Aalto University
School of Electrical
Engineering

Embedding Trust into the Network *and 6G*

Raimo Kantola
raimo.kantola@aalto.fi
Aalto University, Comnet, Finland

6G Vision Webinar, Oct 28th, 2020

Agenda

- **Motivation**
- **Two views**
  - User centric view of trust
  - Network centric view of trust
- **How to get there**
- **So, what is the challenge?**

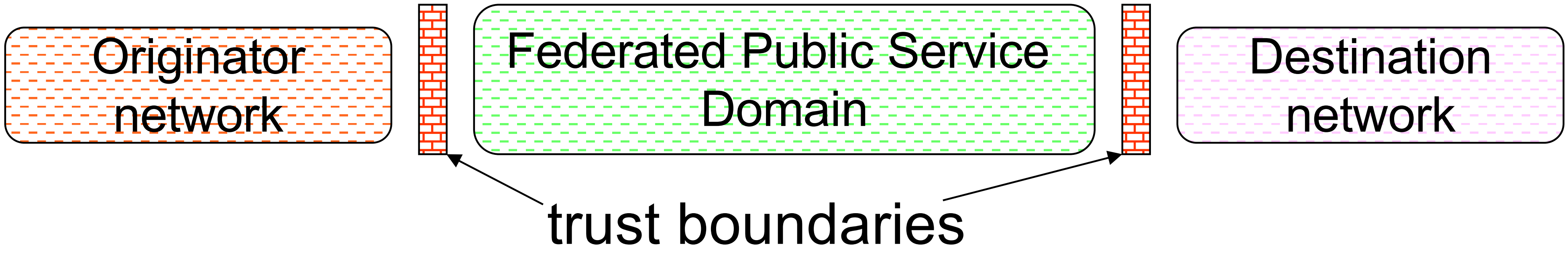
Boundary between digital and physical worlds in the new battleground

- **6G is about integration of sensing/communication and programming the world → digital + physical world crime can use it!**
  - Already 5G is at the agenda of superpower politics.
  - 6G will be at the heart of it!
  - SDGs are about Global Cooperation → Enhancing trust is key to success!
- **Vertical use cases: 5/6G is used in vertical markets to carry industrial data within control loops**
  - New attack vectors; new types of crime!
  - Hacking –> physical world crime can be supported by networks more than before!
- **Security=safety; only MNOs/ISPs could help by using cloud services**

6G CyberSecurity threats – End to End

- **6G terminals/networks support high bitrates → powerful attack tools in the hands of hackers**
- **Vertical markets: boundary of physical/digital world, if hacked**
  - Many critical infra use cases: industry, health, traffic…
  - Physical world crime can be supported by hacking
  - People can be killed by ”accidents” that are hard to investigate
  - IoT manufacturers have a business interest to gain access to usage data – high level of end-to-end security does not help in this, rather the opposite
  - Very attractive targets for Hybrid warfare!
- **Classical Internet security threats: DDoS, Prefix hijacking, global kill switches in current Internet, ransomware, epionage etc.**

User Centric view of embedding trust

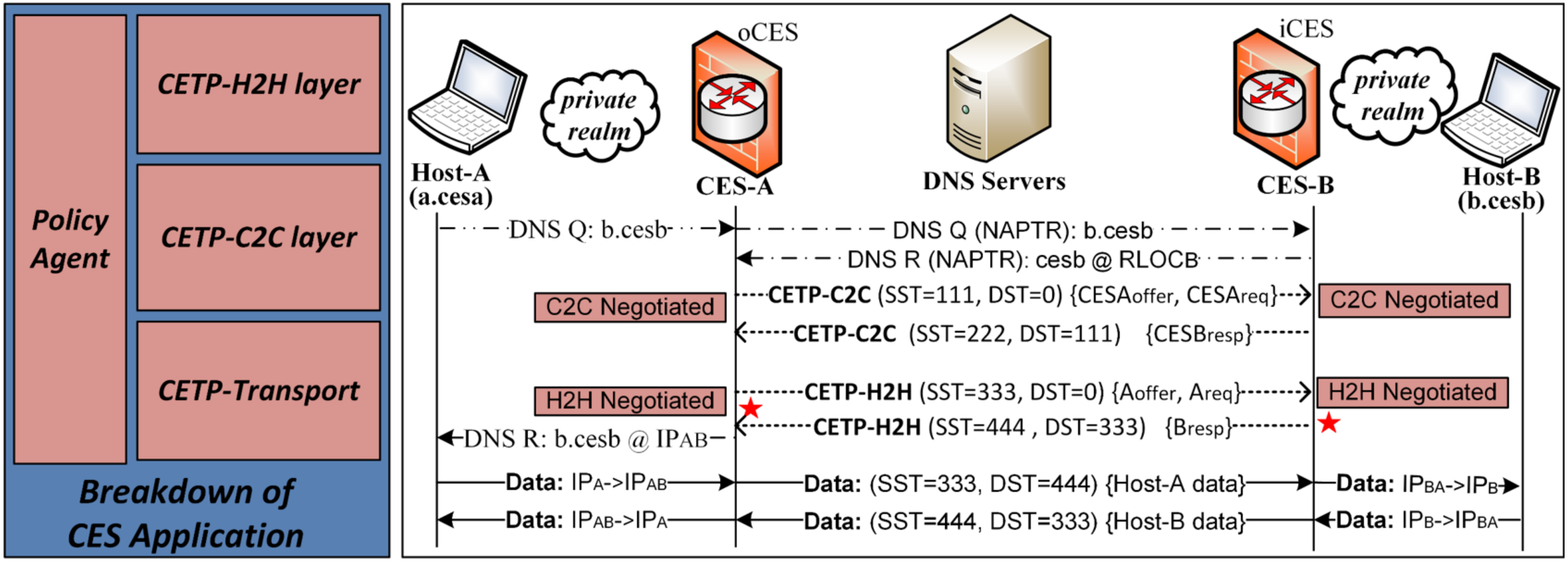


Originator and Destination are customer networks (stub networks in terms of IP routing)

Trust Boundary == cooperative firewall carries responsibility of the device behavior

- resides e.g. in telco cloud
- executes policies – all flows are admitted by policy
- device level policies governed by users
- ISP/MNO level policies governed by the operator

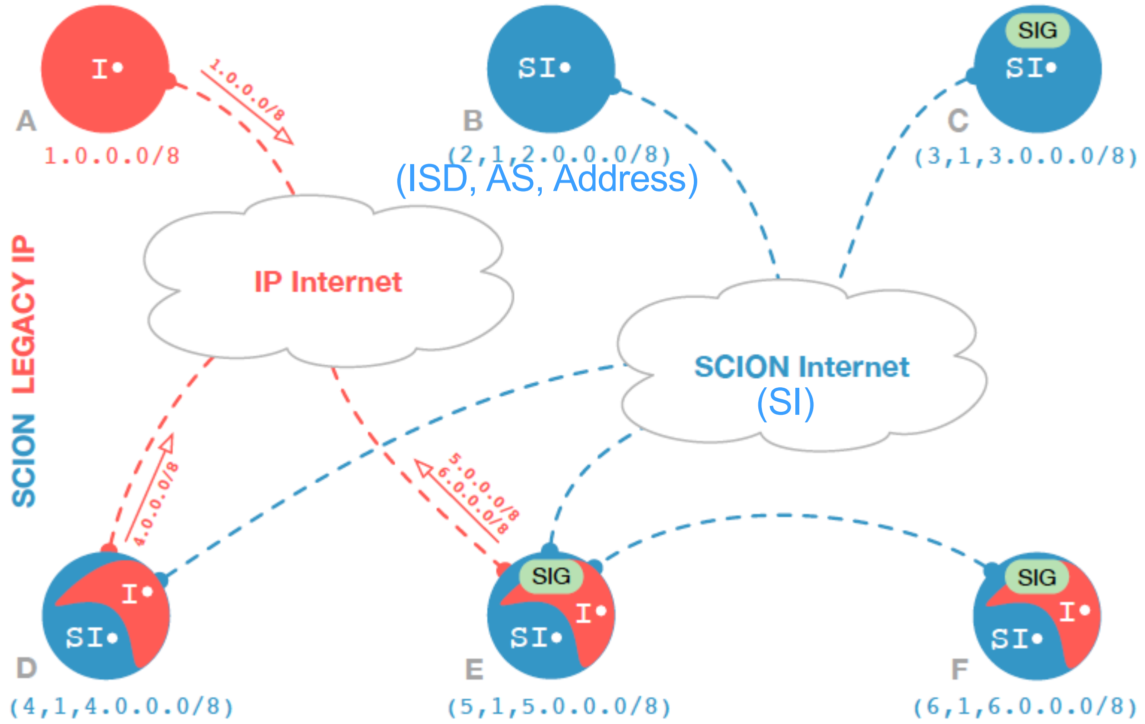
Edge to edge policy negotiation



ITU-T has a very similar initial architecture in Y.3052 – Y.3053

Network centric view of embedding trust:

SCION is a proposed replacement for BGPv4 --> solution for the federated public domain that could possibly be trusted



Source: Scion-book

SIG: Scion-IP Gateway
ISD – Isolation domain, AS – Autonomous System

Features

- **Only local roots of trust → no global kill- switch**
- **3 PKIs (Routes, Names, Devices)**
- **No Prefix hijacking**
- **AS-to-AS Source routing**
- **Immedidate multipath for all hosts → high availability services**
- **No Routing Table in Data plane – stateless DP → low kWh**
- **On-demand operation with cached security keys, path segments etc.**
- **Trustworthy names**
- **No spoofing**
- **Authentication on packet level**
- **Embedded DDoS mitigation**

Isolation in Networks Delivers Security

1:1 – client:service	Leased line, Ethernet circuit, MPLS path
N:1 – client:service	VPN (device based, network based), many implementations over routed IP 5G Network slice (wide area network zone)
N:M – client:service	*Specialised network (NN term)* - Are not in current practise, but could be? - About bringing the benefits of cloud style isolation into end to end services over mobile or other networks

Role of ISP/MNO in Embedding trust

- **In SCION a set of core ASes set up an Isolation Domain and will manage Roots of Trust and Federation of Trust**
- **Reputation is used to filter traffic to/from suspect or malicious sources.**
  - *Efficient use of reputation requires sharing of evidence + evidence needs validation by trusted party*
  - *ISP/MNO could/should partner with security intelligence providers – this knowledge can use used in policy validation, reputation based filtering, malicious behaviour detection etc.*
- **Mitigation needs a trustworthy party at the remote end serving the suspect/malicious host – can only be the serving ISP/MNO of the remote user**
- **ISP/MNO is best placed to run the Cloud based firewalling platform/software – <1ms additional delay.**

Summary

- We can not ***program the world*** and carry on with ***routed IP*** as the wide area solution
  - Too much new types of crime would be possible and societies would be too vulnerable
  - 6G will be even more at the center of world politics than 5G
- Mobile Network operators need to become federated trust operators
- Solution: integration of network and user centric trust into the networks → principle of vertical + horizontal isolation on the same L2 substrate

Thank You
(Questions?)