Something Doesn't Feel Right: Using Thermal Warnings to Improve User Security Awareness

Daniela Napoli, Sebastian Navas Chaparro, Sonia Chiasson, Elizabeth Stobert
Carleton University
daniela.napoli@carleton.ca

Abstract

Embodied cognition proposes that people's understanding of the world cannot be separated from their environment and physical senses. In that vein, we explore a novel technique for encouraging increased security awareness through thermal notifications. In this paper, we present our system called NoViz-Thermal and discuss our initial assessments within the context of communicating the security of TLS certificates. In general, we uncover accessibility and usability issues but hypothesize that the thermal stimulation could increase users' confidence and ease while making security assessments. Moreover, thermal warnings could address current limitations in the accessibility of visual-based security warnings and constrained user interfaces of display-less IoT technology.

1 Introduction

It can be difficult to communicate security information to users in a clear and persuasive manner. Much effort in addressing these issues, and identifying ways to encourage security awareness, has focused on adjusting the look and feel of text- and image-based warnings. We propose that by engaging users' bodily senses other than sight we can uncover novel opportunities to improve security awareness and warning adherence.

To explore the potential of non-visual security warnings, we built a thermal notification system which adjusts temperature per the TLS certificate associated with a website. Compared to visual warnings alone, our objectives are to: (1) improve users' accuracy in detecting secure websites, confidence, and ease in making security assessments, and (2) encourage users to spend additional time making better security assessments by gazing at trustworthy security indicators such as lock icons, and warning dialogues.

We assess our proposed methods through a user study and heuristic evaluation. Our findings suggest that the thermal notification system could aid users in assessing website security. We discuss methods of improving the prototype and evaluation techniques to better assess the impact of thermal security warnings.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Boston, MA, USA.

2 Background

While browsing the internet, users are provided a variety of security advice [14] including being told to use reputable software and to be critical of links and downloadable content. Yet, studies [4,8] suggest that users tend to focus on unreliable non-technical indicators such as page content and logos which can be easily spoofed. Other security information dialogues, such as warnings about the lack of TLS certificates, indicating limited data encryption or web host trustworthiness, can help guide users to more secure behaviour. Providing such information is more likely to reduce unsafe behaviours [12] if the information is clear and comprehensible. However, despite advances in the clarity of visual security warnings, users continue to miss security threats [15], suggesting that security warnings have room for improvement.

2.1 Current State of Security Warnings

We describe three areas where visual security warnings are problematic or insufficient.

Users have become fatigued by visual warnings [3] and conditioned to ignore or dismiss warnings [5]. To encourage users to pay attention to security warnings, usable security researchers have suggested dynamic skins [8], full-page warnings [10], and jiggling or colour-changing warnings [6].

Users with visual impairments, due to temporary or permanent effects such as screen-glare, age, or disability, are

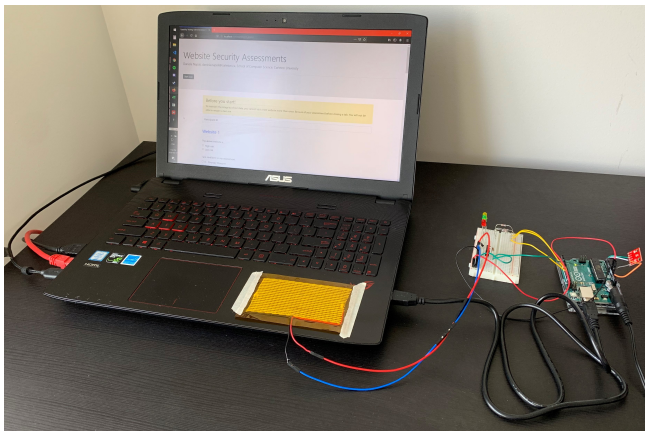

Figure 1: The thermal notification system includes a heating pad affixed to an area on the laptop chassis where the user's wrists naturally rest during use.

placed at a disadvantage while assessing their state of security and privacy [1, 2] with current visualizations. Security cues that provide more than vision-based information can better integrate usability and accessibility principles and serve as more equitable solutions.

Non-visual security warnings, such as our proposed thermal system, could help users when dealing with display-less interfaces. Smart home devices such as virtual assistants, smart lights, and smart locks are becoming increasingly popular. These devices can have security problems resulting from usability issues posed by display-less interfaces. The lack of displays on these devices makes it difficult for users to monitor their devices and remediate potential security breaches [7].

Some interfaces use audio cues, either on their own or as supplemental cues to gain users' attention. While useful in some circumstances, these also have drawbacks. Used individually, audio cues would also exclude some portion of the population who are unable to hear either due to physical impairments or environmental circumstances. Audio cues may also draw attention from nearby individuals, which could be disruptive or could lead to privacy violations for the user.

2.2 Embodied Cognition

Non-visual security warnings could address issues relating to the current state of security warnings. We propose leveraging other bodily senses can be effective means to improving user's security awareness and adherence to warnings due to the effects physical intervention can have on a user's cognition.

Embodied cognition [17] suggests that people's thoughts and actions are influenced by their interactions with their tools and surroundings. Some claims of embodied cognition such as *symbolic off-loading*, and the *distribution of cognition across mind and environment* are of particular relevance to security warnings.

TLS Certificate	Risk	Max Temperature
None	High	30°C / 86°F
Domain Validated (DV)	Medium	25°C / 77°F
Extended Validation (EV)	Low	20°C / 68°F

Table 1: The heating pad changes temperatures according to a website's TLS certificate, denoting various levels of security risk.

Symbolic off-loading refers to the act of involving external stimuli to store and manipulate details of a situation. This behaviour can aid in understanding and formulating solutions for problems. A classic example is counting on our fingers for simple math.

Off-loading techniques are effective under the assumption that our mind and body are equally important when understanding data and making decisions. Embodied cognition hinges on the concept that a cognitive system is defined by the relationships between its aggregate elements, thus users' thoughts and actions cannot be defined without the context of the environment in which they take place. Therefore, changes in environment can result in changes to security thoughts and actions. Security warnings that physically impact users could increase security awareness and encourage users to make more secure decisions.

In related research, Wilson, Maxwell and Just [16] explored users' associations between temperature and various states of security. For Wilson et al.'s study, participants interacted with two Peltier thermal stimulators and selected a temperature between 20°C and 38°C to physically represent the state of security of provided websites. In their study, higher temperatures were most often associated with insecure websites because participants tended to associate higher temperatures with offline heat related dangers like fire.

3 NoViz-Thermal Notification System

The NoViz-Thermal[1] was inspired by Wilson et al.'s [16] work. To leverage users' tendencies to associate heat with web threats, we built a thermal notification system that can assess website TLS certificates and communicate security states to a user through various temperatures. Our system, shown in Figure 1, includes a heating pad affixed to the chassis of a laptop near the trackpad and keyboard where users naturally rest their hands while using their computer. In this position, thermal notifications can be communicated to a user in an readily available and unobtrusive manner.

[1] Available at www.github.com/danielanapoli/thermaltrackpad

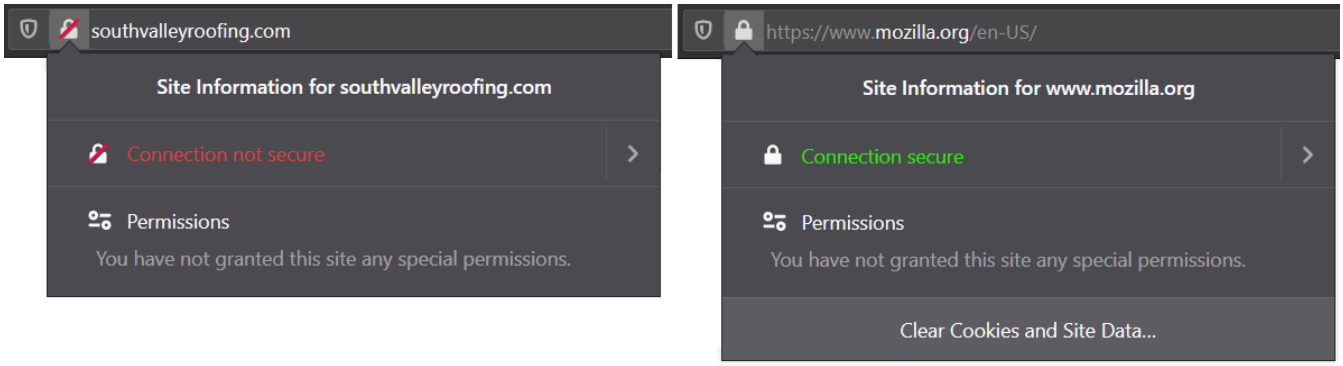

Figure 2: Visual security warnings in Mozilla Firefox 75.0 which accompany our thermal notifications.

3.1 Hardware

Our main hardware includes an Arduino Uno Rev3 circuit board, a 5cm x 10cm heating pad, a TMP102 breakout temperature sensor, and an N-Channel MOSFET. The heating pad is composed of woven conductive fiber and is powered by an external 7-volt power adapter to reach warm temperatures. We use a breakout temperature sensor to monitor the heating pad, and the MOSFET to control the electrical current to the heating pad including stopping current if the pad approaches harmful temperatures. The system has three coloured LEDs which turn on depending on the temperature of the prototype. These LEDs are affixed to the prototype's breadboard and are not visible to users during testing; rather they were intended to help researchers monitor the heating pad during testing. For this early iteration, we affixed the heating pad to the laptop chassis with tape. Future iterations should include a more robust method for mounting the heating pad to avoid situations where users unintentionally move the pad during use.

As we will discuss in Section 4.1, the role of an adequate heat sink is crucial for a thermal notification system such as ours. Our initial prototype did not include sufficient means to reduce residual heat. In our next iteration of the prototype, we will consider other actuators and encasing materials to better address this limitation.

3.2 Software

We programmed the heating pad to change temperatures depending on the type of TLS certificate held by a website. We created a Mozilla Firefox browser extension to detect the security certificate associated with a visited website and communicated this data to the Arduino board controlling the heating pad.

As shown in Table 1, we considered three potential risk scenarios including: (1) **high risk**, HTTP-only websites where data is not encrypted and web hosts are not vetted by a certificate authority (CA); (2) **medium risk** websites with a domain validated (DV) certificate, where data is encrypted during transmission but hosts can acquire the certificates from a CA regardless of their identity; and, (3) **low risk** websites with an extended validation (EV) certificate where data is encrypted and hosts receive more scrutiny by CAs before being issued certificates. In our prototype, the heating pad has three distinct temperature settings. Temperatures are warmest when visiting high risk websites and incrementally cool until it reaches room temperature for low risk websites.

We use the `webRequest` API to collect certificate information upon receiving HTTP headers from a website. This data is sent to our server via a XMLHTTPRequest object. The server sends a signal to the Arduino to control the heating pad's temperature depending on the type of certificate.

As shown in Figure 2, Firefox also shows security warnings depending on TLS information. Specifically, the lock icon in the URL address bar and the security dialogue vary to suggest whether the connection to the website is secure or insecure. Firefox uses only two levels of risk: the lock icon and security dialogue are the same for DV and EV certificates. The different risk between these two certificates is only demonstrated through the temperature changes in our thermal notification system.

4 Initial Assessments

As an initial gauge of the thermal notification system, we piloted a user study[2] and conducted an expert evaluation. In these initial assessments, we explored the role of thermal stimulation when visiting high and low risk websites. Due to issues with the breakout temperature sensor, we did not include medium risk sites.

We used Censys [9] to survey public EV certificates and formulated a list of websites which involve risk-related transactions such as providing login credentials or personally-identifiable information. We chose English-language sites with minimal use of security-related

[2]Further user testing was halted due to the COVID-19 pandemic.

keywords for testing. For websites without a certificate, we searched Censys' database for invalid TLS certificates and supplemented that list with further internet searches for HTTP-only websites.

Pilot study: One participant was asked to assess the security of six (3 high risk, 3 low risk) websites presented in random order on a laptop equipped with the thermal notification system. They were told the heating pad would get warmer on insecure websites. Before starting, the participant completed the SA-6 [11] questionnaire to help us gauge initial security awareness. Then, the participant viewed each website and reported whether the site was high or low risk based on their security assessment. They also rated whether they were confident in their assessment and found the task easy to complete based on a 5-point Likert scale ranging from 0 (strongly disagree) to 4 (strongly agree). Additionally, we timed each task from when the participant clicked the hyperlink to when they submitted their assessment.

Expert evaluation: The lead researcher visited the same websites and walked through the process of assessing website security with the thermal notification system. During the walkthrough, they identified issues which contradict accessible and usable security heuristics [13].

4.1 Results

Pilot study: Prior to completing tasks, the participant scored an average of 3.67 ($SD = 0.47$) on the SA-6 suggesting that they are somewhat attentive and engaged with security measures. During the tasks, the participant correctly identified the risk level for 4 out of 6 websites. In their responses, they identified all but one website as low risk. However, the participant spent more time assessing high risk websites ($M = 199.5sec, SD = 87.0$) than assessing low risk websites ($M = 150.5sec, SD = 62.9$) and reported higher confidence ratings after assessing high risk websites ($M = 2.5, SD = 0.5$) than low risk websites ($M = 1.5, SD = 0.5$). Our data is too limited to draw any conclusions however, these preliminary findings suggest that, compared to the low risk condition with no heat applied, the thermal stimulation may: (1) improve a user's confidence in assessing the security of websites, and (2) encourage a user to spend additional time when drawing conclusions about websites.

After the study, the participant mentioned they forgot about the heating pad and instead focused their assessments on webpage content, URL addresses, and Firefox's security dialogue. Their impression of the thermal feedback was consistent with Wilson et al.'s [16] findings: "If I felt something hot on my computer, I would think something was wrong with it." However, ultimately, they were not inclined to consciously integrate the thermal notification system in their assessments. Issues we uncovered in our expert evaluation may partially explain the lack of adoption.

Expert evaluation: During the expert evaluation, we uncovered some highly severe accessibility and usability issues. The first major issue pertains to a lack of reliability. When switching from a insecure website to a secure website, the heating pad retained some residual heat. If the heating pad is consistently warm regardless of website security, this could lead to users perceiving the system's assessment of the website as flawed or untrustworthy, and this is likely why the participant eventually ignored the thermal indicator.

The second major issue pertains to lack of feedback. Warm computers are often a sign of a system malfunction. Although our participant was aware that the premise of the prototype was to warm up with insecure settings, there is no evident relationship in the interface between the heating pad's temperature and Firefox's security warnings, thus there is little reminding the user that the thermal indicator is a security warning. Without proper feedback, as we observed during our pilot study, users may still consider an insecure website as low risk despite the warmth of the heating pad.

5 Discussion and Conclusion

Based on the premise that physical interactions can change cognition and behaviours, we built and tested NoViz-Thermal to augment or replace traditional visual security warnings. There is much room for improving our prototype; however, as users continue to off-load security information to trusted indicators and warnings, we remain hopeful that future prototypes will serve as an extra security cue which can be used either consciously or subconsciously.

While we continue to improve our thermal notification system, we will explore other opportunities for non-visual security warnings such as haptic cues and force-feedback. We will also explore the role of non-visual security warnings in other contexts such as indicating whether a system has been compromised by malware or is not properly configured for optimal security.

We will conduct further usability testing with users, and compare the effectiveness of our prototypes to existing visual warnings. Additionally, with user interviews, we can better understand the role of non-visual stimulation within the context of users' security mental models and behaviours.

Acknowledgments

The authors acknowledge funding from Natural Sciences and Engineering Research Council of Canada (NSERC) through the Canada Graduate Scholarships Doctoral program (Napoli), Discovery Grant program (Chiasson, Stobert), and Canada Research Chair program (Chiasson).

References

[1] A. Abdolrahmani and R. Kuber. Should I trust it when I cannot see it? Credibility assessment for blind web users. In *SIGACCESS Conference on Computers and Accessibility*, pages 191–199. ACM, 2016.

[2] T. Ahmed, R. Hoyle, K. Connelly, D. Crandall, and A. Kapadia. Privacy concerns and behaviors of people with visual impairments. In *Conference on Human Factors in Computing Systems (CHI)*, pages 3523–3532. ACM, 2015.

[3] D. Akhawe and A. P. Felt. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *Security Symposium*, pages 257–272. USENIX, 2013.

[4] M. Alsharnouby, F. Alaca, and S. Chiasson. Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82:69 – 82, 2015.

[5] B. Anderson, T. Vance, B. Kirwan, D. Eargle, and S. Howard. Users aren't (necessarily) lazy: Using neurois to explain habituation to security warnings. 2014.

[6] B. B. Anderson, C. B. Kirwan, J. L. Jenkins, D. Eargle, S. Howard, and A. Vance. How polymorphic warnings reduce habituation in the brain: Insights from an fmri study. In *Conference on Human Factors in Computing Systems (CHI)*, pages 2883–2892. ACM, 2015.

[7] C. Bellman and P. C van Oorschot. Analysis, implications, and challenges of an evolving consumer iot security landscape. In *International Conference on Privacy, Security and Trust (PST)*, pages 1–7. IEEE, 2019.

[8] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Conference on Human Factors in Computing Systems (CHI)*, page 581–590, New York, NY, USA, 2006. ACM.

[9] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman. A search engine backed by internet-wide scanning. In *SIGSAC Conference on Computer and Communications Security*, page 542–553. ACM, 2015.

[10] S. Egelman, L. F. Cranor, and J. Hong. You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Conference on Human Factors in Computing Systems (CHI)*, page 1065–1074, New York, NY, USA, 2008. ACM.

[11] C. Faklaris, L. A. Dabbish, and J. I. Hong. A self-report measure of end-user security attitudes (sa-6). In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2019.

[12] A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S Thyagaraja, A. Bettes, H. Harris, and J. Grimes. Improving SSL warnings: Comprehension and adherence. In *Conference on Human Factors in Computing Systems (CHI)*, page 2893–2902. Association for Computing Machinery, 2015.

[13] D. Napoli. Developing accessible and usable security (ACCUS) heuristics. In *Conference on Human Factors in Computing Systems (Extended Abstracts)*. ACM, 2018.

[14] R. W. Reeder, I. Ion, and S. Consolvo. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security Privacy*, 15(5):55–64, 2017.

[15] M. Stojmenović, E. Spero, T. Oyelowo, and R. Biddle. Website identity notification: Testing the simplest thing that could possibly work. In *International Conference on Privacy, Security and Trust (PST)*, pages 1–7, 2019.

[16] G. Wilson, H. Maxwell, and M. Just. Everything's cool: Extending security warnings with thermal feedback. In *Conference on Human Factors in Computing Systems (Extended Abstracts)*, page 2232–2239. ACM, 2017.

[17] M. Wilson. Six views of embodied cognition. *Psychonomic Bulletin & Review*, 9(4):625–636, 2002.