Huawei proposes a 'New IP', but it is already here!

Huawei's 'New IP' has spurred intensive discussions in recent weeks. The 'New IP' research proposal was first unveiled at the International Telecommunications Union meeting in September 2019 and the white paper describing it as well as a few PowerPoint presentations were made available to the public [1] [2] [3]. At the end of March 2020, the Financial Times published an article [4] covering this. A flurry of articles with rather inflammatory headlines followed, such as, "China Wants to Control All the internet With 'New IP' Plan"[5], or "China's 'New IP' proposal to replace TCP/IP has a built in 'shut up command' for censorship"[6].

The Chinese government is known for censoring their domestic internet through the Great Firewall and we are sympathetic to the fierce reactions this proposal and its suspected implications sparked. **But we also believe that simply bashing it without closer inspection does not do it justice.**

The classical internet has issues that are not trivially dealt with. People in the networking community have repeatedly been hopeful that a proposed patch or extension to the core technologies would solve some long-standing problems, only to be disappointed years later when the sluggish speed of adoption became apparent. Even worse, some of these patches introduced unforeseen new issues that exacerbated the resistance to deployment.

Huawei are not the only ones that believe that small changes might not be enough, that the design principles used to create the original internet are incomplete given today's requirements and a clean redesign is necessary to truly address some of its fundamental problems.

Resolving the internet's issues has been a continuous research topic in the Network Security group under Adrian Perrig for over a decade and we second the opinion that incremental changes are unlikely to achieve a satisfactory level of security. Therefore, we proposed the SCION secure internet architecture. SCION stands for Scalability, Control and Isolation on Next-generation networks and is the first clean-slate internet architecture with security as the core design goal.

‘New IP’ has already arrived, and it is called SCION.

This article aims to shed light on Huawei’s ‘New IP’ proposal and to contrast it with our future internet architecture. **We especially would like to emphasise that a next-generation internet can be achieved while staying true to the important principles of openness and decentralization that are valued throughout the internet community.**

Before we dive into Huawei’s proposal, we need to introduce a bit of background on the origin of the internet Protocol (IP):

IP was developed in the 1970s to provide a unified addressing scheme for any device wanting to use the interconnecting network that was just beginning to form. In these early stages, this was mainly meant to connect local networks in the academic and military context. The people involved in this effort had no way to predict how fast this would grow into the internet we know today, and what problems would have to be tackled at a later stage. The IP scheme was designed with a 32-bit fixed address length, as the designers envisioned the resulting ~4.3 billion addresses to be sufficient for their purposes. Additionally, IP does not come with any inherent security mechanisms since the small number of early network participants could trust each other, and the most pressing issues for the early internet were to design an operational internetwork.

By the late 1980s, when the internet experienced much growth, people started anticipating that the allocated address space would not be enough. IPv6 was introduced as a draft standard in 1998, which quadrupled the length of addresses. More than 20 years later, only about a quarter of networks actively announce that they can reach machines via IPv6[7]. This example illustrates how difficult it is to make changes to a globally deployed system, which involves modifications of the core protocols.

Missing security features of IP and related protocols were no big deal when the network was only used by a few select industries. But as the network expanded and became accessible to the general public this quickly changed. Now, malware could be sent directly through the network instead of having to rely on floppy disks for spreading. In the year 2000 the first large-scale denial of service attacks was recorded. A denial of service attack attempts to exhaust resources of a service, often related to the network, such that legitimate users are blocked from accessing it. The internet protocols are deliberately misused to hide and amplify such attacks, and the lack of intrinsic security in their design makes this possible. A series of systems were built on top of the core protocols to try and mitigate such issues. But just as with IPv6, those mechanisms are slow to be deployed globally.

Huawei identifies a series of issues which stem, in part, from the security oblivious design of these early internet protocols. Let us take a closer look.

A point they stress repeatedly is the *inflexibility* of the original *addressing scheme*. Addresses are fixed size and they are typically assigned according to topological connectivity. This was sensible in the early days when computers were still clunky human-sized boxes standing in data centres. Nowadays, with the rise of mobile phones and the internet of Things, this could indeed be seen as a handicap. Some applications which are power constrained might benefit from using shorter addresses to conserve energy for transmission, but today this is only possible by setting up a separate system which translates the smaller addresses back to standard IP before forwarding packets to the general internet. They argue that this will lead to the formation of 'ManyNets', meaning that the internet could degrade into a collection of islands with incompatible communication protocols which then would have to be painfully reconnected through protocol translators. Additionally, Huawei argues that the correspondence of IP addresses to geographic location raises privacy issues.

The second point they make is that today's networks are too unreliable and do not make enough of a *distinction for different types of traffic* with respect to forwarding. On parts of the internet today, a mechanism is in place which treats traffic differently based on ten general service classes[8] [9]. One notable application example is Voice over IP (VoIP), which is very sensitive to high communication latency. This traffic can be marked for the network to attempt speeding up delivery. But this is very coarse grained as no finer distinction can be made between the pre-set traffic classes. Practically, this system cannot provide any guarantees—in terms of latency and bandwidth—for traffic transported by the inherently heterogeneous internet.

Further, they directly critique the *lack of security in the core protocols* which, in combination with the flat and open structure, renders the internet vulnerable to denial of service attacks. Moreover, today's end-to-end encryption system (the secure hypertext transfer protocol HTTPS), whose goal is to make sure that communications over the network cannot be read by passive eavesdroppers on the forwarding path, is ill-designed and vulnerable to so called man-in-the-middle attacks, where an active entity intercepts the secure connection.

To address these issues Huawei proposes an array of requirements the new networks should meet:

1. A flexible and variable-length addressing scheme, which provides stronger privacy than today's location-based addressing.
2. A mechanism to provide different Quality of Service for different traffic types mainly in relation to latency and bandwidth. This includes the use of multiple paths to meet high bandwidth requirements.
3. An improved key exchange mechanism to mitigate man-in-the-middle attacks.
4. The possibility to audit and shut down connections to protect against denial of service attacks.

What are the concrete solutions envisioned by Huawei?

The focus of the white paper is on the flexible addressing scheme where they sketch a preliminary proposed conceptual implementation for their 'New IP' header. It is only in the technical presentation that we can find a bit more detail on how this would work. In a nutshell, they propose to decouple the identity and location of a user by assigning different IDs to both. An Encrypted Identifier would be assigned to each user binding the identity through an Identity Manager. The inner address would get obfuscated at the domain border router, providing additional privacy. Subsequently the border router encapsulates this inner ID with a second address (called the Locator) which is then used to route through the internet. The second geographically significant address would not be tied to the individual user, but rather the network where the packet originated from, removing some potential for tracing.

To enable Quality of Service, they mention the possibility for encoding user preferences for traffic treatment in their 'New IP' header. There is very little detail on this, and it is unclear how the network would succeed in delivering these guarantees. There is no more mention of multipath after they list it as a requirement to meet the needs of high bandwidth applications.

Security is only mentioned in the presentations and this is the point that aggravated people and spurred the wave of articles. Their slide describing the network architecture includes an 'Accountability Manager'. This is labelled as a 'Decentralized Public Key Database' and they explain that this module together with the Identity Manager can be used to audit and therefore trace a connection. They present this in combination with the controversial 'shut off' protocol, which should be used to filter malicious traffic and protect the network from denial of service attacks. There are no details on an improved key exchange mechanism, but our assumption is that this would also be implemented through this 'Accountability Manager'.

It is important to stress that these designs are very preliminary. There are barely any details on how the network would function and, depending on the implementation, very different outcomes are possible. If the Identity Manager and the Accountability Manager would be controlled by the same entity, this would indeed constitute a worrisome mechanism that could be abused for censorship, built into the core of the internet. But as it stands right now, such claims seem premature.

Huawei identifies several valid problems of today's internet and tries to propose solutions for some of them. They further claim that these proposals are intended to spur worldwide research in this field, which is a motivation we agree with. The attitude that "The internet cannot be changed" has put enough of a damper on bold ideas and it is time that we start taking proposals seriously on redesigning the internet.

Isn't SCION already offering solutions there?

We already mentioned at the start of this article, that Huawei are not the only ones thinking about how to solve some of the internet Protocol's intrinsic problems. Even though the idea has remained somewhat niche, a workshop proposing the consideration of a clean-slate design for the next-generation secure internet can be found as early as 2005[10]. We from the Network Security group at ETH Zürich are convinced that the study of such systems will prove crucial to solve many of the issues of today's ossified internet. **Towards this goal, we have done extensive research on the basis of our proposed architecture—SCION.**

Let us dive into it.

The SCION internet architecture aims to replace the current internet core protocols on a global level. But locally everything can stay the same if people wish to keep it that way. **It is important to keep the next networks compatible with existing infrastructure or the new system will not stand a chance at being deployed.**

SCION represents a fundamental departure from today's routing-table based internet. Instead of routers learning which of their direct neighbours can reach a set of addresses, we encode the end-to-end path (**over all the ISPs**) of the packet directly in the packet header. This approach greatly simplifies multipath communication since choosing a different path does not need to be signalled to the routers but can simply happen by switching the path in the header of the packets. **With this capability, the sender of the traffic can choose which regions of the world the packets will traverse, making sure it does not cross untrusted parts.**

SCION provides numerous features and additions to improve internet communication, for instance a decentralized public key infrastructure that can be used to authenticate traffic.

Let us briefly take a look at how SCION already meets the requirements listed by Huawei:

1. Since the SCION architecture does not impose any limitations on how local networks are managed, administrators are free to implement any addressing scheme they want. The EDGE will encapsulate local traffic with the SCION header in order to forward it over the global network. Huawei's approach is conceptually very similar.
2. A new system built on top of SCION (currently in R&D) provides Quality of Service guarantees (end-to-end, meaning over multiple ISPs) based on the idea of myopic local resource reservations.
3. The public key infrastructure in SCION is built in and supports heterogeneous trust relationships.
4. **We disagree that an audit system is needed to protect against denial of service attacks.** Instead the new way paths are chosen and encoded makes it possible to 'hide' certain paths by not announcing them publicly. These paths can then be communicated to legitimate users out of band creating 'virtual leased lines' which cannot be used by an adversary who does not know of the cryptographic values needed to use these paths. Furthermore, one of the fundamental requirements we aim to provide through the new Quality of Service system is 'botnet-size independence'. This means that guarantees will be upheld even while the network is under a denial of service attack.

The last point is where our approaches fundamentally differ. We aim to provide a decentralized way to defend against denial of service attacks while preserving the key property of openness that is highly valued and arguably, the internet's greatest strength. These mechanisms cannot be abused for censorship as an audit system might.

But this is not all.

While Huawei mentions in passing that the current way paths on the internet are discovered is insecure, they so far did not provide an alternative. Changing and securing this mechanism is an active area of research in our group. In SCION the paths get discovered through a process called 'beaconing' which is a hierarchical approach to disseminating paths, inherently more scalable than today's mechanism. SCION's decentralized public key infrastructure is designed to capture the heterogeneous trust relationships present in today's geopolitical climate. This flexible mechanism ensures that the logic of the network responsible for learning routes cannot be disrupted by untrusted entities, which is not the case on today's internet. Furthermore, the decentralized nature ensures that multiple parties have to collude to achieve disruption which greatly lowers the likelihood.

Much thought has been put into making SCION compatible with today's networks to allow incremental deployment. We believe that such considerations are indispensable for a system's adoption.

How far along is SCION?

Fortunately, the SCION internet is more than just a proposal aiming at spurring further research in this area.

First, **a research network called SCIONLab has been operational since 2016.** The current infrastructure is based on 34 Autonomous Systems (AS) distributed across the world, connecting over 100 user ASes running on heterogeneous systems. Much of the connectivity is running as overlay on top of the current internet but several connections between networks are native SCION.

SCION also has an open source reference implementation, and anyone is welcome to join the global research network and experiment with this new infrastructure.

For more information about SCION visit scion-architecture.net[11]

Second, when the word about SCION spread, the demand for a commercial solution grew. In mid-2017, Anapaya Systems was founded to fill this need.

Now, several ISPs are offering better availability, security and control guarantees to public and private organisations which are looking for improved communications over a public network. Together, these ISPs form the kickstart of the next-generation internet, reliable and secure.

For more information about Anapaya's industrial-grade products visit https://www.anapaya.net[12]

Conclusion

Huawei's 'New IP' proposal has spurred renewed interest in the area of next-generation Internet architectures. While some claim that no additional clean-slate designs are needed and that the current Internet works just fine, others are more open to address the fundamental issues of a 30+ year old architecture with a next-generation solution. While we do not have a crystal ball to know the best way forward, our determination as researchers drives us to imagine and invent the ideal future network. Even if not deployed, we will at least have a measuring stick to assess the quality of the current Internet. But sometimes new technologies do disrupt the existing systems, even if deemed unlikely at first.

About the author

Christelle Gloor is a PhD student in the NetSec group with a passion for better teaching technology. In her spare time, she loves to sing or play volleyball.

References:

This article refers to the following sources as available on 25 May 2020.

---

[1] S. Jiang, "New IP Networking for Network 2030,": https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019101416/Documents/Sheng_Jiang_Presentation.pdf

[2] Huawei Technologies Co. Ltd. (China), China Unicom, and Ministry of Industry and Information Technology (MIIT), "'New IP, Shaping Future Network': Propose to initiate the discussion of strategy transformation for ITU-T." Sep. 23, 2019: http://prod-upp-image-read.ft.com/ec34d7aa-70e6-11ea-95fe-fcd274e920ca

[3] Z. Chen, C. Wang, G. Li, Z. Lou, S. Jiang, and A. Galis, "NEW IP Framework and Protocol for Future Applications," p. 4

[4] A. Gross and M. Murgia, "China and Huawei propose reinvention of the internet," Mar. 27, 2020: https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2

[5] R. Jennings, "China Wants to Control All the internet With 'New IP' Plan," *Security Boulevard*, Apr. 24, 2020: https://securityboulevard.com/2020/04/china-wants-to-control-all-the-internet-with-new-ip-plan/

[6] C. Chen, "China's 'New IP' proposal to replace TCP/IP has a built in 'shut up command' for censorship," *Private internet Access*, Apr. 03, 2020: https://www.privateinternetaccess.com/blog/chinas-new-ip-proposal-to-replace-tcp-ip-has-a-built-in-shut-up-command-for-censorship/

[7] RIPE NCC, "IPv6 Enabled Networks." http://v6asns.ripe.net/v/6?s=_ALL

[8] R. Barik, M. Welzl, A. Elmokashfi, T. Dreibholz, S. Islam, and S. Gjessing, "On the utility of unregulated IP DiffServ Code Point (DSCP) usage by end systems," *Perform. Eval.*, vol. 135, p. 102036, Nov. 2019, doi: 10.1016/j.peva.2019.102036.

[9] K. H. Chan, J. Babiarz, and F. Baker, "Configuration Guidelines for DiffServ Service Classes." https://tools.ietf.org/html/rfc4594#section-4

[10] S. M. Bellovin, D. D. Clark, A. Perrig, and D. Song, "A Clean-Slate Design for the Next-Generation Secure internet," in *Report for NSF Global Environment for Network Innovations (GENI) workshop*, Pittsburgh, PA, Jul. 2005, p. 27.

[11] "SCION internet Architecture." https://www.scion-architecture.net/

[12] "Next Generation internet. Reliable. Secure." https://www.anapaya.net/