Poster abstract: Characterizing Digital Homelessness

Matt Comi
University of Kansas

Walter Goettlich
University of Kansas

Jacob Marshall
University of Kansas

Sarah Smith
University of Kansas

Jon Volden
University of Kansas

Perry Alexander
University of Kansas

Drew Davidson
University of Kansas

William Staples
University of Kansas

Abstract

Many social and economic expectations of modern society assume that individuals own a personal computer. When this expectation is not met, individuals must rely on shared, public computers, such as those offered at public libraries to meet these expectations. Numerous inequalities stem from this reliance, both in the suitability of the public computer for social and economic expectations, and in threats to the security and privacy of exclusively- or primarily-public computer users.

To identify and characterize these inequalities, we completed a one year study in multiple libraries to characterize the experiences of public-access internet users. We observed that those users who relied on public access computers because they lacked dedicated, internet enabled home computers faced intersecting and compounding inequalities stemming from the absence of a digital 'home'. Similarly, while access to library computers is important, their current operation does not provide the social function of a personal computer and thereby disadvantage users reliant on these systems. In light of these similarities, we suggest the term *digital homelessness* to describe the state of relying primarily or exclusively on public computers. Those experiencing digital homelessness are frequently not accounted for in software design, both for regular utilities and for security and privacy tools. Thus, although a complete answer to digital homelessness requires a multifaceted approach, several of the important problems can be addressed with technical solutions.

The primary goal of our work is to characterize and highlight the unique security and privacy disadvantages by those experiencing digital homelessness, in the hopes of initiating a field of study on mitigating those disadvantages. To that end, one of the main contributions of this work is to articulate the threats that the user population is particular exposed to, and to which the population is particularly concerned about. We hope these findings serve as a framework for security and privacy research in the area.

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

1 Introduction

Many of the mechanisms used to defend the security and privacy of web users rely on a simple assumption: that the user of the system has their own device upon which to deploy that mechanism. In many cases, this assumption is valid; users either administer their own personal device (such as a smartphone, laptop, or home desktop workstation) or are the exclusive user of a machine administered by another (either a workplace IT department, family member, etc). Unfortunately, this model does not account for a population at particular risk of certain kinds of privacy invasions: those users who do not have a computing platform of their own, but instead rely upon public, multi-user systems such as library computers.

On one hand, those who rely exclusively or primarily on library computers lack the resources to avail themselves of many traditional defense mechanisms: even simple browser preferences such as the "Do Not Track" header [1], ad-blockers and cookie preferences become onerous to use when they must be re-configured each time a user begins a session at a public computer. If the default security posture of the public computer does not meet their preferences, the user may also need to reconfigure the machine. Similarly, the threat of password-stealing via shoulder surfing is especially pronounced in a public venue, but the availability of password managers or other auto-fill solutions is limited by the very nature of the venue. Our work identifies these problems, in the hope that future solutions consider the various problems of this space in their design. We are particularly concerned with securing the data and functionality by considering the unique security challenges in this domain.

Although all of the factors of this domain cannot be ad-

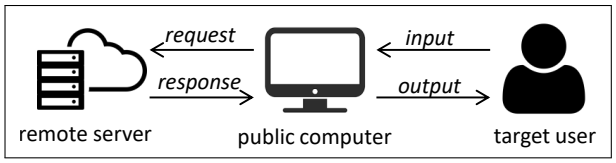

Figure 1: The basic interaction points at which an adversary might attack. The local observer snoops upon the input relation between the user and the local computer (i.e., shoulder surfing the user's keystrokes. The remote network-based attacker can insert content into web responses, including JavaScript that may profile the user or perform other privacy-invasive behaviors against the user.

dressed by technical solutions, those that can are shaped by the characteristics of the public computer facility, equipment, users, administrators, and potential adversaries. In order to better understand the nature of digital homelessness, we interviewed 39 participants at three sites throughout Northeastern Kansas: the Lawrence Public Library, the main branch of the Kansas City, Kansas public library system, and the west branch of the Kansas City, Kansas public library system.

Our participants included staff and patrons of these sites using participant observation and interview techniques [6, 9]. We present findings that are particularly relevant to security and privacy in Section 2, and then general usability and other high-level findings in Section 3. We present recommendations for future work in Section 4.

2 Security and Privacy Concerns

We identify two different types of attackers that are particularly relevant to this domain. While these adversaries are not novel, they pose a marked threat in this context because users cannot avail themselves to traditional defenses. Many study respondents also voiced concern about these attacks.

Local observer attackers: A commonly-cited best practice for good security is to only use a trusted device for security and privacy-sensitive operations, and to only do so in an environment where all physically present parties are trusted. However, this option is simply unavailable to users that do not have access to such a device and environment. In our interactions, public library patrons cited a number of concerns due to the public nature of the computers, and the context in which they are used. Thus, one of the key threat models for the public computer user is the existence of a local observer adversary. Although an adversary of this form in not novel to our work, many of the existing mechanisms to defend against the threats do not apply. As noted above, the user cannot simply wait until they are in private to perform a sensitive task. The main attack vector for the local observer adversary is shoulder surfing the keyboard: the observer simply notes the keystrokes that the user is making when entering a password, thus stealing credentials for later use.

Adversarial Capabilities: The major capability of the local observer adversary is the ability to see what the user is typing on their keyboard. We note that the most likely way for the adversary to accomplish this attack is through shoulder surfing. We expect that the adversary will not be able to mount a sustained attack, as doing so may arouse suspicion.

Adversarial Goals: We consider the adversary to only be interested in credential stealing via shoulder surfing the user's keystrokes.

Network-based attackers: The second type of adversary that we consider is remote to the public computer. The network-based attacker may represent a hacker who effects a data breach against a server for a service to which the user subscribes. The network-based attacker may also represent a less overtly malicious actor who harvests a profile of the user for the purpose of data collection. This adversary represents a threat to the user's privacy, either through the creation of a profile with the express intention of violating the user's privacy, or indirectly by the creation of a profile that might be sold to a 3rd party or unintentionally leaked through a compromise. Additionally, we also consider the adversary to be capable of maintaining short-term state on the host operating system's browser.

Adversarial Capabilities This adversary is meant to capture the threat of a privacy-invasive third-party, often realized in practice as a 3rd-party advertiser. As such, we assume that the adversary can place an advertisement into the web content visited by the exclusively-public computer user.

Adversarial Goals The adversary's goal is to build an accurate, personalized profile of the user's activities, preferences, behaviors, and characteristics. This adversary's behavior is representative of an advertiser or online merchant in the most legitimate case, but may also be representative of a more nefarious actor depending on how the profile is leveraged.

The major categories of attack described above exist in contexts outside of our focus of study, but are particularly relevant within it: users of public computers are particularly defenseless against these adversaries because of their circumstances. Because they are in a public environment by definition, it is more difficult to be aware of shoulder surfing attacks in progress. Because the user does not have administrator privileges, many of the best-practice security tools and configuration options are not available. For example, the user may wish to use a browser with a more aggressive privacy stance, such as the browser Brave, which considers user privacy a first-order principle [2, 7]. Similarly, privacy focused utilities such as anti-tracking and ad-blocking mechanisms can close down attack vectors [8]. However, these tools may not be available to the user. If users do have privileges to install unconstrained software, they need to be wary that a previous user may have installed malware on the machine that they are now using (inadvertently or not).

Putting aside issues of user privilege, the first-time setup

required to install and configure privacy-preserving utilities is significant. The user is likely required to tweak browser settings, deploy extensions, etc. Here, the assumption of persistence is in full force: for a privacy-conscious user, this cost is a one-time affair. For the user of a public computer, they are required to begin each work session by re-installing and re-configuring every relevant tool. Thus, the latter user must incur a per-session cost that creates a significant disadvantage for security and privacy. This disadvantage manifests itself particularly strongly for users who lack the patience or expertise to quickly and repeatedly set up the tools, meaning they are likely to forego their use entirely.

The public computer itself plays the role of both threat vector and possible victim. The former role exists because another user may have misconfigured the security settings or (perhaps accidentally) infected the machine with malware, thus adversely affecting the security of the user. The latter role exists because the public computer may begin the session in a benign state, and the legitimate user who we are trying to serve may inadvertently infect or misconfigure the machine.

Administration: We were also interested in the role that site administrators play as an element of concern to patrons. Overall, patrons placed significant trust in library staff. Staff reported that users would freely give sensitive security credentials such as credit card numbers and authentication information to staff. Additionally, staff are responsible for administration of machines to prevent the actions of patrons from affecting one others security. All of the sites that we surveyed use *reboot to restore* software, such as Faronics Deep Freeze, which allows the public computer's software platform to be checkpointed at a clean state and restored between logins [5]. Several patrons reported data loss as a result of rollback to checkpoints, and many patrons indicated the need to take extra steps to maintain working data, such as using USB keys.

3 Other Findings

In this section, we describe some of the high-level findings of our user study. These factors are of interest in a general sense, but also as a guide for particular usability constraints in this space.

Motivation and use cases: While public access computer use is driven by a swath of motivations, we are primarily concerned with users who rely on public access computers out of necessity: namely the lack of reliable access to a computer or broadband internet. Many patrons reported having financial limitations or experiencing (traditional) homelessness as a reason. Several patrons cited outdated or broken hardware, and an inability to administer a private computer. A majority of our patron interviewees indicated that they currently or formerly had used library computers for employment-related purposes. Users noted that job applications often required resumes to be formatted using Microsoft Word, and many noted that employment-related activities are not suitable to the small screens and available applications for mobile devices.

Many users had engaged in financially-sensitive activities. These activities included searching for local giveaways, garage sales, and buying/selling items on online marketplaces. Several used the library to view pay stubs or find and apply for public assistance benefits such as SNAP, social security, or VA benefits. One patron used the public computers to manage an online shop. Several of the patrons who experienced significant financial disadvantage used the public computers to complete online surveys for a small monetary reward.

Exclusively-public computer users also used public facilities for hobbies, self-help, and advancing job training or education. The latter included completing coursework, improving GED scores, and applying for academic financial aid. Patrons also used the machines for entertainment and social networking.

Technical expertise: Another set of key findings of our user study involves the degree of technical expertise held by subjects of our user studies. We gathered qualitative data based on self-assessment on the part of patrons and general impressions of average patrons on the part of staff. Many participants (patrons and staff alike) noticed that patrons were uncomfortable with security and privacy concepts, and in some cases basic operation of the public computer. One staff member interviewed noted that patrons "Don't even understand the difference between right and left clicking". Staff also mentioned numerous frustrating experiences with patrons, including experiences in which a patron "didn't know anything about computers, didn't care" and that "it's really frustrating how many times I have to tell [patrons] the exact same stuff". Our participant observations also revealed a low level of technical expertise.

Many patrons reporting using poor password hygiene, since remembering a long list of hardened passwords requires significant cognitive effort. Users would instead report using common variations on the same password, writing down passwords on notes that they carried to the public computer, or reusing passwords.

Design lessons learned: We discovered a number of key design constraints for improving the security and privacy of primarily-public computer users. One of our first observations is that users require familiar, entry-level software tools. We found that users were uncomfortable learning technologies that were unfamiliar, even to the extent of being unwilling to use alternative word processing tools such as browser-based suites such as Google Docs. Instead, users expressed significant preference for the Windows operating system and the Microsoft Office Suite, since these were tools to which they had most commonly been exposed.

Another observation of our study is that meeting the needs of our target population requires keeping low barriers to beginning and ending a work session. Fundamentally, many of the assumptions of "typical" personal computer use rely on

two key properties: *personalization* and *persistence*. We use personalization to broadly refer to a user's ability to customize his or her computing experience; the user should be able to install the programs necessary to fulfill the task at hand and to configure these tools to the extent available to a personal computer user. We use persistence to broadly refer to the ability of a user to maintain data, both in the form of personalization preferences and data processed as part of the work that they are doing. We believe these two properties account for the main pain points for users.

4 Future Work

User and administrator education: We believe that a long-term effort to introduce users to free tools that may have a steeper learning curve may improve outcomes for primarily-public computer users.

Reduced trust in the Operating System: As discussed in Section 2, we assume a semi-trusted host system, whereby malicious user-mode processes or browser configurations may be present. Ultimately, we feel that the unique threat models of the exclusively-public computer user provide an interesting use case for trusted hardware, or software-based isolation.

Novel Systems: We believe that our findings concerning persistence and personalization motivate new technical solutions that can allow users to maintain state. Indeed, the greatest element of dissatisfaction of our patron participants was a lack of persistence, even in the context of basic usability. However, granting persistent state to public computer users must not interfere with other patrons. Furthermore, a single, standardized computing environment cannot meet the privacy stances of various users. As such, novel systems in this domain cannot rely on a static pre-configuration.

5 Related Work

Although different in terms of technical approaches, a recent line of work has emerged that focuses on the specific needs of vulnerable user populations. Chen et al.focused on the role that technology plays in a human trafficking survivor's recovery [3]. This work specifically focused on technical considerations for victim service providers. Havron et al.considered the role of computer security specifically for victims of intimate partner violence [4]. Although our work targets a different (though potentially overlapping) population of disadvantaged users, we are motivated by previous work such as this to address the needs of specific populations who may have unique computing threats and needs. In contrast to these two particular papers, our solution focuses primarily on addressing the needs of our target population through a new computing platform.

Adherence to Ethical Standards

We acknowledge that all studies involving human subjects were conducted by properly trained individuals and in accordance with applicable university institutional review boards and standards.

References

[1] Do not track: A universal third-party web tracking opt out, March 2011. https://tools.ietf.org/html/draft-mayer-do-not-track-00.

[2] Brave Browser. Fingerprint protection mode, 2017.

[3] Christine Chen, Nicola Dell, and Franziska Roesner. Computer security and privacy in the interactions between victim service providers and human trafficking survivors. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pages 89–104, 2019.

[4] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. Clinical computer security for victims of intimate partner violence. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 105–122, Santa Clara, CA, August 2019. USENIX Association.

[5] Dale L Lunsford. Virtualization technologies in information systems education. *Journal of Information Systems Education*, 20(3):339, 2009.

[6] Janice M Morse. Mixing qualitative methods, 2009.

[7] J Newman. Mozilla co-founder's ad-blocking brave browser will pay you bitcoin to see safe ads. *PC World*, 2016.

[8] Rishab Nithyanand, Sheharbano Khattak, Mobin Javed, Narseo Vallina-Rodriguez, Marjan Falahrastegar, Julia E Powles, Emiliano De Cristofaro, Hamed Haddadi, and Steven J Murdoch. Adblocking and counter blocking: A slice of the arms race. In *6th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 16)*, 2016.

[9] John Van Maanen. *Tales of the field: On writing ethnography*. University of Chicago Press, 2011.