The Visual Design of Network Data to Enhance Cyber Security Awareness of the Everyday Internet User

[1]Fiona Carroll*, [2]Phil Legg and [1]Bastian Bønkel
[1]School of Technologies, Cardiff Metropolitan University
[2]Department of Computer Science and Creative Technologies, University of the West of England

***Abstract*—Technology and the use of online services are very prevalent across much of our everyday lives. As our digital interactions continue to grow, there is a need to improve public awareness of the risks to our personal online privacy and security. Designing for cyber security awareness has never been so important. In this work, we consider people's current impressions towards their privacy and security online. We also explore how abnormal network activity data can be visually conveyed to afford a heightened cyber security awareness. In detail, the paper documents the different effects of visual variables in an edge and node DoS visualisation to depict abnormally high volumes of traffic. The results from two studies show that people are generally becoming more concerned about their privacy and security online. Moreover, we have found that the more focus based visual techniques (i.e. blur) and geometry-based techniques (i.e. jaggedness and sketchiness) afford stronger impressions of uncertainty from abnormally high volumes of network traffic. In terms of security, these impressions and feelings alert in the end-user that something is not quite as it should be and hence develop a heightened cyber security awareness.**

I. Introduction

The cyber security market is thriving on the development of new specialist's technological protection such as event management and monitoring mechanisms for a safe and secure cyberspace (e.g. SIEMs, ELK, SPLUNK, Sguil, Elsa, Squert etc.). These tools are designed mainly for network administrators and engineers to monitor a network, diagnose an anomaly, troubleshoot an issue etc and are generally of no interest to the every day end user. However, as the advancement of the internet continues to create significant changes to our everyday lives (i.e. technology has an impact on everything we do), we believe it is important to make the everyday person more aware of what is going on when they exist and interact online. By the everyday person, we mean the ordinary person in society rather than the elite network or technology expert. Indeed, the everyday person needs to start to care more about what is happening to them and their data whilst online. As our digital footprints grow exponentially, designing for privacy and security online has never been so important. In this instance, information security is often considered as maintaining confidentiality, integrity, and availability to the end-user [1]. Information privacy has a much broader scope, and refers to the desire of individuals to control or have some influence over data about themselves [2], including how their information is collected, used and disclosed to others. In this sense, privacy is very much related to security. As Cranor & Garfinkel [3] point out you can build very secure systems that enhance privacy. The question we ask is whether we can design systems to enable the end-user to maintain awareness of their own privacy and security online? Can we build 'supports' to allow the everyday user to take more informed control of their lives online?

This work considers the visual design of network data and how this could potentially support the every day user in making decisions around their privacy and security online. For example, Kinkeldey et al. [4] highlight that communicating information about data uncertainty has the potential to increase trust in the results and also to support decision making. Endlsey [5] talks about situation awareness (SA) as being a critical foundation for successful decision-making across a broad range of situations. She broke SA into three segments: perception of the elements in the environment, comprehension of the situation, and projection of future status [5]. In line with this, the work presented in this paper is the first of a series of studies that will investigate the concepts of privacy and security in an online environment and/or situation. It will explore the visual design of network data as a means to afford impressions of uncertainty and in doing so, change the way the everyday user thinks and makes decisions around their personal security online. The paper is organized as follows. Section 2 presents a discussion on what we mean by abnormality/ uncertainty in data visualisation. Section 3 documents two studies and their main findings. Section 4 summarises the main outcomes and challenges of the work. Finally, section 5 reviews future investigations and concludes the paper.

II. Abnormality, Uncertainty and Visual Variables

One of the most challenging aspects of data visualization is the visualization of uncertainty. For a visualization to successfully communicate uncertainty, the designer must 1) recognize the value of uncertainty information for receivers of their messages, and 2) identify effective ways to communicate it [6]. That done, it is important to then note that there are different forms of uncertainty with different consequences for behaviour and learning and also the processing of uncertainty highly depends on situation and context [7]. When it comes to the internet and network data, the volume, velocity and variety of data available can be massive. As a result, large-scale networks have become increasingly challenging to manage and in terms of security awareness and monitoring, network administrators face the difficult task of continuously checking their networks for abnormal behaviour and suspicious activities. Like in the business world, abnormal activity can be closely linked to uncertainty (e.g. abnormal trading volume around earnings announcement periods increases with the level of market uncertainty [8]). Indeed, uncertainties in network data can impact the network administrators and how they reason and understand the analytical outputs. As Griethe and Heidrun [9] highlight there could be errors in measuring and/or logging devices or simulation runs, statistical variations, unavoidable or for performance reasons intended losses in the transformation or even in the presentation of the data. Uncertainty 'arises from both an imperfect understanding of the rare events and processes, and the imperfect, out-of-date, and incomplete data that one must work with in order to try and understand these events and processes' [10, p.1].

In terms of cyber security awareness of the everyday person, this paper focuses on how we might design for abnormal network behaviour; the authors feel that communicating the uncertainty caused by abnormal network activity could improve judgements and decisions made whilst online. Kinkeldey et al. [4] describe uncertainty visualisation approaches using three main dichotomies: coincident/adjacent; intrinsic/extrinsic; and static/dynamic. Intrinsic techniques alter the existing symbology to represent uncertainty, basically through manipulation of visual variables, e.g. colour value [4]. We feel that visualising the uncertainty caused by a network's abnormal behaviour has the potential to inform the security decisions made not only by the network administrator but also by the everyday user. As research indicates displaying uncertainty has the power to improve trust and decision-making in everyday contexts [11]; an enhanced network visualization - focusing on the representation of uncertainty - could be used to support the confirmation of analytical facts whilst also help to discover yet unknown abnormalities within the raw data. By better understanding how people cognitively work with uncertainty in the knowledge-construction and decision-making process, it could be possible to better direct the efforts to represent uncertainty in network visualisations. [10].

A network can be defined as a set of nodes that are connected by a set of edges [12]. Decker at al. [13] highlight three entities on the network in which uncertainty may exist in various forms: nodes (actors on the network), edges (connections between nodes), and subnets. He points out that nodes have a variety of categorical (e.g. type), discrete (number of users or peripherals), and continuous variables (bandwidth, trust, et al.) and similarly, edges have categorical properties such as connection (existence) and communication protocols used [13]. Our previous works have explored how non-expert users use visualisation techniques for examining home networking traffic [14], and also how networking traffic can be visually mapped to familiar concepts for non-experts, such as a cityscape, to encourage inspection of network activity for improve situational awareness at home [15]. In this research (study 2), we extend on this work to focus on the network edges and in particular how the PCAP data is mapped to the visual designs of the edge to allow us to not only represent the amount of traffic travelling along that connection but also in doing so, to afford uncertainty about the incoming traffic to indicate activities of interest. Indeed, network and network traffic data is complex but visualizing uncertainties in network data can provide valuable insight into the network activity and what could actually be happening. Uncertainty has been described to include statistical variations or spread, errors and differences (i.e. minimum maximum range values), noisy or missing data [16]. In itself, data can be inherently uncertain, due to error, noise or unreliable sources [17]. However, when network activity is abnormal, it is critically important that analysis tools, including information visualization tools, make users aware of the presence, nature, and degree of abnormality and hence uncertainty about the data as these factors can greatly impact decision-making around network security [18]. In fact, as data is pre-processed, transformed, and mapped to a visual representation, this uncertainty can be compounded and propagated, making it difficult to preserve the quality of data along the reasoning process [17].

The National Institute of Standards and Technology (NIST) wrote a standards report in 1994 which identified two categories of uncertainty according to the method used to estimate their numerical values, these two categories included those which are evaluated by statistical methods and those which are evaluated by other means [19]. Olston and Mackinlay [18] advocate that to convey this *statistical* uncertainty, it is appropriate to display the most likely value along with error bars or other glyphs and then to convey what they call *bounded* uncertainty, they advocate a systematic technique based on widening the boundaries and positions of graphical elements and rendering the uncertain region in fuzzy ink. Boukhelifa et al. [20] go on to show that some variables are considered more intuitive for visualising uncertainty, they provide an easier reading of uncertainty. Indeed, visual variables such as size, colour (colour saturation), value, texture, focus, blur are all aesthetic features that have been used to depict uncertainty. As MacEachren [21] details size and value are the most appropriate for depicting uncertainty in numerical information, while color (hue), shape, and perhaps orientation can be used for uncertainty in nominal information. As Brown [22] notes blurring has the most immediate and intuitive mapping to uncertainty, as it simulates the visual percept caused by an incorrectly focused visual system. Needless to say, the task of including the additional uncertainty information into an existing or new visualization while maintaining ease of comprehension for both the data and the uncertainty is not easy [23].

III. Study 1 and 2

Visualising uncertainty has been described as one of the most challenging aspects of data visualization (i.e.there is still not a comprehensive understanding of the parameters that influence successful uncertainty visualization [24]). However, one thing is sure and that is the fact that decision-making is improved from understanding the uncertainty in the data and information being used [25]. That includes decision outcomes, correctness of decisions, kinds of errors made, decision time, confidence in a decision, willingness to make a decision, how much workload decision- making causes and finally how a decision is made [25]. This research is divided in two parts; Study 1, explores people's thoughts and feelings on their own online privacy and security and how it might be improved. Study 2 explores the visual design of a Network Denial of Service (DoS) attack (using an edge and node structure) to afford uncertainty amongst participants. Denial of Service (DoS) attack or Distributed Denial of Service (DDoS) attack is a type of network attack that attempts to make a target computer unavailable to the intended users on the Internet (i.e. by overwhelming it with large amounts of traffic that it is unable to handle) and research highlights that human monitoring and analysis is crucial because the attacks have grown increasingly more sophisticated [26]. This study focuses on the visual design of the edge in the visualisation (i.e. visual variables are used to represent the abnormal high volume of traffic being sent by a node) and in doing so, the aim is to afford an uncertainty amongst participants.

A. Study 1

This is a preliminary study with the specific goal to explore student's perceptions, opinions and attitudes towards online privacy and security. It took place at Cardiffmet University in spring 2019 and aims to give some initial insight into individuals' understanding of their personal privacy and security online and how they might improve it. Seventeen master students (six female and ten male participants) from computing backgrounds between the ages of 18-45 years completed the study. The study took approximately fifteen minutes in duration. The experimental procedure was approved by the Ethics Board of School of Technologies, Cardiffmet and subjects provided written consent for study participation and the academic use of de-identified data.

1) Data Collection: The study was conducted using the Qualtrics online survey software. Participants were presented with a series of sixteen questions. To detail, questions such as the following were asked: ***What do you understand by internet privacy?***, ***How concerned are you about exposing yourself to potential risks?***, ***In your opinion, what type of data do websites/ online organisations collect about you?*** The study also collected data on participants descriptions of ***what they think their user profile would be (i.e. who the machine thinks you are)?***. Finally, participants were were asked to rate the importance of... ***to protect online personal privacy?***, ***that online activity is safe and secure***, ***to know how my devices communicate online***, ***to have control over how my devices communicate online***.

2) Findings: When asked ***What do you understand by internet privacy?*** The responses were interesting in that they were generally based around data and keeping it safe: it is about ensuring that 'the information and data we transmit over the network is safe' and that 'consumer sensitive data that should not be shared'. Participants aligned their understanding of 'internet privacy' very much around their own personal data, that is was about 'keeping my information safe', 'personal information should be secured' and 'Keeping my own personal data, and especially social media posts private or limited to the domain I want. Keep things private and secure for the purposes I intend and no other use'. They saw it as their own personal right 'your right to maintain your privacy at all time whenever you access platforms on the internet'. Other participants started to question the ownership of the data and went as far as saying 'You have right to access your information but if put your information online, it is no longer your property. This is on the internet forever'. The thinking started to move to the notion that they themselves might be the reason why their privacy is being compromised as they themselves are putting the information online 'if someone can see my information which have been put online by myself'; one participant addressed the need for 'authorised access to resources on the internet'.

Moreover, fifteen of the participants clearly stated that they did not think that their data was safe online. When asked ***In your opinion, what type of data do websites/ online organisations collect about you?*** The findings show that participants felt that a range of personal data was collected: 'everything they can, type from websites e.g. shopping online, education categories etc.)'. This included personal information (i.e. names, ages, addresses, mobile numbers, friends) to shopping records to 'habits, related info, personal details, likes, wants, needs, recent searches, contact relationships... Limitless'. A few participants mentioned the generation of user profiles and the collection of data from their search and browsing histories to enable organisations with enough data to build a 'profile of my online habits and interests'. When asked what they thought their user profile would be (i.e. who the machine thinks they are)? One participant confidently shared 'Music lover, tech and social enterprise enthusiasts, Podcasts and software Engineer, sneaker head', another imagined a profile like 'Reckless money spender, and information seeker'. What is clear is that all participants felt it would be an amalgamation of all their data, it would 'Reflect of my activities, things I like', it would be a 'Set of personal data and private information as if am a product'. One participant simply said 'human'.

3) Conclusion: From the findings, it is clear that participants are concerned about their online privacy, however, there is an underlying sense that not everyone knows how they might take control of their privacy online. When questioned if they would consider a privacy/ security monitor that they could use to check their network for malicious behaviour, ten participants (including two participants with a maybe) would consider it.

The question we ask is: 'Are these online experiences designed effectively to make people care about/ take control of their privacy?' The next study will explore the visual design of a DoS attack to afford uncertainty amongst participants as a way of heightening their cyber security awareness.

B. Study 2

This study will explore how visual variables (i.e. sketchiness, blur, tone and others) can be used in the visualization of DoS attacks to communicate uncertainty amongst participants. This a type of security threat was chosen purely for its capacity to have a big impact on the online experience of the end user. The DoS attack has the potential to exhaust online resources and thereby, violating the availability (one of the security components) of the online experience for the end-user (something the end-user has very little knowledge or awareness of). The study took place at Cardiffmet University in the autumn of 2019. Thirty undergraduate students (one female, twenty-nine male participants) from computing backgrounds between the ages of 18-35 years completed the study. The study took approximately thirty minutes in duration.

1) Experimental Design: To create these visualisations (see fig 1-7), a SYN Flood pcap file was generated in Kali Linux using Hping3, TCPdump and Wireshark. Hping3 was used to produce the packet data (i.e. it sent 30,000 packets of syn requests with a different false IP Address for each one), TCPdump was used to capture the traffic and then Wireshark was used to inspect the PCAP file. The DoS attack lasts for a minute and a half of normal browsing, thirty-forty seconds of flooding, followed by a minute or so of normal browsing. Approximately 30,000 different hosts are simulated, however they only send a single packet each. This has been condensed in the visualisation to ten hosts (including the victim host, regular hosts and attacking host/s). The amount of data that each host is sending is represented through a visual variable on the edge in the visualisations. For example in the blur visual variable, the regular host communication (regular traffic) is solid whilst the attacking host communication (excessive amounts of traffic) is blurred etc. To achieve this, a python script is used to extract the data from the PCAP files, for the regular hosts it groups the data by two second intervals whilst for the attacking hosts the data is grouped in intervals of one microsecond. Presently, the length and positioning of each host is random, except for the middle one (the victim host).

D3.js is used to visualise the differences between the regular traffic, and excessive amounts of traffic. The focus of this study is on exploring participant's perceptions of the visual variables (i.e. blur, hue, jagged edges, tone, saturation, scale and sketch) within the context of the DoS attack. We are particularly interested in exploring if these visual variables afford any feelings of uncertainty amongst the participants. We group these visual variables into three main categories: (1) color-based techniques that manipulate hue, saturation, or tone dimensions; (2) focus based techniques that modify contour crispness, transparency, or resolution (i.e.blur) ; and (3) geometry-based techniques that distort line marks by applying a rendering style as in jaggedness and sketchiness.

2) Results: When asked ***In terms of the lines/links/edges between the nodes (circles), what is your first impression of this DoS visualisation? (note: the green node is the targeted node).***

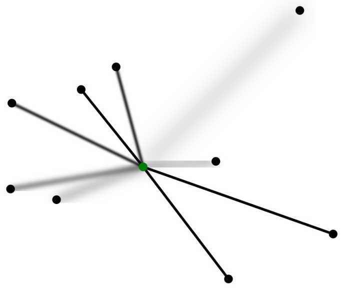


Fig. 1. DoS visualisation using the blur visual variable

The findings show different impressions towards the different visual variables and hence visualisations. For the blur visual variable visualisation (see fig.1), participants were clearly aware of differences in the edges, 'I feel like some of the attacks are not as strong as the links are wider' and 'Some of the links are coming from different distances away from the target'. One participant felt that the blurred lines 'shows that something is being overwhelmed'. Other participants were not sure what was happening, they sensed an uncertainty, 'poorly design the link. don't really understand what is happening' and 'initially unsure of what the graphic is trying to represent but eventually understanding the vary strengths it's trying to signify'. In the Hue visualisation (see fig.2), it seems that participants were feeling slightly more confused. They were 'confused by all the colours', that it was 'Too colourful'. One participant noted the strong colours as 'strong attacks on the green node' whilst others felt that the colours represented groups of people 'It shows different groups are attacking the victim', 'The different coloured connections are different people trying to DoS but within the same group'. Finally, one

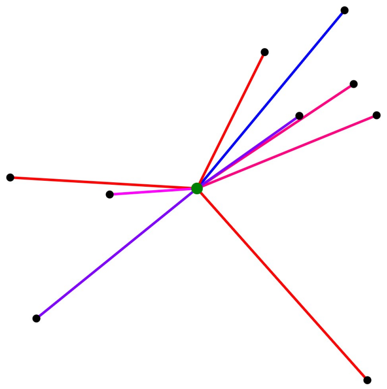


Fig. 2. DoS visualisation using the hue visual variable

participant felt the 'different colours indicate different levels of traffic'.

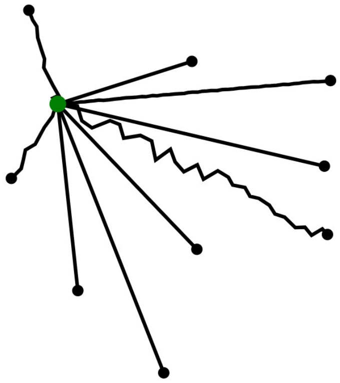


Fig. 3. DoS visualisation using the jagged visual variable

Interestingly, in the jagged visualisation (see fig.3), participants started to dig a little deeper (i.e. probe their understanding a little further): 'I think the attack is coming from one side', another participant felt that 'Some take alternative routes before getting to the targeted node', then another thought it was 'Multiple strong connections but different attack styles'. Needless to say, there were a few that sensed 'The scruffier lines look more menacing than the straighter lines' and 'the more ridged the line, more traffic is being transmitted'.

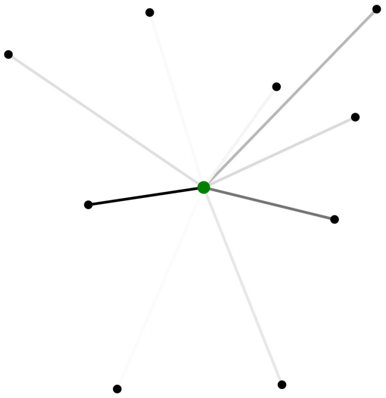


Fig. 4. DoS visualisation using the tone visual variable

For the Tone visualisation (see fig.4), participants felt that the 'darker lines really 'pop' and stand out, the white do not'. As a result it was interesting to see that some participants correlated the lighter tones of colour with weaker attacks and visa versa. 'I can see the different lines and that they are a different shade. Im assuming that the darker the shade the more powerful the attack is', 'The darkest ones are sending the most data'. It was clear from the findings that participants felt that 'Links have different strengths' and that they could see that 'This attempt there is many weak connections', that the tone 'shows strength'. However, contrarily to the design intentions, they seemed to feel that the darker lines had the most traffic.

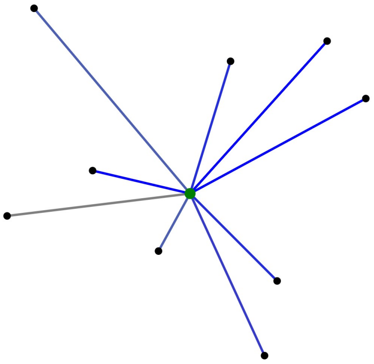


Fig. 5. DoS visualisation using the saturation visual variable

Again, in the Saturation visualisation (see fig.5), participants started to equate the different colours with different styles of attack, that 'multiple connections with different colours indicates different attack styles', 'The nodes are using different methods to attack the victim'. One participant clearly noted that 'The links are different' however, the general consensus is that the visualisation is not clear, it 'looks complicated and all strong' and 'Very basic, no labelling to tell the viewer what is happening (direction of lines)'. One participant had no idea what was going on. In contrast, participants who experienced the scale visualisation (see fig.6), clearly felt that 'some of the attacks are weaker and less direct than others', that there was 'a mixed level of different attacks due to the sizes of lines', that there 'might be the big group and other groups attacking the victim' and 'Different nodes can deliver varying amounts of traffic to the target'. In terms of the design, one participant highlighted that 'One node is different to the rest' however, another participant felt it was 'Not a good way to display the "amount" of data flowing through connections, overlapping lines is bad design'.

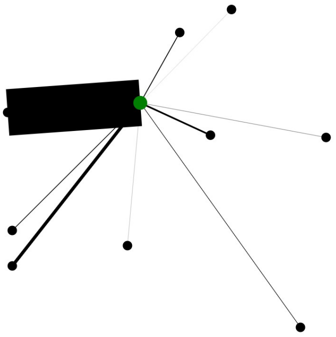


Fig. 6. DoS visualisation using the scale visual variable

Finally, in the sketch visualisation (see fig.7), one participant confidently noted that 'the more ridged the links, the more traffic is being sent from the node', another felt it was 'a bit

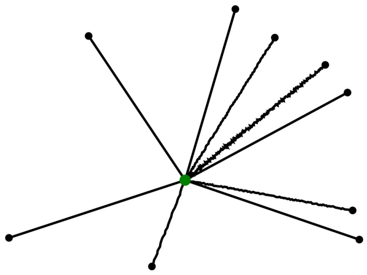


Fig. 7. DoS visualisation using the sketch visual variable

confusing, but you understand it after looking at it for a while, the 'scruffier' lines make the attack look more malicious'. Others felt that 'The links may be sent from different machines using different methods', that 'This shows that some are more powerful than others' and 'I feel like some of the links are weaker than others'.

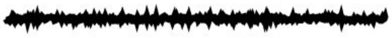


Fig. 8. Edge with high level of sketch

Fig. 9. Edge with no level of sketch

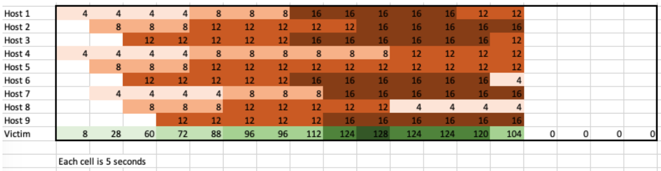
3) Conclusion: According to French [27], stochastic, epistemological and analytical uncertainties can be addressed by modelling, data analysis and drawing in scientific and other expertise. However, ambiguities and value uncertainties are of a different character, they reflect not uncertainty in the world out there, but uncertainty about ourselves [27].This study has allowed us to identify what impressions the participants were nurturing after experiencing the DoS visualisations. More importantly, it has given us some insight into what actual visual variables triggered more deeper thoughts and feelings around the DoS attack. As we have seen uncertainty comes in many different forms, from the findings, we can see that that the hue and saturation visualisations seemed to confuse and obscure the story that the visualisation is trying to tell more so than the other visualisations. The colours are ambiguous and depending on the participant, they are affording thoughts around different groups of people, different attack styles and different attack methods as well as different levels of traffic. This is seen to create a negative effect amongst participants in that the increase in vagueness brings with it individual confusion (i.e. no clear impression about what the visual variable represents). Whilst the scale, tone, sketch and jagged visualisations offered a slightly more direct analytical sense of difference. For example, participants looking at these visualisation clearly identified that the edges were different and generally, equated them to weak and/ or stronger links. In terms of affording uncertainty, the context/description of the DoS attack (provided to the participant) helped to link the visual variable/ edge more closely with an abnormal activity. When asked to rank the visualisations in order of their ability to show/ represent uncertainty on the network edge/ link and to warn of danger on the network? More participants chose the sketch visualisation than the other visualisations. Also when asked to rate the level of sketchiness in terms of uncertainty, thirteen participants felt that the high sketch 'edge' visualisation (see fig 8) had a strong level on uncertainty. Whilst in the fig. 9, only three participants thought it had a strong sense of uncertainty. Also, the findings from the question referring to how informed and/or uniformed they felt after the sketch visualisation shows that ten participants felt more informed, fifteen participants were neutral.

IV. Summary

This research has highlighted that generally people are becoming more concerned about their privacy and security online. However, as the participant sample for this study 1 were from computer science backgrounds, we would hope that this would be the case. The findings from study 2 are more convincing in that we have started to determine the different effects of visual variables in an edge and node DoS visualisation to depict high volumes of traffic and hence uncertainty. For example, participants found the more colour-based techniques particularly those that manipulated hue and saturation more difficult to decipher. Participants couldn't quite work out what the colours represented, they were uncertain about what was being displayed and hence the ambiguity resulted in confusion. For the more focus based techniques (i.e. blur) and geometry-based techniques (i.e. jaggedness and sketchiness), participants seemed more confidant in eliciting certain understandings which in turn engaged and guided them into a clearer mode of thinking and feeling around the volume of traffic on the edges. For example, the blurred edges gave many participants a feeling that some edges were stronger than others. Similarly, in the sketchiness and jagged visualisations, they felt that they were experiencing more menacing edges. These visualisations were clearly more effective in conveying the uncertainty that was present within the data to the participant. The next phase of work proposes to further investigate how we design for uncertainty, manipulating visual variables to make the end-user more aware that there is something a miss with their privacy and security online.

V. Further investigation

In terms of providing a thorough rendition what actually happens during a DoS attack, it could be argued that the visualisation designs used in study 2 have been a little inconclusive in that they have looked solely at the edge and node network structure to depict heightened volumes of traffic. The temporal aspect of the transaction has currently not been designed for. For example, the design represented in fig. 10, has started to tease out a more in-depth understanding of what is actually happening during the DoS attack. Each host is a row and the victim is a row. Each cell is five seconds and the visual variable colour is related to the number of packets sent per second. In this design, we can see which nodes are contributing most towards the DoS on the victim, and also the overall amount of traffic hitting the victim within a set time-frame. This visualisation combines the visual variable with the number value (i.e. exploring both analytic and intuitive understandings), however, it would be interesting to further test this format of visualization focusing solely on the visual variable. In detail, how a subjective appreciation of a visual variable can feed into and impact on one's interpretation and understanding of the DoS attack. Also how it might extend the visualisation to highlight the available throughput remaining on the victim to show that a DoS has impacted them.



Host 1	4	4	4	4	8	8	8	16	16	16	16	16	12	12				
Host 2		8	8	8	12	12	12	12	12	16	16	16	16	16				
Host 3			12	12	12	12	12	16	16	16	16	16	16	12				
Host 4	4	4	4	4	8	8	8	8	8	8	12	12	12	12				
Host 5		8	8	8	12	12	12	12	12	12	12	12	12	12				
Host 6			12	12	12	12	12	16	16	16	16	16	16	4				
Host 7		4	4	4	4	8	8	8	16	16	16	16	16	16				
Host 8			8	8	8	12	12	12	12	12	4	4	4	4				
Host 9				12	12	12	12	12	16	16	16	16	16	16				
Victim	8	28	60	72	88	96	96	112	124	128	124	124	120	104	0	0	0	0

Each cell is 5 seconds

Fig. 10. Example visualisation looking at volume of activity for individual hosts on a network over time

Moreover, it would be interesting to expand how these visual variables can be further designed to relate more intuitively to uncertainty. In the context of this study, we correlated the high volume of traffic with the feeling of uncertainty around the edge. However, streaming a movie from Netflix involves a high volume of traffic from one host, yet, there is little uncertainty as we understand the context of why there is traffic. In different contexts, the characteristic that matches to uncertainty could be very different (i.e. a transmission that suddenly had a gap, or some thing was missing).

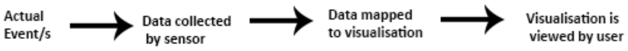


Fig. 11. Sources of uncertainty in the visualisation process

The next steps will be to explore the concept of uncertainty in more detail, as we can see from fig. 11 each arrow introduces a potential source of uncertainty. The challenge will be in how we can aesthetically manipulate the visual variables to fully instil in us an uncertainty about what has happened along each phase of the development of the visualisation.

References

[1] M. E. Whitman and H. J. Mattord, *Principles of information security*. Cengage Learning, 2011.

[2] F. Bélanger and R. E. Crossler, "Privacy in the digital age: A review of information privacy research in information systems," *MIS Q.*, vol. 35, p. 1017–1042, Dec. 2011.

[3] F. Cranor and S. Garfinkel, *Security and Usability: Designing secure systems that people can use*. USA: O'Reilly, 2005.

[4] C. Kinkeldey, A. MacEachren, and J. Schiewe, "How to assess visual communication of uncertainty? a systematic review of geospatial uncertainty visualisation user studies," *The Cartographic Journal*, vol. 51, no. 4, pp. 372–386, 2014.

[5] M. Endsley, "Toward a theory of situation awareness in dynamic systems. human factors journal 37(1), 32-64," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, pp. 32–64, 03 1995.

[6] J. Hullman, "Why Authors Don't Visualize Uncertainty," *IEEE Transactions on Visualization and Computer Graphics*, 2020.

[7] K. Preuschoff, P. Mohr, and M. Hsu, "Decision making under uncertainty," *Frontiers in neuroscience*, vol. 7, p. 218, 11 2013.

[8] H. M. Choi, "Market uncertainty and trading volume around earnings announcements," *Finance Research Letters*, vol. 30, pp. 14 – 22, 2019.

[9] H. Griethe and H. Schumann, "Visualizing uncertainty for improved decision making," in *Proceedings of the 4th International Conference on Business Informatics Research (BIR)*, 2005.

[10] M. Harrower, "Representing uncertainty: Does it help people make better decisions?," tech. rep., University Consortium for Geographic Information Science, Geospatial Visualization and Knowledge Discovery Workshop White Paper, 2003.

[11] M. Kay, T. Kola, J. R. Hullman, and S. A. Munson, "When (ish) is my bus? User-centered visualizations of uncertainty in everyday, mobile predictive systems," in *Conference on Human Factors in Computing Systems - Proceedings*, 2016.

[12] D. R. Farine and A. Strandburg-Peshkin, "Estimating uncertainty and reliability of social network data using Bayesian inference," *Royal Society Open Science*, 2015.

[13] J. W. Decker, M. A. Livingston, S. Russell, and P. Hyden, "Use Cases for Visualizing Uncertain Computer Networks," tech. rep., 2011.

[14] P. A. Legg, "Enhancing cyber situation awareness for non-expert users using visual analytics," in *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, 2016.

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

[16] A. T. Pang, C. M. Wittenbrink, and S. K. Lodha, "Approaches to uncertainty visualization," *Visual Computer*, vol. 13, no. 8, pp. 370–390, 1997.

[17] C. D. Correa, Y. H. Chan, and M. Kwan-Liu, "A framework for uncertainty-aware visual analytics," in *VAST 09 - IEEE Symposium on Visual Analytics Science and Technology, Proceedings*, 2009.

[18] C. Olston and J. D. Mackinlay, "Visualizing data with bounded uncertainty," in *Proceedings - IEEE Symposium on Information Visualization, INFO VIS*, 2002.

[19] B. N. Taylor and C. E. Kuyatt, "NIST Technical Note 1297 1994 Edition, Guidelines for Evaluating and Expressing the Uncertainty of NIST Measurement Results," *National Institute of Standards and Technology*, 1994.

[20] N. Boukhelifa, A. Bezerianos, T. Isenberg, and J. D. Fekete, "Evaluating sketchiness as a visual variable for the depiction of qualitative uncertainty," *IEEE Transactions on Visualization and Computer Graphics*, 2012.

[21] A. M. MacEachren, "Visualizing Uncertain Information," *Cartographic Perspectives*, 1992.

[22] R. Brown, "Animated visual vibrations as an uncertainty visualisation technique," in *Proceedings GRAPHITE 2004 - 2nd International Conference on Computer Graphics and Interactive Techniques in Australasia and Southeast Asia*, 2004.

[23] T. Zuk and S. Carpendale, "Theoretical analysis of uncertainty visualizations," in *Visualization and Data Analysis*, 2006.

[24] M. Riveiro, T. Helldin, G. Falkman, and M. Lebram, "Effects of visualizing uncertainty on decision-making in a target identification scenario," *Computers & Graphics*, vol. 41, 06 2014.

[25] J. Kleineberg Polina Levontin Jo Lindsay Walton, "A Publication of the Analysis Under Uncertainty for Decision Makers Network," tech. rep., 2019.

[26] A. Shrestha, Y. Zhu, and K. Manandhar, "NetTimeView: Applying spatio-temporal data visualization techniques to DDoS attack analysis," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014.

[27] K. Roelich and J. Giesekam, "Decision making under uncertainty in climate change mitigation: introducing multiple actor motivations, agency and influence," *Climate Policy*, vol. 19, no. 2, pp. 175–188, 2019.