TLS Inspection: How Often and Who Cares?

TLS inspection — inline decryption, inspection, and reencryption of TLS traffic — is a controversial practice used for both benevolent and malicious purposes. This article describes measurements of how often TLS inspection occurs and reports on a survey of the general public regarding the practice of TLS inspection. This helps inform security researchers and policymakers regarding current practices and user preferences.

Mark O'Neill and Scott Ruoti
Brigham Young University and Sandia National Laboratories

Kent Seamons and Daniel Zappala
Brigham Young University

In 2013, one of us received email from a former student expressing dismay that his employer was inspecting his TLS traffic. His understanding was that this wouldn't be possible if his browser lock icon indicated that he had a secure TLS session with a webserver. He asked whether the practice was illegal or at least unethical without the employer notifying all of the employees that this was happening.

In fact, it's common practice for companies to inspect employees' encrypted traffic to protect their network from potential threats. This inspection is usually accomplished with a network device that acts as a TLS proxy, sitting in the middle of the communication between a browser and webserver, where it can intercept, decrypt, inspect, then re-encrypt and forward on the user's traffic to its original destination. This is done without any visible notification to the user that their encrypted traffic is being inspected. Although security experts view the inspection of encrypted traffic by attackers and governments as undesirable, it's less controversial for businesses and organizations to inspect their own encrypted traffic to secure their own network and intellectual property.

In this article, we first describe a measurement we conducted that demonstrates that TLS inspection is used actively for a small number of Internet connections, for both benevolent and malicious purposes. We then describe research we conducted to survey general users' opinions regarding the use of TLS inspection, to help inform security researchers and policymakers regarding their preferences.

TLS Proxies

When a web browser attempts to validate a website's identity, it relies on certificate authorities (CAs) that digitally sign certificates vouching for the identity of servers. Web browsers authenticate a site by validating a chain of trust from the site's certificate back to one of a set of trusted root certificates. These certificates comprise the root store and

Published by the IEEE Computer Society
1089-7801/17/$33.00 © 2017 IEEE

Related Work on User Attitudes about Online Security and Privacy

Prior studies have surveyed user's attitudes about their online security and privacy. Several themes in this research reflect similar findings in our work. Annie Anton and colleagues[1] found that users in both the United States and Europe are highly concerned about receiving proper notice and awareness of privacy risks. Users in our study strongly prefer notification and consent when their encrypted traffic is inspected.

Aleecia McDonald and Lorrie Cranor[2] reported on the chilling effect of online behavior advertising, with 40 percent of users self-reporting they would change their behavior if they learned advertisers were collecting data. We also found that users would change their behavior once they learned their encrypted traffic was being inspected.

Blasé Ur and colleagues[3] and Richard Shay and colleagues[4] find in both interviews and surveys that users have nuanced opinions about security and privacy, with respondents giving high-quality responses to open-response questions and discussing tradeoffs and implications of technologies in use. We likewise find that participants in our study are highly engaged in a technically dense topic and grapple with tradeoffs affecting their security and privacy.

References

1. A.I. Antón, J.B. Earp, and J.D. Young, "How Internet Users' Privacy Concerns Have Evolved Since 2002," *IEEE Security & Privacy*, vol. 8, no. 1, 2010, pp. 21–27.
2. A.M. McDonald and L.F. Cranor, "Americans' Attitudes about Internet Behavioral Advertising Practices," *Proc. 9th Ann. ACM Workshop on Privacy in the Electronic Soc.*, 2010, pp. 63–72.
3. B. Ur et al., "Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising," *Proc. 8th Symp. Usable Privacy and Security*, 2012, article no. 4.
4. R. Shay et al., "My Religious Aunt Asked Why I Was Trying to Sell Her Viagra: Experiences with Account Hijacking," *Proc. Sigchi Conf. Human Factors in Computing Systems*, 2014, pp. 2657–2666.

are typically bundled with the operating system or browser.

This validation system is currently being co-opted by the use of TLS proxies that act as a man-in-the-middle for TLS connections. A TLS proxy can issue a substitute certificate for any site the user visits, so that the user establishes an encrypted connection to the proxy rather than the desired website. The proxy can then decrypt and monitor or modify all user traffic, before passing it along via a second encrypted channel to the desired website.

TLS proxies can be used for both benevolent and malicious purposes. Some companies use TLS proxies to filter malware and viruses, prevent the leak of company secrets and intellectual property, block harmful websites, or catch malicious insiders. However, less scrupulous companies, government agencies, crime organizations, and others may also use proxies to steal a user's sensitive data, conduct surveillance, or commit identity theft. Currently, browsers and users have no method for distinguishing between benevolent and malicious TLS proxies, and the user is entirely unaware that an organization or attacker is intercepting encrypted traffic, except in the unlikely case that they manually inspect the certificate chain. Even when a TLS proxy is present, browsers display a lock icon that supposedly indicates the browser is communicating securely with the website.

To avoid browser warnings, TLS proxies generate substitute certificates signed by a CA that the user's machine trusts. This can be done in several ways:

- purchasing an intermediate certificate authority certificate;
- installing a new trusted root certificate on the user's machine (this can be done either by a business when configuring a machine or by malware);
- including a root certificate on a device's root store when it's manufactured;
- controlling a root certificate authority (governments are in a position to coerce authorities into granting them certificates for domains they don't own); or
- stealing existing root and intermediate CA certificates.

A variety of anecdotes have been shared in the press regarding the use of TLS proxies, where inspection of encrypted traffic is documented as having occurred. Reports have notified the public that both Nokia and Lenovo used TLS proxies to decrypt customer (not employee) traffic to improve performance or to insert advertising. Public outcry caused both companies to stop accessing encrypted traffic. Government surveillance has been reported to use similar methods,[1] such as a 2011 incident when Iran monitored 300,000 citizens online using a stolen certificate from DigiNotar, a trusted CA.[2]

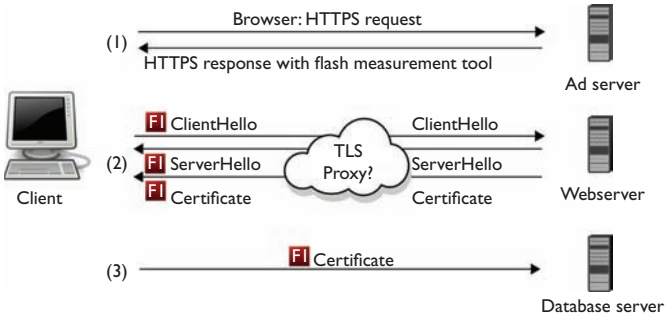

Figure 1. To detect TLS proxies, we embed a Flash application in an advertisement, which is automatically downloaded from an ad server and run by the browser. The application initiates a TLS handshake, records the messages received, and terminates the handshake. The application then forwards the retrieved certificates to the database server for analysis.

Measurement

Two recent measurement studies, including one we conducted, have sought to understand the prevalence and nature of TLS proxies on the Internet.[3,4] These showed that the vast majority of connections monitored by TLS proxies are (self-reported to be) for benevolent purposes, but a small percentage appear to be adware, grayware, and generally suspicious.

For our measurement study, we built a Flash application that could determine the presence of a TLS proxy and delivered it using an online advertisement. The tool runs silently from the user's perspective, with no user action required to install or run it, as Figure 1 shows.

Utilizing Google AdWords as a distribution mechanism, we successfully scanned for TLS proxy presence in 2.8 million connections across 142 countries in just two weeks. Of those tests, 11,764 (approximately 1 in 250) returned a different X.509 certificate than was served by our secure webserver, indicating the presence of a TLS proxy. The advertisement campaign cost just under US$5,000.

We found that many of the proxies self-identified through the Issuer Organization field of the substitute certificate. Table 1 shows a breakdown of the most common identities shown in the substitute certificates.

Most of the substitute certificates carry the names of popular client firewall software (such as Bitdefender) or companies (for example, Target Corporation), although it's also possible for an attacker to lie about who it is in the Issuer Organization field. There were also several Issuer Organization values of special note (marked with an asterisk in Table 1): self-identified malware (WebMakerPlus, Sweesh LTD), falsified Certificate Authorities (DigitCert Inc), and omission of any identification (Null). We categorized the reported Issuer Organization fields (see Table 2) and found that most were for personal or business firewalls. We also found numerous instances of negligent behavior by TLS proxies. For instance, Kurupira, a firewall technology that utilizes a TLS proxy and was detected in our study, fails to perform adequate certificate validation in the case of a man-in-the-middle attack. That is, if a user of Kurupira is behind a malicious proxy, Kurupira will blindly accept the attacker's certificate, exposing the user's sensitive data. We also found that TLS proxies downgraded the public key size of the original certificate when issuing a substitute in half of the studied connections. In addition to this behavior, we found 49 instances where TLS proxies had masqueraded as the CA of the original certificate and 110 instances where proxies modified the subject (owner) of the original certificate.

TLS proxy prevalence varies by region. While the overall proxy prevalence was found to be 0.41 percent, the top five most-proxied countries by percentage were France (1.09 percent), Canada (0.87 percent), Belgium (0.81 percent), the United States (0.79 percent), and Romania (0.74 percent).

Surveying the General Public

The diversity of TLS proxy behavior and prevalence found in our study prompted us to conduct a survey on user attitudes toward TLS proxies in the general public. The security community at large generally has considered TLS proxies to be malicious, yet our measurements suggested that many organizations and individuals were utilizing them for protective measures. Reconciling these two attitudes required additional insight from users themselves. We were especially curious about how users felt about TLS proxy use in different institutions and circumstances.

Accordingly, we surveyed 1,976 people across two surveys regarding their opinions of TLS proxies and their use in inspecting encrypted traffic.[5] Both surveys were conducted using the Amazon Mechanical Turk (Mturk) crowdsourcing service, a popular method for gathering participant data

for usability studies and user surveys. Research has demonstrated that data from Mturk participants is at least as reliable as those obtained via more traditional methods.[6,7] Participants were given $1 as compensation for completing each survey, and both surveys were approved by our Institutional Review Board.

The first survey asked 1,049 participants to share their opinions regarding the use of TLS proxies and the inspection of encrypted traffic. Participants were also asked their reasoning for why TLS proxies should or shouldn't be allowed, about their concerns, and what, if any, measures should be used to regulate their use. The results of this first survey showed a surprising willingness by participants to accept TLS inspection, provided they're notified first. To follow up on this result, which came from an open-response question, we conducted a second survey asking 927 participants about specific scenarios and whether it was acceptable for a TLS proxy to be used in each of these cases.

The full survey details and data from participants is available at https://soups2016.isrl.byu.edu.

Instructing Participants

One of the unique features of the surveys we conducted is that they cover a fairly technical topic that isn't common knowledge among average users. Limiting the survey to individuals with preexisting knowledge regarding TLS proxies would have limited us to participants with highly technical backgrounds, thus failing to gather information about broader opinions related to the inspection of encrypted traffic. Thus, we chose to first instruct participants about TLS proxies and their use in the inspection of encrypted traffic, before asking their opinions.

We developed neutral instructional material explaining the nature of TLS proxies to participants, which we presented at the start of both surveys.

Demographics

Most participants for the two surveys were from the United States (87 and 94 percent, respectively), with the rest primarily from India (11.5 and 5.7 percent, respectively). Participants were skewed toward males (61 percent), and ages were centered around 25–32 (46 percent). Most participants were single (60 percent) and had no children (62 percent). Nearly all participants had completed high school, with the majority having completed some level of higher education (57 percent). Participants were asked to self-report their level of knowledge of Internet security,

Table 1. The Issuer Organization field of the substitute certificates we detected provides hints as to their purpose.

Rank	Issuer Organization	Connections
1	Bitdefender	4,788
2	PSafe Tecnologia S.A.	1,200
3	Sendori Inc	966
4	ESET spol. s.r.o.	927
5	Null*	829
6	Kaspersky Lab ZAO	589
7	Fortinet	310
8	Kurupira.NET	267
9	POSCO	167
10	Qustodio	109
11	WebMakerPlus Ltd*	95
12	Southern Company Services	62
13	NordNet	61
14	Target Corporation	52
15	DigiCert Inc*	49
16	ContentWatch, Inc.	42
17	NetSpark, Inc.	42
18	Sweesh LTD*	39
19	IBRD	26
20	Cloud Services	23
	Other (332)	1,121

* Suspicious Issuer Organizations.

Table 2. Our classification of the Issuer Organization of the substitute certificates indicates most are firewalls, with some malware.

Proxy type	Connections	Percent
Business/personal firewall	8,101	68.86
Organization	1,394	12.66
Malware	1,112	8.65
Unknown	840	7.14
Parental control	156	1.33
Business firewall	69	0.59
Certificate authority	49	0.42
School	32	0.27
Personal firewall	11	0.09
Telecom	0	0

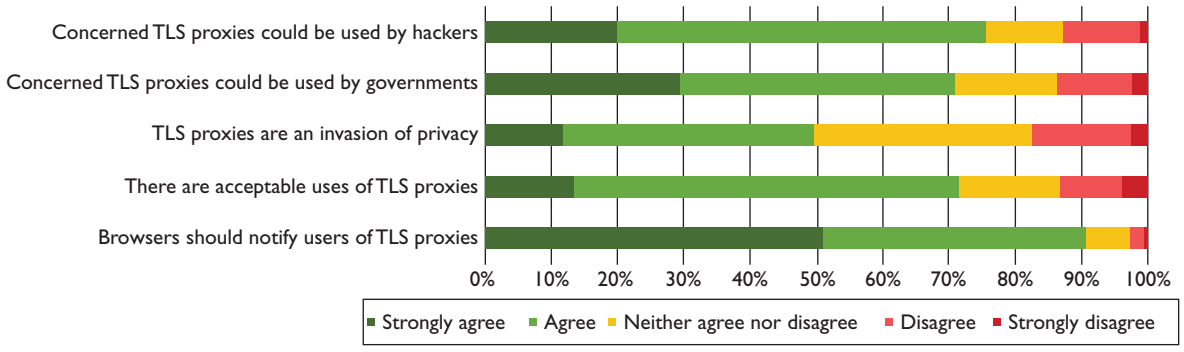

Figure 2. A 100-percent stacked bar graph of participant attitudes toward TLS proxies (N = 1,049). Colored segments represent the share their corresponding option has of total responses. There's strong support for notification by browsers.

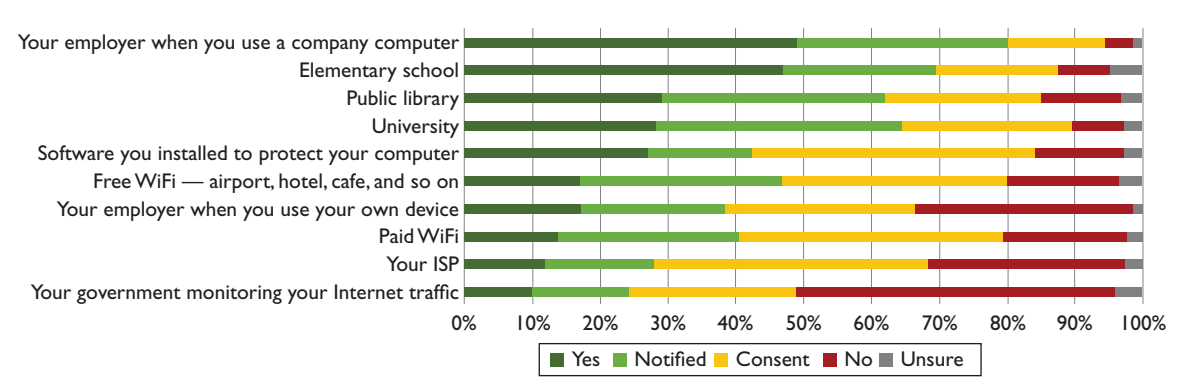

Figure 3. A 100-percent stacked bar graph of participant responses for scenarios to the question, Should the organization be allowed to run a TLS proxy? (N = 927). Colored segments represent the share their corresponding option has of total responses. From the top bar down, we see decreasing support for the mentioned organization running a TLS proxy.

with most rating somewhere between somewhat knowledgeable and mildly knowledgeable (78 percent). Most participants reported having little to no awareness of TLS proxies before the survey.

Survey Results

In this section, unless otherwise indicated, results are from the first survey of 1,049 participants.

Attitudes Toward TLS Proxies

As Figure 2 shows, participant opinions toward TLS proxies and the inspection of encrypted traffic are nuanced. Three-fourths of the participants (795; 75.8 percent) mentioned they worried about hackers, nearly as many were concerned about the possibility for governmental spying (743; 70.9 percent), and almost half (522; 49.8 percent) indicated that TLS proxies are an invasion of privacy. Despite these concerns, participants largely (752; 71.7 percent) felt that there were acceptable uses for TLS proxies.

One way to resolve these conflicts is for a proxy to notify users that it's present and to give users a chance to consent to their encrypted traffic being inspected. An overwhelming majority of participants (951; 90.7 percent) asserted that they wanted to be notified by their browsers of the presence of TLS proxies.

Acceptable Uses of TLS Proxies

Figure 3 contains a summary of results from the second survey, where participants were asked about their opinions regarding TLS inspection in specific scenarios. Participants are generally

willing to accept the use of TLS proxies in most situations, with acceptance ranging from 65–90 percent of participants, when summing together those who accept it, those who desire notification, and those who desire both notification and consent. For both employers (when you use your own computer) and elementary schools, the support for using TLS proxies without notification or consent from users is surprisingly strong (455; 49.1 percent and 434; 46.8 percent). In both cases, there's still strong support for either notification or consent (419; 45.2 percent and 377; 40.7 percent).

The strongest objections to any kind of TLS proxy are for government monitoring (437; 47.1 percent), using your own device at work (297; 32.0 percent), or using your own ISP (271; 29.2 percent). Note these latter two map to situations where the user has paid for the device or for network access. Users have stronger objections to TLS proxies when they pay for network access through a home ISP than when they pay for Wi-Fi when they're away from home.

When examining the differences among opinions for notification versus consent, participants generally favor consent in cases where they feel in control (at home, free Wi-Fi, or their own device at work) versus notification when an organization is in control (public library, school, or company computer). The strongest support for consent is with a personal firewall (385; 41.5 percent), your ISP (375; 40.5 percent), and paid Wi-Fi (358; 38.6 percent).

Notification and Consent

Participant answers to open response questions give further insight on their desires for notification and consent. A typical response was,

> *Well for some things it would be understandable, I'd just like to be informed so I know the risk I'm taking.*

One participant expressed,

> *If I encrypt something no one has the right to unencrypt it unless I give them the right to, simple as that.*

Participants expressed extreme distrust for those who would use TLS proxies without informing users, going so far as to say they "would hate them," "would wonder what they are looking for," and "would assume they were up to no good."

Others stated they would change their behavior if notified about a proxy, such as avoiding commercial transactions, using a VPN to circumvent a proxy, or self-censoring their Google searches and other online communication.

Informed Participants

Most of the participants showed a high level of engagement in the survey, sometimes offering lengthy and detailed responses. Participants clearly understood that there were tradeoffs involved with the use of TLS proxies to inspect encrypted traffic, weighing the benevolent uses for schools or workplaces and the danger of misuse by insiders or by hackers. As they struggled with this tradeoff, participant responses indicated confusion, doubt, worry, equivocation, and reasoned conclusions. One participant considered both good and bad uses and worried, "How are you supposed to know which is happening?"

Some participants weighed the tradeoffs and resolved the dilemma by deciding that proxies should only be used by consent. For example, one participant expressed,

> *I believe that TLS proxies are an invasion of privacy, as is anything that monitors my Internet usage without my permission. However, if you are using someone else's (like a company's) network, they have every right to make the rules of use. ... This is one of those doubled-edged swords — it can be used for your good and security and it can be used to harm and spy on you. Because of the distinct possibility of lost privacy, this type of proxy should [not be] used, except by your agreement, not by anyone else.*

Others wanted companies or schools to be able to use TLS proxies for security purposes, but also wanted to prevent them from being used for government surveillance or by hackers. Still others felt TLS proxies should only be used by the government to catch terrorists or criminals. Similarly, of the participants who were against the use of TLS proxies, the reasons for opposing TLS proxies were not amorphous, but concrete and rational. For example, one participant stated,

> *I think TLS proxies don't sound very safe because it sounds like an invasion of privacy. I don't think organizations should be able to decrypt your internet traffic and modify it and re-encrypt it. Perhaps they are just trying to protect against viruses and the like but it doesn't sound safe for the person using the Internet. What if this technology was*

misused? Someone could get [h]old of your financial information for example. It sounds to[o] risky. I wouldn't want to buy something online and risk someone having access to my credit card number.

The security and privacy community faces three challenges moving forward. First, our work clearly demonstrates users prefer notification and consent when legitimate proxies intercept their traffic. However, while there has been some work in the IETF proposing mechanisms that provide this functionality, there appears to be little community support for this work.[8,9] Moreover, even with such technical mechanisms in place, educating the general public about security and privacy indicators is hard,[10] and helping them to take action that matches their security preferences is equally hard.[11]

Second, our work highlights the need for stronger protection against malicious TLS proxies. Better safeguards should be employed to ensure that new trusted roots aren't added by malware and instead only by explicit administrator approval, with appropriate warnings. Monitoring software should quickly and automatically remove malicious certificates. Monitoring should also ensure that legitimate proxies correctly generate and use substitute certificates.[12]

Finally, better measurement tools are needed to continue monitoring the prevalence and nature of TLS proxies. Browsers are beginning to phase out support for Flash and major advertising networks are blocking the method we use. In the future, a community-driven, voluntary measurement platform might be the best way to collect these measurements, but getting a platform adopted by large numbers of users is a significant obstacle.

Acknowledgments

This work was supported by Sandia National Laboratories, a 2014 Google Faculty Research Award, and the US National Science Foundation under grant CNS-1528022. Mark O'Neill and Scott Ruoti contributed equally to this work.

References

1. C. Soghoian and S. Stamm, "Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL," *Proc. Int'l Financial Cryptography and Data Security*, Springer, 2012, pp. 250–259.
2. E. Galperin, S. Schoen, and P. Eckersley, "A Post Mortem on the Iranian DigiNotar Attack," Electronic Frontier Foundation, 13 Sept. 2011; https://www.eff.org/deeplinks/2011/09/post-mortem-iranian-diginotar-attack.
3. L.-S. Huang et al., "Analyzing Forged SSL Certificates in the Wild," *Proc. IEEE Symp. Security and Privacy*, 2014, pp. 83–97.
4. M. O'Neill et al., "TLS Proxies: Friend or Foe?" *Proc. Internet Measurement Conf.*, 2016, pp. 551–557.
5. S. Ruoti et al., "User Attitudes Toward the Inspection of Encrypted Traffic," *Proc. 12th Symp. Usable Privacy and Security*, 2016; www.usenix.org/node/197314.
6. M. Buhrmester, T. Kwang, and S.D. Gosling, "Amazon's Mechanical Turk: A New source of Inexpensive, Yet High-Quality, Data?" *Perspectives on Psychological Science*, vol. 6, no. 1, 2011; http://journals.sagepub.com/doi/pdf/10.1177/1745691610393980.
7. A. Kittur, E.H. Chi, and B. Suh, "Crowdsourcing User Studies with Mechanical Turk," *Proc. Sigchi Conf. Human Factors in Computing Systems*, 2008, pp. 453–456.
8. S. Loreto et al., "Explicit Trusted Proxy in HTTP/2.0," IETF Internet draft, work in progress, Feb. 2014.
9. D. McGrew et al., "TLS Proxy Server Extension," IETF TLS Working Group Internet draft, work in progress, July 2012.
10. A.P. Felt et al., "Rethinking Connection Security Indicators," *Proc. 12th Symp. Usable Privacy and Security*, 2016; www.usenix.org/system/files/conference/soups2016/soups2016-paper-porter-felt.pdf.
11. B. Berendt, O. Günther, and S. Spiekermann. "Privacy in e-Commerce: Stated Preferences vs. Actual Behavior," *Comm. ACM*, vol. 48, no. 4, 2005, pp. 101–106.
12. X. d.C. de Carnavalet and M. Mannan, "Killed by Proxy: Analyzing Client-End TLS Interception Software," *Network and Distributed System Security Symp.*, Internet Soc., 2016; https://madiba.encs.concordia.ca/~x_decarn/papers/tls-proxy-ndss2016.pdf.

Mark O'Neill is a PhD candidate in the Computer Science Department of Brigham Young University. His research interests include authentication, privacy, anonymity, and game theory. O'Neill has an MS in computer science from Brigham Young University. He's a member of ACM. Contact him at mto@byu.edu.

Scott Ruoti is a researcher at MIT Lincoln Laboratory, but he completed this work when he was a PhD candidate in the Computer Science Department of Brigham Young University. His research interests include usable security, secure email, cloud security, and blockchain-based research. Ruoti has a PhD in computer science from Brigham Young University. He's a member of ACM and Usenix. Contact him at scott@ruoti.org.

Kent Seamons is an associate professor in the Computer Science Department at Brigham Young University. His research interests include usable security, authentication, identity management, and privacy. Seamons has a PhD in computer science from the University of Illinois. He's a member of ACM and Usenix. Contact him at seamons@cs.byu.edu.

Daniel Zappala is an associate professor in the Computer Science Department at Brigham Young University. His research interests are at the intersection of networking, security, and usability. Zappala has a PhD in computer science from the University of Southern California. He's a member of ACM and Usenix. Contact him at zappala@cs.byu.edu.