Trust Networking for Beyond 5G and 6G

Raimo Kantola
Dept. of Communications and Networking,
Aalto University
Espoo, Finland
raimo.kantola@aalto.fi

***Abstract*— Trust in a network context is about expected outcomes of decisions to communicate with a remote party, to click on a link or to believe in what an email says. The possible outcomes are either the positive value of the communication or being hacked or cheated in some way. Trust spans all protocol layers from the IP layer to applications and content. ITU-T is working on the framework architecture for trust networking. The White Paper after 1st IEEE 6G Summit advocated embedding trust into the 6G network in its networking chapter. We have worked on a concept we call Customer Edge Switching or cooperative firewalling for several years. In this paper, we analyze the proposed frameworks for the context of 6G and point out directions of future work. We offer several use cases where the framework could be first used and what are the regulatory issues in using the technology for Internet Access under the "open Internet" regulation.**

Keywords—trust, security, policy management, trust management

I. Introduction

Numerous definitions of trust or digital trust can be found in the literature. In this paper we focus only on issues of trust in a network context. In this context, trust is about helping the user or network node to make the right decision to communicate or not, to transmit a packet or drop it, to allocate some processing recourses to an incoming flow or not, to click on a link or not, to believe a seen content or not in a communication. The decision depends on the expected outcome of either obtaining the positive value of communication or being cheated on in some way. The cheating takes many forms from spoofed source addresses, to distributed denial of service attacks, infecting the receiver's machine with a virus, loss of data to a malicious party, loss of privacy in a long-term process etc.

While the Internet is limited to the digital world only, the damage caused by the cheating is somewhat limited, too. Future networks, e.g. 6G will in addition build a physical/digital world boundary. Computer programs start sensing what is happening in the physical world, understand it and control it. With the enlarging scope of computing, the security threats will become wider. Physical safety will depend on the behavior of the computers. If some of them have been hacked, lots of property can be damaged by malicious actors, people can die because of accidents caused by the adversaries, foreign actors can threaten the national security of nation states. For these reasons, digital trust is becoming more and more important in future networks.

The networking chapter of the 1st IEEE 6G Summit White Paper [1] advocated embedding trust into the 6G network. In 2019 we published a paper [2] expanding the justification of trust networking and discussing the key prerequisite of adopting the ID/Locator split for trust networking, where the ID is the stable key against which all network entities can collect evidence of behavior and as a result, the network entities can produce the reputation for all entities. In late 2018, ITU-T Study Group 13 published a recommendation on a framework for trustworthy networking over trust domains [3]. ITU-T also discusses the terms and concepts for trust networking in [4].

As early as in 2010, we published the first paper on this very subject [5]. This has been followed by first a proof of concept implementation reported in [6, 7] and by 2019, a running code level implementation in [8, 12]. This line of work has started building trust into networks from bottom-up, i.e. from the TCP/IP layers. Other papers study motivation [9], trust management [10, 11] and the issues of adoption. This approach and its implementation are well ahead of the ITU-T framework. Nevertheless, the ITU-T and Customer Edge Switching (CES) frameworks agree on many aspects, such as the ID/Locator split, reasoning behind the split, use of private and public addressing and many components that make up the framework, although the components have different names. Whichever starting point we take, additional work is needed to create a trustworthy networking system for the use cases that are becoming feasible with beyond 5G and 6G systems.

In this paper, Section 2 discusses the key concepts promoted by ITU-T and worked out under cooperative firewalling in the CES context. Section 3 presents the CES framework. Section 4 presents the ITU-T framework architecture. Section 5 gives a detailed comparison of the two in relation of 6G requirements as we see the requirements. Section 6 discusses future work in several subsections such as regulation, deployment constraints, more potential use cases and finally the required technology development. Section 7 concludes.

II. Trust Network concepts

A. Trust in network context

ITU-T [2] defines trust as "*the measurable belief and/or confidence which represents accumulated value from history and expecting value for the future*". The definition takes the basis in "expectation" or "belief" that can be seen as some probability or conditional probability. We have used a definition in a networking context: *trust is the willingness to accept a risk in an interaction*. This view on trust ties the concept to concrete decisions that must be taken in a networking context. More theoretically, this definition ties trust to the strategy choices parties have in an interaction or a game such as the Prisoner's Dilemma, i.e. to cooperate or to defect. Prisoner's Dilemma can be used to model interactions over the network as a game [9]. The latter kind of trust in a network context implies e.g. an admit decision in a firewall or a positive access control decision.

For both definition styles, trust can be supported by good reputation of the remote party. Reputation can be based on self-collected evidence or the evidence of behavior can be shared within a domain. In some papers these are called direct trust and indirect trust. In CES we advocate ubiquitous evidence collection in all edge nodes and in hosts. Received evidence does not need to be taken at face value. To make the system robust against system attacks such as ballot stuffing, whitewashing or bad-mouthing, evidence is evaluated and aggregated before producing a reputation value for the entity.

Whichever definition of trust, in the communication context, it should help in addressing questions like: can this host communicate with a remote party without being attacked or hacked in the process? Can this interaction lead to loss of data? Should flows from a remote network be served or not under heavy load? Or would it be best to drop this flow and devote resources to other flows? Is it possible that an incoming packet uses a spoofed source address? When communicating with a remote party, how does this host minimize its exposure to possible future attacks or long-term loss of privacy?

ITU-T [3] focuses on applying the abstract framework to a routed IP network. CES design and implementation has been done in Software Defined Networks (SDN) with a separation of the control plane (CP) and data plane (DP) in the network edge, i.e. in the CES node. When the SDN controller of a customer network is placed under the control of a cooperative CES firewall that uses fine grained policies (everything denied except known normal traffic) in its operation, the whole network can be turned into a firewall: all flows are admitted by policy, and consequently, only expected traffic is carried in the network and any new unexpected socket is immediately under scrutiny for malicious activity detection. The hypothesis is that this would be suitable for safety critical use cases like the one in next subsection. Under cooperative firewalling, privacy protection by an additional layer of software between the device and the remote cloud is also feasible.

B. *A Use case for testing the concepts*

A vehicle is equipped with 6G and other sensors. 6G is also used for communication to and from the vehicle. The sensors are able to sense and recognize people and objects that may be relevant to the vehicle. The vehicle receives input in real time from other vehicles and road side sensors and actuators. Although, most of the time the vehicle decision making is autonomous, in some situations e.g. because of lack of direct line of sight from the vehicle, the supplementary information from external sources becomes important.

Due to the powerful capabilities of the used sensors, the sensed and processed information often violates people's privacy if leaked to 3rd parties. For privacy protection, it should be used for a limited purpose of ensuring safety. If fake information can be inserted into the system, risk of accidents will raise. Accidents cause damage of property and/or loss of life. If information is leaked to a malicious party, people who were sensed in the data, may be in danger depending on the goals of the malicious party.

Using trust networking, the likelihood of any of the undesirable events in the use case should be made extremely low.

C. *Trust domain*

Trust domain by ITU-T in [3, 4] is a set of network entities, that trust each other without extra security procedures. In the CES context only self-trust, i.e. each entity trusts itself, is used. However, entities within a trust domain share evidence of malicious and benevolent behavior of other observed entities. Following the principle of self-trust, the evidence is not taken at face value, instead it is weighted and aggregated in order to make the system robust against bad-mouthing and other similar system attacks.

How would we apply the ITU-T [3,4] trust domain to a multi-stakeholder use case of the previous subsection? How could the vehicles owned by different people and entities trust each other blindly? Or how could the vehicles trust the road-side infrastructure blindly? It would seem more realistic to adopt the CES style self-trust-only in all multi-stakeholder scenarios where devices owned by different entities communicate and cooperate. The Y.3053 concept of trust domain may only be considered when all entities within the domain are under the same administration. However, even in this case, a breach of security within the domain easily leads to compromising all entities within the domain. We should also ask, why do we need an international recommendation for single administration networking?

D. *Policy*

The concept of policy is mentioned in ITU-T [3, 4] and it is said in [3] that the admin defines policy. However, [3] leaves the concept of policy quite obscure. In the CES context, policy is subdivided into (a) communications security policy executed on the control plane on edge nodes, (b) firewalling policy for the data plane, (c) nodal policy. The former two are descriptions of expected traffic at a host, typically on a socket level. Nodal policies allow finetuning the processing in the edge nodes. Overall, the policies and policy tools are the means to adapt the generic trust/security engine of CES into any use case and context. In CES, policies are hierarchical, which e.g. can be used to separate admin-defined and user-defined policies. Semi-automated tools are proposed to make the policy definition user friendly. Host-to-host or user defined polices are clearly separated from policies that would be naturally defined by the network administrator. Also, user policies can be hierarchical. For example, a small company running its firewalling in the cloud using CES technology could have some generic company level policies that could be further specialized for individual services and hosts.

For CES, a security policy management system (SPM) has been developed and is presented in [8, 13]. In SPM any JSON formatted policy can be stored against a so-called service fully qualified domain name (SFQDN) usually pointing to a socket or an application on a host or network entity. The policies are executed by the cooperative firewalls or CES nodes.

It is worth noticing that on the consumer markets the idea that admin defines the policy like in Y.3053 will not be enough to create fine grained policies. It would go against all the tradition of the "open Internet" that the ISP/MNO would define exactly what applications the subscriber can use. If the admin defines policy, it must be the same for all users. For personalized policies, the consumer him-/herself should be the only party that defines the host level policies. The operator could be allowed to overwrite the end user's policy only in case of limiting a clearly malicious activity. Making policy definition user friendly, policy tools that hide all the nitty-gritty details of the policies are needed. It would be the subscriber's choice either to accept the policies created based on the best available security intelligence or learn enough to be able to make high level decisions like: I do not wish to hear or see any stuff from the app *X* between 10 pm and 6 am.

III. Customer Edge Switching model

Because an experimental implementation exists, in addition to the framework level abstract functional model, we will describe a high-level architecture. Figure 1 present an end to end model of Customer Edge Switching.

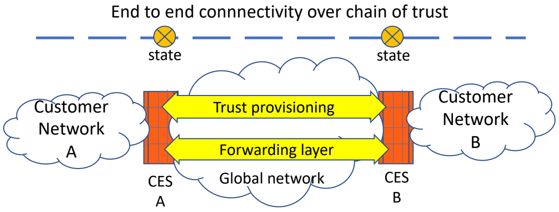

Figure 1. Communication over chain of trust

When a host *A* in customer network A wishes to communicate with host *B* in customer network B, trust chain establishment is triggered by the DNS query by host *A*. Signaling edge to edge is initiated on DNS response from the remote end by the outbound edge node. First the admin level trust and communications conditions are established and then host to host trust can be negotiated. Only after this, host *A* will receive the response to its initial DNS query. End to end connectivity layer in Figure 1 uses private addresses in both customer networks and globally unique CES node routing locators between the edge nodes over the global packet transport or routed wide area IP network. Due to the SDN based implementation, all forwarding protocols supported by Open Flow Switch (OVS) are supported by the experimental implementation. So, using IPv4, IPv6, GRE, VXLAN, MPLS, IPSEC or 802.1 variants for forwarding is handled in the same way and controlled by the same controller.

The architecture is compatible with NAT-friendly protocols, NAT-unfriendly protocols will need either applications layer gateways or will have to use legacy means of NAT traversal.

Figure 2 presents the functional model of cooperative firewalling in Customer Edge Switching based on our implementation in [8].

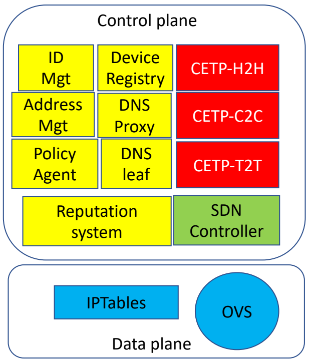

Figure 2: Functions in CES node

Figure 2 shows the SDN based architecture of the control and data plane split. On the data plane, the system carries the end-to- end host to host flow where the Open Flow Switch (OVS) can mangle packets between all the forwarding formats mentioned earlier and Iptables is used to manage the kernel firewalling rules in Netfilter in the Linux kernel on the flow. Typically, a host to host session will require inserting two new entries into the OVS flow tables for bidirectional connectivity. Often the CES to CES level flow state can be cached for many host-to-host connections. Due to the OVS mangling capability, the architecture allows tunneling of user flows edge to edge. When the tunnel is plain text, OVS offers a tunnel end-point and many destinations can be reached from the same end-point. If the tunnel is encrypted using IPSEC, it needs to be dedicated for a single destination.

The CES control plane has a three-layer Customer Edge Traversal Protocol (CETP). The lowest layer establishes a signaling transport relation possibly using multiple routing locators for the CP elements, CES-to-CES layer manages the CES to CES trust relation and finally the host to host protocol layer seeks to establish a policy match between the two hosts. In CETP, all aspects of the protocol and all phases of the trust negotiation are policy controlled. Under lax policy, signaling overhead is kept to a minimum, under a strict policy, certificates can be used etc.

Figure 2 shows that a CES node has the registry of served hosts, it acts as the authoritative DNS server for the served hosts, and naturally it is the default DNS server for the hosts as well. By bundling the DNS, address and ID management and device registry services into the edge node, the edge node can take responsibility for the served hosts' behavior while it sticks to the approach of self-trust only. The policy agent caches policies retrieving them from a separate Security Policy Management system (SPM) not shown in this paper for brevity. SPM is presented in [8, 13].

Another component of the CES framework that is omitted in this paper is the Realm gateway (RGW). It provides an interworking solution for the case when the remote customer is not behind a CES node but is a legacy IP host. RGW can act as a source NAT and a dynamic destination NAT. It allows servers in a private address to be dynamically reachable without polling. Because the RGW is a natural attack surface, we recommend to package it into a separate virtual machine so that it cannot hog the CES node resources. In addition, there are two implementations of SYNPROXY in [8]. Both RGW and CES node can be protected from SYN attacks by the SYNPROXY. A high-level description of Customer Edge Switching is available in [14].

In the CES framework, the edge node has an embedded reputation system using either self-collected evidence or also accepting evidence from other nodes in the same trust domain. In addition, we have worked on Internet wide hierarchical trust management systems and their possible adoption [10,11].

IV. ITU-T trust Framework in Y.3053

Y.3053 defines an architecture for trustworthy networking over trust domains reproduced in Figure 3.

The different functions in Figure 3 for access and delivery control are:

IRS-FE – ID based Routing Support
DTP-FE – Data Transport & Processing
APCS-FE – Access and Peering Control

For Domain administration:

ILMS-FE – ID/Locator Mgt Service
DMM-FE – Domain Membership Management
DPM-FE – Domain Policy Management

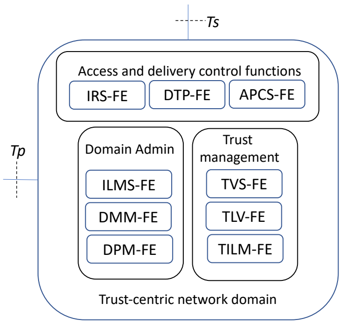

Figure 3: Trustworthy networking in Y.3053 [3].

For Trust management:
TVS-FE – Trust Verification Support
TLV-FE – Trust Level Validation
TILM-FE – Trust Information Life-cycle management

The reference points are:
Tp – reference point to another trust centric domain
Ts – reference point for applications.

Since the Y.3053 language is rather abstract, we immediately point out the corresponding functionality in the CES framework in Table 1:

Table 1: Y.3053 functions in CES

Y.3053	**Customer Edge Switching**
IRS-FE	Data plane RLOC policy
DTP-FE	Ryu controller + OVS + Netfilter
APCS-FE	CES to CES, and signaling transport policy
ILMS-FE	Domain Name system authoritative server, ID and Address management
DMM-FE	Device/host registry on CES/RGW
DPM-FE	Security policy management system (SPM)
TVS-FE TLV-FE	Embedded reputation system
TILM-FE	Reputation aging
Tp	CETP protocol
Ts	IDS can provide input to reputation system

Table 1 shows that for all network functions in the ITU-T framework, we can point a corresponding functionality in the CES architecture. This speaks for high level of similarity of the two frameworks.

V. Comparison of the trust netwokring frameworks

Besides having corresponding or similar functionality, both frameworks agree on several important principles. At least the following can be listed:

- A trust network uses ID/Locator split that introduces stable IDs for trust evidence collection.
- Private addresses can be used in local networks for hosts while the wide area network uses globally unique addresses.
- Policy is a way to tailor the system to a use case and individual needs.
- The concept of trust domain is a way of grouping entities together for scalability.

Several differences can also be pointed out.

ITU-T framework [3] seems to be at an early stage of development, while CES has been developed over many years and can offer experimental verification of all the proposed network algorithms and solutions. The main areas in the ITU-T framework that seem to need further development are at least the following:

- The concept of trust domain in Y.3053 is optimistic and clearly not suitable for use cases where devices cooperate but belong to different administrations. Due to the self-trust only used in CES, this framework is clearly more generic, i.e. applicable to a wider range of use cases.
- The concept of policy in Y.3053 is at an early stage of development. Even the definition of policy is unclear. There is no idea of personalization of trust using policies. In CES the policy and policy tools are the means to tailor the system to meet the needs of a particular use case, while the trust/security engine is as generic as possible. Policies are implementable using known Linux tools or by the newly developed experimental software. Policies are divided to admin level and host level personalized policies.
- The application of IP routed networks in Y.3053 is written in a way that implies changes in hosts. Deployment scenarios where both hosts and network nodes are updated are possible only in limited single administration use cases. In the CES architecture, care has been taken to avoid all compulsory changes in hosts while allowing new optional tools/applications in hosts for convenience.
- Y.3053 does not discuss application of the framework into SDN networks. The application to routed IP is useful but would give a lesser level of control over traffic in the network than what is possible with SDN.
- In a routed IP network like in [3], flow admission decisions are partially done by hosts. Therefore, a clearly lesser level of control by the network on the carried traffic is possible. This case is less about trust networking and more about security processing on hosts.
- A difference is also that in the SDN case more of the security and trust processing can be centrally managed in the cloud with uniform and high-quality security intelligence immediately deployed without having to upgrade numerous devices. This is because the control plane of the edge node is a virtualized network function allowing to expect a lower level of operational expenditure for information security than in the case of routed IP where the security software is fragmented into the devices and thus harder and slower to manage.

VI. Future Work

In the first subsection we discuss open Internet regulation based on the EU guidelines [15, 16] because it may seriously limit the use cases where advanced trust networking could be deployed. Then in subsection *B*, we will point out generic deployment constraints that are based on past Interworking experience. In subsection *C*, we give various 6G and other use cases that are promising for trust networking. Finally, subsection *D* lists the technology that still needs to be specified and deployed to make trust networking happen.

A. Regulation

Under current EU regulation [15, 16] Internet Service Providers (ISP) or Mobile Network Operators (MNO) are not allowed to filter traffic based on per user policies in Internet

Access Services (IAS). If filtering is applied, it will apply in the same way to all users. Under the current regulation, if an operator uses its telco cloud, the cloud is seen as a part of the network and thus is under regulation. If the global giants such as AWS, MS Azure, Apple or Google process user's traffic in their cloud for any reason, this is out of scope for the regulation. These limitations are justified under the "open internet" or net neutrality rules. In addition to IAS, ISPs and MNOs can provide non-IAS networks and services. These include so called specialized networks that can not replace IAS. Machine to machine communication is not under the open Internet regulation either. Many of the 5G vertical use cases are not IAS, so "open internet" regulation does not stop their deployment even if network-based filtering is needed for security.

Since IAS is where the money is for the MNOs, the limitations create uncertainty as to whether it makes sense for them to invest into the "compute" functions and virtualization in 5G/Beyond-5G/6G at all. The MNOs could use these new functions in their business that is not under "net neutrality", e.g. in machine to machine or many of the vertical markets. Some of these markets will require highly predictable, highly reliable and highly secure network services. The physical world/ digital world boundary largely falls into this category. On these markets, lots of new privacy sensitive information will be collected and processed. The question is whether such new use cases are worth the costs of telco investments into the cloud and local compute capacity. Another question is what happens to privacy if all the new privacy sensitive information falls into the hands of the global cloud giants?

Already 5G uses network function virtualization, i.e. the cloud technology. 6G will do the same, it is likely to even more cloud centric if possible. We have argued [17] that if we stick to this kind of regulation, the result is that much of the new functionality that uses the "compute" element in the 5G architecture, will be pushed to the business turf of the US based cloud giants that are near monopolies while the MNOs will be in an unfair competitive disadvantage. We also argue that under this model, EU regulator's will be unable to protect the privacy of EU citizens. If on the other hand, this new physical/digital boundary would be in the hands of the locally based MNOs or similar operators, the regulator would be in a position to create an enforceable regulatory framework for the use of the privacy sensitive information.

In [17] we argue that the ISP/MNO cloud should be deregulated when it is used of offer Infrastructure/ Platform/ Software as a Service (IaaS, PaaS or SaaS) style services to Over-the-Top (OTT) providers such as Netflix or to the subscribers of the operator. We argue that e.g. with SaaS model the subscribers could use the power of cloud to implement the best security and trust solutions for themselves running the cloud software in close proximity to their network access link on the telco cloud platform. Close proximity to the user is needed to keep the end to end delays low and to save energy.

B. Deployment constraints

From the outset, we have accepted the constraint on the new security/trust architecture, that the deployment should be possible one network at a time and that when an admin decides to invest into it, it will gain some benefits. Since a change is needed in the network, it follows from the constraint that no compulsory changes are allowed on hosts. We argue that since Y.3053 does not stick to this constraint, it, at best, could be considered for single admin deployments. If that is the case, the next question on Y.3053 is why is a global recommendation needed for single admin deployments?

Our view is that in particular on the physical/digital world boundary we will need lots of low power, limited compute power devices that potentially belong to several administrations and users with possibly conflicting interests. Fortunately for trust and security, software on these systems must be carefully managed, does not change often, there will not be unpredictable users on the devices that could download any of the millions of Apps from a play store onto the devices. Most of the devices do not have their own keyboard/display or any local user interface. We expect that for these systems, it will be possible with suitable tools, to collect an accurate description of the expected traffic on the physical/digital boundary into a policy database that will act as reference for capturing any unexpected or malicious traffic for scrutiny by more advanced tools and human operators. That being the case, the firewalling can be all-is-denied except known normal traffic. In some of these use cases with the SDN oriented framework of Customer Edge Switching, the whole network, possibly a slice in 5G, B5G or 6G network could be turned into a firewall and thus the network would carry just the expected traffic. An example use case for this concept that we are working on, is the Smart Grid.

C. Potential other use cases

Trust networking could be applied to different networks such as specialized networks for automated driving, the smart grid or for e-health. Such specialized networks will require remote access to experts for monitoring and debugging. This could be accomplished over the 5G/6G cellular network assuming that the device the expert would be using would have a SIM card and would be directly connected to a cellular network. To secure the remote access, it would be best to isolate all communication to/from the expert's device to/from the managed device completely from the current consumer Internet. This can be done by creating a special packet data network (SPDN) where one or more cellular networks are connected to in addition to the gateways to one or more of the above-mentioned specialized networks. The SPDN would apply trust networking to its own operation but run on the same packet transport that is used to run the normal Internet and all the VPNs the operators are providing to their customers. To secure this solution in the best possible way, access to the SPDN must be properly restricted in the subscription management system of the MNOs and by using suitable security policies on the SPDN. If more than one MNO use the same SPDN, they will need to agree on certain policies and emergency response processes on this SPDN. If MNOs can agree to share a SPDN, large national specialized networks become possible so that remote access is provided from any national MNO network.

Yet another possible use case of trust networking is such that a trustworthy network would be offered to consumers of any smart phone or similar device for special services such as banking, or e-government. The purpose would be to provide access to these services without fear of some denial of service attack taking down the service. The challenge is how such a "trustworthy network" can stay secure under untrusted end user devices? How could possible viruses or malware on the end user device be isolated from interfering or disturbing the "trustworthy network" in any way? Although this use case requires further research, trustworthy networking will help as compared to using the normal Internet connected service. Under trustworthy networking, it is always possible to put blame on some network entity or host immediately upon detection of any suspicious activity. Also, any attack will have to originate from device with SIM cards, so the attacks will be more costly to carry out than when normal poor security Internet hosts can be used as bots by the hackers.

The final test for the usability and scalability of the trust networking idea is whether it could be used to process all Internet or mobile user traffic in such a way that most of the security related processing would be moved to the cloud, would be professionally operated using the best available security intelligence, would offer fast deployment of security patches to all known vulnerabilities and as a result offer a major security upgrade to the Internet security for Beyond-5G/ 6G users as a whole.

D. *Required technology development*

Since the concept of Policy in the ITU-T framework is unclear, it is hard to define what technology will be needed to actually implement the framework. In case of CES this is easier to point out. In addition to framework or architecture level recommendations, at least the following best practice documents, interfaces, formal descriptions and application programming interfaces (API) will be needed:

- A comprehensive policy definition language.
- Edge to edge trust signaling for admin functions.
- Edge to edge trust signaling for host policy matching.
- An API for the user agent consisting of the host to host signaling layer and the needed policy storage to use the services of the admin level trust network.
- An API for feeding security intelligence into trust networks
- Best practices of using DNS for trust networking.

Optionally, alternative to DNS mechanisms for address /naming/ identification could be specified. We however, believe that trust networking can be supported by DNS, enhanced DNS, DNSSEC possibly further enhanced for the purpose. So, we advocate that the possible move to alternative naming/address management infrastructure should not be tied to the introduction of trust networking.

VII. Conclusions

Trust networking is emerging as a new promising type of technology and service that could be deployed for special services over 5G/B5G or 6G networks with the goal of taking a major step in providing a much more predictable level of service as compared with what we must today be satisfied with. This technology will help implement unprecedented use cases for mobile networks some of which are safety critical, many create lots of privacy sensitive information on the physical world/ digital world boundary, and some could potentially be used against nation states by either terrorist organizations or other nation states. Thus, many of these use cases will be of high interest for national security.

It is an open question to what extent the same technology could be offered to produce consumer services while we are under the current liberal no certification policies for consumer devices and no liability on fit for purpose software licensing arrangements for applications. However, if it will turn out that despite best efforts for creating smart policy creation tools for the consumer market use cases, we are unable to create and maintain fine grained policies for all consumer devices, we may be able to create policy tools for all-is-allowed-except known-malware-use kind approach. Even in this case, trust networking when applied to the general Internet Access Services would finally put an end to source address spoofing and make most distributed denial of service attacks from botnets created from consumer devices ineffective. Also, any detected malicious activity could easily and immediately be attributed to the involved entities increasing the level of automation and lowering the cost of information security.

Acknowledgment

Customer Edge Switching has been developed in several consecutive projects in partnership with many companies, to mention the most important ones, they are Nokia and Ericsson and lately F-Secure. Funding has been mostly national, from TEKES, from BusinessFinland and private foundations (Technology Industry Foundation and Sanoma Foundation).

References

[1] Levi White Paper 2019, Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence, Oulu University, 9/2019.

[2] R. Kantola, 6G Network Needs to Support Embedded Trust, Proceedings of ARES 2019.

[3] ITU-T, Y.3053 Framework of Trustworthy Networking with Trust-centric Network Domains.

[4] ITU-T, Y.3052, Overview of Trust Provisioning in Information and Communication Technology Infrastructures and Services.

[5] R. Kantola, Implementing Trust to Trust Using Customer Edge Switching, AINA 2010 WS on Advances in Mobile Computing and Applications: Security, Privacy and Trust

[6] R. Kantola, J. Llorente Santos, N. Beijar, Policy Based Communications for 5G Mobile with Customer Edge Switching, Wiley Security and Communication Networks, 05/2015.

[7] J. Llorente Santos, N. Beijar, R. Kantola, P. Leppäaho, Implementing NAT Traveral with Private Realm Gateway, IEEE Int'l Conference on Communications (ICC'13) 9-13 June 2013, Budapest

[8] GitHub/Aalto5G referenced December 16, 2019.

[9] R. Kantola, H. Kabir, P. Loiseau, Cooperation and end-to-end in the Internet, International Journal of Communication Systems,Wiley, 02/2017.

[10] Z. Yan, Ra. Kantola, Y. Shen, Unwanted Traffic Control via Hybrid Trust Management, IEEE TrustCom2012, Liverpool, UK .

[11] Y. Shen, Z. Yan, R. Kantola, Analysis of the Acceptance of Global Trust Management for Unwanted Traffic Control based on Game Theory, Elsevier Computers&Security, 2014.

[12] H. Kabir, J. Llorente Santos, R. Kantola, Securing the Private Realm Gateway, IFIP Networking, 2016.

[13] H. Kabir, H. Mohsin, R. Kantola, Implementing Security Policy Management for 5G Customer Edge Nodes, to appear in NOMS 2020.

[14] R. Kantola, White Paper, Cooperative Security for 5G and the Internet, Nov 2018, Aalto University, available at re2ee.org.

[15] EU Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union *OJ L 310, 26.11.2015, p. 1–18* ELI: http://data.europa.eu/eli/reg/2015/2120/oj

[16] Body of European Regulators for Electronic Communications, BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules.

[17] R. Kantola, Comments to BEREC Hearing on Open Internet/5G, 11/ 2019, available in re2ee.org; publications.