# Implementing Trust to Trust Using Customer Edge Switching

Raimo Kantola

Aalto University

Finland

# Agenda

- Big picture
- Identities
- Customer edge switching in operation
- Deployment and Challenges
- Conclusions

Work partially sponsored by FP7 ETNA project and ICT SHOK in Finland

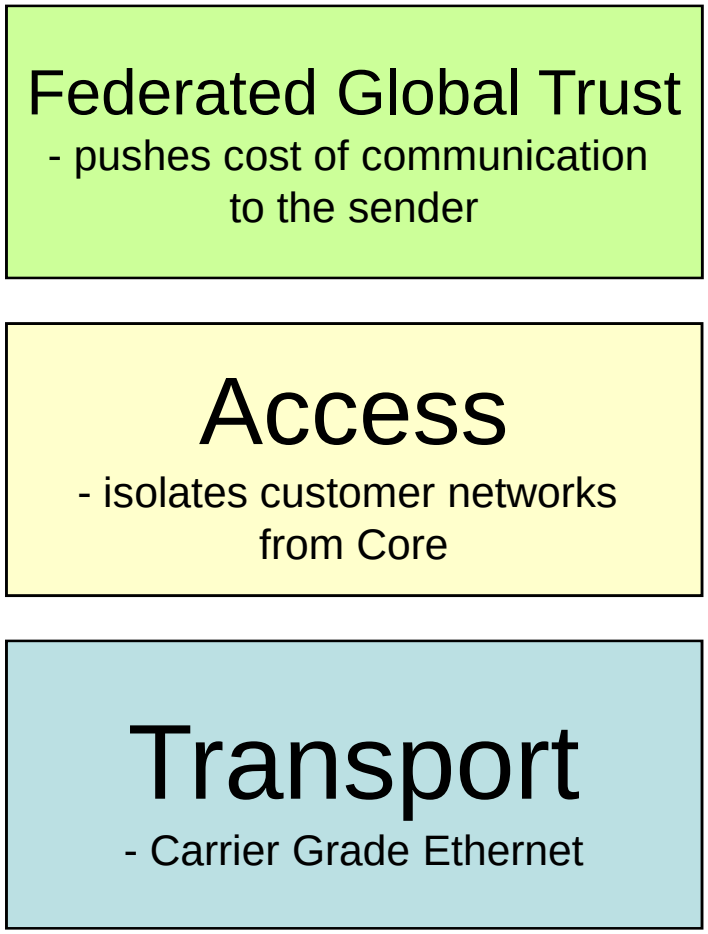
# Problems in the Internet

- Lack of Trust – middleboxes: NATs and Firewalls are not part of the ”Architecture”
  - Recommended NAT Traversal method = UNSAF does not scale well to mobile devices
  - FW on mobile device exhausts battery
- Scaling the core, multi-homing
  - Tunneling based edge – not yet an accepted technology
- Unwanted traffic – cost of communication is born by the receiver

# Principles: from End to End → Trust to Trust

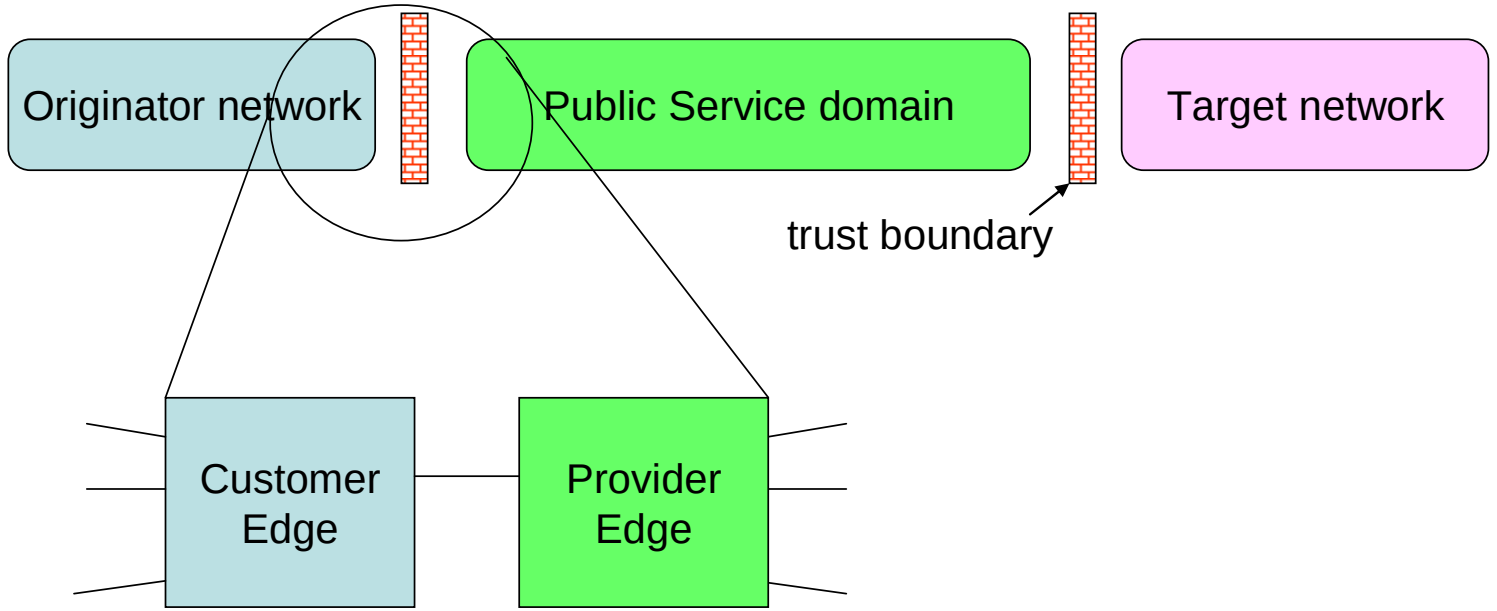
- By Dave Clark
  - End to End argument, 1984
  - Trust to trust, 2007:
    *The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at points where it can be trusted to perform its job properly.*

# Three Tier Program for Trusted Internet




- The war against unwanted traffic can not be won by defense only
  → Global Trust System
- Each tier can progress independent of the others

# Communication Path is a Chain of Trust Domains




Trust domains do not publish address information to each other.

A Packet crosses a Trust Boundary by presenting 2 IDs: source ID and target ID.

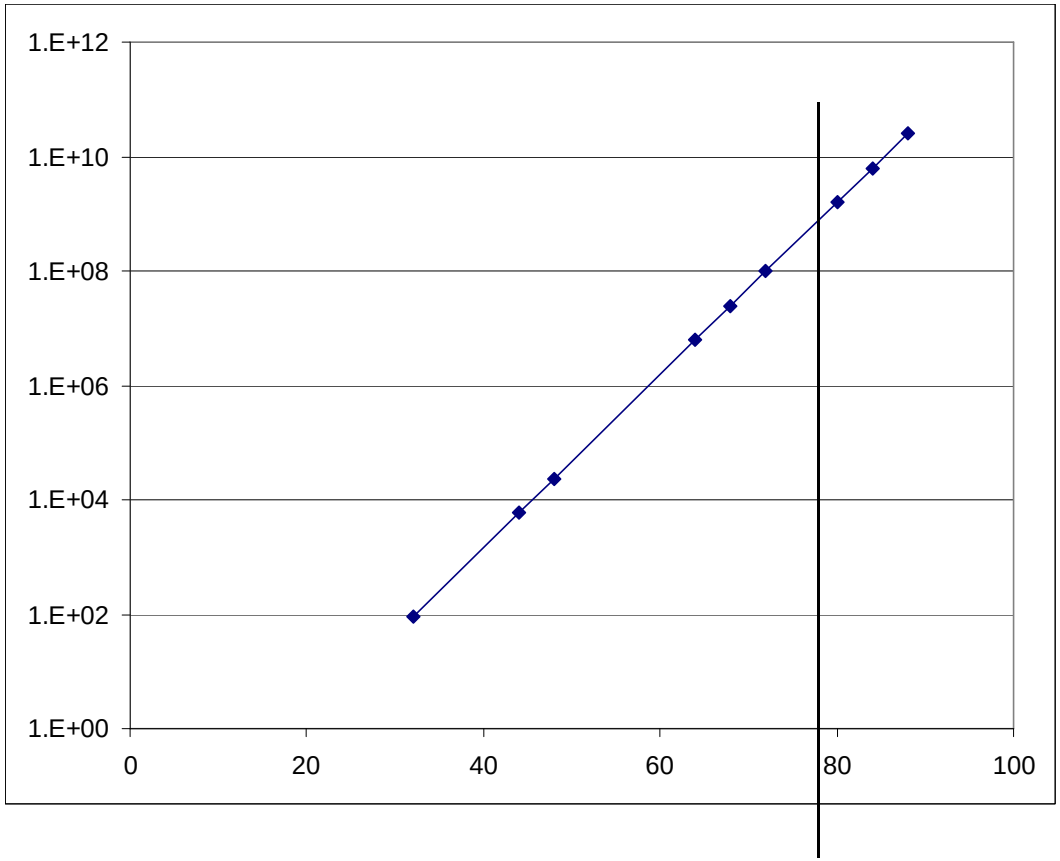
There is  connection state on the Trust Boundary.

# What kind of IDs

- Globally unique deterministic IDs
  - high OPEX
- Temporary ID is managed by the visited Network
  - How to preserve ID in case of multi-homed networks and roaming accross national borders
  - ID blocks are allocated like frequencies in GSM → management cost
- Random IDs managed by the home network
  - Clear responsibilities for trust provisioning
  - ID does not need to change in case of multi-homing or roaming → if ID stretched to hosts, TCP session can be preserved

## How many bits are needed for random user identities used in CES nodes?

NROF Ids
In a single
CES




NROF Bits

This is based on the birtday paradox. We assume that the probability of a clash of identities is < 1 in a million when all uits are compared one by one. If uit dependent filtering akin to address dependent filtering in NATs is used, a pair of uits is compared to another pair of uits. This gives an additional safety margin.

# Assumptions

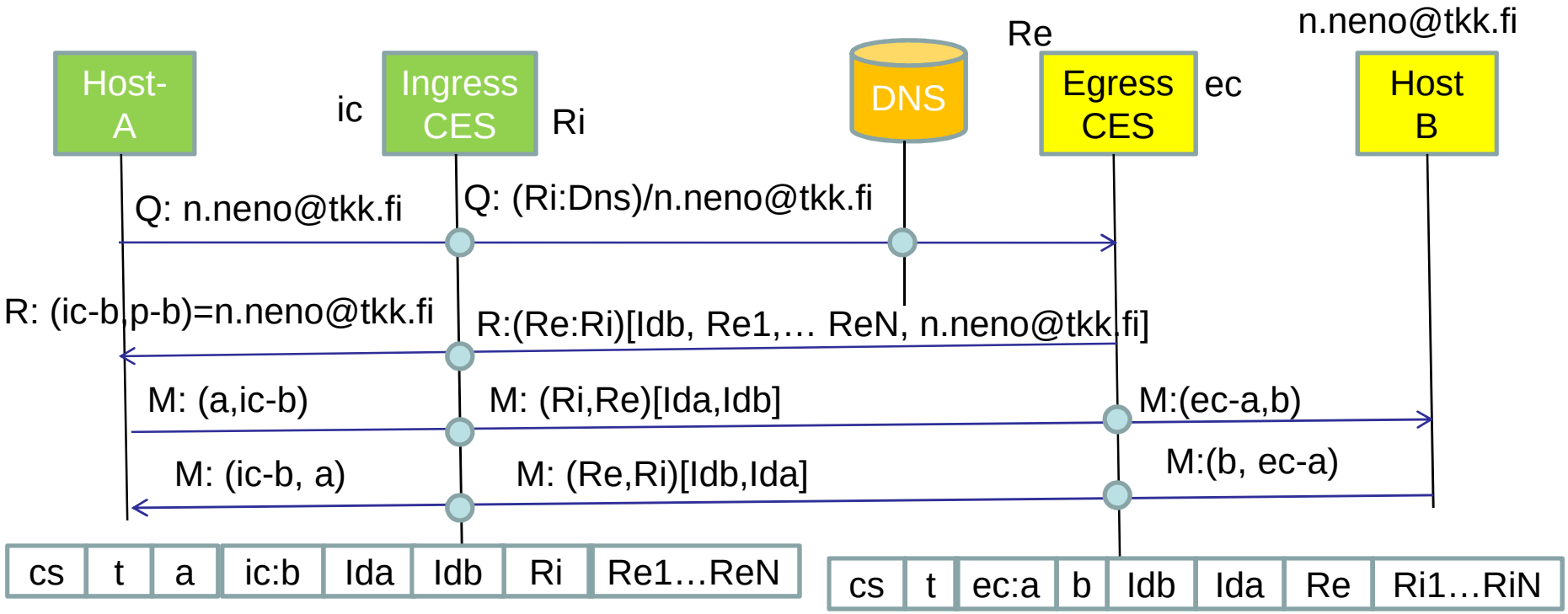
- Transport: routed IP, IP/MPLS, MPLS-TP or Carrier Grade Ethernet (a'la ETNA)
- Users are connected to User Networks (UN) (stub networks
  - UN-A is the network of the initiator of communication, UN-B is the destination UN
  - each has one or several Customer Edge Switches each with one or more routing locators
  - CES-A is in sender's network, CES-B in the target network
  - CES owns a large pool of IP addresses (s) in its private network
  - User network can be e.g. mobile access or a corporate network
- There is a DS – Directory Service
  - e.g. DNS with particular configuration (no new RRs or changes to the protocol) can be used

# Customer Edge Switching

variant with random IDs managed by the home network

- CES = Customer Edge Switch
- User Identity Tag = UIT identifies a user or a service or a host (or an application on a host).
  - is generated from a name + other parameters by a hash (or other) algorithm selected by the home network administrator
- Protocol stack
  - IP over ”MAC”-in-MAC
  - IP over new T2T protocol over IP
  - Etc → Forwarding method is orthogonal to how we do the access

# Message Flow




a – IP address of host a
ic – address pool of ingress CES
ic:b – IP address representing host b to host a
p-b – port allocated by i-CES for communication with host b
Ri (Ri1….RiN) – Routing locators of ingress CES
Re (Re1 …ReN) – Routing locators of egress CES

Ida – ID of host a
Idb – ID of host b
ec – address pool of egress CES
ec:a – IP address representing host a to host b
cs – connection state, t - timeout

# Trust processing for inbound flows in Egress CES

- Any sender is a suspect → track behavior, deny all service to and black-list scanners and too active senders
- ACK TCP SYN to detect source address spoofing, similarly send COOKIE in SCTP
- Send a puzzle to the sender
- Authenticate the sender
- Tighten policy towards suspects
- Swap all IDs when under attack
- Firewall rules managed by hosts
- etc

# Ease of deployment

ALL CASES
+ develop CES as an extended NAT
+ configure DNS appropriately
+ egress CES also hosts proxy ingress CES for compatibility with legacy senders
+ no changes in hosts
+ provides incentives to invest both to mobile operators and corporations
+ no ”alternative topology” like in LISP

**Carrier Grade Ethernet core**

- Low header overhead
- Full OAM for mission critical communications

**IP core**

- Cuts into MTU like LISP

# Challenges

- http, ssh, mail protocols traverse CES nicely
- SIP, FTP (others) that pass IP address information on a control channel rather than query DNS do not traverse a simple CES
- Solution: CES has to look up protocol field and use an *application specific state machine* (similar to what Firewalls do)
  - protocols such as SIP/SDP should really use names instead of IP addresses…
  - Are needed for DNS, FTP and SIP/SDP

# Conclusions

- CES is an implementation of the Trust-to-Trust principle advocated by Dave Clark
- Global communication takes place using global names, local addresses and local IDs.
- End-to-End connectivity is based on switching on trust boundaries + routing elsewhere
  - is like NATxNAT
  - why do we need IPv6?
  - scales as well as NAT scales in terms of the network and better for mobile hosts
- Works with Ethernet Core, with IP or IP/MPLS or MPLS-TP core