**Trust-to-Trust in Networks**

The Internet was developed for users who were friends or colleagues, and shared the same academic values. The users trusted each other, and the use was controlled by self-regulation. However, during the past 15 years the Internet has been a commercial network where users do not trust each other, and a small minority of users earns money by exploiting the majority. Hence, unwanted traffic is an every-day phenomenon.

Various malware, unwanted advertisements and unwanted emails or SPAM are spread via the Internet. Spamming is a business run by a couple of hundred actors. The remaining 1.7 billion Internet users suffer from this activity. Wireless traffic makes the problem worse, because radio frequencies are a limited resource and user devices are battery powered. Spamming is the starting point for a value chain of gray economy on the Internet. The chain includes professional hackers. This type of operation is profitable, because service fees are not associated with traffic volumes and since the Internet's "best effort" principle means that everything possible is done to serve the sender. The result is that the cost of the communication is born by the receiver both in terms of the wasted time and energy and in terms of equipment purchases and their operational costs.

To protect their private networks and own users, corporations use private IP addresses that are inaccessible directly from the Internet. The client program on a host in a private address space must initiate the connection. Corporations also use firewalls to protect their private networks. Today, firewall programs are commonly used on end users' own computers as well. None of these belong to the Internet's "official" architecture.

Within the next few years we will be running out of IPv4 addresses. At the same time, more equipment, especially wireless devices, are being connected to the network. The official solution offered for the future Internet technology is IPv6, in which the routing addresses are 16 octets long. The address field makes it possible to issue a different IP address for roughly 50,000 quadrillion ($10^{24}$) devices per each inhabitant on the Earth.

For myself, I would certainly not find it desirable that trillions of devices, if I will ever own that many, perhaps even including my own home's security protection, heating, or contents of my fridge, would be visible to any user on the Internet. It is quite likely that also in the IPv6 environment, users will want to hide behind private IP address spaces and to protect themselves with firewalls. Besides, having a firewall only in a wireless device does not really work. Unwanted traffic must be bounced off before it consumes the battery of the wireless device or capacity of the radio interface.

There is a good reason to ask ourselves, what we really need this gigantic IPv6 address space for? Lately, I have been telling that we don't need it at all. It does more harm than good. It aggravates the scalability problems on the Internet and increases unwanted traffic.

In my opinion, the future Internet must be thought of as a network of trust domains. Each trust domain has its own address space. The trust domains never show their addresses to each other. In addition to the address, each packet contains the identity of the receiver and the sender. At the trust boundary, we create state for each connection, flow or session between two or more users. The identities are the search keys for finding this state, and the interface device can legitimize the connection to the desired extent. Depending on the policy applied, the interface device can allow new inbound packet flows to pass directly or, for example, identify the sender based on a method supported by the trust domain network. This solution would allow us to continue using IPv4 on host computers and in domain wide networks.

Every corporation or home is a natural private trust domain. Due to scalability, the IP networks providing public services could be organized as a separate public service trust domain with reciprocal relationships managed between administrations, not per packet but through an umbrella system working on the background.

Firewalls and private address spaces represent reactive means of protection. We know that the problem of unwanted traffic cannot be solved by defensive methods only. Like in war, you need to attack in order to win. Therefore, we need a system that tracks down and evaluates the senders, and sending networks based on the proportion of traffic sent that is unwanted by the receivers. This might be a starting point for rolling costs of communication from the receiver to the sender.

Raimo Kantola
Professor on Telecommunications Technology
Aalto University