, N.: Protection or punishment? relating the design space of parental control apps and perceptions about them to support parenting for online safety. Proceedings of the ACM on Human-Computer Interaction **5**(CSCW2), 1–26 (2021)
26. Xu, C., Chen, S., Su, J., Yiu, S.M., Hui, L.C.: A survey on regular expression matching for deep packet inspection: Applications, algorithms, and hardware platforms. IEEE Communications Surveys & Tutorials **18**(4), 2991–3029 (2016)

27. Zakaria, N., Yew, L.K., Alias, N.M.A., Husain, W.: Protecting privacy of children in social networking sites with rule-based privacy tool. In: 8th International Conference on High-capacity Optical Networks and Emerging Technologies. pp. 253–257 (2011). https://doi.org/10.1109/HONET.2011.6149828
28. zetago: Ipsec modern ikev2 road-warrior configuration. https://openwrt.org/docs/guide-user/services/vpn/strongswan/roadwarrior