Professor Raimo Kantola
Ph.D students: Jesus Llorente Santos and
Hammad Kabir

IEEE TrustCom 2015
Tutorial – Customer Edge Switching

Room 11;
Friday, Aug-21, 15.15 – 17.00
Saturday, Aug 22, 10.20 – 12.05

Customer Edge Switching (CES) is a novel network architecture aiming to improve Internet security by admitting all traffic only after policy negotiation between the receiver and the sender. CES introduces customer network edge nodes that execute the policies defined by the receiver and the sender. A CES node is a replacement of a Network Address Translator making it possible to unilaterally initiate flows to hosts in a private address space. It is also a cooperative stateful firewall that, in addition to admitting and dropping flows based on local rules, can make additional queries before the final admit/drop decision. All aspects of CES are policy controlled.

Traffic from a CES node to a CES node is tunneled using a suitable tunneling method.

By defining suitable policies, the receiver's edge node can eliminate source address spoofing before admitting a flow – a result is that flooding a host, e.g. a mobile host and its air interface with attack traffic becomes impossible with classical simple methods. Another result is that for admitted traffic, it is always possible to put blame on the sender and its network administrator. The consequence is that CES increases the motivation of collecting evidence on all malicious activity, sharing that evidence among administrations and using reputation and trust evaluation for making better admission decisions.

CES is augmented with the functionality of Realm Gateway (RG). Due to RG, a legacy Internet host can unilaterally initiate a flow to a private host served by the receiver's RG. The RG uses heuristic methods to counter DDoS and other attacks. Flow admission is based on a local policy or a policy based on shared information within a trust domain.

Due the RG functionality, CES can be introduced one network at a time. CES and RG translate between forwarding protocols such as IPv4, IPv6 and Ethernet making the choice of the forwarding protocol a decision that can be taken by each administration independently.

We propose to introduce CES as a part of 5G networking functionality. The justification is that 5G is expected to provide ultra-reliable communications in particular for machine-to-machine. The argument is that no network where legitimate services can fail due to malicious activity can be ultra-reliable. Malicious activity is inherently unpredictable. Therefore, the reliability of network service under failures due to malicious activity is undefined: one cannot even put a number on it.

CES blends the boundary between closed, VPN-like, and open, Internet-like, networking. We believe that this serves the needs of an economy where X-as-a-Service is commonplace.

The tutorial explains and demonstrates the concepts, the algorithms and the testing results of Customer Edge Switching and Real Gateway developed at the Comnet/ Aalto University. Our implementation is geared to comply with the concept of Software Defined Networking (SDN) and uses OpenFlow between the Control and the Data planes.