Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89
	)	

WRITTEN *EX PARTE* SUBMISSION OF HUAWEI TECHNOLOGIES CO., LTD., AND HUAWEI TECHNOLOGIES USA, INC.

Huawei Technologies Co., Ltd., and Huawei Technologies USA, Inc. (collectively, "Huawei"), by their undersigned counsel, submit this *ex parte* presentation to the Federal Communications Commission ("FCC" or "Commission") to supplement the record in the above-captioned docket.

Huawei submits as **Attachment 1** the expert report of Professor Valtteri Niemi,[1] which analyzes how security is addressed in 5G network standards. Huawei understands and commends the U.S. Government's efforts to mitigate cybersecurity risks in its telecommunications infrastructure. However, as Huawei has explained extensively in the record, the Commission's proposed rule would harm a substantial number of carriers—and in particular carriers in rural and remote areas. The Commission is obligated to weigh carefully the costs and benefits of its proposed rule. In doing so, the Commission should take into account the enhanced security requirements and features built into the standards for 5G networks. For example, a recent report about 5G

[1] *See* Valtteri Niemi, "Expert Report on 5G Security," (Nov. 1, 2019) ("Niemi Report"). Professor Niemi leads the Secure Systems Research Group and serves as Deputy Head of the Computer Science Department at the University of Helsinki.

cybersecurity recognizes that “5G technologies and standards could improve security compared to previous generations of mobile networks, due to several new security functions, such as stricter authentication processes in the radio interface.”[2] Moreover, “contingency approaches have been defined through standardization level by 3GPP” to mitigate many of the “identified risks” linked to 5G technology.[3] Proceeding to adopt the proposed rule, which does not account for the unique security features of 5G networks, would be arbitrary and capricious.

Respectfully submitted,

/s/_Andrew D. Lipman_______

Glen D. Nager
Bruce A. Olcott
Ryan J. Watson

Jones Day
51 Louisiana Ave., NW
Washington, D.C. 20001
(202) 879-3939
(202) 626-1700 (Fax)
gdnager@jonesday.com
bolcott@jonesday.com
rwatson@jonesday.com

Andrew D. Lipman
Russell M. Blau
David B. Salmons

Morgan, Lewis & Bockius LLP
1111 Pennsylvania Ave., NW
Washington, D.C. 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com
david.salmons@morganlewis.com

Counsel to Huawei Technologies Co., Ltd.,
and Huawei Technologies USA, Inc.

November 1, 2019

[2] *See* NIS Coordination Group, “EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks: Report,” para. 1.18, (Oct. 9, 2019), available at: https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf.

[3] *Id.*, para. 3.7.

Attachment 1

“Expert Report on 5G Security” by Professor Valtteri Niemi

Expert report on 5G security

Personal Background and Qualifications

I am a Professor of Computer Science at University of Helsinki where I lead the Secure Systems research group and am the Deputy Head of the Computer Science Department. Prior to my work with the University of Helsinki, I was a Professor of Mathematics in two other Finnish universities: (1) University of Vaasa from 1993 until 1997 and (2) University of Turku from 2012 until 2015. I also served for 15 years in various roles at Nokia Research Center and was nominated as a Nokia Fellow in 2009. At Nokia, I worked on various wireless security topics. I participated in the 3GPP SA3 security standardization group from its beginning and served as chairman of the group from 2003 until 2009. I have published more than 80 scientific articles and am a co-author of four books about mobile communications security.

A complete statement of my qualifications is set forth in my curriculum vitae, attached hereto as Exhibit A.

I have prepared this report at the request of Huawei Technologies Co. Ltd. and Huawei Technologies USA, Inc. (collectively, "Huawei"). This report represents my independent assessment and opinions.

Introduction

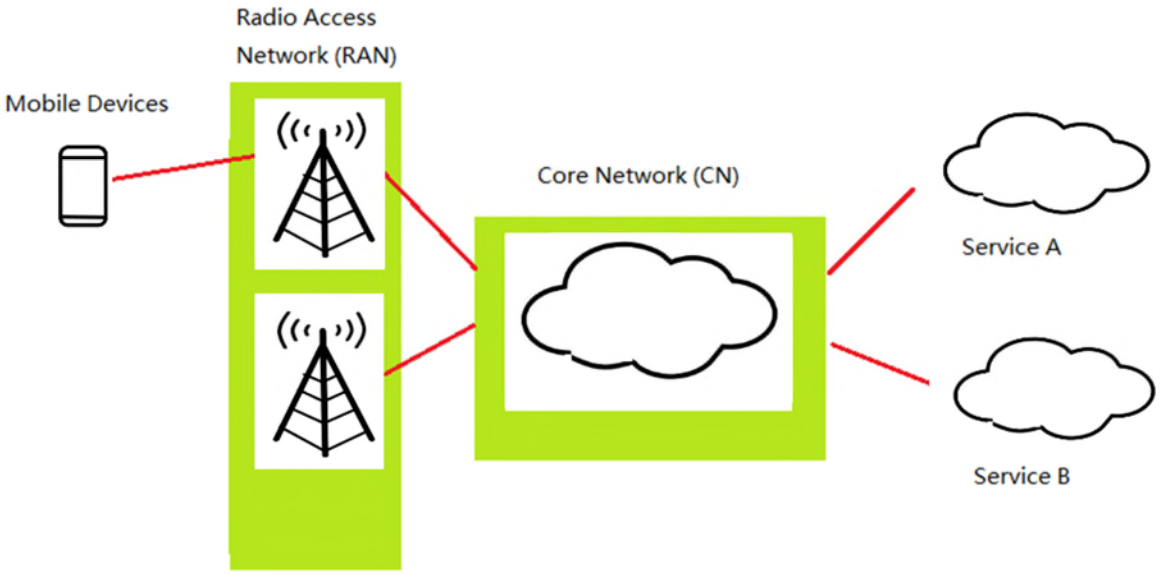
In considering adoption of rules that would prohibit the use of universal service funds for the purchase of equipment or services from providers identified as posing a national security risk to telecommunications networks, the Federal Communications Commission ("FCC") should consider how security will be addressed in 5G networks.[1] As this report explains, security has been a central topic in the development of 5G standards. As a result, those standards build in not only the security requirements and features of today's fourth generation wireless networks, but also additional requirements that will enhance security. Furthermore, those standards also reduce the likelihood for telecommunications networks to be subject to attack by bad actors.

[1] *See* Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, Notice of Proposed Rulemaking, WC Docket No. 18-89, 33 FCC Rcd 4058 (2018).

5G basics

The term 5G refers to the 5th generation of mobile communication technologies. A mobile network contains both a network of base stations called the radio access network (RAN) and a core network (CN). Mobile devices communicate with base stations through radio links, and base stations connect with the CN typically by a wired link, although some may connect via wireless technologies. In mobile networks, the RAN equipment is often supplied by a different vendor than the CN equipment. The CN contains elements that are responsible for keeping track of the whereabouts of mobile devices, setting up calls, storing information about user subscriptions, managing base stations, authentication, charging and billing, and many other functions. The manufacturer of any element in the network does not take part in the operation of the element unless there is a specific agreement about such an arrangement between the network operator and manufacturer.

For each of the generations of wireless network technology prior to 5G, several different standardized technologies were created and deployed. However, one technology, referred to as Long Term Evolution (LTE), is clearly dominant in the 4th generation. The LTE standards were created by an organization that consists of seven different regional telecommunications standard bodies referred to as the 3rd Generation Partnership Project or 3GPP.[2] With respect to 5G, 3GPP has already developed the first standards applicable to this new technology, and current 5G deployments are based on these 3GPP standards. The standards keep evolving with advanced features and performance.



[2] *See* Introduction of 3GPP Organizational Partner, available at: https://www.3gpp.org/about-3gpp/partners.

The scope of 5G can be understood at least in three different ways. The narrowest view is to look at the way in which a mobile device, such as a smart phone or a tablet, communicates wirelessly with a base station. The 3GPP adopted a new radio interface called 5G New Radio (NR). It enables significantly higher bit rates than what can be provided by LTE technology.

A broader view of 5G considers the whole system. The first 5G deployments, appearing in several countries during the first half of 2019, follow a model where the existing LTE network is extended with 5G NR base stations. This model is referred to as 5G Non-Standalone (5G NSA) because it relies on the LTE core network and NR base stations are added into the RAN. The 3GPP has also developed specifications for a whole new core network, and in the 5G Standalone (5G SA) model, 5G NR base stations are connected to the 5G core network.

Finally, the broadest view of 5G is to consider all the different applications and services that would use 5G technologies in some manner. The commonly shared vision for 5G is that it would be used extensively for a much wider set of services than LTE. Examples of such services are ones needed for smart cities and for controlling robots in a factory. 3GPP has identified two main domains for new services: first, a Massive Internet of Things (MIoT); and second, Ultra Reliable and Low Latency communications (URLLC). The main characteristic of MIoT is the presence of a huge number of devices that are connected to a larger private network or public network, *i.e.*, the internet. The domain of URLLC supports use cases such as autonomous vehicles where communication has to be very reliable, the speed at which data traverses a network must be very fast, and the latency must be very low.

As with prior generations such as LTE, users of 5G networks create subscriptions with home networks. Home networks can have roaming agreements with other networks. Roaming agreements allow users to seamlessly create trust relationships with other networks when travelling outside users' home networks' coverage areas into coverage areas of these other networks.

In this report, I discuss security aspects for each of the three different viewpoints of 5G.

Overview of 3GPP work

The 3GPP specifications are developed by the international telecommunications industry and government players, with wide participation from all areas of the mobile communications ecosystem. Mobile network providers such as Verizon and China Mobile, network equipment vendors such as Ericsson and Huawei, mobile device vendors such as Apple and Samsung, and chipset vendors such as Qualcomm and Intel, are all contributing to these specifications, together with telecommunications regulators such as the FCC and representatives of vertical industries that plan to utilize these technologies. Participants through October 28, 2019, include 686 individual member companies[3] across 45 countries and 18 organizations representing different segments of the telecommunications marketplace.[4]

3GPP is widely recognized as a successful and influential standards-setting organization. Since its establishment 20 years ago, working procedures of 3GPP have remained stable with only minor revisions. 3GPP aims for open and fair technical discussions, and its basic principle for reaching agreement is by consensus. The 3G and 4G standards developed by 3GPP have been widely deployed in the world. There is a high likelihood that the 5G standard developed by 3GPP will be the only 5G standard in the world, and a number of telecommunications companies are deploying 5G based on specifications provided for in 3GPP's first release (Release 15).

The working group SA3 is responsible for security technologies in 3GPP. There are more than 50 companies participating in SA3 meetings and more than 100 experts jointly worked on the 5G security standard by participating in the meetings, with many more experts contributing to the work from company offices. Key players in SA3 include Apple, AT&T, Ericsson, Huawei, Nokia, Qualcomm, Samsung, T-Mobile, and Vodafone, among others.

The first 5G security standard is associated with 5G Release 15 and provides the standardized security solutions for the features included in the first phase of 5G. Prior to the creation of the 5G security standard, the working group SA3 carried out an extensive study phase identifying key security issues as well as consideration of potential solutions to resolve identified vulnerabilities associated with the technology and the corresponding standards. The security standard continues to evolve in Release 16 and onwards to address new and additional security vulnerabilities attendant to the introduction of the new features and functionalities enabled by each 5G Release. For example, 5G enables new use cases for mobile networks and devices based on the capabilities of MIoT and URLLC. The potential vulnerabilities associated with these use cases require evaluation and consideration on an ongoing basis.

Security for 5G Non Standalone

In all generations of mobile networks, starting from GSM, certain important security features have been included and embedded in the radio level procedures. For example, encryption of the communication is handled between the mobile device and the RAN. The encryption is based on a shared secret key. This key is generated during the process whereby the mobile device and the mobile network authenticate each other. The core network is responsible for the authentication and key agreement procedure. After the key is generated, the core network sends it to the RAN. The mobile device is able to generate the same key based on the data it receives from the network, during the authentication procedure. These

[3] *See* 3GPP Membership, available at: https://webapp.etsi.org/3gppmembership/Results.asp?Member=ALL_PARTNERS&SortMember=Name&DirMember=ASC&SortPartner=Name&DirPartner=ASC&SortMarket=Name&DirMarket=ASC&SortObserver=Name&DirObserver=ASC&SortGuest=Name&DirGuest=ASC&Name=&search=Search.

[4] *See* 3GPP Market Representation Partners, available at: https://www.3gpp.org/about-3gpp/partners.

principles have been followed for 3G and 4G technologies, and the same is true for 5G. Therefore, security for 5G New Radio is very similar to LTE radio security.

There are differences in the specifics as to how encryption between the device and the network occurs in a 5G-based network compared to one based on 4G or 3G technologies due to the details associated with the different technological environments that devices and networks operate in based on these differing technologies. However, the overall principle of using encryption to transmit information between the device and network (and *vice versa*) and authentication procedures is similar across all technologies.

Starting with LTE, radio base stations have been sometimes placed in vulnerable locations where they are exposed to potential intruders, e.g., unsecured indoor locations or on roof-tops. As a result, LTE security solutions included platform security measures to protect base stations. Similar protection methods apply to 5G NR. It is important to note, however, that it is not possible to influence the authentication procedure by penetrating base stations, no matter whether the network in question is a 4G or 5G network. Moreover, 5G networks are designed to be resilient so that even if a base station is damaged or otherwise unable to operate the rest of the network is still able to function normally.

In summary, security for 5G New Radio is a result of a fairly straight-forward modification of LTE radio security. Because the 5G NSA system is formed by just adding 5G NR base stations to a LTE system without replacing the core network, the security of 5G NSA is very similar to that of the LTE system.

Security for 5G networks

The main part of the 5G authentication procedure between the mobile device and the network is identical to the corresponding procedure in LTE networks. However, the 5G authentication procedure includes an important additional feature. When operating in a 5G environment, home networks, in roaming situations, verify to ensure that roaming partner networks actually execute authentication procedures as expected. This new functionality assists 5G providers in offering users a more secure operating environment even when roaming.

As briefly described above, authentication is inherently tied with generation of secret keys. Starting with GSM, in all mobile networks, the master shared key for each user is stored in a tamper-resistant module that is called a SIM card for GSM. The corresponding module for 3G networks, LTE networks and 5G networks is called a Universal Integrated Circuit Card (UICC). In 5G networks, as in LTE networks, another key is derived from the above mentioned key to be used as a local master key in the visited network. From this derived master key, many more keys are derived, e.g., a different key for each base station. In 5G, the number of different types of keys that various network elements share with the mobile device is higher than in LTE networks. This provides support for more flexible network configurations and enhanced security. The security is enhanced in 5G networks as compared to earlier generations of mobile networks because in each context a separate key is in use, and it is not possible to derive any other key from one such key. Hence, even if one key is compromised, other keys remain secure thereby limiting vulnerabilities to fewer devices and also requiring multiple layers of penetration by attackers.

5G networks also enhance security associated with user identities transmitted over such networks. Starting with GSM, and in all subsequent mobile network generations, user identities have been protected against potential radio eavesdroppers. These kinds of attackers would tune in to the radio frequencies reserved and licensed for mobile communications. Such attackers cannot determine users' identities because the network employs the use of temporary identities, i.e., pseudonyms, for users and transmits information about pseudonyms over encrypted channels. Eavesdroppers cannot decrypt the protected information because they do not know or otherwise have access to the shared key. However, in mobile networks that pre-date 5G, determining users' identities is possible for sophisticated attackers. In contrast, public key cryptography is used in 5G to prevent a rogue base station from obtaining a user's permanent identity. This is because a user's permanent identity is always delivered in encrypted form, and only the user's home network can decrypt the identity. The home network provides later the decrypted permanent user's identity to a serving network.

The 5G core network allows access for users through technologies other than 5G New Radio. Other radio interfaces defined by 3GPP, such as LTE or 3G, are supported, as well as access via Wi-Fi or other technologies that are not defined in 3GPP. Regardless of the technology used to access the 5G core network, 5G networks employ a unified authentication framework. For example, it is possible to derive a shared key usable over a Wi-Fi connection from the local master key allowing for the secure exchange of information between the Wi-Fi connection and the 5G network.

The Cloud is one of the key technologies influencing the 5G core network, and to some extent the 5G RAN in some deployment scenarios. Instead of relying on full-featured devices, 5G networks allow for implementing various functions as software on top of general-purpose hardware, typically residing at the data center level. In this way, the network becomes more flexible. This approach is called Network Function Virtualization (NFV). The virtualization approach for the 5G core network has been taken into account beginning already in the design phase for 5G. One result of NFV is the ease of adding new functions to the 5G core network that has a Service-Based Architecture (SBA) compared to LTE that employs a traditional network architecture. In the SBA setting, in order to add a new network function, it is sufficient to define how other functions can make requests to the new function and how the new function would respond to those requests. In contrast, if a new network function is added to the traditional network architecture, one typically needs to define different interfaces from the new function towards all such existing network functions with which the new function may need to communicate. This is done in order to allow the new functions to cooperate with the existing functions in the network architecture.

The SA3 working group has specified a security solution for SBA. The key component of the solution is inclusion of a Security Edge Protection Proxy (SEPP). This proxy acts as a gate-keeper for the network and transmits over a secure channel with similar proxies on other networks, which arrangement is needed and applicable for users roaming on third-party service provider networks. Mobile networks that preceded 5G have been found to be vulnerable to attacks in roaming environments where attackers could manipulate third party devices controlled by roaming carriers. Accordingly, as compared to earlier generations of mobile networks, 5G is more secure due to SBA SEPP preventing these and similar attacks from tampering with critical data that is exchanged between core networks.

One aspect that is carried over from LTE security procedures to 5G is the functional split of RAN and the CN. The key security functions, i.e., authentication, access control, subscriber identity privacy and lawful interception, reside on the CN rather than on the RAN. The inclusion of Multi-Access Edge Computing (MEC) as a core network function according to the 3GPP specification in Release 15 sometimes causes confusion with respect to the functional security split between RAN and the CN. The MEC functionality, defined as a core network function according to the 3GPP specification, enhances applications' responses to users by enabling such functionality at locations geographically closer to users at the edge of the core of the 5G network. However, the edge of the network in this sense is the edge of the external data network, not the edge of the mobile network and this does not change the functional split between the RAN and the core network. Thus, the security arrangements associated with the functional split of RAN and CN remains in place in 5G networks.

In conclusion, security procedures for 5G networks are consistent with principles of LTE network security but are also enhanced and extended in several important ways that make 5G networks inherently more secure than prior generations of mobile networks. Several new security mechanisms have been introduced while no security mechanisms that exist in the LTE network architecture have been discontinued.

Security for services that use 5G networks

When 5G is interpreted broadly to include all services and applications that utilize 5G networks and technologies, 3GPP's Release 16 addresses a wider scope of security issues than those covered by Release 15. These service-specific security issues are beyond the scope of this report, though required security solutions for all Release 16 features will be defined by 3GPP's Release 16. Moreover, 3GPP can provide generic enablers and standards that may be useful for many services that deal with massive IoT or URLLC. Several studies have already been carried out in the SA3 working group about key security issues in these domains and potential solutions. 3GPP has enabled network players to take care of the security of the wireless communication network itself. The additional service and application security, however, is the responsibility of application and service providers. For example, the application provider is responsible for encryption in the application layer. Through end-to-end encryption enabled by the application provider, information sent by a user is encrypted from its source (i.e., the user sending out the information using the application), with decryption only taking place at the information's destination (e.g., another user receiving the information using the same application).

Security for 5G deployments

In addition to effective security standards built into the 5G standards, it is important to test products against the standards to assure that implementation is aligned with the standards. The SA3 working group has created many specifications that can be used to verify whether implementations of security features operate as intended. This is called security assurance work. There are separate specifications for all different elements in the network.

The GSM Association (GSMA) also has established the Network Equipment Security Assurance Scheme (NESAS) for the purpose of security test work. The 3GPP expects to publish the first version of the relevant standards in 2019. The draft version is under review by all stakeholders including regulators from key countries including the United States. 3GPP approved the Security Assurance Specification (SCAS) for 5G base stations in June 2019, and corresponding SCAS specifications for core network functions were approved in September 2019.

There are also other activities on this front. For example, an industry forum Next Generation Mobile Networks (NGMN) plans to establish a lab for 5G security testing work.

Conclusions

As this report notes, there are several different perspectives on 5G security. The first viewpoint concerns the new radio interface. As I have explained in this report, security for 5G New Radio is a result of a fairly straight-forward modification from LTE radio security. Because the 5G Non-Standalone system is formed by just adding 5G New Radio base stations to an existing LTE system without replacing the core network, the security of 5G Non-Standalone is very similar to that of the LTE system.

The second viewpoint is for the new core network. As I have explained in this report, security procedures for 5G core networks are consistent with principles of LTE network security, but are also enhanced and extended in several important ways. The functional split between the RAN and the core network for key security functions such as authentication remains for 5G networks, while additional mechanisms such as the use of many security keys meaningfully enhance the security of 5G networks.

The third viewpoint is about the 5G service ecosystem. The 3GPP has enabled network players to address the security of the network itself. Additional service and application security is taken care of by application and service providers.

There is also the matter of 5G deployments. Several activities have been established by different parties for providing assurance of appropriate security measures in products and deployments in compliance with 3GPP's 5G standards.

Exhibit A

Curriculum Vitae of Professor Valtteri Niemi

CURRICULUM VITAE

13th May 2019

Name: Pentti **Valtteri NIEMI**
Male, Finnish citizen, born 11th September 1960
Postal address: Velusmaantie 61, 21140 Rymättylä, NAANTALI, Finland
Tel: +358 50 4837327
email: valtteri.niemi@helsinki.fi

Education and degrees:

Doctor of Philosophy, 25th May 1989, University of Turku, Department of Mathematics; Ph.D. thesis with highest grade (laudatur)
Master of Science, 29th January 1987, University of Turku, Department of Mathematics: highest grades

Current employment:

Professor in Computer Science, with specialty in Information Security, University of Helsinki, Finland, Department of Computer Science, from beginning of 2015. Deputy Head of the Department since 2016.

Most important career duties and titles:

Several positions in Academy of Finland projects, University of Turku and Vaasa Polytechnic Institute 1983-1992 (total 97 months); University of Turku, Associate Professor(acting) (*vs. apulaisprofessori),* 1992-93 (12 months); University of Vaasa, Department of Mathematics and Statistics, Associate Professor in Mathematics (*ma. apulaisprofessori)*, 1993-97 (4 years); Nokia Research Center, Helsinki, various positions: starting as Senior Research Engineer and ending as Research Fellow and Distinguished Research Leader 1997-2008; Nokia Research Center, Lausanne, Switzerland, as Research Fellow 2008 and Nokia Fellow, 2008-2010; Nokia Research Center, Helsinki: as Distinguished Research Leader and Nokia Fellow, 2011-2012 (total 15 years);
University of Turku, Department of Mathematics and Statistics, Professor in Mathematics (cryptography), 2012-2014 (part time still in 2015-2016)

Research visits:

Selected as a "High-end foreign expert" in China for 2014, located with Xidian University, Xi'an; spent in total two months there. Visited for total of one month also during each of the years 2016, 2017 and 2018.

Main awards:

Rolf Nevanlinna Ph.D. thesis award, 1990, for the best Finnish Ph.D. thesis in Mathematics; Nokia Quality Award, 2005, for the best Nokia research project (together with a team); Nokia Breakthrough Award 2008 for major impact technology transfer; Finnish Cyber Security Researcher of the Year 2016.

Recent research funding:

Academy of Finland project "Cloud Security Services", 2014-2016: 250 kiloEuros; sequel project "Cloud-assisted Security Services", funded by TEKES, 2016-2019: 450 kE; TEKES project TAKE-5, 2015-2018: 176 kE; Huawei Technologies bilateral research projects, 2016-2019: 830 kE; Intel donation grants, 2017-2018: 150 kE; EU H2020 project HELIOS, 2019-2021: 255 kE; Business Finland project 5GFORCE, 2019-2021: 550 kE.

Research leadership and supervision of doctoral and master level theses:

Contributions to several EU projects: Nokia-side leader in SHAMAN (Secure Heterogeneous Access for Mobile Applications and Networks) 2000-2002 and CYBERVOTE (An innovative cyber voting system for Internet terminals and mobile phones) 2000-2003; Contributions to several TEKES projects:

Nokia-side leader in TiViT SHOK program “Future Internet” 2011-2012; Nokia-side responsible for planning of TiViT SHOK program “Internet of Things” that started in 2012; Coordinator and Principal Investigator in Finnish Academy project “Cloud Security Services”, 2014-2016, PI in TEKES project “Cloud-assisted Security Services”, 2016-2018; PI and security task leader in TEKES project “TAKE-5” for 5G technologies, 2015-2018.
Approx. ten M.Sc. theses supervised, several more co-supervised from Nokia side; During Nokia time I had no official role in Ph.D. thesis supervision but some Ph.D. theses have been completed by members of my team(s) in Nokia, including Y. Zheng, 2007, D. Forsberg, 2010, K. Kostiainen 2012, J.-E. Ekberg 2013, all in TKK/Aalto.
One Ph.D. student officially supervised in University of Turku (Noora Nieminen, March 2017); Internet Laboratory responsible person for NRC Ph.D. program 2007-2008

Other scientific and academic duties:

Opponent/Committee member for Ph.D. dissertations:
Marko Hassinen, Univ. of Kuopio, Finland, 2006, Geir Koien, Univ of Aalborg, Denmark, 2008, Julien Freudiger, EPFL, Lausanne, Switzerland, 2010, Ravishankar Borgaonkar, TU Berlin, Germany, 2013, Matus Harvan, ETHZ, Zürich, Switzerland, 2013,Tuomas Kortelainen, Univ. of Oulu, Finland, 2014, Juha Partala, Univ. of Oulu, Finland, 2015, Yki Kortesniemi, Aalto University, Finland, 2015, Huihui Yang, Univ. of Agder, Norway, 2016, Sanna Suoranta, Aalto University, Finland, 2016, Mingjun Wang, Xidian University, China, 2017, Wenxiu Ding, Xidian University, China, 2017
External examiner for Ph.D. theses: six times
Several assessment duties for Adjunct Professorships (Docent)
In addition to job-related teaching, more than 10 additional courses lectured in academia and industry.
Recent Technical Program Committee memberships:
ETSI security workshop 2011-2013, FRUCT workshops 2011-2019, SSR 2014, 2016, 2018, IEEE CIT 2014, IEEE Trustcom 2015, ACM WiSec 2009, 2016, 2017, NordSec 2016, NSS 2017
Major role in organizing committees:
Eurocrypt 1998 (Financial Officer), Finnish Mathematical Days, 1995, Diderot Forum 2001, IEEE CIT 2014 (Panel Chair), IEEE Trustcom 2015 (co-General Chair), EAI MobiMedia 2016 (Workshop co-Chair/Panel Chair), NSS 2017 (co-General Chair), FRUCT 21 (General Chair), 2017, FRUCT 25 (General Chair), 2019.
Peer reviewer for many scientific journals and conferences

Other significant duties in industry/society:

Leader of several collaboration projects between Nokia and academic partners, Leader of more than 20 Nokia internal research projects and programs, Founding member of the Nokia Research Center Lausanne laboratory at EPFL campus 2008, Promoted to the highest technical expert rank of “Nokia Fellow” as fifth person in the company history in 2009, Chairman of the 3rd Generation Partnership Project (3GPP) security working group 2003-2009, (Vice chairman 2001-2003, Nokia main delegate in the above working group in 1999-2003), Nokia main delegate in ETSI GSM security working group (SMG10) 1997-1999, Board Member of Nokia Foundation 2010-2018 (vice chair 2017), Member of MATINE (Scientific Advisory Board for Defence) working group for ICT since 2013 (vice chair since 2016) and theme group for cybersecurity since 2016; Member of Finnish government working group for preparing voting over Internet, 2013-2015; Professor Union (*Professoriliitto,* in Finland): participation in various meetings as Univ. of Vaasa section representative 1994-97

Patents, invited lectures in conferences, publications:

34 patent families co-authored; Many essential patents for cellular standards; some used in litigation: e.g. two patents in Nokia vs Qualcomm; as a result Qualcomm acquired one of the patents; two other patents in Nokia vs. Apple; as a result Apple agreed to pay lump sum and royalties; in addition, 21 patent applications co-authored
22 invited talks in scientific conferences, seminars and workshops
18 invited talks in industrial conferences, seminars and workshops
80 original scientific articles in journals, refereed conferences and edited books
25 other scientific publications
4 published monographs, some translated to Chinese, Spanish and Russian
Total citations: 3340, h-index: 26 (Google Scholar)