Identifying the Disease from the Symptoms: Lessons for Networking in the COVID-19 Era

submission to IAB COVID-19 Network Impacts Workshop, 10/16/20

Alex Afanasyev (FIU), Lan Wang (Univ. Memphis), Edmund Yeh (Northeastern Univ.),
Beichuan Zhang (Univ. Arizona), Lixia Zhang (UCLA)

Although the Internet has long been an indispensable part in the daily life, the COVID-19 crisis has, as never before, accentuated the role of the Internet as the most critical lifeline for the economy and society at large. In the era of telecommuting and social distancing, network connectivity has been vital in maintaining the heartbeat of business (e.g., remote working, online shopping, and delivery services), education (e.g., remote learning), health (e.g., telemedicine), and social interaction (e.g., video and voice calls). At the same time, the pandemic has also presented the Internet with its most challenging stress test to date. This test has revealed striking shortcomings in today's Internet. As supporting evidences to this claim, we list below three specific issues: network resiliency, and equitable access, and cyberspace security.

Network Connectivity and Resiliency

Regarding Internet connectivity, although it has worked out amazingly well in general, our own experience from remote working also offered plenty of anecdotes about the inadequacy of the existing network infrastructure:

- During a recent online conference, a panel could not proceed as planned because the panel moderator lost his network connectivity at home;
- Our online lectures have experienced network outages now and then over time; and
- A few times when students were to take oral exams or give presentations, they had to go to the campus to perform the work, because their home network connectivity is not stable enough.

The last bullet hits the issue right on: home network connectivity used to be just that: network connectivity at home which is deemed non-critical, it seems adequate and economical; usually with a large disparity between down- and up-link capacities. However, the pandemic has made home network connectivity the connectivity for *WORK,* which is critical and requires reliable and robust throughputs in both directions.

If remote working is to stay, as all signs indicate it would be, a big challenge is how to enhance the vast number of residential networks (since people live everywhere) with the reliability and resiliency of campus and corporate networks. As explained in his 1977 paper,[1] Baran's vision for resilient network connectivity is by utilizing *any* existing physical connectivity. Unfortunately, that vision is not realized at the edges. Although in large cities, there is abundance of potential connectivity from multiple wired and wireless providers, home users by and large are dependent on a single ISP for connectivity. If we were to embrace Baran's vision, all of the available capacity across different providers and technologies could be effectively shared by the users, whilst intermittent failures of a single ISP not affecting the quality of experience of users. However, the reality is a virtual lack of choice when failures happen and limited capability (for home users) to easily utilize other existing/potential physical connectivity.

Equitable Access

While we identified the inadequacy of residential networks in supporting remote work, we also notice that the pandemic crisis has underscored the connectivity divide and challenges in equitable access. Roughly three million children in the US lack Internet access, consequently they cannot participate in remote learning. Networking and computing resources in rural and poorer areas are often seriously inadequate,

[1] "Some Perspectives on Networks—Past, Present And Future" by Paul Baran, 1977 IFIP Congress Proceedings. http://web.cs.ucla.edu/classes/cs217/ifip.pdf

putting the population living in those areas at a significant disadvantage in pursuing their livelihoods during this crisis.

The following news articles offer a glimpse into the evidence that COVID-19 has only intensified the digital divide in the society global wide:

- Digital Disparities in the Time of Coronavirus[2]
- COVID-19 has only intensified the broadband gap[3]
- Five ways coronavirus is deepening global inequality[4]
- "Pay the wi-fi or feed the children": Coronavirus has intensified the UK's digital divide[5]

Again, if remote working, remote education, and telemedicine are to stay, then it becomes imperative for the Internet technical community to find effective solutions to bridge the gap, instead of seeing the gap further widened. While the equitable access to the global Internet needs to be addressed on a level beyond the Internet architecture, equitable access to digital services does not necessarily require "global" Internet. In many cases, a localized access to computing, storage, and physical communication resources (which are increasingly plentiful and economical at the edges) should be enough to connect people and accomplish the tasks. The question becomes how to accomplish this and address the equitable access challenge, perhaps by exploring the use of "*data mules*" to bridge isolated communities (e.g., delay-tolerant networking to the very high delay end), and by establishing local community networks (e.g., to run locally scoped remote education sessions). However, neither of these can be easily realized with today's applications, which are increasingly cloud-focused, requiring "far-away" cloud rendezvous even when all parties are confined in a local environment.

Who is Responsible for Cyberspace Security?

Among the most salient networking challenges arising from the COVID19 crisis is the security of both network infrastructure and applications. Observation showed increasing incidences of DDoS attacks,[6] some of which were directed at websites critical to COVID-19 mitigation efforts.[7,8] As for application security challenges, the collaborative working platform Zoom offers an exemplifying case: Zoom usage exploded in a matter of days in March and suffered from widely-reported security and privacy crisis; yet the problem continues to this day:

> ***From:*** *Vice Chancellors of UCLA*
> ***Subject: Protecting our Community from "Zoom bombing"***
> ***Date:*** *October 9, 2020 at 1:06:52 PM PDT*
>
> *Over the course of the first week of the fall term[9], several Zoom classes and online community spaces were disrupted by individuals using racist, anti-Black, anti-Semitic, homophobic, transphobic, xenophobic and other hateful and discriminatory language. .....*
> *We are exploring additional security measures based on what we have learned from these disruptions. We also encourage instructors and other Zoom meeting hosts to review instructions on how to create a more secure Zoom session and what to do if a meeting is disrupted.*

[2] https://ksr.hkspublications.org/2020/04/10/digital-disparities-in-the-time-of-coronavirus/
[3] https://blogs.microsoft.com/on-the-issues/2020/05/21/broadband-gap-covid-19-airband/
[4] https://www.wider.unu.edu/publication/five-ways-coronavirus-deepening-global-inequality
[5] https://www.cam.ac.uk/stories/digitaldivide
[6] "Kaspersky: DDoS Attacks Spike During COVID-19 Pandemic", https://ksr.hkspublications.org/2020/04/10/digital-disparities-in-the-time-of-coronavirus/
[7] https://www.cisomag.com/attackers-launch-ddos-attack-on-food-delivery-startup-liefrando/
[8] https://www.vox.com/recode/2020/3/16/21181825/health-human-services-coronavirus-website-ddos-cyber-attack
[9] UCLA's fall term started on October 5, 2020.

More than a dozen security and privacy flaws have been discovered in Zoom.[10] To date, it still does not offer end-to-end data encryption for every user. It would be viewed as absurd if a car owner were asked to be responsible for enhancing the car's safety protection, but that is what UCLA is asking the campus community to do: going beyond simply setting up online lectures to figure out how to secure them and how to mitigate security incidents. We also note that Zoom had been a popular conferencing tool long before the pandemic. While some of its security vulnerabilities were evident, they were exploited on a large scale only after COVID-19 pushed it to become a frontline application. We speculate that security risks are likely pervasive in most Internet applications, and stand to be exploited in crisis situations, as they were for Zoom. The fundamental problem is that the Internet architecture lacks built-in support for data authenticity, integrity, confidentiality, and availability. Over the years many ad-hoc security fixes have been developed as add-on's to the existing protocol stack, without addressing the core architectural issues. Consequently the responsibility fell on application developers who have to become security experts to use these security fixes, and on end users who are expected to know how to choose strong secure passwords and how to configure various knobs for these mechanisms.

If a driver is not asked to enhance his/her car's safety protection, should a Zoom user be asked to assume such responsibility? Is Zoom the company responsible for it? Should the security responsibility be left to individual application development and deployment, or do we really need principled solutions for developing secure applications in general, just as car manufacturers develop principles for how to build safe vehicles?

Learn for the Future

The three specific issues mentioned in this writeup are not new. They had long been latent, but were brought to the fore by the COVID-19 crisis. We believe they are symptomatic of deeper underlying issues rooted in the existing network architecture. Baran's design of packet switching is an innovation that rose to the challenge of building a resilient communication network, which eventually led to the development of the Internet. Yet years of patch work around armoring TCP/IP's point-to-point communication channels has not brought strong defense against miscreants. The ever-increasing security threats have pushed the Internet away from Baran's vision into centralization within a short decade: centralized cloud services gain from economies-of-scale, as well as security protection that individuals simply cannot afford. Today's *cloud-centric security* efforts to secure data centers and the pipes to reach the data centers i) do not directly secure distributed applications (e.g., Zoom conferencing), ii) do not help with true edge computing, and iii) do not help with leveraging multitude of physical (shared) user connectivity, as well as iv) hinders creation of secure, direct peer-to-peer applications at the edge.

We believe it is time for the IAB to seriously examine today's situation, to forecast where the Internet would be ten years down the road by following its current trajectory, and to ask the hard question of whether a deep dive into an architecture re-examination is due, and if so, a serious exploration of a new Internet protocol architecture should follow. Developing a new architecture will take decades of efforts. TCP/IP itself took about two decades starting from Cerf/Kahn's 1974 seminal paper[16] to the rise of World Wide Web in the mid 90's. Named Data Networking (NDN) provides a concrete example of a new architecture that embeds systematic security layer, embraces multi-connectivity, and edge communication/computing. We would be happy to discuss at the workshop how NDN may help mitigate the above-mentioned challenges as well as other challenges facing the networked community today, and discuss how one may take a first step moving toward the NDN direction.

[10] "Zoom security issues: Here's everything that's gone wrong (so far)", https://www.tomsguide.com/news/zoom-security-privacy-woes

[16] "A Protocol for Packet Network Intercommunication," IEEE Transactions on Communications, May 1974.