Aalto University
School of Electrical
Engineering

5G – TAKE5 TEST NETWORK and 5G@II

Raimo Kantola
raimo.kantola@aalto.fi

www.re2ee.org

November 17th, 2016

Agenda

- TAKE 5 Test Network - Otaniemi and Helsinki City center: 2017 - 2018
  - What and why
  - Network Slicing: in practice and so what
- 5G meets Industrial Internet (5G@II): 2017-18
  - Motivation
  - Access control using policy
- Why should Elisa care?

Disclaimer: This talk presents a research vision. Commercial availability is another matter.

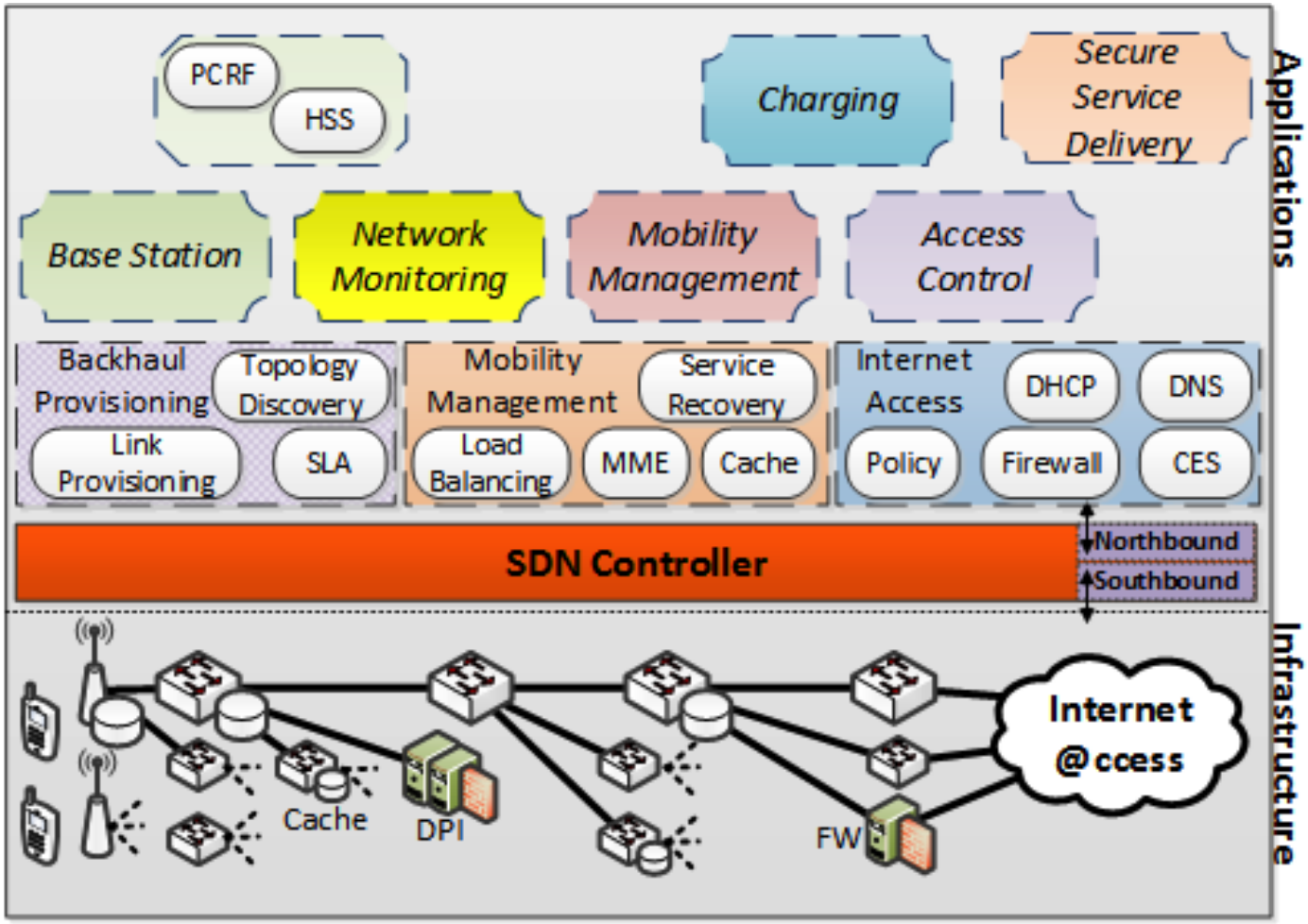
5G Principles

- Core network is based on Software Defined Networking
  - Separation of Data Plane and Control plane
  - OpenFlow switches (and Ethernet/MPLS switches) in DP
- Core functions are virtualized in containers (NFV)
- Network Slicing
  - Each slice has its own Core network + other Virtualized Network Functions (VNFs)
  - Each mobile attaches (based on SIM/USIM) attaches to its slice
  - RF capacity can be attached to a slice
  - Provisioning can be used to assign transport capacity to a slice – a proactive SDN App is needed
  - Setting up a slice takes minutes (not hours or days)

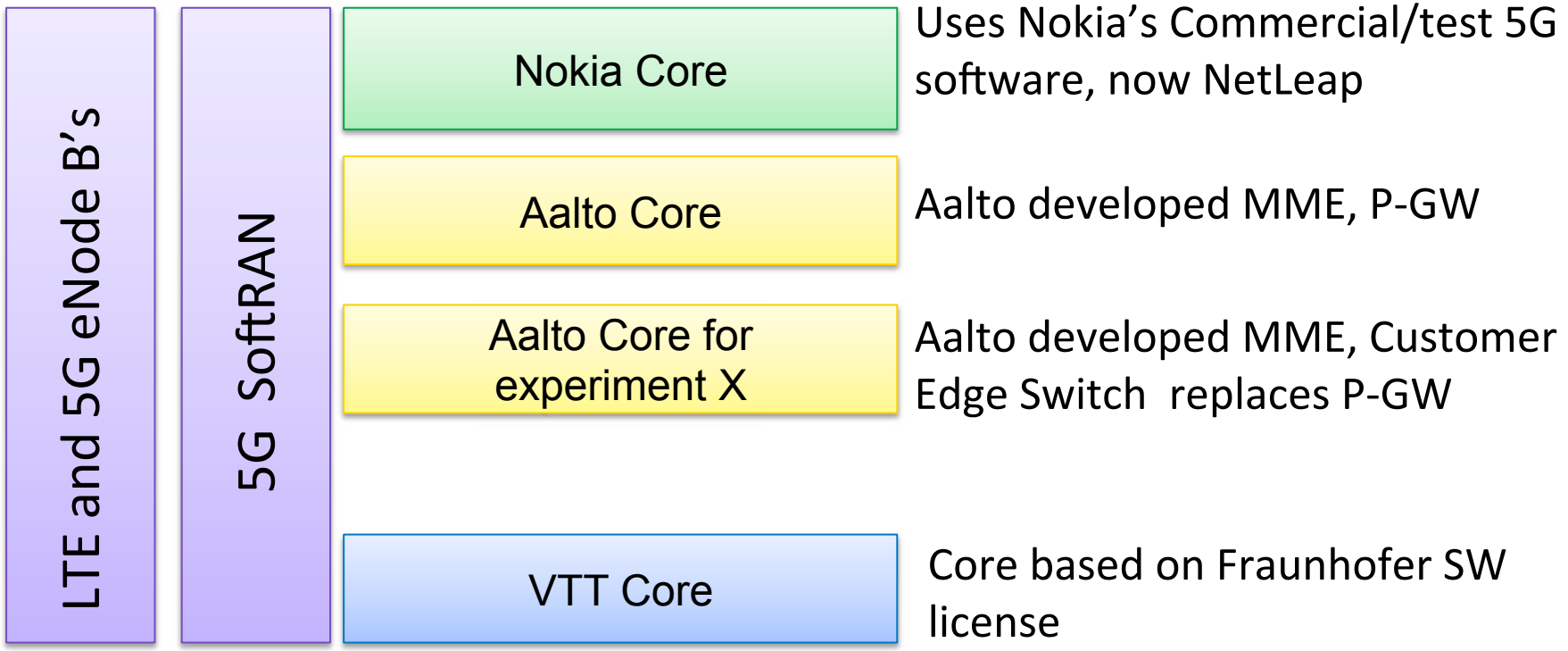
What is a network slice?

- Bigger deal than VPN
  - Covers communications end to end
- If needed can have RF, transport etc. resource allocations of its own
  - Due to SDN controlled resources, resource allocations can be dynamic
- Network support for any functions can be added on top of std network functions
  - Extra security, extra reliability, extra interfaces for data collection etc.
- Needs a significant business case
  - Can be set up in minutes + additional resource allocations may take more time
  - Can change the business landscape quickly

5G Control as a Group of SDN Apps



TAKE 5 Architecture



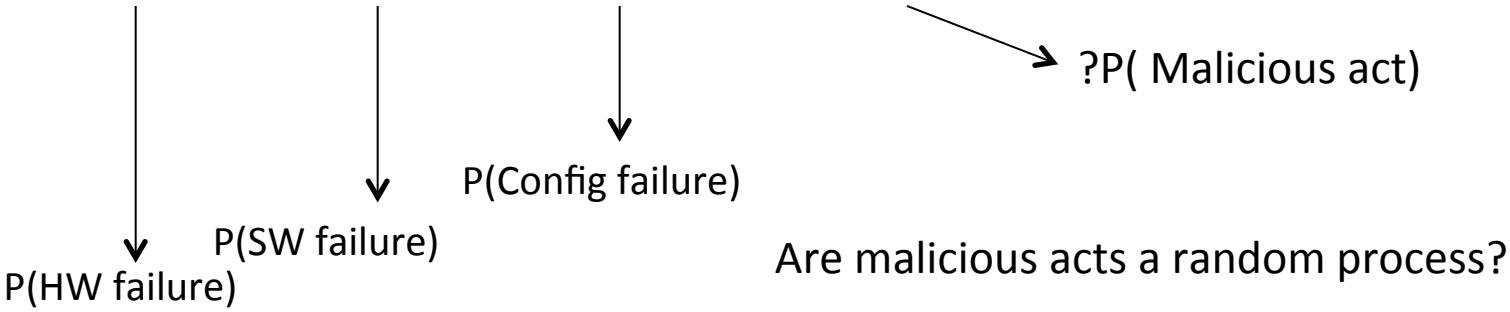
5G meets Industrial Internet (5G@II)

- A raising theme in European Research
- II → machine to machine communication
- 5G delivers to II:
  - Ultra high reliability
  - Low delay (1ms in radio)→ radio can be in a control loop
  - High capacity
  - New RF capacity regimes (free vs. licensed spectrum)

5G – ultra reliable communications

- Is it a very secure network over which malicious actors can effectively conduct fraud?
- Or will the MOs do their best to prevent fraud and protect their customers using whatever means are technically feasible?

$$R = (1 - F1)\,(1 - F2)\,(1 - F3)\,(1 - F4)$$



5G@II – how to manage billions of IoT devices

- Site = one or several masters + N service/hw providers + many outsourcing contracts.
- Physical transport: industry wide applications
- Data flows within a provider + between providers either for data collection OR real time control loops
- Must be possible
  - to audit that real data flows correspond to cooperation or outsourcing contracts
  - to change the access rights to data as contracts change

Alternatives for managing II devices

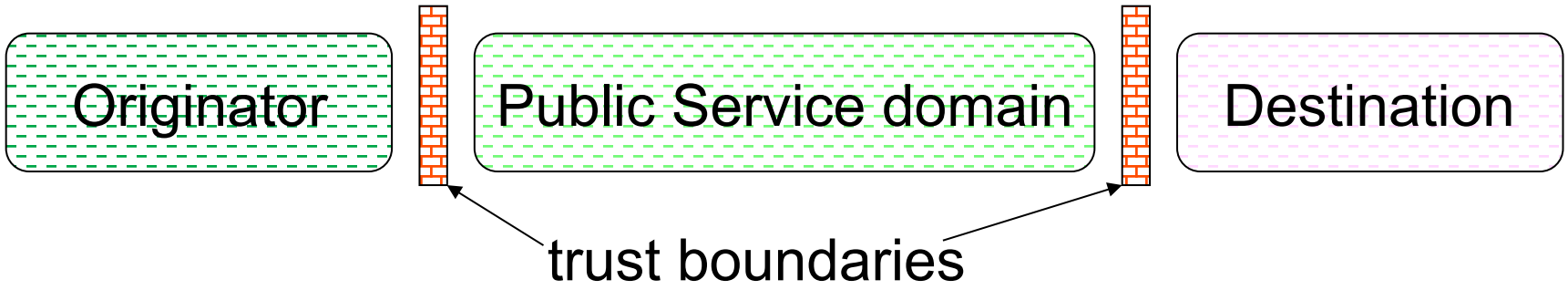
- Virtual Private networks
  - Take existing technology and patch it up
  - Internet core will have scaling challenges if millions of VPNs
  - When business relations change → heavy management burden
  - How to scale to data sharing across multiple players?
- Push all access control to network edge
  - Core has transport allocations
  - Security logic is at the edge
  - All flows are policy controlled
  - Aalto has been developing a new Cooperative Firewalling technology for this purpose

Trust Model for the Internet

Why: Prerequisites for cooperative behaviour are not in place directly between all hosts. Must be un-ending/frequent communication between actors, who understand reputation, have long memory and gossip effectively → hold for ISPs, mobile operators etc.

- The customer network will accept responsibility for good behaviour and misbehaviour of the hosts that it is serving
- ISP networks form federated trust domains
- Evidence of (host, application, customer network) behaviour is collected by each entity and aggregated by an **Internet wide trust management system** (can be many)
- Each entity (host, customer network etc.) has an ID; due to variability of needs of applications, many types of IDs should be supported.

Communication over Trust Domains

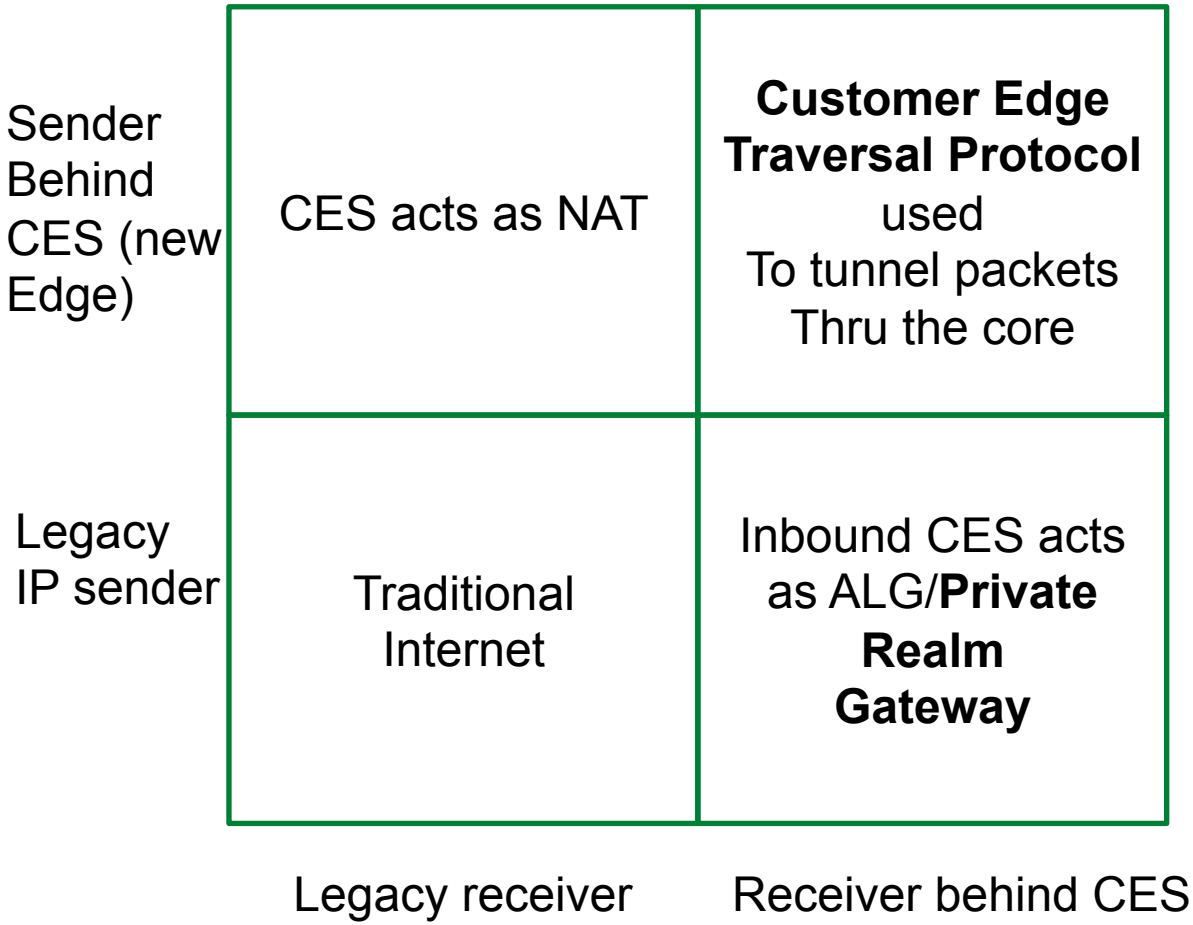


Originator and Destination are customer networks (stub networks in terms of IP routing)
+ each of them may have one or many private address spaces;
+ extreme case: mobile network addressing model: each user device is in its own address space and all communication takes place through the gateway or edge node connecting the user devices to the Internet

Trust Boundary == Customer Edge Switch == cooperative firewall

A CES has one or several RLOCs (routing locators) that make it reachable in the public service domain

Signaling Cases



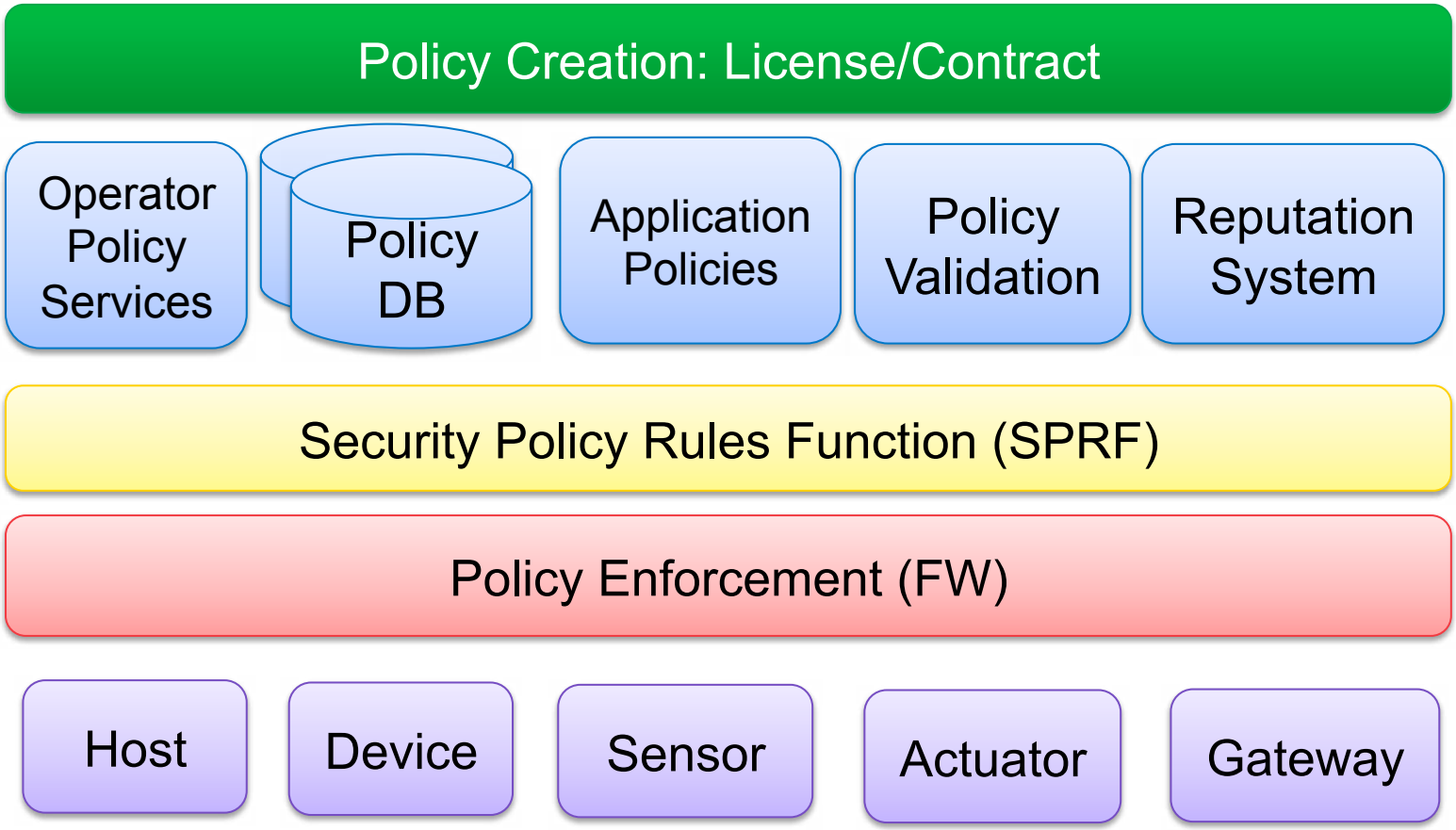
What can we achieve for SECURITY by CES and Internet wide trust management?

- CES
  - Eliminate Source Address spoofing
  - Tackle DDoS attacks efficiently
  - Dissolve boundary between closed and open networks
  - Push access control to the edge nodes
  - Leverage Mobile network style IDs for data communications
- Trust:
  - Fast location of bots → "useful" lifetime of a bot is reduced → bot renting business becomes less profitable
- Together: improved robustness of critical infra → national security
- **BUT: most vulnerabilities are on application layer → security should be based on multiple layers of defense + proactive trust mgt**

Using Trust Management for 5G

- Each entity has trust value and credibility of reporting
- Evidence collection is ubiquitous; hosts encrypt their reports
- ISP: aggregates host reports in encrypted form
- IDs are anonymous while information is unreliable: after aggregation/verification suspect IDs are translated to addresses
- Greylisting: CES nodes can ramp up their security checks dynamically
- Blacklisting = put host into sandbox

Policy Architecture manages access at the edge



Policies are dynamic – they change depending on security situation

- **When under attack, network gateway may ask for more secure credentials**
- **Emergency situations (Fire, terrorist attack etc…)**
- **Admission may depend on the reputation of the sender**
  - Blacklisting
  - Greylisting
  - Whitelisting

CES can be applied to Mobile Broadband: Benefits to Mobile Operators (1)

- Technical benefits:
  - No spoofing over Air interface, no polling for NAT traversal over air interface, no cluttering of mobile Apps, DDoS resistance; saving of device battery; less useless/non-chargeable traffic over mobile networks; more robust service (malicious actors can not disrupt service); ease of renumbering; isolation of technology choices; multi-homing with no impact on non-default core network routing tables…
- MO can become a trust broker among customers: mediate customer to customer trust
  - Leverage mobile IDs (USIM+HSS) to datacoms
- Makes sense to build an alternative non-default core for the Internet with entry points in every major eyeball ISP using CES nodes → spoofing and DDoS mitigation for all traffic
  - When under attack makes sense to prefer traffic sourced through this new trusted non-default core
  - Still need to verify this use case!

Benefits to Mobile Operators (2)

- MO can sell Trust as a cloud service (e.g. Firewall in the cloud) – (Silver Service)
  - Fast trace back of attacks
  - FW rules can be per subscriber and follow the sub while the sub is roaming
  - Business customers and Families
  - Dissolving the closed/open network boundary: implementing “Family and Friends” or “me and my gadgets” –like service by defining a suitable policy.
  - Help in cleanup after infection; may be security can be sold as insurance? Clean-up fee for opt-out customers?
- MO can sell Security as a cloud service (Gold Service)
  - Cloud knows exactly what Apps mobile device is running and automatically takes care of updates; admits exactly this traffic.
  - Probably together with security software companies and App Stores
  - Trust processing must know that such customers are not careless!

Benefits to Mobile Users

- Battery saving when using communications apps
- Fast session setup for VOIP, (even P2PSIP) for all communications apps → VOIP matures to Quality of experience where it is a real alternative to circuit telephony (ITU-T requirement for session setup: 2s)
- Better protection against all attacks
- Other
  - Non-repudiation of Transactions such as sw or even file download, commercial operations?
  - Parental control using FW in the cloud (like Internet is closed 2200-0500 for teens)
  - Tailored to corporations: security as a cloud service

CES Managing access in Industrial Internet

- CES owned, operated by site master of the site such as port, paper mill owner etc.
  - Likely scenario: master has also mobile core (MME etc)
  - Alternative: CES can be managed by Mobile Operator on behalf of the site master
- Industry wide app: Ecosystem forms a trust domain, may have many CES owners and operators but all share trust information and follow ecosystem wide security policy guidelines
  - Using SDN/NFV may easily make use of incumbent MO infra anywhere, in any country based on contracts?

Why should Elisa care?

- SDN+NFV
  - Fast provisioning of transport capacity to events to corporate customers to virtual operators
  - Infra for Cloud of things
  - Cooperation with superhubs (Google, FB, Netflix, Alibaba, Amazon etc.): e.g. edge caching services
- SDN + Virtualization + Network Slicing
  - New business opportunities in particular in corporate business segment may open quickly
  - An operator like Elisa can become a coordinator in ecosystems that each use a network slice of their own – this role and capability will not be developed over night