lanacion·com

Saturday July 18, 2015 | Published in print
The compu

Internet Spy is to attack the system

rres | NATION CONTINUE

thor and others Try it How it works

View profile

In general, we use the network without thinking about how it works. It is here and now. However, there is a group of men and women, mostly volunteers-that make the Internet should go, to be there and now. Part of the IETF, the Internet Engineering Task Force (Task Force Internet Engineering) which gives rise to the standards of the network, in particular those related to the package TCP / IP protocols.

One month, one of the organizations related to the inner workings of the Internet, almost exactly the Internet Corporation for Assigned Names and Numbers (ICANN, for its acronym in English), made its fifty-third session here in Buenos Aires and then I had the opportunity to sit and talk with Finn Jari Arkko, Chair of the IETF (a position equivalent to president, although the IETF tend to avoid those formalities). He also was with us Barry Leiba, who besides working in Huawei, working with the IETF in applications and security-related standards.

"The main reason we're here Arkko- plucked saying is that it is conducting an ICANN meeting and, although we are not Icann, we are together in the transfer of some of the roles of the US government in maintaining Internet to a community of ICANN and the IETF (http://www.lanacion.com.ar/1674480), and that is the reason why so many people have come to participate in this joint project this week. For us It is a great place, Buenos Aires is a beautiful city, but also in April 2016 will have a meeting of IETF here. It will be the first time in South America.

Why first? Why did not you come earlier?

Jari Arkko: -Tendemos to go places where participants are originally. 10 or 15 years ago were the United States and Europe. Recently, Asia has become an important source of Internet technology. So we traveled a lot there. Now we see a growing participation of Latin America, and we want to be here. But we also want to be open to different types of organizations: academia, manufacturers, operators, governments, regulators. We are here for everyone, not for a select group. That's our goal, and meetings are only part of the issue.

-¿Tradicionalmente, Latin America has not contributed significantly to Internet technology, do you?

JA: -The participation is growing. In some cases the participants are not currently living in the region but are originally from here.

Cristian O'Flaherty, who works for Global Crossing's senior education manager of the Internet Society (www.internetsociety.org), and who is also with us in the talk, she gives examples: "Those who are developing in Latin America are not the most popular protocols, such as HTTP or IP, but, for example, Argentina is very active in security technologies. " Meanwhile, Leiba notes: "We record where contributions are, in terms of who publishes proposals and who come to meetings, for example, in the case of China, first the interest and participation grew, and then that. it became a major publishing standards. In the case of Latin America are seeing the same growth curve, with increased interest and participation in meetings, perhaps 30 or 40 people. " "There are now more people in the meetings, but most of the participation is through mailing lists, and that's hard to measure," O'Flaherty observed.

I have listed several questions here. This is perhaps not the most important, but its profile in the IETF says you usually communicate with your washing machine through Facebook. what does that mean? [Laughs]

JA: Let me explain. Many of the people who work in the IETF is voluntary. I work for Ericsson Research, in Finland, where I take care of the Internet of Things (IoT; https://es.wikipedia.org/wiki/Internet_de_las_cosas), through prototypes and that sort of thing. But before we begin that task was already a hobbyist that made all kinds of things that sound pretty crazy, and that gave me a firsthand experience of what works and what does not. One of those things I tried is a kind of social interface for IoT, it is easier for me, as a human, for receiving messages within the same stream of posts where everything else read.

-Querría Clarify something that is little known Internet. Is it true that anyone can propose an RFC (https://es.wikipedia.org/wiki/Request_for_Comments) and thus expand the possibilities of the Internet?

JA: Yes, that is so.

-how do you do that. A mail is sent?

JA: -One way is to join a mailing list, see if others have a need or a similar problem (if it's something very specific like mine with washing machine, probably not flourish), and then on the move developing. The beauty of the Internet is that anyone can build things on it without asking the government or network operators or your mother.

But that is partly changing.

JA: I dare say no.

Otherwise I'll say: There is a danger that this state of affairs changed.

JA: There is a danger, yes, some threats to innovation without permission. Yet certain things are happening, like what Barry is doing with real-time communication using the browser, something that was previously reserved for Skype and other companies were able to provide VOIP (https: //es.wikipedia .org / wiki / Voz_sobre_Protocolo_de_Internet) and video conferencing. Now anyone with a browser can do the same. The same with the IoT are doing so you do not have to build a separate network to communicate with your toaster or whatever you want to communicate.

I was thinking more along the concentration (YouTube, Facebook, Netflix). I wonder how would a startup, as they were once Google or Facebook, to grow in the current environment.

Barry Leiba: When YouTube allowed people to climb video that was something new, something people could not do before. They came up with the idea, created the system and put it online and became popular. The key here is to bring a sense of something that people will be interested. I think there is no danger of that stops occur in the meantime keep available the model of innovation without permission. The fact that Google has grown so much and offer so many services and is not limited everywhere who else has an idea and implemented.

I must assume that the IETF is in favor of net neutrality.

JA: -The net neutrality is a significant issue. The IETF has discussed that, but what we do is make sure that the services and protocols that are developing are available to all. We are trying to clarify how the administration of the network can operate in a neutral way and we are recommending these mechanisms. What we can not force anyone to work a certain way. But we want to provide the recommendations and skills to operate in a neutral way.

What do you think of the latest decision of the FCC neutrality (http://www.lanacion.com.ar/1765804-proponen-que-internet-sea-un-servicio-publico)?

IETF -the per se does not have an opinion on the issue of neutrality. One problem in analyzing neutrality is that it is too easy to put it in terms of black and white. In practice it takes to make decisions, and that makes it not a matter of black and white, as commercial and political discussions often make it appear. I am optimistic that we will still have the model of innovation without permission in the future.

Okay, let's talk about your work rather than policy [laughs]. Internet is seen as something that has a vulnerability that allows it to turn it off. this is so?

BL: That's mostly like that, yeah.

'Is there any great weakness in Internet?

JA: Let me mention to both. A few years ago I was concerned that the Internet is too stable, we could not change anything important, that we would always have IPv4 (https://es.wikipedia.org/wiki/IPv4) and TCP (https: //es.wikipedia. org / wiki / Transmission_Control_Protocol) and the same versions of all protocols, and that could not be fundamental changes. In the last two years I have seen that it is not, there is a huge amount of innovation in the area of the Web, which just launched the HTTP / 2 protocol (https://es.wikipedia.org/wiki/HTTP / 2), which is the first major redesign in its history, and we are already thinking about what comes next, HTTP / 3. And we're also seeing how we reorganized all other protocols. For example, TCP, does only control or security must also do? We think of how to combine the things we have today in new ways. So that weakness is not.

-and the other?

JA: 'The other is security. When we talk about Internet security seems banal; if we safer Internet, everyone will be happy. But it is not so simple. It is a huge issue, it is very complicated and has technical components, but also other. I'll say briefly what we are doing in the IETF about this. We are always concerned about safety, of course, and in several respects. For example, we have had many fights in the past two decades about whether to allow encryption in the network. Fortunately, it was decided so. Without that decision, the e-commerce could not exist. In addition, we have revelations that many more surveillance than we thought, and more widespread, and the IETF, after much debate, decided that mass surveillance is a threat to Internet communications. And we decided that because if the protocols have some weakness that a security agency can exploit, then criminals can do tomorrow. So we can not really leave any vulnerability. We are trying to eliminate those weaknesses. We are working on algorithms that operate under HTTPS (https://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure) and TLS (https://es.wikipedia.org/wiki/Transport_Layer_Security), and a new version of TLS . HTTP / 2 is faster, but also more efficient in terms of safety. That is, the security of the connection will not impact the performance of the connection, as before. And we have created new working groups, after Snowden's revelations, specifically to address the privacy issue.

-You Published a document (https://tools.ietf.org/html/rfc7258) where specifically say the widespread surveillance amounts to an attack. That's strong. Why put the same height monitoring an intelligence agency and an attack on the Net?

BL: If you can not tell someone who is doing surveillance and is considered the good that is intercepting the data on the Web and is a criminal, if protocols can be operated, then it is an attack on the system. It is not a political statement. We only say that if there is a vulnerability, we have to fix it.

He assumes, however, that it is monitoring because it can not be detected. Is a vulnerability or attack?

BL: -Interceptar private data is an attack.

But that's the mission of the NSA (www.nsa.gov), to cite an agency.

JA: Yes, it is. We are not making a political statement or a value judgment. We are making a technical statement. If there is a protocol that has a weakness that allows monitoring the communication, there is a problem.

Is it a problem with the monitor or the protocol?

BL: It's a problem with the protocol. We are not saying whether the NSA or other security agencies had the right to carry out this monitoring, and if that is right or wrong. What we say is that if a protocol that allows monitoring, then it is not safe and we must change that.

I love to see the IETF widespread monitoring equated with an attack on the communications, but what is possible shielding protocols and network infrastructure so that even an agency with vast resources of the NSA can perform this monitoring ?

JA: Yes and no. No we have perfect knowledge, but the recommendations of everyone in the community say cryptographic tools strong encryption and cryptographic protocols are still our best bet and they will ensure against attacks, of course if we use the correct algorithms . So I think it is possible to protect us, if we are careful and properly designed our technology. But that's only part that concerns the security of telecommunications, because if you communicate with someone you do not trust completely, that person may be induced by the government to deliver your data.

My feeling is that we will never feel safe, after Snowden's revelations.

JA: And we'll never have a perfect safety. The best we can do is apply the best technologies we know. That means it's the best we can do, not their best. Not to say that no one is going to break that security, but it is better than we do.

'Meanwhile more than 1000 million people are jumping on Facebook almost every little detail of their private lives.

BL: And do voluntarily and completely insecure.

JA: -Tools very popular encryption such as PGP (https://es.wikipedia.org/wiki/Pretty_Good_Privacy) have come a long way, but remain vulnerable to things like, "Do you trust your computer?"

-Many People believe, and that includes me, that the Internet was born as a military development, given the circumstances in which it was created. That is, that Arpanet originally had the goal of providing the US a communication mechanism that could withstand a nuclear attack. US denies today. What is the truth?

BL: Nor Jari and I were at this time, but ARPA [today DARPA; http://www.darpa.mil] is a government agency that is part of the Department of Defense. Their projects were solved by the military, but most of the developments made universities. I think the US is sincere when he says he did not create Arpanet as a military system, but developed with military backgrounds, so there was at least the idea of a communication system for disaster, if not anything more.

JA: 'I think it's an interesting perspective, but ultimately does not matter, because what we have is a general purpose technology that is flexible and that is why it has been so enormously successful.

BL: I think that what happened does not affect Internet today.

If it's true, we have transformed a military project in the most democratizing technology from Gutenberg to here, and a disruptive form of communication for 3000 million. We did not do too bad.

BL: It's especially interesting because it has changed the lives of millions of people, for good.

You spoke of the IoT few minutes ago, and it's something interesting and largely unavoidable. We are moving towards a world in which everything is interconnected (even your washing machine). But what are the challenges?

JA: There's multiple problems. There is a widespread security problem. And there's a privacy issue. That is, how much information distributed, and that on many levels. And there's a maintenance problem. Many devices there are, where they are, what their addresses and others. There has to be a smarter way to manage and maintain all that by hand. So there are problems, yes, a lot of work to do.

I know that nobody likes to risk predictions, but what changes provide for in 10 or 15 years?

BL: Well, some things are easy to predict, as the number of connected devices will grow and we have to do something with that. But within 10 or 20 years there could be a radical change in the nature of things. For example, you think of your self as something that has. Perhaps in the future it is no longer so, maybe cars are a service you purchase. And everything will be connected, the car will go to load naphtha for theirs when needed. For many of us it will be strange, because we have the mind shaped differently and see the cars as possessions. But for younger that it will be natural. Even the concept of many businesses will change, I think that will be something that comes.

-Díganme Something that has drawn attention of Buenos Aires.

BL: This is my first trip to Buenos Aires and now I've had from meeting to meeting, I have not seen much.

JA: It's a lovely city, starting with the fact that your winters are warmer than our summers.

New York Times | Technology