From the Editors —
Isolating Insecurely: A Call to Arms to the Security and Privacy Community in the Time of COVID-19

Sean Peisert
April 14, 2020

Let's begin by saying this was not the letter I had originally planned on writing. However, I have the dubious distinction of writing this piece while the world is dealing with the coronavirus (COVID-19) pandemic. As I write this note, well over 1 million confirmed cases have been reported, and tens of thousands of people have died from the disease. Surely those figures will have risen substantially by the time this column will be published. Very thankfully, hundreds of thousands more who were positively diagnosed have now recovered.

Undeniably, our first duty is to keep ourselves, our families, our communities, and the general public around the world safe by following shelter-in-place rules and other, related public health measures, in order to contain the outbreak. Beyond that key measure, what else can the rest of us be doing to help improve the situation, perhaps beyond donating compute cycles on our laptops to the "Folding@home" COVID-19 effort [1]?

I find myself observing many colleagues in the life sciences participating directly in the response effort. Government agencies and philanthropists are sponsoring massive efforts to track the spread of the virus, stand up testing facilities, manufacture protective equipment, analyze the virus and its mutations, develop vaccines, and more. For the rest of us without advanced degrees in domains such as virology, microbiology, biochemistry, and biomedicine, being unable to directly contribute to the response can instill a helpless feeling, and I admit feeling some envy of my life science colleagues who are helping to prevent further casualties around the world.

At the same time, all of us can observe, unfortunately, that attackers have not taken a break from their usual activities. In many cases, their attacks may simply reflect run-of-the-mill escalations in the usual activity on the Internet, through an increase in COVID-19 related phishing [2], for example, to take advantage of increased anxiety and distraction due to the situation. Other attacks are more specific to the situation, more targeted, and more destructive. It is here where, even though, as cybersecurity and privacy professionals, we are not on the front lines of the virus response, we must rise to the occasion to provide support for the individuals and institutions who *are* on those front lines, and who will ultimately bring us through and past this situation.

Much of Planet Earth is now undergoing some form of "sheltering in place." In addition to sheltering in place, many of those who are still employed are teleworking. For those of us who live in areas with reasonable broadband network access, we are thankful the Internet can help get us through this time, be it socializing by video, online grocery delivery, or attending work or school. Indeed, around the world, students from kindergarten all the way through graduate school are trying to participate in remote learning activities. Recently, the lynchpin for much of this remote school and work activity, other than email and basic broadband Internet connectivity (which is not available in many rural areas around the world), has been videoconferencing, particularly the service provided by Zoom

Video Communications, Inc. In many cases, Zoom is now a lifeline that the world has suddenly come to depend on to function in an environment of physical isolation.

Alas, let us count the ways in which Zoom has failed its customers with respect to security and privacy [3]. Zoom's security-related processes and major security flaws will undoubtedly be rectified, and privacy practices addressed, now that they have been put in the spotlight. However, Zoom's failings are only one part of the story. The other part is the huge and rapid adoption of a software service, and the nature of the new user base. Zoom's traditional usage has been for business customers, who often have IT departments and security teams. In contrast, given the COVID-19 situation, tens of millions of very inexperienced users have begun to use Zoom for online classes and corporate meetings, and even some very large public meetings, and are often administering and using Zoom without sufficient expertise or training typically required for such an application. The consequences of adoption of key software by inexperienced users is something that all software developers should keep in mind — it has been a fundamental tenet of software engineering for decades that users should never be required to do what developers might expect.

While "Zoombombing" exemplifies the perfect storm of software flaws meeting inexperienced users, it is representative of a much broader set of computer security problems created by the pandemic. Among the more concerning ones that come to mind include the researchers working on COVID-19 who are now storing regulated data on their home computer systems. Or the testing labs running networked, automated machinery to suddenly examine thousands of samples a day to determine presence of the virus, only to fall victim to ransomware [4]. Imagine the potential effects of malware disrupting testing labs at scale, reducing or even tainting their output — experts in cyber-physical system security are immediately needed to examine the processes and build in the necessary safeguards. Or the global surveillance networks that are looked upon to provide authoritative information about the extent of the virus's spread, which are also highly vulnerable [5]. Consider the potential effects of tainting the inputs to the global surveillance network — expertise in data integrity, fault tolerance, cryptography, and other related disciplines are also clearly needed to make the network more resilient. In all these, and other related cases, we as cybersecurity and privacy professionals realize where we can best devote our attention, when we are at our most reliant on vulnerable digital systems.

I was heartened to read of the "COVID-19 CTI League" of security professionals that has banded together as a public service to help mitigate global cybersecurity threats, among others [6]. The scientific computing community, including one I am involved with, the NSF Cybersecurity Center of Excellence, "Trusted CI," has also stepped up to the plate to help support the science community's cybersecurity needs during this time [7].

Thus, like looters after London air raids or Atlantic hurricanes, it is discouraging, though not surprising, to see miscreants step up for their own benefit. It is at least as *encouraging* to see the other side of the coin in which the public, including cybersecurity professionals, have stepped up as volunteers to support public good.

One note of caution is that volunteer work from the security and privacy community must primarily or even exclusively be in the service of the cause, not in the service of future fame and glory from research publications. Security and privacy researchers descending on medical professionals in service of data for their next conference publication are likely doing

more harm than good. But researchers genuinely interested in bringing the *right* tools to bear on solving the problem at hand, by *listening* to medical professionals and putting *their* needs as primary, as I wrote about in this space last year, are desperately needed.

And yet there is much more work to do. The privacy question is one that has only begun to be addressed. While on one hand, many of the staunchest privacy advocates have argued for relaxation of privacy controls in order to develop better tests, "back to work" protocols, and vaccines and other treatments, the same advocates point out that any loss of privacy for the public good should be temporary, transparent, necessary, proportionate, and follow a due process [8,9]. What should solutions look like for data gathering, sharing, use, and disposal; or for protocols requiring strong individual identity verification and validation? Nobody really knows yet.

"Limited waivers" of enforcement of sanctions and penalties for the HIPAA Privacy Rule in the United States have already been put into place [10]. What direction will European countries take, with respect to GDPR? Will COVID-19 mitigation needs lead to the public's electronic health records (EHRs) and gene sequences being made even more broadly available for analysis, perhaps dramatically so? If so, how will it be done, and what will the effect be? Or, will the United States and European countries adopt somewhat Orwellian sounding smartphone-based "all clear" and "free to travel" indicators as China has? Or will a solution come to light that preserves individual privacy more strongly? There is a need and opportunity for experts in privacy-preserving analysis computation techniques, such as differential privacy or secure multiparty computation, to very quickly engage with stakeholders to bring usable and practical solutions to bear on these critical problems that properly balance key privacy and analysis properties.

Meanwhile, in the United States and elsewhere throughout the world (e.g., Croatia, Egypt, Iceland, New Zealand, Poland), all of this is happening in an election year, in which many primaries and perhaps even the entire general election may move to remote voting systems. In some cases, the shift will be to a vote-by-mail system, which for large states that still do a majority of voting in person, the shift might be challenging enough — securely managing lists of eligible voters, automatically printing and mailing ballots, automated signature comparison software, and securely leveraging systems to automatically count cast paper ballots. However, we now see numerous U.S. states advocating for a shift to voting over the Internet, which, given observations of past attempts in this area, the unequivocal conclusions of a recent National Academies report ("…the Internet should not be used for the return of marked ballots. … [N]o known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.") [11, 12], and letter from the American Association for the Advancement of Science's Center for Scientific Evidence in Public Issues (and other experts) [13], seems fraught with disaster. Legislatures of a range of sizes and jurisdictions are also considering online voting. Even without the scale of U.S. public elections, or the typical requirement in public elections of preventing association of individual voters with individual cast ballots, legislative voting presents its own set of challenges that must be carefully implemented for such processes to be properly secured [12]. The importance of election and computer security experts helping policymakers and election officials understand the conclusions from the National Academies report — even, or perhaps especially in light of the pandemic — cannot be understated. Readers of this piece: get engaged in anything from volunteer support for your city and county IT staff involved in elections, to helping educate policymakers.

Thankfully, again, I am heartened to see that the cybersecurity community seems prepared to step up to face these challenges. In addition to the aforementioned community efforts, Apple and Google recently jointly announced privacy-preserving solutions for contract tracing [14] (in addition to a variety of similar academic efforts [15,16]), largely to the approval of privacy experts, and Apple and Google have announced differential privacy and cryptographic mechanisms to monitor mobility without exposing individual identities [17]. I also see academic colleagues with expertise in machine learning addressing active disinformation campaigns that are spreading conspiracy theories about causes of and remedies for COVID-19 [18]. Finally, I see election process experts helping to educate policymakers, voting officials, and the public on the best paths forward for conducting elections by remote means (by mail, using paper ballots).

While I envy those who can directly contribute to the biological or medical portion of the crisis at hand, I'm also glad to support the biological and medical response through security and privacy, as well as providing the infrastructure that we rely on to get us through this time, and eventually have a key role in putting society back together again.

For my part, it's "all-hands-on-deck" to contribute everything I have to the response effort. For those security and privacy professionals who can, please join me — the challenges we face now and over the coming months require our expertise, and this is the time to bring your energy to being part of the Home Guard, to keep things running while the virologists and geneticists develop the solution that stems the tide of layoffs, infection, and death; that allows people to take off their masks and go back to work to earn livings; and lets the children go back to school and playgrounds to reopen.

References

[1] Folding@home COVID-19. https://foldingathome.org/covid19/

[2] U.S. CERT, "Defending Against COVID-19 Cyber Scams," March 6, 2020. https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams

[3] Glenn Fleishman, "Every Zoom Security and Privacy Flaw So Far, and What You Can Do to Protect Yourself," *TidBITS*, April 3, 2020. https://tidbits.com/2020/04/03/every-zoom-security-and-privacy-flaw-so-far-and-what-you-can-do-to-protect-yourself/

[4] Ionut Ilascu, "COVID-19 Testing Center Hit By Cyberattack," *BleepingComputer*, March 14, 2020. https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/

[5] Bruce Schneier, "Security of Health Information," March 5, 2020. https://www.schneier.com/blog/archives/2020/03/security_of_hea.html

[6] "International Cybersecurity Experts Come Together to Fight COVID-19 Related Cyberthreats," *CISOMAG*, March 31, 2020.

https://www.cisomag.com/international-cybersecurity-experts-come-together-to-fight-covid-19-related-cyberthreats/

[7] Von Welch, "Trusted CI, NSF CI CoE Pilot, and SGCI Offering Priority help to projects tackling COVID-19," Trusted CI Blog, March 17, 2020. https://blog.trustedci.org/2020/03/trusted-ci-nsf-ci-coe-pilot-and-sgci.html

[8] Cindy Cohn, "EFF and COVID-19: Protecting Openness, Security, and Civil Liberties," March 23, 2020. https://www.eff.org/deeplinks/2020/03/eff-and-covid-19-protecting-openness-security-and-civil-liberties

[9] New York Times Editorial Board, "Privacy Cannot Be a Casualty of the Coronavirus," *The New York* Times, April 7, 2020. https://www.nytimes.com/2020/04/07/opinion/digital-privacy-coronavirus.html

[10] U.S. Department of Health and Human Services, "COVID-19 & HIPAA Bulletin: Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency," March 2020. https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf

[11] National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy*, 2018. https://doi.org/10.17226/25120

[12] Andrew Appel, "Can Legislatures Safely Vote by Internet?" April 10, 2020. https://freedom-to-tinker.com/2020/04/10/can-legislatures-safely-vote-by-internet/

[13] American Association for the Advancement of Science, Center for Scientific Evidence in Public Issues (EPI), and other leading experts in cybersecurity and computing, "Letter to Governors and Secretaries of State on the insecurity of online voting," April 9, 2020. https://www.aaas.org/programs/epi-center/internet-voting-letter

[14] Apple, Inc. and Google, "Apple and Google partner on COVID-19 contact tracing technology," April 10, 2020. https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

[15] Carmela Troncoso, et al., "Decentralized Privacy-Preserving Proximity Tracing," April 10, 2020. https://github.com/DP-3T/documents

[16] Ron Rivest, et al., "PACT: An Open, Privacy-Preserving Protocol," April 8, 2020. https://pact.mit.edu/wp-content/uploads/2020/04/The-PACT-protocol-specification-ver-0.1.pdf

[17] Apple, "Mobility Trends Reports." https://www.apple.com/covid19/mobility

[18] Julian E. Barnes, Matthew Rosenberg and Edward Wong, "As Virus Spreads, China and Russia See Openings for Disinformation," *New York Times*, March 28, 2020. https://www.nytimes.com/2020/03/28/us/politics/china-russia-coronavirus-disinformation.html