Toward Dynamic Human Knowledge Assessment to Tailor Network Traffic Visual Platform Interfaces

Bernardo Breve[1,*], Vincenzo Deufemia[1]

[1]University of Salerno, Via Giovanni Paolo II, 132, 84084 Fisciano, Salerno, Italy

Abstract

Nowadays, a vast amount of data flows through networks, with many users inadvertently agreeing to their personal data being processed by network providers, frequently lacking comprehension regarding its management or sharing among various entities. Various network data analytics tools have been introduced in recent years, aiming to simplify visual representations for network traffic analysis. However, these platforms often fail to account for the diverse technical knowledge and cyber risk awareness levels of modern Internet users. To address this issue, we propose the introduction of a Large Language Model (LLM)-based conversational agent with a dynamically structured visual platform. This combination allows for the assessment of users' comprehension through adaptive questioning, enabling personalized interface adaptations that enhance user comprehension and engagement. In this paper, we discuss the architecture and components of the proposed solution, emphasizing the importance of adaptive interfaces in enhancing user experience and fostering security awareness. Through the incorporation of LLMs for human knowledge assessment, our approach endeavors to craft a more personalized and efficient visual platform for analyzing network traffic and cyber threats.

Keywords

Cybersecurity, Network traffic, Human Assessment, Usable Security and Privacy, Large Language Models

1. Introduction

The exponential proliferation of Internet-connected devices has precipitated a monumental surge in the daily volume of data generated. The advent of the Internet of Things (IoT) has not only expanded the sheer quantity of networked devices but has also diversified their types and functions. From ubiquitous smartphones and smartwatches to cutting-edge smart cars, these devices incessantly produce data packets stemming from everyday interactions, seamlessly transmitting them across the vast expanse of the Internet to network providers that serve as nodes of the intricate web of connectivity. According to the latest statistical analysis[1], 328.77 million terabytes of data is produced daily, culminating in 120 zettabytes annually.

This data contains valuable insights into user behavior, providing a fingerprint of their activities, preferences, and desires. Although nowadays most network traffic is encrypted utilizing several techniques, such as TLS, SSL, HTTPS, etc. [1], there are still approaches that can extract knowledge from the traffic by extrapolating patterns [2]. By analyzing the information extracted from the traffic, providers can better tailor needs by promoting personalized advertisements that have a higher probability of convincing the user to navigate toward those pages [3]. Thus, the vast amounts of data generated can potentially serve as a significant source of revenue for network providers [4], at the expense of users' privacy [5]. In addition, online activities can often expose users to the wide range of cyber-attacks that characterize the web, making the user who approaches it particularly vulnerable. Malware [6], DDOS attacks [7], port scanning/mapping [8], IP spoofing, phishing [9], are just some of the types of cyber threats that an Internet user may encounter on a daily basis.

First International Workshop on Detection And Mitigation Of Cyber attacks that exploit human vuLnerabilitiES (DAMOCLES). Workshop co-located with AVI 2024, June 3rd, 2024, Arenzano, Genoa, Italy.

*Corresponding author.

†These authors contributed equally.

bbreve@unisa.it (B. Breve); deufemia@unisa.it (V. Deufemia)

0000-0002-3898-7512 (B. Breve); 0000-0002-6711-3590 (V. Deufemia)

[1]https://explodingtopics.com/blog/data-generated-per-day

In this scenario, it is crucial to provide users with solutions that can properly assess and hopefully increase their level of awareness regarding how easily online activities could affect their privacy and make them susceptible to cyber-attacks. To this end, the literature has seen the rise of several platforms whose purpose is to monitor their activities and alert users to the risks associated with the improper use of Internet-connected devices [10] and the network anomalies to which they are exposed [11]. These approaches primarily use visual metaphors and/or the introduction of layers of abstraction to present users with the progress of their online activities [12] and be alerted to any attack that may be targeted at them [13, 14].

Such platforms could significantly play a role in enhancing users' awareness; however, all of them considerably lack tailorability with respect to the mental model of the user approaching them. In fact, with the enormous expansion of the Internet and the introduction of connected features in devices of all kinds, the pool of users who need to use these devices has grown considerably, and with it the different types of technical knowledge base, awareness of cyber risks, and so on. In fact, the difference between novice and expert users, and the need to adapt the interaction process accordingly, has been the subject of recent research in the literature [15]. This diversity of mental models is not reflected in visual platforms, which maintain the same structure and presentation style regardless of the type of user approaching them. Therefore, it is necessary to develop dynamic solutions that ensure adaptability in terms of the information to be displayed and the way in which it is displayed, based on the knowledge level of the end user.

Visual interfaces that adapt to user needs are an emerging area of research aimed at enhancing user experience and performance [16]. These interfaces leverage various inputs and contextual information to tailor the user experience to individual preferences, behaviors, and requirements. Adaptive algorithms within user interface design environments show promise in improving automated design system performance by considering stylistic preferences and flexible success standards [17]. User inputs such as physiological, behavioral, qualitative, or multimodal data are being utilized to adapt visualizations and interfaces, with research trends focusing on mixed reality, physiological computing, visual analytics, and proficiency-aware systems [18]. Logical frameworks using formal knowledge and reasoning components, like Answer Set Programming (ASP), enable the generation of web user interfaces that adapt to user needs, including those of older individuals, by adjusting visual aspects like element sizes and colors [19]. Adaptive interfaces in smart environments can self-improve by observing user behavior, using user modeling algorithms to draw conclusions from user-system interactions, and triggering adaptations through an ontology-based semantic layer [20]. In addition, a range of methods and tools exist for adapting user interfaces to improve accessibility, including built-in adaptation mechanisms within applications and external transformation approaches [21]. To achieve the tailoring we advise for our interfaces, Large Language Models (LLMs) at the base of a conversational agent could provide a valuable medium to perform the assessment of the user's mental model. The use of LLMs instead of more traditional interaction approaches may be able to ensure sufficient dynamism in the assessment phase by formulating questions whose specificity results as a function of the answers obtained to previous questions. Once the type of user has been defined, along with his or her needs and gaps, the subsequent visual platform should display information in accordance with what the user's level of knowledge allows him or her to understand.

In this position paper, we present an overall architecture of an LLM-based conversational agent for human knowledge assessment in conjunction with a dynamically structured visual platform to assist users in analyzing network traffic and the attacks to which they may be susceptible.

2. Related Work

In this section, we present several network data analytics tools presented in the literature whose purposes are to visualize and summarize network traffic through simplified visual metaphors.

One of the pioneering approaches documented in literature is FlowScan [22], which scrutinizes and presents insights from flow data extracted by Internet Protocol routers. It comprises Perl scripts and

modules, serving as the cohesive element integrating various freely available components, including a flow collection engine, a high-performance database, and a visualization tool. Once integrated, the FlowScan system generates graphical images suitable for web pages, offering a continuous, nearly real-time depiction of network traffic across a network's perimeter.

In [12], the authors propose CHRAVAT, a visual platform focused on monitoring network traffic during normal web browsing. The tool tracks incoming and outgoing traffic from the computer and identifies the providers that receive requests made while web pages are loading. Each provider is then represented by a node in a graph, colored differently depending on the type of provider, and populated in real-time, as well as a set of quantitative data showing the number of providers contacted.

Nfsight [23] is a tool aimed at enhancing network awareness with three main features: passive identification of client and server assets, a web interface for querying and visualizing network activity, and a heuristic-based intrusion detection and alerting system. The Service Detector identifies endpoints using heuristics and Bayesian inference from NetFlow flows, while the Intrusion Detector flags suspicious activity with graphlet-based signatures.

NetMod [24] is a tool offering detailed analysis of system performances for designers working on large interconnected local area networks. Tested on a campus-wide network, NetMod employs simple analytical models and a user-friendly interface.

MVSec, as described in [25], is a visual analytics system assisting analysts in comprehending information flows over secure networks. This system facilitates data fusion activities among heterogeneous datasets using various visual metaphors. The authors established multiple coordinated views to enable analysts to characterize loud events, uncover subtle events, and explore relationships within datasets. Case studies demonstrate MVSec's capability in constructing analytical storylines of networking and understanding network changes.

The study by Attipoe *et al.* [26] examined 13 network visualization tools to delineate their strengths and weaknesses. Employing qualitative coding as part of their research methodology, they extracted metrics from the advantages and disadvantages of these tools. Their aim is to aid analysts in constructing evaluation methodologies for measuring visualization tool effectiveness via usability studies.

In [27], Constantinescu *et al.* introduce a prototype 3D visualization system for real-time monitoring of networked devices' status (wired, wireless, IoT devices) and network dynamics ("pulse"), including configuration, load, traffic, abnormal events, and suspicious connections. Users can intuitively visualize network status from any location on the Internet, including mobile devices, and receive alerts via short text or instant messages for significant network events.

Other approaches reviewed in the literature proposed solutions to increase awareness by alerting users to phishing attacks, the type of attack to which end users are more susceptible. For example, the authors in [28] propose the development of a real-time tool to detect and distinguish phishing websites from safe ones using machine learning techniques, mainly linear regression, multinomial NB and logistic regression. The aim is to increase cybersecurity awareness by preventing users from accessing risky URLs and protecting their personal data. [14] introduce an approach for generating warning dialogs in response to phishing attacks. Unlike traditional solutions that simply alert users about the attack, this technique provides explanations concerning why a website is deemed suspicious. The underlying premise is that offering these explanations helps users comprehend the presented information, instills trust in the communicated message, and enhances awareness of the situation.

Although all of the tools discussed in this section provide important support in improving the level of user awareness and knowledge of risks, none of them contemplates the possibility of preemptively assessing the end user's level of knowledge, and subsequently making the decision to adapt the content of the information shown based on the user's assessment, which limits the use of the platforms exclusively to that group of users who can understand them when shown. In the following, we propose the addition of a dynamic assessment module with consequent adaptability of the tools to the user's level of knowledge.

3. Dynamic human knowledge assessment using Large-Language-Models

In this section, we describe the features we envisage in our proposal regarding the introduction of a module that should interpose between the user and the network traffic visualization platform. In our vision, the purpose of this module is to provide a mechanism to dynamically assess the level of basic technical knowledge, i.e., to present the user who approaches it with a series of questions of different natures to determine the level of knowledge he or she has. The dynamic nature of the approach lies in its adaptability to the type of questions asked, based on the answers given by the user. In fact, a series of wrong and/or inaccurate answers is an indication of important lacks in that particular aspect, which is why certain features of the platform need to be removed or simplified to make the user's experience easier. For example, if the user responds "I don't know" or gives an incorrect answer to the question "What is a graph?", this may be sufficient to provide sufficient guidance not to use such a visual metaphor to present such information to the user. However, such an approach runs the risk of reducing the assessment process to a checklist, where a set of questions about a particular concept is associated with a particular answer and an interface adaptation. This poses the danger of oversimplifying the assessment process, potentially resulting in inaccurate evaluations. In fact, to return to the graph example, the user may not even be aware of the term "graph," but he or she may still be able to interpret the visual metaphor correctly. Verifying this possibility is something that can be done if, for example, the user's ability to understand the representation of connected nodes and arcs has been inferred from the previous questions.

For this reason, the knowledge assessment is based on the need for something that is necessarily non-deterministic, and for which the determination of the next question to be asked for the evaluation phase takes into account the direction of the interaction. In this scenario, the use of complex natural language models turns out to be a particularly suitable choice for accomplishing this kind of task. In fact, it may be possible to set up the evaluation phase as a simple conversation between the user and what is essentially an LLM-based conversational agent. Conversational agents powered by LLMs are increasingly sophisticated tools that simulate human-like interactions and support a variety of applications, from language learning to mental well-being. LLMs are used in language learning, acting as virtual teachers or conversational partners to enhance vocabulary, pronunciation, and conversational skills [29]. For instance, fine-tuned LLMs demonstrated the ability to perceive and generate multimodal content, indicating a move towards models that can handle multiple modalities seamlessly [30]. LLMs have been used for conversational interaction with mobile UIs, allowing for language-based mobile interactions without the need for task-specific datasets and models [31]. Moreover, personality traits can be measured and shaped in LLM outputs, which is important for the effectiveness of communication in conversational agents [32]. Finally, in conversational recommender systems, LLMs can provide personalized recommendations and engage in multi-turn dialogues, despite challenges in understanding and controlling complex conversations [33]. To seek our goal, in this manuscript, we will discuss a way to achieve the human knowledge assessment inspired by the type of approach pursued in [32], where the authors used LLMs to conduct an assessment of a user's personal traits. They did this by instructing LLMs through a prompt engineering activity. Subsequently, they pinpointed basic components that specify the behavioral requirements for LLMs to fulfill the given task. In this position paper, we outline the primary components that a prompt should encompass for effective assessment:

- Task Description - Describes the type of analysis to be performed, for example, assessing the level of knowledge of a particular term, assessing the level of awareness of a particular cyber-attack, and so on.
- Target Topic - Indicates the domain of terms, or aspects, on which the assessment is to be carried out.
- Test Instruction - Summarizes the features of which the test is to be composed, particularly the manner in which it is to be administered, the number of questions to be asked, and the manner in which the result of the test administered is to be reported.

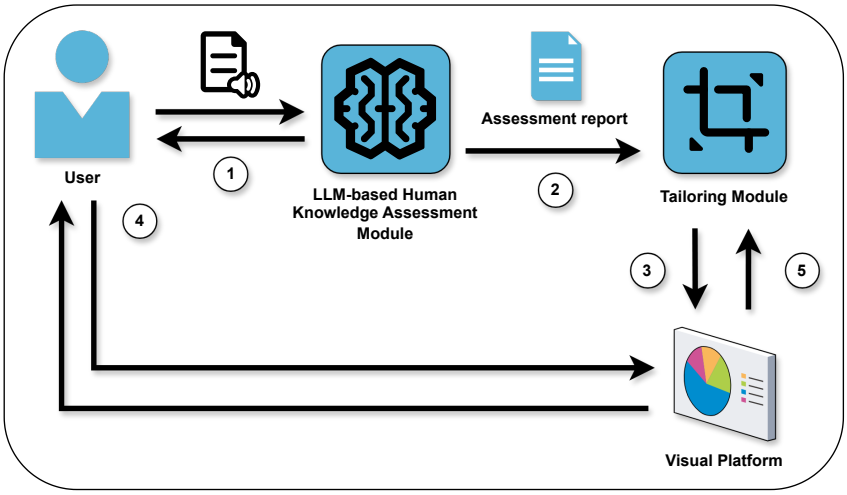

Figure 1: Pipeline of the proposed approach.

In the following, we outline an example of a preliminary engineered prompt for assessing the user's knowledge about graphs as a visual metaphor for a specific task.

> *"Your task is to assess my ability to understand graphs as a medium to represent how packets are transferred between network providers. Ask questions that can become easier or harder according to how I answer each question. After 5 questions, output your decision about my knowledge level."*

An initial analysis of the interaction process resulting from this prompt reveals the LLM's adeptness (in this specific case ChatGPT) in conducting evaluations by posing diverse questions to grasp the potential representations of nodes and arcs in depicting the exchange of network packets between providers.

Figure 1 provides an overview of the pipeline of components engaged in the proposed approach. Initially, the process starts with the assessment phase, wherein an interaction, whether voice or text-based, occurs between the user and the LLM-based Human Knowledge Assessment Module (1). Following the assessment phase, the generated report determining the user's level of knowledge and understanding is transmitted to the Tailoring Module (2), which adapts and refines the interface mechanism of the visual platform based on the insights derived from the report (3). Subsequently, the user gains access to a platform featuring visual elements and interfaces aligned with their comprehension level, fostering a more effective user experience (4). Additionally, we envision ongoing communication between the platform and the tailoring module during the user-platform interaction, enabling further interface modifications based on the user's interactions with the platform (5).

4. Conclusion

In conclusion, our proposal outlines a dynamic approach to assessing users' technical knowledge through an intermediary module that engages users in a conversational evaluation. By leveraging sophisticated language models, such as ChatGPT, this module can adaptively pose questions based on previous user responses, enabling a nuanced understanding of user capabilities beyond mere checklist assessments. This approach aims to enhance user experiences with visualization platforms by tailoring interface adaptations to individual skill levels, ensuring effective and user-friendly interactions. Through prompt engineering activities inspired by prior work in personality assessment, we advocate for thoughtful integration of language models into knowledge assessment processes, fostering more personalized and engaging user interactions in diverse applications.

Acknowledgments

This work has been supported by the Italian Ministry of University and Research (MUR) and by the European Union - NextGenerationEU, under grant PRIN 2022 PNRR "DAMOCLES: Detection And Mitigation Of Cyber attacks that exploit human vuLnerabilitiES" (Grant P2022FXP5B).

References

[1] X. Cai, R. Nithyanand, T. Wang, R. Johnson, I. Goldberg, A systematic approach to developing and evaluating website fingerprinting defenses, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014, pp. 227–238.

[2] J. Hu, C. Lin, X. Li, Relationship privacy leakage in network traffics, in: Proceedings of the 25th International Conference on Computer Communication and Networks (ICCCN), IEEE, 2016, pp. 1–9.

[3] J. L. Hayes, N. H. Brinson, G. J. Bott, C. M. Moeller, The influence of consumer–brand relationship on the personalized advertising privacy calculus in social media, Journal of Interactive Marketing 55 (2021) 16–30.

[4] W. Badewitz, S. Kloker, C. Weinhardt, The data provision game: researching revenue sharing in collaborative data networks, in: Proceedings of the 22nd IEEE Conference on Business Informatics (CBI), volume 1, IEEE, 2020, pp. 191–200.

[5] B. Zhang, N. Wang, H. Jin, Privacy concerns in online recommender systems: influences of control and user data input, in: Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS 2014), 2014, pp. 159–173.

[6] M. R. Faghani, A. Matrawy, C.-H. Lung, A study of trojan propagation in online social networks, in: Proceedings of the 5th International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 2012, pp. 1–5.

[7] A. Roohi, M. Adeel, M. A. Shah, DDoS in IoT: a roadmap towards security & countermeasures, in: Proceedings of the 25th International Conference on Automation and Computing (ICAC), IEEE, 2019, pp. 1–6.

[8] M. De Vivo, E. Carrasco, G. Isern, G. O. De Vivo, A review of port scanning techniques, ACM SIGCOMM Computer Communication Review 29 (1999) 41–48.

[9] A. Karakasiliotis, S. Furnell, M. Papadaki, An assessment of end-user vulnerability to phishing attacks, Journal of Information Warfare 6 (2007) 17–28.

[10] I. Sharafaldin, A. H. Lashkari, A. A. Ghorbani, An evaluation framework for network security visualizations, Computers & Security 84 (2019) 70–92.

[11] T. Zhang, X. Wang, Z. Li, F. Guo, Y. Ma, W. Chen, A survey of network anomaly visualization, Science China Information Sciences 60 (2017) 1–17.

[12] B. Breve, S. Cirillo, D. Desiato, Chravat-chronology awareness visual analytic tool, in: Proceedings of the 23rd International Conference Information Visualisation (IV), IEEE, 2019, pp. 255–260.

[13] B. Breve, G. Desolda, V. Deufemia, F. Greco, M. Matera, An end-user development approach to secure smart environments, in: Proceedings of the International Symposium on End User Development (ISEUD'21), Springer, 2021, pp. 36–52.

[14] G. Desolda, J. Aneke, C. Ardito, R. Lanzilotti, M. F. Costabile, Explanations in warning dialogs to help users defend against phishing attacks, International Journal of Human-Computer Studies 176 (2023) 103056.

[15] B. Breve, G. Desolda, F. Greco, V. Deufemia, Democratizing cybersecurity in smart environments: Investigating the mental models of novices and experts, in: Proceedings of the International Symposium on End User Development (ISEUD'23), Springer, 2023, pp. 145–161.

[16] A. Bunt, C. Conati, J. McGrenere, Supporting interface customization using a mixed-initiative approach, in: Proceedings of the 12th International Conference on Intelligent User Interfaces, 2007, pp. 92–101.

[17] J. Eisenstein, A. Puerta, Adaptation in automated user-interface design, in: Proceedings of the 5th International Conference on Intelligent User Interfaces, 2000, p. 74–81.
[18] F. Chiossi, J. Zagermann, J. Karolus, N. Rodrigues, P. Balestrucci, D. Weiskopf, B. V. Ehinger, T. M. Feuchtner, H. Reiterer, L. L. Chuang, M. Ernst, A. Bulling, S. Mayer, A. Schmidt, Adapting visualizations and interfaces to the user, it - Information Technology 64 (2022) 133 – 143.
[19] J. Zakraoui, W. Zagler, A logical approach to web user interface adaptation, in: A. Holzinger, K.-M. Simonic (Eds.), Information Quality in e-Health, 2011, pp. 645–656.
[20] M. Akazue, B. Ojeme, N. Ogini, User interface adaptability for all users, International Journal of Natural and Applied Sciences 6 (2010).
[21] S. Firmenich, A. Garrido, F. Paternò, G. Rossi, User Interface Adaptation for Accessibility, 2019, pp. 547–568.
[22] D. Plonka, FlowScan: A network traffic flow reporting and visualization tool, in: Proceedings of the 14th Systems Administration Conference (LISA 2000), 2000.
[23] R. Berthier, M. Cukier, M. Hiltunen, D. Kormann, G. Vesonder, D. Sheleheda, Nfsight: netflow-based network awareness tool, in: Proceedings of the 24th International Conference on Large Installation System Administration, USENIX Association, 2010, p. 1–8.
[24] D. W. Bachmann, M. E. Segal, M. M. Srinivasan, T. J. Teorey, Netmod: A design tool for large-scale heterogeneous campus networks, IEEE Journal on Selected Areas in Communications 9 (1991) 15–24.
[25] Y. Zhao, X. Liang, X. Fan, Y. Wang, M. Yang, F. Zhou, Mvsec: multi-perspective and deductive visual analytics on heterogeneous network security data, Journal of Visualization 17 (2014) 181–196.
[26] A. E. Attipoe, J. Yan, C. Turner, D. Richards, Visualization tools for network security, Electronic Imaging 28 (2016) 1–8.
[27] Z. Constantinescu, M. Vlădoiu, G. Moise, Viznet—dynamic visualization of networks and internet of things, in: Proceedings of the 15th RoEduNet Conference: Networking in Education and Research, IEEE, 2016, pp. 1–6.
[28] A. K. Jha, R. Muthalagu, P. M. Pawar, Intelligent phishing website detection using machine learning, Multimedia Tools and Applications 82 (2023) 29431–29456.
[29] F. Xiao, P. Zhao, H. Sha, D. Yang, M. Warschauer, Conversational agents in language learning, Journal of China Computer-Assisted Language Learning (2023).
[30] D. Zhang, S. Li, X. Zhang, J. Zhan, P. Wang, Y. Zhou, X. Qiu, SpeechGPT: Empowering large language models with intrinsic cross-modal conversational abilities, in: H. Bouamor, J. Pino, K. Bali (Eds.), Findings of the Association for Computational Linguistics: EMNLP 2023, 2023, pp. 15757–15773.
[31] B. Wang, G. Li, Y. Li, Enabling conversational interaction with mobile UI using large language models, in: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, CHI '23, 2023.
[32] M. Safdari, G. Serapio-Garcia, C. Crepy, S. Fitz, P. Romero, L. Sun, M. Abdulhai, A. Faust, M. J. Matari'c, Personality traits in large language models, ArXiv abs/2307.00184 (2023). doi:10.48550/arXiv.2307.00184.
[33] L. Friedman, S. Ahuja, D. Allen, Z. Tan, H. Sidahmed, C. Long, J. Xie, G. Schubiner, A. Patel, H. Lara, B. Chu, Z. Chen, M. Tiwari, Leveraging large language models in conversational recommender systems, ArXiv abs/2305.07961 (2023). doi:10.48550/arXiv.2305.07961.