Exploring Website Location as a Security Indicator

Der-Yeuan Yu, Elizabeth Stobert, David Basin, and Srdjan Capkun
Department of Computer Science, ETH Zurich

***Abstract*—Authenticating websites is an ongoing problem for users. Recent proposals have suggested strengthening current server authentication methods by incorporating website location as a comprehensible additional trust factor. In this work, we explore users' acceptance of location information and how it affects decision-making for security and privacy. We conducted a series of qualitative interviews to learn how location can be integrated into users' decision-making for security, and we designed a security indicator to alert the user to changes in website locations. We evaluated our tool in a 44-participant user study and found that users were less likely to perform security-sensitive tasks when alerted to location changes. Our results suggest that website location can be used as an effective indicator for users' security assessments.**

I. Introduction

Users' increasing reliance on the Internet for critical services, such as banking, data storage, and communication, highlights the importance of data security and privacy. However, users can currently do little to ascertain whether their security is ensured and their privacy is respected by online services.

Users' trust in websites is strongly tied to the problem of server authentication, which is currently achieved using public key certificates and browser security warnings. Unfortunately, research has found that users frequently ignore or bypass related warnings, exposing themselves to online threats [4], [5], [34]. Users also often fail to notice or understand certificate information [33], [13], which has been partly addressed with improved interface design [15], [14], [35], [31].

Recent research on strengthening server authentication has proposed using the servers geographic location as an additional trust factor [2], [39]. These proposals integrate web server location into the TLS protocol to increase the security of server authentication, but they require the user to assess and decide whether these locations are trustworthy in situations where the protocol fails (similar to current implementations of certificates). Although there are techniques to display information about server locations, it remains unexplored how such information should be presented and how users would react to it when they make security decisions.

In this paper, we explore users' decision-making processes regarding their security when they are provided with the location information of websites. Our goal is to better understand how the proposed website localization techniques will affect users. Using a user-centered design approach, we gathered requirements, designed a location indicator, and evaluated its usability and effect on security decision making.

We conducted semi-structured interviews with 15 participants and applied thematic analysis to identify issues relevant to online trust. Based on our themes, we developed a model to describe the factors in users' trust and analyzed the role of website locations in their decisions. We found that users' perceptions of online security and web authenticity are often intermixed with their concerns about privacy. Our participants often assessed their security on a conceptual level by gauging their risks in terms of financial security and personal privacy. We also found that participants, while describing various trust concerns about their online security, expressed preferences for particular locations when dealing with sensitive information or transactions. These findings suggest that the website location is a tangible concept and such knowledge affects users' security decisions.

Based on the qualitative analysis, we derived requirements for a location tool to inform users of website locations. We designed and implemented LocationWatch, a Chrome extension that makes website locations available to users and alerts them to changes in server locations. Using LocationWatch, we conducted a user study with 44 participants to analyze how website locations affect their security decisions. Our statistical analysis showed that participants' decisions were significantly affected by website locations, with fewer users completing sensitive tasks when the website location had changed. The participants' decisions also varied depending on the sensitivity of data in different application scenarios.

The effects of website location knowledge on users' decision-making processes have not been investigated until now. With recent proposals for strengthening authentication using website locations, it is important to evaluate how this information is perceived by users and how it can be best leveraged in their decision-making processes. Our results show that users are sensitive to website locations when informed in a non-intrusive way. This shows the promise of using location information as an additional factor to improve user security and privacy.

II. Background

Current research on location-based website authentication raises the question of how users might leverage such location information in decision-making. Compared to digital certificates, the tangibility of location and its clear relationship to the real world suggest that location can play a role in users' security and privacy awareness.

NDSS Workshop on Usable Security (USEC) 2018
18-21 February 2018, San Diego, CA, USA
www.ndss-symposium.org

A. Location-based Decision-Making

Psychological research on decision-making has found that people tend to underestimate risk. Since safety and security are abstract concepts, users are unmotivated to pay attention to these risks. Research examining how users make decisions about computer security has found that users reason inconsistently about their gains and losses, and are likely to overprioritize the cost of losses [38]. For security, because the gains are abstract and the consequences seem random, users often focus on costs, which are immediate and tangible [38]. Users may consider gains, such as protecting information, money, and property, but that they are unaware of risks relating to money and property loss online [20]. Users are also concerned about personal inconvenience in using online services.

Users' security decisions often serve to protect their personal privacy. Research has found that users' privacy preferences are context-dependent and can be easily influenced [3]. Users also experience high uncertainty about whether and to what extent they should be concerned about data privacy. Human decision-making can appear inconsistent, but it is governed by a complex calculus of decision-making [25] that factors in additional information such as social norms and emotional responses.

Recently, Ruoti et al. [29] explored how people determine the security measures they use to protect their online activities. They conducted 23 semi-structured interviews with middle-aged residents in Washington state and found that users were often pragmatic about their security decisions due to the appreciation of the convenience brought by the Internet. They also found that users often have misconceptions of existing TLS security indicators, resulting in insecure behaviors that put their privacy at risk.

Little research to date has analyzed users' perceptions of where their data is stored or to what locations it is transmitted over the Internet. Kang et al. [23] conducted a qualitative study investigating users' mental models of the Internet and found that users had only a vague understanding of where data is stored online. They also found that factors such as reputation and appearance were likely to influence users' perceptions of what was happening to their data. Ion et al. [21] interviewed users about their data privacy awareness and their attitudes about where their online data should be kept. They found that users generally preferred sensitive data to be stored locally than uploaded to cloud storage. They also identified cultural differences that affect users' understanding and preference for their online privacy. A large-scale study of website credibility [17] found that websites were more believable when they communicated the "real world" aspect of the organization, were professional and easy to use, and included indicators of trustworthiness. It remains unexplored how users might integrate information about the website's location into their evaluation of these environmental cues.

B. Website Location and Authentication

Websites are currently authenticated using TLS, which requires the server to have a valid X.509 public-key certificate [11]. The client's browser must validate this certificate upon connection to the server by checking a certificate authority's (CA) signature and other fields. However, recent incidents have demonstrated the weaknesses of public key infrastructure against a strong adversary [27]. More specifically, attackers have been able to compromise CAs to obtain a fraudulent certificate of an arbitrary website to impersonate it. Such attacks have been addressed by a wide range of enhancements to TLS authentication, such as Certificate Transparency [24], and pinning [32]. Despite improvements to certificate validation, a strong attacker may still be able to compromise a web server and obtain the private key associated with the public key in its certificate, e.g., by exploiting TLS implementation bugs [1] or zero-day vulnerabilities. In these scenarios, server impersonation attacks can be performed remotely by the adversary that controls the network.

Recent work has proposed using website location as an additional authentication factor to strengthen website authentication. Verifying a server's location during authentication detects remote server impersonation attacks resulting from the compromise of CAs or websites' private keys. Yu et al. proposed adding location information to digital certificates to authenticate servers in TLS handshakes [39]. In this approach, a trusted party estimates the location of a website server and issue a signed statement binding the server location to a particular connection with the client. The browser can either perform automatic verification (e.g., during the TLS handshake) of the location information or directly display it to the user. Abdou and van Oorschot proposed similar methods of augmenting TLS by actively estimating website locations using delay-based measurements from multiple locations [2]. These approaches leverage the uniqueness and verifiability of private web server locations to supplement existing server authentication.

Using location as an authentication factor is increasingly possible due to the availability of pervasive location information, IP geolocation services, and general localization techniques. A non-technical approach to website localization is the use of public ledgers to record and make available the location of data centers. Online services often host their web servers in data centers, whose locations are publicly known. For example, online resources such as Data Center Knowledge [28] provide a public listing of data center deployment and news about web hosting companies. Companies are also increasingly disclosing their server locations to the public [18], [6], and using on-site security to protect critical online services from physical intrusion by malicious parties [19], [36]. In addition to out-of-band channels, CAs can also verify the locations of online firms and store them in Extended Validation (EV) certificates [10], which can be extracted by the browser.

Currently, IP geolocation is the most common source of website location data. There also already exist software solutions showing IP geolocation data to users, such as Flagfox [12] and IP Whois & Flags [26]. However, they do not guarantee that the web servers really are at these locations upon client connection.

In general, with these website location solutions, users are called upon to notice location information and react appropriately. The impact to users' security awareness and decisions has not been explored in depth.

III. Research Overview

Given recent trends in data localization and proposals for location-based authentication, we aim to explore how server location information can be leveraged as a part of users' trust in online services.

Since we are investigating users' involvement with location information, we inherit the same attacker model proposed in related work on TLS [11] and website location authentication [2], [39]. Specifically, we assume that the attacker is able to impersonate the server by compromising its public key certificate, e.g., by obtaining a fraudulent certificate from a compromised CA or learning the server's private key. We also inherit the assumption that the remote attacker is unable to physically co-locate with the victim's website and resides in a separate location. The attacker's goals may consist of stealing user data (e.g., passwords, credit card numbers, or personal files) or providing false information (e.g., fake news). We specifically aimed to answer the following research questions about user behavior.

RQ1 How do users currently make online security decisions and how could location play a role in these decisions?
RQ2 Does information about website locations affect users' behavior when they perform online tasks?

We explored these problems using a user-centered approach [22]. To answer RQ1, we conducted a series of qualitative interviews and applied thematic analysis to understand users' decision-making processes for online security. The themes we identified allowed us to develop a model of users' trust assessments and derive design requirements for a website location tool for a broad range of web users. To answer RQ2, we designed a location tool that displays web server locations, which we implemented as a Chrome browser extension. We conducted a user study to evaluate the usability of our location tool and analyze the impact of location information on users' decisions in real-world application settings. All studies involving human subjects were approved by the ethics committee in our institution.

IV. Study 1: Qualitative Interviews

We first interviewed users about how they currently determine websites' trustworthiness. Our goal was to understand how location information could fit into users' decision-making practices and to identify design requirements for a location indicator.

A. Study Design

We chose a semi-structured interview approach to ensure that we covered topics of interest while giving participants the freedom to discuss their decision-making processes and concerns. Our interview covered three areas: Internet use, security awareness, and location-related preferences. We carefully selected topics that might have associated security or privacy concerns for different Internet usage scenarios: online file storage, emails and calendars, online financial transactions (banking and shopping), and social media. For each topic, we asked about how participants used these services, the kinds of data they stored or obtained through those services, and what kinds of security and privacy concerns they had around these activities. Regarding security awareness, we asked participants about their general security and privacy precautions and where they thought Internet data was stored and served from. Because we were interested in the development of a security indicator, we asked about how they currently determine that websites are legitimate or trustworthy. In the final part of our interview, we explained the concept of website location as a security indicator, and asked participants how they might use it if it were available.[1] Our interview script can be found in the appendix.

Because using location as a website security indicator is a novel concept, we did not expect participants to explicitly identify it during the interviews. We therefore framed our interview broadly and encouraged discussion on a wide range of topics with relevant security and privacy concerns. By eliciting detailed feedback about users' current decision-making strategies, we sought to understand how location is currently perceived and how it can be used in users' security decisions. Rather than specifically introducing technical concepts of location-based authentication, we introduced topics that naturally led to the subject of location. If participants did not bring up the subject of location on their own, we attempted to steer the conversation in that direction.

We audio-recorded the interviews to facilitate subsequent note-taking and transcription for analysis. Participants also completed a brief demographic questionnaire before the interview. Each interview lasted between 30 and 60 minutes.

B. Participants

We aimed to represent a diverse array of perspectives and therefore recruited people of different genders, ages, education levels, occupations, and diverse nationalities. We deliberately advertised outside our institution using public bulletin boards, online forums, and mailing lists. While our sample is likely not representative of the larger population, a wide variety of viewpoints were expressed in our interviews. The perspectives and experiences expressed by our participants were in line with the results of similar studies [23], [16].

We reached saturation at 15 participants (8 female, 7 male). They ranged in age from 20 to 59, with most (13) aged between 20 and 39 years old. Participants had a variety of educational backgrounds, and their areas of specialty or occupation included social and natural sciences, engineering/informatics, and healthcare. Their occupations included artist, scientist, and student (with 8 students making up the majority). To provide a rough measure of the participants' level of international experience, we asked participants for their nationality, and how many countries they had visited. Participants' nationalities spanned 12 countries, and each participant had visited a median of 10 countries.

C. Thematic Analysis

We reviewed the audio recordings and transcribed each interview. This produced a qualitative dataset that we analyzed using thematic analysis [8], a flexible qualitative analysis

[1] To make it easier for the participants to understand, we used the term "website locations" in our user studies. We use the terms "website locations" and "server locations" interchangeably throughout the rest of the paper.

methodology that allowed us to identify themes and relationships in the data. We began our analysis with open coding. We traversed and reviewed the transcriptions line by line and assigned codes to recurring ideas. To ensure consistency, each interview was coded by two researchers, and codes were cross-checked to improve reliability.

An example of our open coding is shown in the following quote, where a participant was asked how she verifies website authenticity:

> "I didn't think of [authenticating websites] before. I think every website will give us some legal documents to read before we give information to them. I will scan the documents." – P5

We assigned the code *lack of awareness* to highlight the participant's lack of concern. Because she mentioned her attention to legal documents, we assigned the code *legal concern*. We identified 46 open codes in our data. Following the process of open coding, we refined the codes and classified them into themes, described in the subsequent sections. These themes highlight patterns of typical behavior, rather than representing categories of users.

1) Trusting by Default: When asked about their online decision-making, many participants described taking the security of websites for granted without much investigation.

> "You just go to the webpage, it looks familiar, and then it never crosses your mind that it may have been forged." – P12

We also noticed users' default approach to trust in the way they described their automatic use of various online services, such as synchronization of data (e.g., contacts and files) across different devices linked to the same platform.

> "I do use sometimes iCloud. I think it just come automatically with my iPhone. Each two weeks, asking me if I want to store it [...] I just let it." – P1

Many participants embraced the convenience of automated functions, such as allowing web email servers to automatically store email addresses of frequent contacts.

Most participants' initial approach toward online security was to trust that the default configurations are secure. Few participants mentioned looking out for browser security indicators, such as the lock icon or website certificates. When asked about decision-making, participants did not frequently engage in discussions of security and privacy until potential online risks were specifically brought up. Most participants reported using the Internet by simply trusting the way it is.

> "One keeps hearing about Internet security and all this, but unless something happens, you don't pay a lot of attention to it." – P12

2) Having Diverse Areas of Concern: Although their default approach was to view the Internet as secure, most participants were able to elaborate areas of specific concern regarding the security and privacy of their data. Among these areas were concerns about personal privacy, financial safety, and freedom of speech.

Personal privacy was a major concern that was brought up repeatedly during the interviews. Participants discussed privacy concerns about sharing information with both online services and other users of those services (and often conflated these two threats).

> "I just kind of like the idea of not being very traceable, not because I'm hiding something specifically but because it's my own business kind of, where I am, what people I'm seeing." – P14

Some participants were aware of data collection but were ignoring the implications or did not perceive this as a threat.

However, other participants acknowledged the necessity of disclosing personal information. For example, P5 stated that "sometimes we have to be checked by other people" (referring to public security). Others regarded the purpose of the Internet as being to share information, and said that curtailing this sharing would render their online presence less meaningful.

> "If someone knows where I worked, that's not a problem because it actually helps me connect with other people." – P15

A major concern repeatedly mentioned was financial security. Many participants discussed security concerns around online banking and shopping. For example, many participants declined to allow websites to store their credit card information.

Regarding freedom of speech, a few were concerned about unforeseen consequences of disclosing their opinions.

> "I don't really trust that [my words] might not one day be used against me... a lot of this information is stored and it's just uncomfortable." – P14

3) Relying on Multiple Trust Factors: When discussing how they decided to trust websites, participants mentioned a variety of factors. Most participants associated website trustworthiness with subjective impressions, such as familiarity of brand presentation, the website interface, and the past experiences of themselves and friends. Even knowledgeable participants admitted to relying on such non-technical cues.

> "The first [thing I notice] would be the brand, the logo itself [...] does it look the same?" – P2

One major trust factor was the company's reputation. For example, when asked about why they trust particular storage services, some participants relied on the brand name: "I think having Apple's name behind it, it's quite safe." (P3) Participants also listed firms like Google and Amazon as their trusted service providers. Many preferred to avoid unknown shopping websites and rely on payment services with buyer protection policies (e.g., PayPal).

In addition to their own previous experiences, participants also relied on experience from friends or website reviews to judge whether websites were trustworthy. These social cues were used to help discern trustworthiness.

> "[How do you choose where to shop online?] ... usually based on the community. [...] I always try to think or to ask friends if they have ever bought something in that website." – P10

4) Taking Risks for Practicality: Most participants described heuristics for decision making based on their trust factors and concerns. These included using pseudonyms, providing fake profile information, avoiding saving credit card information, and only buying from known vendors.

However, participants often admitted to making exceptions for practical reasons. They justified these decisions by discussing the acceptability or manageability of the potential risks, e.g., a small financial risk when ordering from an untrustworthy merchant. Such decisions often depended on the urgency of the matter at hand.

> "If I'm doing stuff on the Internet, I just want it done as fast as possible so I can do something else." – P14

Compromises were thus often made in the presence of security warnings. Users put themselves in insecure situations (e.g., by ignoring certificate warnings) to ensure convenience and access to online services. In such situations, participants described a tradeoff between personal security and service accessibility when making their decisions. Though security compromises were made, participants mentioned various secondary measures to reinforce their decisions, such as obtaining tangible proofs of their transactions ("I want to have photocopy or paper as proof" –P1) or contacting customer service.

5) Helplessness and Learning from Consequences: When discussing their decision-making processes and concerns, participants often expressed frustration over missing information or knowledge that prevented them from behaving securely. Many expressed a kind of learned helplessness relating to their inability to understand security measures.

Another aspect of this helplessness originated from users' inability to affect corporate policy and their lack of control over where sensitive data is stored. One participant told us that "a company could say one thing and do another thing" (P2), suggesting their lack of control and distrust in the companies.

However, though participants expressed a lack of contentment about not being able to control the security of their information, some mentioned that having that control could be a burden to them.

> "If location would be available for me, I would have a feeling that from that time I am the one who has to be responsible for that." – P7

We also noticed that some users seemed to have eventually developed a helpless attitude, and described the process of making decisions online as akin to taking a leap of faith: "I make a wish... I wish nothing happens" (P6).

D. The Process of Decision-Making

There was considerable variation in how individual participants made trust decisions in online and real-life scenarios. Our participants described many elements for decision-making, and they were left to combine these elements into each single decision. We identified a model of how users reach a security-related decision based on various considerations.

The user's decision-making process begins by incorporating the materials used by the user to determine the trustworthiness of a website: their default trust, their varying concerns about security and privacy, the list of factors that give them confidence, their past experiences in similar situations, and the demands of the primary task. During decision-making, certain elements outweigh others, and the user must obtain a single decision that combines all of their priorities, concerns, and trust. In our interviews, participants seemed unable to give clear descriptions of exactly how they weighted these varying considerations, and it was clear that there was a complex personal calculus that formed each decision [25]. However, users did often describe the tensions of having to make a single decision from an overload of information (and sometimes, a lack of relevant information).

Following this decision, its consequences (e.g., improved security, identify theft) may impact not only a single user but also their friends and family as other users look for information to feed into their own decision-making processes. If the user chose not to trust a website, they might have a primary task that remains incomplete, and still be looking for ways to accomplish that task. If they did trust the website, and no security problems result, they may relate that positive experience in user reviews or feedback to other users. In other situations, the exact consequences may be unclear, but the experience of having to make that decision may feed into feelings of a lack of a control or learned helplessness.

E. The Role of Website Locations

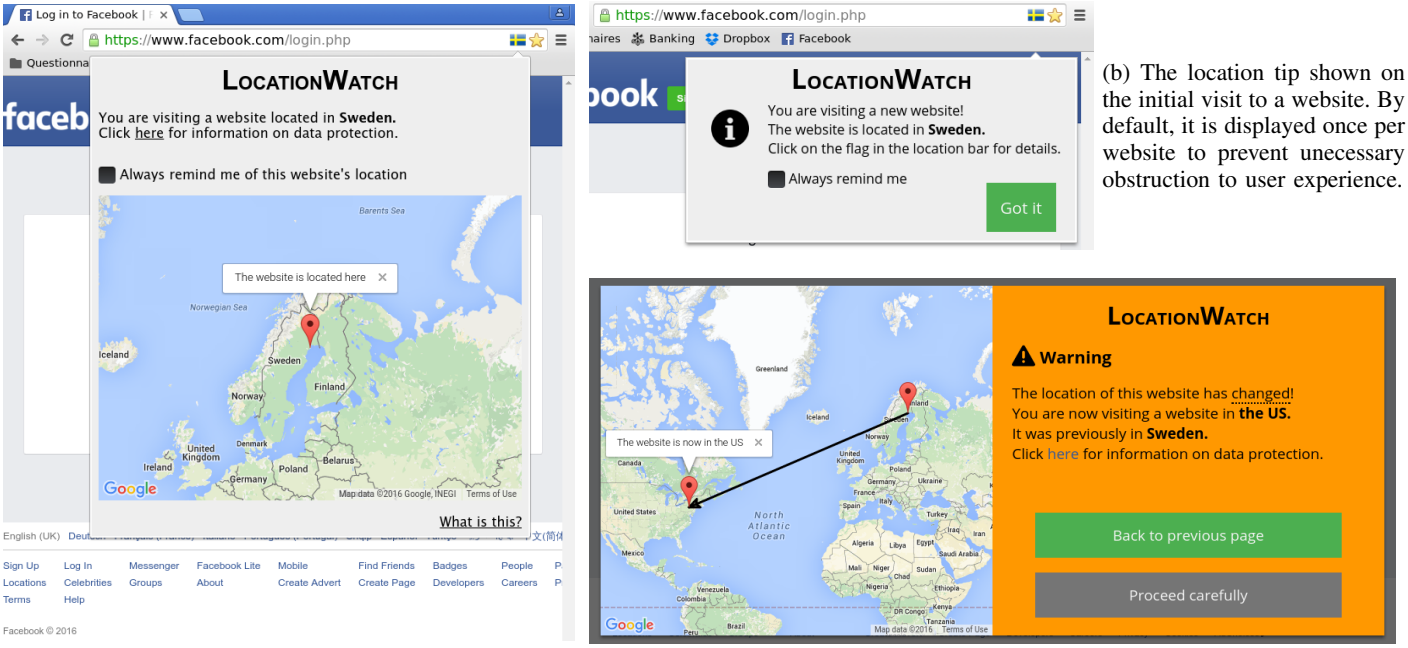
In the final segment of our interviews, we briefly explained the concept of location-based website authentication to participants, and asked them for feedback about how they thought it could (or could not) be useful. Users were primed to discuss security in this part of the interview, but since our goal was to design a tool for users, we wanted to understand their desires.

Unsurprisingly, participants had not typically related website locations to Internet security. Similar to previous findings [21], they were mostly unaware of the geographic locations where their data was stored. Several speculated that data must be stored in the same countries where the parent companies were based. These responses were sensible and expected since the Internet abstracts away the physical locations of website content and data storage. Participants also mostly conflated security (the authenticity of the website) with privacy (where and how users' data is stored or collected).

When asked about the presentation of location information, most participants discussed the idea of location on the country level (as opposed to the city or continent level). Participants often brought up the legal implications of having data stored in different countries (mainly in the context of financial information). They also occasionally referred to public disclosures of nation level surveillance programs (e.g., mass surveillance in the USA) and other data-gathering concerns when discussing where they avoided sharing or storing personal data.

> "It is important to be sure they are stored in countries with high security levels... legal regulations [on] who is allowed to have access and under what conditions someone could have access to such data. And in Europe, I would say such [legal institutions] are on a high standard." – P11

Participants suggested that location can be incorporated into existing security mechanisms for critical applications.



(a) The flag indicator and popup.

(b) The location tip shown on the initial visit to a website. By default, it is displayed once per website to prevent unecessary obstruction to user experience.

(c) The warning when a website's location has changed

Fig. 1: Features of LocationWatch, our location indicator.

> "I think in the end it will be used everywhere because it would be like an adapted protocol. I think for me it would be useful [in] banking." – P4

Participants often related website location to the implication of disclosing their data to the foreign governments. Aside from security concerns due to server impersonation, participants cared about how foreign governments could harm their privacy when websites are hosted abroad.

Regarding trust factors, we noticed that participants were more receptive to discussions of website locations as opposed to traditional security solutions, such as public key certificates or authentication. Users had opinions about locations, and were willing to discuss how they might relate website locations to other information about countries or services. One participants discussed the utility of location information in relation to logistical concerns such as shipping and postage when shopping online. Another participant wanted to be able to consider environmental implications of web server locations, and discussed her concerns about the damage inflicted by large heat-generating data centers. Another participant mentioned a similar concern, but related her desire to know that her data was being stored in a location where workers were being treated and paid fairly.

V. Design of LocationWatch

Based on our qualitative analysis, we developed a set of design requirements for our location tool, LocationWatch. LocationWatch is intended to act as a visual indicator to inform users about the result of server location verification, envisioned to use recently-proposed methods [2], [39]. We implemented LocationWatch as a Chrome extension featuring a flag indicator, a location tip, and a warning message. In real-world deployment, LocationWatch would be incorporated into existing security indicators; in this paper, we implemented a prototype as a browser extension. Before website location verification methods are widely deployed, LocationWatch can use IP geolocation databases as a reference.

LocationWatch's main features include a flag indicator, a location tip, and a warning message. The flag indicator (Figure 1a) is an icon near the address bar showing the flag of the server's residing country. It also shows more information in a popup window when clicked by the user. The location tip (Figure 1b) is a small window on the upper-right corner of the web content that appears on the first visit to a website. The warning message (Figure 1c) appears when a website's location has changed since the user's previous visit and allows the user to decide whether to continue visiting it. In the event of a server impersonation attack (i.e., using a fraudulent certificate or a compromised server's private key), this tool would display the location of the attacker's server.

A. Design Rationale

We aimed to implement LocationWatch as an unobtrusive and effective tool to assist users in assessing the inputs to their decision. We discuss its potential integration with existing security indicators in Section VII.

Default Trust. Since users often trust websites by default and without understanding security indicators, security information should be made intuitive for them. Some may even prefer not to be bothered with location details since website security is not their primary task. We therefore designed LocationWatch to be non-intrusive by showing only the flag icon by default.

Stage	Tasks	Website location	Available indicators	
			Ctrl features	Expt features
1	Dropbox: upload passport scan	United States	Flag	Flag + Tip
Initial visit	Facebook: update status	Sweden	Flag	Flag + Tip
	Banking: check 1st account balance	Switzerland	Flag	Flag + Tip
2	Dropbox: upload password list	United States	Flag	Flag (+ Tip*)
Re-visit	Facebook: update status	Sweden	Flag	Flag (+ Tip*)
without change	Banking: check 2nd account balance	Switzerland	Flag	Flag (+ Tip*)
3	Dropbox: upload credit card	China	Flag	Flag + Warning
Re-visit	Facebook: upload party photo	United States	Flag	Flag + Warning
with change	Banking: check 3rd account balance	Japan	Flag	Flag + Warning

*The tip is only shown if the participant checked the "always remind me" option in Stage 1.

TABLE I: Study 2 tasks and location configuration for the control and experiment groups.

Diverse Concerns. Participants were often concerned about how their data was used or misused by governing nations in which the web servers reside. Since legal protection laws differ across countries, the location of where data is stored or sent may prompt different user concerns and influence subsequent decision-making. We therefore designed a popup (Figure 1a) that appears when the user clicks on the flag icon. This popup shows the server's governing country and information on that country's data protection laws for the users' reference.

Trust Factors. Most participants did not initially think of location as a trust factor. To strengthen users' attention to location, the location tip appears on the user's initial visit to a website (Figure 1b). While slightly obtrusive, this tip provides an attentive user a first impression of where this website is originally located and it is designed to only appear once by default. We also use the popup window (Figure 1a) to show more detailed information for interested users.

Past Experience. Previous experience plays an important role since many participants considered the visual familiarity of websites as a primary factor for trust. Therefore, we chose to show a visual cue to inform the user when the website location has changed. This is realized using a warning message (Figure 1c) showing the current and previous website locations.

Practicality. Participants admitted to bypassing warnings for practical reasons such as convenience or an acceptable level of risk. Our location indicator does not prohibit such choices, similar to certificate warnings. In the warning message, we provided two buttons: "leave the website" and "proceed carefully" (Figure 1c).

VI. Study 2: User Evaluation

We conducted a user study to evaluate the impact of website location on users' decision-making. First, we aimed to evaluate how users' security behavior changes when website locations are provided. Second, we aimed to evaluate the usability of LocationWatch to see if it satisfied our design concepts and requirements. Since the interviewed participants mostly relied on experiences and impressions, we hypothesized that website location changes across subsequent visits would affect users' decisions.

A. Study Design

To evaluate LocationWatch and users' response to website locations, we designed an experiment where participants used three web services (file storage, social networking, and online banking) and performed routine but potentially sensitive tasks. We chose these services to prompt typical concerns from the qualitative analysis: personal privacy, identity safety, and financial security. We aimed to measure how online behavior varied when participants were given website location information using LocationWatch.

Our study had a mixed design, where group was a between-subjects factor and stage was a within-subjects factor. There were two groups: control and experiment. In the control condition, the location interface was configured to show only the flag icon and the popup window (making it similar to existing tools [12], [26]). In the experiment condition, participants used the fully-featured version of LocationWatch, including the location tip and the location change warning. The study had three stages and in each stage the participant was asked to perform three tasks, as shown in Table I. We used a Latin square design to shuffle the task order across different participants in each stage to avoid order effects.

Each participant was given a brief introduction to the study's purpose as a usability evaluation of a software tool. All participants received the same tutorial on LocationWatch, introducing the concept of geographic locations of websites, the flag icon, and the popup features. To avoid priming users to expect location changes, we did not introduce the location tip and warning (only visible to the experiment group). Participants were then given login information for the accounts and files created for the study, and instructed to treat them as if they were their own.

B. Selecting Test Locations

To evaluate user reactions to various locations, we programmed fake locations to be displayed by LocationWatch. We configured our tool to show three types of locations: countries associated with good privacy impressions (Sweden, Switzerland, Japan), a developed country with prominently reported data privacy breaches (the USA), and a developing country with known Internet censorship (China). For the last stage, we programmed LocationWatch to simulate location

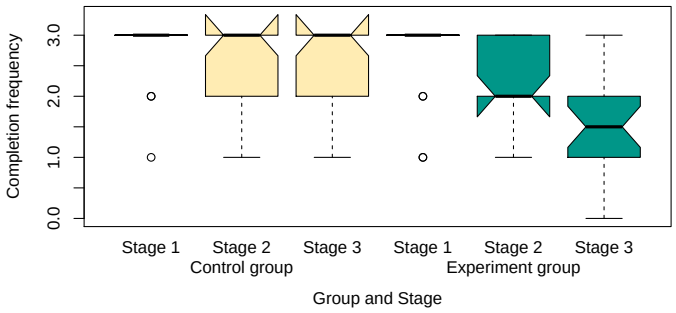


Fig. 2: Box plots of task completion scores across different stages for all websites.[2]

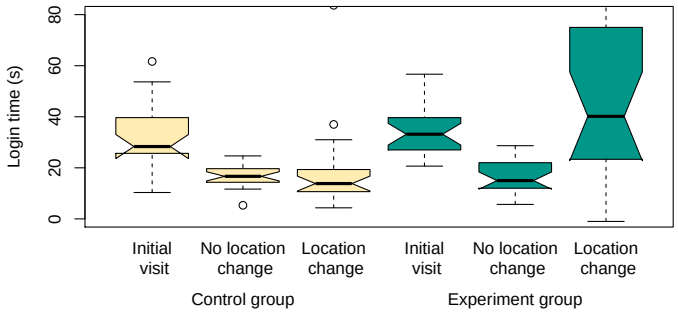


Fig. 3: Box plots of time spent deciding to log into websites, averaged over all three websites in each stage.

changes: Dropbox from the USA to China, Facebook from Sweden to the USA, and the online bank from Switzerland to Japan. For the control group, this led to a change of the country flag and popup contents. For the experiment group, the location change warnings were additionally shown.

Any choice of countries would naturally subject our study to various user-side cultural biases, and we therefore fixed the country assignments across different participants rather than randomizing them to minimize experiment variation. Since we were focused on observing whether location plays a role at all, we leave the design of a more large-scale and ecologically valid study as future work.

Each session lasted between 30 and 60 minutes. In addition to the instrumented measurements about their activities, the participants completed three questionnaires: a demographic questionnaire, a pre-test questionnaire about their online decision-making habits, and a post-test questionnaire about their impressions of LocationWatch.

C. Participants

We recruited users who were aged 18 years or above, spoke English, and had Internet experiences, including online banking, file storage, and email. 44 participants completed the study (23 female and 21 male), most of whom were students (32). They ranged in age from 20 to 59, with most (34) being between 20 and 29 years old. Participants' nationalities spanned 17 countries and they had visited a median of 15 countries. They come from various backgrounds, including social sciences, humanities, natural sciences, and engineering. Each study lasted between 25 and 40 minutes.

D. Results

We evaluated participant behavior based on the number of completed tasks and the decision-making time.

1) Task Completion: We recorded how often users completed the tasks in each stage and each condition of the experiment, and used task completion as a measure of how location affected participants' behavior. We defined task completion as having logged into the web service *and* completed the given task. We encoded completed tasks as 1, and uncompleted tasks as 0. For each stage we summed the scores from the three websites to produce an aggregate score between 0 and 3.

Figure 2 shows the distributions of completion scores. While most control group participants completed all tasks in all stages, fewer experiment group participants completed the task when the location changed. Descriptive statistics are detailed in Table II in the appendix.

We first looked for differences in task completion between the control and experiment groups. Since task completion was based on counts, we performed a between-subjects Chi-squared test on the sum of completion scores across all stages and found a significant difference between the two conditions ($\chi^2(1) = 9.44, p = 0.002$). Post-hoc pairwise Chi-squared tests using a Bonferroni correction showed that this difference occurred in Stage 3 ($\chi^2(1) = 10.52, p = 0.011$), where the warning made participants in the experiment group less likely to complete the task.

In the absence of an omnibus test for categorical data, we conducted Chi-squared tests to look for differences between the stages in each condition. We found a significant effect of stages in the experiment group ($\chi^2(2) = 30.86, p < 0.001$), but no effect in the control group ($\chi^2(2) = 7.35, p = 0.228$). Table III in the appendix shows the results of post-hoc pairwise Chi-squared tests. We found significant differences in task completion between Stage 1 and Stage 3 ($\chi^2(1) = 26.15, p < 0.001$), and between Stage 2 and Stage 3 ($\chi^2(1) = 10.52, p = 0.011$) for the experiment group, showing that the warning for location changes significantly affected whether participants completed critical tasks.

2) Decision-Making Times: As an indication of how much attention participants paid to making decisions about location, we recorded the time taken in the login process. We measured the time between when the webpage loaded and when the user clicked the login button (in seconds). This measurement included the time that the user spent deliberating about whether to login. We aggregated the times for each participant in each stage by taking the mean of the times for the three websites. Figure 3 shows the distribution of times across the three stages.

Table IV in the appendix shows descriptive statistics of the times that participants took to log in by group and stage. The times in Stages 1 and 2 were similar across the two groups, the times decreased in Stage 2 (from ∼30 seconds to ∼17 seconds). In Stage 3, the experiment group spent more time considering their login decision (54 seconds).

[2]The notches in the box plots represent the 95% confidence intervals around the median. When the intervals fall outside the 1st or 3rd quartiles, the notches extend beyond the box.

We used a mixed two-way ANOVA to analyze the differences in login times between the two conditions and between the stages. There were significant effects of both condition ($F(1, 41) = 12.73, p < 0.001$) and stage ($F(2, 82) = 9.92, p < 0.001$) and a significant interaction between condition and stage ($F(2, 82) = 10.65, p < 0.001$).

We then used post-hoc pairwise t-tests to examine the differences between the two groups. There were significant differences only in Stage 3 ($t(21) = -3.08, p = 0.051$), implying that the warning made the experiment group spend more time than the control group.

We further conducted post-hoc pairwise t-tests with a Bonferroni correction to look for differences within each group (Table V in the appendix). There were significant differences between Stages 1 and 2 for both conditions ($t(21) = 6.01, p < 0.001$ for control, $t(21) = 7.24, p < 0.001$ for experiment), possibly because the participants got used to the login process. The experiment group had significantly different login times between Stages 2 and 3 ($t(21) = -3.43, p = 0.023$), implying that the warning affected their time spent deciding to log in.

3) Task Completion on Different Websites: We aggregated completion scores within the same stage in our initial task completion analysis. Here, we performed an exploratory analysis to investigate how users reacted to different location changes on different websites. The scale of our study prevented us from exhaustively testing different websites and locations. However, in our study design we attempted to pick security-sensitive websites, and to choose location changes that might represent different attacks. We included location changes to countries that were neutral but implausible (Switzerland to Japan, banking), locations with well-publicized privacy issues (USA to China, Dropbox), and changes between plausible locations (Sweden to USA, Facebook). Our exploratory analysis evaluates whether there was an effect of website (and the corresponding country change) on task completion.

Similar to analyzing task completion across stages, we defined a participant's task completion score for each website, ranging between 0 (no tasks completed) and 3 (tasks completed in all websites). The distributions of website task completion scores for the control and the experiment groups are shown in Figure 4. In both conditions, participants completed fewer tasks on Dropbox (Table VI in the appendix).

A Chi-squared test using a Bonferroni correction showed a significant effect of website in both the control condition ($\chi^2(2) = 29.17, p < 0.001$) and the experiment condition ($\chi^2(2) = 32.07, p < 0.001$). Post-hoc pairwise tests revealed that in both conditions, significantly fewer participants completed the tasks on Dropbox than on Facebook or banking, as shown in Table VII in the appendix.

4) Usability: We used the System Usability Scale [9] to evaluate the usability of our location interface. Both variants of our interface were ranked as "excellent" (scores greater than 80) [30]. The average scores were 81.61 for the control group and 82.2 for the experiment group. A Mann-Whitney test showed no significant difference in usability between the two versions ($U = 254.5, p = 0.78$).

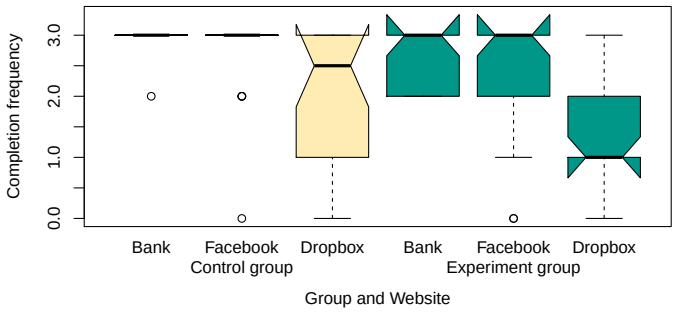


Fig. 4: Box plots of the task completion scores across different websites for all stages.

E. Summary

Participants' decisions were indeed affected by their knowledge and perception of the websites' locations. There were statistically significant behavior changes in task completion when website locations changed in the experiment condition. This suggested that participants noticed the changes and some avoided sensitive tasks. Participants who completed the tasks despite location changes mainly cited the website's reputation as the main reason.

We also noticed that when warned of website location changes, two users in the experiment group still signed in to inspect the website (Facebook and Dropbox) before refusing to perform the given task. This suggests that for some users, the decision point for personal security or privacy lies past the sign-in process. This supports previous work on browser warnings [31] that prevent users from leaking personal credentials before ascertaining their trustworthiness. It also suggests that security indicators could be more useful if they were presented right before critical tasks.

LocationWatch did not interrupt users in non-critical cases since both groups took similar times in the login process in Stages 1 and 2. There was a significant difference in Stage 3, during which warnings were shown to the experiment group participants, who took extra time to look up reference information or decide whether to proceed. Combined with the task completion, this showed that the tool managed to attract users' attention with the warning message.

We also found preliminary evidence that location information may have increased significance in tasks involving sensitive data. Significantly fewer participants completed the Dropbox tasks, citing that they did not feel comfortable uploading personal information in such situations. However, many participants still logged in despite warnings in the banking task, which our interview results showed to be the most sensitive. It is difficult to know exactly why this occurred, but it suggests that participants interpret location information differently in different contexts.

Our evaluation also showed that LocationWatch was usable. The SUS scores were good and similar for both groups, implying that the version with the location change warning was as usable as existing solutions, which primarily show the country flag (as in the control group).

VII. Discussion

The results of our studies suggest that website location is a promising research direction for helping users authenticate websites. We discuss various aspects of using website location as a factor for users to relate to their security and privacy.

A. Adoption and Deployment

With the trend of data localization [7], location verification could become an important consideration for data center deployment, which is presently concerned with infrastructure and sustainability [37]. Companies often host their websites using content delivery networks (CDNs), which serve data from servers closer to the clients (often to the same city or region). We envision that market and regulatory pressure would encourage companies to choose CDNs in preferred locations. We see the beginnings of this with EV certificates [10], which contain verified information about company office locations. The security benefits of automatic and verifiable location information would further encourage wider adoption.

For real-world deployment, website owners could opt in to provide detailed and up-to-date location information upon client connection, as a service to provide extra security assurance. We envision that LocationWatch would store legitimate server locations for each supported website, which might consist of multiple locations. If the tool detects that the website is being served from an unlisted location, it would display a warning similar to that in LocationWatch. We found that users' security awareness could be raised by such warnings, allowing them to take further caution with their private data.

B. Challenges of Location Authentication

One challenge with any added security mechanism is that it may distract or overwhelm users, who in response bypass or ignore warnings, and this has been addressed with ongoing research [14]. We implemented LocationWatch as a separate tool to minimize the influence of other TLS warnings in our studies. However, we envision that it could be integrated with existing indicators to provide users with security information in a consolidated manner.

There are also challenges inherited from location-based authentication techniques due to the Internet infrastructure. First, it is likely that many websites are physically hosted on the same CDN server. This allows an attacker that compromises a website to host a phishing website on the same CDN, effectively serving arbitrary content from the same location. This attack is not detectable in the currently proposed location-verification protocols [2], [39] since the location ceases to be a unique factor of the website for verification. However, critical websites can resist such attacks if they host their login web pages on privately owned data centers. The warnings of our location indicator are effective only if the TLS endpoint of the website is served from unique and private locations.

Another limitation of location-based authentication stems from the use of third-party resources (like CSS and JavaScript), which can be served from other locations. Like current security indicators, LocationWatch shows the location of the top-level web server, while the locations of embedded content are not displayed. This is a design choice made to avoid confusing users, as they typically view complete webpages and do not consider individual webpage elements. Creating a design that allows users to explore the locations of individual elements in a single page is an open challenge.

Adversarial co-location and third-party resources are fundamental limitations of recent location-based authentication mechanisms. While our exploration of location as a security factor inherits such limitations, we found that there is potential for location information as a comprehensible security indicator.

C. Study Limitations

This type of work is unavoidably affected by participants' views. We conducted our studies in person to obtain richer data about users' interactions with LocationWatch and how they perceived the warnings. However, it limited the diversity of perspectives that we captured (both in terms of participants and the number of websites and locations we could present). In future work, it would be interesting to conduct a larger study using crowdsourcing platforms to evaluate location's influence and a more global perspective.

Our study was also affected by the aforementioned challenges of location-based authentication. However, the in-person experiments allowed us to interactively observe users and their diverse contingent actions (e.g., retroactively deleting files or reasoning about warnings).

VIII. Conclusion

Authenticating websites is an important problem that affects users because they must make decisions about whether a website is trustworthy. The current certificate model forces users to interpret dense and unfamiliar technical information, which results in users expressing confusion about warnings or ignoring them in favor of non-technical cues [13]. Recent proposals suggest the addition of web server location authentication [2], [39] to strengthen TLS. Our work is the first to explore the usability aspects of these proposals. We investigated how location information can fit into users' decision-making processes, and whether location information affects the decisions that users make about security-sensitive tasks.

We designed LocationWatch, a browser extension to notify users of website locations and their changes. We conducted a user study and found that when alerted to a location change, users understood the change and interpreted it in light of their current task. As a result, they were less likely to complete security-sensitive tasks when warned about location changes. Our findings suggest that website location indication has the potential to be a usable approach to helping users make informed decisions about privacy and security.

IX. Acknowledgment

We are grateful for Marco Guarnieri for his feedback on improving the paper. We also thank the anonymous reviewers and shepherd for their helpful comments. Der-Yeuan Yu was funded by ABB Corporate Research, Switzerland. This paper represents authors' views.

REFERENCES

[1] "CVE-2014-0160," https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160, 2014.

[2] A. Abdou and P. van Oorschot, "Server location verification and server location pinning: Augmenting tls authentication," *arXiv preprint arXiv:1608.03939*, 2016.

[3] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6211, pp. p509–514, Jan. 2015.

[4] D. Akhawe and A. P. Felt, "Alice in warningland: A large-scale field study of browser security warning effectiveness," in *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*, 2013, pp. 257–272.

[5] H. Almuhimedi, A. P. Felt, R. W. Reeder, and S. Consolvo, "Your Reputation Precedes You: History, Reputation, and the Chrome Malware Warning," in *SOUPS*, 2014, pp. 113–128.

[6] Amazon Web Services, "AWS Global Infrastructure," https://aws.amazon.com/about-aws/global-infrastructure/, 2016.

[7] C. Bowman, "Data localization laws: an emerging global trend," 2017.

[8] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. p77–101, Jan. 2006.

[9] J. Brooke, "SUS-A quick and dirty usability scale," *Usability evaluation in industry*, vol. 189, no. 194, pp. p4–7, 1996.

[10] CAB Forum, "EV SSL Certificate Guidelines," https://cabforum.org/extended-validation/, 2016.

[11] J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements," in *IEEE Symposium on Security and Privacy (S&P)*, 2013.

[12] Dave G, "Flagfox," https://flagfox.net/, 2016.

[13] 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 *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, 2015, pp. p2893–2902.

[14] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acer, E. Morant, and S. Consolvo, "Rethinking Connection Security Indicators," in *Twelfth Symposium on Usable Privacy and Security (SOUPS)*, 2016.

[15] A. P. Felt, R. W. Reeder, H. Almuhimedi, and S. Consolvo, "Experimenting at scale with google chrome's SSL warning," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 2667–2670.

[16] D. Fisher, L. Dorner, and D. Wagner, "Short paper: Location privacy: User behavior in the field," in *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*. ACM, 2012, pp. p51–56.

[17] B. J. Fogg, P. Swani, M. Treinen, J. Marshall, O. Laraki, A. Osipovich, C. Varma, N. Fang, J. Paul, A. Rangnekar, and J. Shon, "What makes Web sites credible?" in *Proceedings of the International Conference on Human Factors in Computing Systems (CHI)*. ACM, 2001, pp. p61–68.

[18] Google, "Google Data Center Locations," http://www.google.com/about/datacenters/inside/locations/index.html, 2016.

[19] ——, "Google for Work Security and Compliance Whitepaper," https://static.googleusercontent.com/media/www.google.com/en/US/work/apps/business/files/google-apps-security-and-compliance-whitepaper.pdf, 2016.

[20] J. B. Hardee, R. West, and C. B. Mayhorn, "To download or not to download: An Examination of Computer Security Decision Making," *ACM SIGCSE Bulletin*, vol. 13, no. 3, pp. 32–37, May 2006.

[21] I. Ion, N. Sachdeva, P. Kumaraguru, and S. Čapkun, "Home is safer than the cloud!: privacy concerns for consumer cloud storage," in *Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2011.

[22] "Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems," International Organization for Standardization, Standard, Mar. 2010.

[23] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, ""My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security," in *Eleventh Symposium On Usable Privacy and Security (SOUPS)*, 2015, pp. p39–52.

[24] A. Langley, E. Kasper, and B. Laurie, "Certificate Transparency," https://tools.ietf.org/html/rfc6962, 2013.

[25] R. S. Laufer and M. Wolfe, "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues*, vol. 33, no. 3, 1977.

[26] myip.ms, "IP Whois and Flags Chrome and Websites Rating," http://chrome.myip.ms/, 2016.

[27] Netcraft, "Fake SSL certificates deployed across the internet," http://news.netcraft.com/archives/2014/02/12/fake-ssl-certificates-deployed-across-the-internet.html, 2014.

[28] Penton, "Data Center Knowledge," http://www.datacenterknowledge.com/, 2016.

[29] S. Ruoti, T. Monson, J. Wu, D. Zappala, and K. Seamons, "Weighing context and trade-offs: How suburban adults selected their online security posture," in *Thirteenth Symposium on Usable Privacy and Security 2017)*. USENIX Association, 2017, pp. 211–228.

[30] S. Ruoti and K. Seamons, "Standard metrics and scenarios for usable authentication," in *Symposium on Usable Privacy and Security (SOUPS)*, 2016.

[31] D. Shin and R. Lopes, "An empirical study of visual security cues to prevent the SSLstripping attack," in *Proceedings of the 27th Annual Computer Security Applications Conference*. ACM, 2011, pp. 287–296.

[32] R. Sleevi, C. Evans, and C. Palmer, "Public Key Pinning Extension for HTTP," https://tools.ietf.org/html/rfc7469, 2015.

[33] J. Sobey, R. Biddle, P. C. van Oorschot, and A. S. Patrick, "Exploring user reactions to new browser cues for extended validation certificates," in *European Symposium on Research in Computer Security*. Springer, 2008, pp. 411–427.

[34] A. Sotirakopoulos, K. Hawkey, and K. Beznosov, "On the challenges in usable security lab studies: lessons learned from replicating a study on SSL warnings," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, 2011, p. 3.

[35] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor, "Crying Wolf: An Empirical Study of SSL Warning Effectiveness," in *USENIX Security Symposium*, 2009, pp. 399–416.

[36] USA Today, "Top secret Visa data center banks on security, even has moat," http://usatoday30.usatoday.com/tech/news/story/2012-03-25/visa-data-center/53774904/1, 2012.

[37] Verne Global, "Data Centre Risk Index," https://verneglobal.com/media/data-centre-risk-index-2013.pdf, 2013.

[38] R. West, "The Psychology of Security," *Communications of the ACM*, vol. 51, no. 4, pp. p34–40, Apr. 2008.

[39] D.-Y. Yu, A. Ranganathan, R. J. Masti, C. Soriente, and S. Capkun, "SALVE: Server Authentication with Location VErification," in *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2016.

APPENDIX

We attach our semi-structured interview script here. We prepared the following interview questions to ask participants about their Internet use, location and security awareness, and preferences on location.

Online Storage

1. Do you use online file storage services (e.g., Dropbox, Apple iCloud, Google Drive)? Could you mention some examples of how you use it?

2. What kinds of data do you store online? Are there types of data that you typically try not to put on the Internet?

3. Is there any information about yourself that you specifically try not to store on the Internet?

Email, Calendars, Contacts

4. Do you use online calendars like the Google Calendar, or the iCloud calendar? Can you elaborate on the types of events you mark on your calendar that you store online?

5. Do you use a web-based email service? What do you use it for?

6. Do you store your contact information online? What kinds of information do you store?

Finance and Shopping

7. Do you use online banking? Could you mention some examples of how you use it? E.g., just checking your balance, transferring funds, stocks investment or financial planning.

8. Do you use your credit card to shop online?

9. How do you choose where to shop online? What kind of considerations are likely to make you trust an online store? Will it make a difference to you if you know you can access a brick-and-mortar branch of that store?

10. When you are shopping online, how would you feel if store's domain indicates a foreign country?

11. What kind of precautions do you take around handling financial transactions online (whether with credit cards or online banking)? Do you store your credit card information online?

12. Are there any aspects of financial management that you would not feel comfortable performing online?

Social Networking

13. Do you use social networking or messenger services, such as Facebook, Google Plus, Twitter, Instagram, etc.? This may also include messaging services like WhatsApp.

14. Is there a difference in the kind of information you share to different platforms? What kind of considerations do you make before putting your information on different types of social media?

15. What are your concerns regarding your privacy on social networking websites, such as Facebook, Twitter, or Instagram?

Knowledge of Locations

16. When you store your files (photos, videos, documents) online, where do you think these files are stored?

17. When you visit a website, such as Wikipedia, Google Maps, or Yahoo News, where do you think the web content is stored?

18. When you visit a website, such as online banking or online storage, how do you know you are actually visiting the real website, as opposed to a forged website to steal your personal information? Are there particular indicators that you pay attention to?

Internet Service Location Preferences

Interviewer: We've so far talked about a lot of things you can do using the Internet. A lot of these services store your data in data centers located somewhere in the world. Companies also use these data centers to store information that you consume, such as news articles. Let's talk about your trust or various preferences regarding these data centers.

1. What are your privacy concerns about your data online? This might include files stored online, personal information, or credit cards?

2. Do you have any concerns about where your data are being stored? What kind of concerns? For example, where would you like your data to be stored?

3. Does your preference of where your data is stored depend on the type of data? Specifically, consider the following types of data: your banking account data, online shopping history, chats, emails, social networking data, hotel or flight bookings, etc.

4. Imagine that you are provided with information regarding the location of where your online services are. How would such information influence your trust in these services?

5. What kind of location information do you have in mind? How detailed would you prefer such information to be presented?

6. Imagine that the location information can be presented to you when you visit a website. How do you think this location information should be displayed?

7. If you had location information available to you, in what kind of services do you think it would be useful?

	Control			Experiment		
Stage	Mean	Mdn	SD	Mean	Mdn	SD
1	2.82	3	0.50	2.73	3	0.63
2	2.55	3	0.60	2.32	2	0.65
3	2.32	3	0.84	1.45	2	0.96

TABLE II: Descriptive statistics of task completion across different stages.

	Control			Experiment		
Stages	χ^2	df	p	χ^2	df	p
All	7.35	2	0.228	30.86	2	< 0.001
S1 vs. S2	–	–	–	3.62	1	0.513
S1 vs. S3	–	–	–	26.15	1	< 0.001
S2 vs. S3	–	–	–	10.52	1	0.011

TABLE III: Chi-squared tests of task completion across different stages using the Bonferroni correction. We did not perform pairwise tests on the control condition since we found no significant differences between all the stages.

Cond	Stage	Mean	Mdn	SD	Skew	Kurtosis
Ctrl	1	33.77	28	13.13	0.61	-0.35
	2	16.83	17	4.22	-0.59	1.44
	3	18.29	14	16.91	3.01	10.93
Expt	1	34.32	33	8.61	0.85	0.86
	2	16.64	15	6.63	0.30	-0.88
	3	54.02	41	45.12	1.11	0.77

TABLE IV: Descriptive statistics of decision-making times.

	Control			Experiment		
Stages	t	df	p	t	df	p
S1 vs. S2	6.01	21	<0.001	7.24	21	<0.001
S1 vs. S3	3.52	21	0.019	-1.74	21	0.868
S2 vs. S3	-0.43	21	1.000	-3.43	21	0.023

TABLE V: t-tests of decision-making times across different stages using the Bonferroni correction.

	Control			Experiment		
Website	Mean	Mdn	SD	Mean	Mdn	SD
Bank	2.95	3	0.21	2.64	3	0.49
Facebook	2.73	3	0.70	2.45	3	0.96
Dropbox	2.00	3	1.15	1.14	1	0.91

TABLE VI: Descriptive statistics of task completion across different websites.

	Control			Experiment		
Tasks	χ^2	df	p	χ^2	df	p
All	29.17	2	<0.001	32.07	2	<0.001
B vs. FB	2.41	1	0.962	0.53	1	1.000
B vs. DB	21.06	1	<0.001	23.32	1	<0.001
FB vs. DB	10.20	1	0.011	15.99	1	<0.001

TABLE VII: Chi-squared tests of task completion across different websites using the Bonferroni correction.