Internet Security Aesthetics: Can internet transparency afford social trust?

Fiona Carroll
Cardiff School of Technologies
Cardiff Metropolitan University
Cardiff, Wales
fcarroll@cardiffmet.ac.uk

Rhyd Lewis
School of Mathematics
Cardiff University
Cardiff, Wales
LewisR9@cardiff.ac.uk

***Abstract*—The internet has made everything convenient. Through the world wide web it has almost single-handily transformed the way we live our lives. In doing so, we have become so fuelled by cravings for fast and cheap web connections that we find it difficult to take in the bigger picture. It is widely documented that we need a safer and more trusting internet, but few know or agree on what this actually means. This paper introduces a new body of research that explores whether there needs to be a fundamental shift in how we design and deliver these online spaces. In detail, the authors suggest the need for an internet security aesthetic that opens up the internet (from end to end) to fully support the people that are using it. Going forward, this research highlights that social trust needs to be a key concern in defining the future value of the internet.**

***Index Terms*—trust, transparency, user centred design (UCD), application layer, internet security aesthetics.**

I. Introduction

Nowadays, a significant part of our lives take place in online environments. The internet has made everything so convenient, that it has almost unconsciously transformed the way we live our lives. In the 1960s, Marshal McLuhan referred to media as an extension of ourselves [1]; in 2022, we certainly rely on the internet for an extension of our capabilities. And it is this reliance that has warped our sense of trust with the internet. The internet uses convenience and offers a false security to earn and then later violate our trust. Despite data breaches, uncertainties about how our data is being used, misinformation, cybercrime and surveillance, we still continue to care little about our safety and privacy when using the internet. It is widely documented that we need a safer and more trusting internet, but few know or agree on what this actually means. This paper introduces a new body of research that focuses on how we need to design the internet to afford trust. The authors feel that, as users, we need to be able to see, understand and focus on the internet in its entirety. We need more transparency and, with that, more trust. This research-in-progress explores how we might rethink the design of the internet to fully support the people that are using it. In particular, it is interested in how we create a trustworthy internet from the network layer to the application layer (i.e. how we tell an end user that they have a trustworthy connection and trustworthy data). The following sections discuss the current internet and trust landscape. They then explore the concept of internet security aesthetics as a way to open up the OSI layers and, in doing so, give a more "felt" experience of internet security.

II. The internet and trustworthiness

Trust is the basis of many human interactions. In particular, social trust has been defined as "perceived honesty, objectivity, consistency, competence and fairness, all of which foster relationships between individuals that must be maintained by the sustained fulfillment of these standards" [2, p.1]. The internet (described as a conglomerate of networks connected through the Internet Protocol with the Web as an information layer on top [3]) needs to maintain this social trust. Indeed, for a network to be qualified as trustworthy, "it needs quality of service that protects user data, ensuring privacy and providing usable and trusted tools to support users in their security management" [4, p.1]. The Open Systems Interconnection (OSI) model – which describes how data is transferred from one device to another – was not designed with security in mind [5]. However, as we spend more and more time online, internet security, and particularly our trust of internet security, can no longer take second place to speed and efficiency. Moreover, "trust needs to span all protocol layers from the IP layer to applications and content" [6, p.1]. Indeed, there needs to be a "trust infrastructure construction technology that enables nodes with mutual trust to autonomously construct trust domains and expand them through domain interworking to block security risks" [7, p.1].

However, as Ali et al. [8, p.402] highlight, "there is no effective way to avoid malicious node attacks". To address this, Cisco have introduced the concept of *zero-trust networking*, which is based on a security model that establishes trust through continuous authentication and monitoring of each network access attempt (in short, the zero-trust philosophy is to *never trust, always verify*) [9]. Some of the "core principles of *zero trust* include verification and continuous monitoring of all communication, as well as encryption of all data in transit and data at rest" [10, p.1]. In addition, NIST [11] is currently working with industry and academia to improve the trustworthiness and applicability of artificial intelligence and machine learning technologies for future networks and distributed systems. To successfully design for trust across the OSI layers, the authors of this paper feel that it is important to understand the value of trust across the internet. Particularly, the *where* and *how* humans and machines need to collaborate to ensure that they can trust one another.

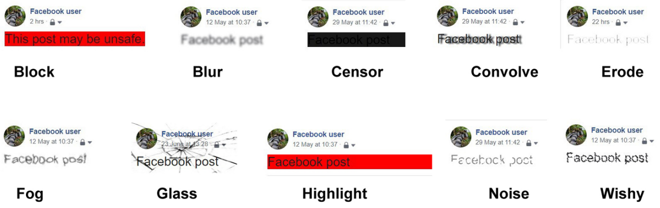
In their paper, Tian et al. [12] note that the future Trustworthy Network needs to include both network behaviour trust and user behaviour trust. When we look at the application layer (the human-computer interaction layer closest to the user), the authors of this paper feel that, in order to be able to find trust, it is important to have a more transparent picture of what happens underneath. In his research, Bauer [13, p.1] promotes an extension to the seven-layer OSI Reference Model to "link applications to human needs as a function of network capabilities". He introduces three HCI layers that can be summarized as: 1) what a user wants to do (i.e., the need), 2) how that need is acted upon by the human, and, 3) the artifacts that the user employs (hardware, software, etc.) [13]. Furthermore, Hesselman et al. [14] believe that improving the internet's transparency, accountability, and controllability is key for users to trust the network.

III. Research in-progress

This research is interested in the development of internet security aesthetics for the application layer (a standard set of warnings and cautions) that will give the end user a deeper and more meaningful insight into the holistic OSI security narrative. In her paper, Strava [15] discusses how security is lived, felt, and perceived through the violences of everyday life. She proposes the "modality of *security aesthetics* as a way to understand how sensory and affective experiences help regulate bodies, spaces, and states in the service of *futureproofing* society against anticipated risks and perils" [15, p.1].

This research builds on previous research [16], [17], [18], [19]. It aims to devise a set of internet security aesthetics that will make the internet experience more transparent to the end user (see fig. 1). Interesting discussions on how graph theory [20] could be enabled to build trust at the network layer has triggered thoughts on how this could be of value and made transparent at the application layer. In our physical world, how do we gauge the trustworthiness of another person? Often, we find it easier to trust someone if they are a friend of a friend. A similar system can be applied to the network layer. By keeping track of what is on a network, and especially the trust relationships between these entities, we can determine what other networks our node is connected to and subsequently the trust value of these connections – high or medium or low. The challenge, from an internet security experience perspective is how we present this to the end user to ensure that they have the means to recognise that a connection or even the data (presented in the application layer) is not a true 'friend'. This research attempts to link the engineering (end to end) of the internet with human needs and, in doing so, aims to advance the research and discussion in the area of the internet, transparency and social trust.

Fig. 1. Example of online warnings for unsafe/ untrustworthy material [18]



Acknowledgment

This research is partially funded by a Global Academy Santander fellowship, Cardiff Metropolitan University.

References

[1] M. Mcluhan and L. H. Lapham, *Understanding Media: The Extensions of Man*. MIT Press, reprint ed., 1994.

[2] J. Boslego, "Engineering social trust," *Harvard International Review*, vol. 27, 2005.

[3] D. van Rooy and J. Bus, "Trust and privacy in the future internet—a research perspective," *Identity in the Information Society*, vol. 3, 2010.

[4] N. Blefari-Melazzi, G. Bianchi, and L. Salgarelli, *Trustworthy Internet*. Springer Publishing Company, Incorporated, 1st ed., 2011.

[5] G. Platsis, "The osi model and you part 7: Stopping threats at the application layer." http//:securityintelligence.com, 2021.

[6] R. Kantola, "Trust networking for beyond 5g and 6g," *2nd 6G Wireless Summit 2020: Gain Edge for the 6G Era, 6G SUMMIT 2020*, 2020.

[7] B. O. Kwak and T. S. Chung, "Design and implementation of trust domain gateway system," *9th International Conference on Information and Communication Technology Convergence: ICT Convergence Powered by Smart Intelligence, ICTC 2018*, 2018.

[8] M. Ali, I. A. A. El-Moghith, M. N. El-Derini, and S. M. Darwish, "Wireless sensor networks routing attacks prevention with blockchain and deep neural network," *Computers, Materials and Continua*, vol. 70, 2022.

[9] Cisco, "What is zero-trust networking?." https://www.cisco.com/c/en/us/solutions/automation/what-is-zero-trust-networking.html zero-trust-explained, 2022.

[10] D. Tyler and T. Viana, "Trust no one? a framework for assisting healthcare organisations in transitioning to a zero-trust network architecture," *Applied Sciences (Switzerland)*, vol. 11, 2021.

[11] NIST, "Trustworthy intelligent networks." https://www.nist.gov/trustworthy-networks, 2022.

[12] L. Tian, C. Lin, and Sunjinxia, "A kind of prediction method of user behaviour for future trustworthy network," *International Conference on Communication Technology Proceedings ICCT*, 2006.

[13] B. Bauer, "A human factors extension to the seven-layer osi reference model ben bauer," *Human Performance*, 2002.

[14] C. Hesselman, P. Grosso, R. Holz, F. Kuipers, J. H. Xue, M. Jonker, J. de Ruiter, A. Sperotto, R. van Rijswijk-Deij, G. C. Moura, A. Pras, and C. de Laat, "A responsible internet to increase trust in the digital world," *Journal of Network and Systems Management*, vol. 28, 2020.

[15] C. Strava, "Futureproof: security aesthetics and the management of life," *Social Anthropology*, vol. 29, 2021.

[16] F. Carroll, P. Legg, and B. Bonkel, "The visual design of network data to enhance cyber security awareness of the everyday internet user," *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020*, 2020.

[17] F. Carroll, A. Chakof, and P. Legg, "What makes for effective visualisation in cyber situational awareness for non-expert users?," *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2019*, 2019.

[18] F. Carroll and B. Bonkel, "Designing for affective warnings cautions to protect against online misinformation threats," 2021.

[19] F. Carroll, *Usable Security and Aesthetics: Designing for Engaging Online Security Warnings and Cautions to Optimise User Security Whilst Affording Ease of Use*. New York, NY, USA: Association for Computing Machinery, 2021.

[20] R. Lewis, *A Guide to Graph Colouring*. Springer, Cham, 2nd ed., 2021.