GLOBAL HEALTH INNOVATION

OPEN UCT PUBLICATIONS

Security architecture for a 5G mHealth system

Bessie Malila*, Tinashe E.M. Mutsvangwa

Division of Biomedical Engineering, Department of Human Biology, University of Cape Town, Cape Town, South Africa

Received 7 May 2019; Accepted 29 May 2019; Published online 30 May 2019

Abstract

Global health challenges and the proliferation of mobile technologies have been key in the adoption of mHealth for provision of low-cost and equitable healthcare. Evolution of mobile networks to 5G is expected to revolutionise healthcare service delivery due to the stringent performance requirements imposed on 5G. However, because of the open nature of 5G systems, securing patient health information has been identified as a significant barrier to the full adoption of mHealth. In this paper, we propose a security architecture for an mHealth system based on a review of standard principles and guidelines for designing 5G security systems. We present a structured approach for developing and implementing an end-to-end 5G mHealth security system. We propose a security architecture that can be realised using keyless signature infrastructure Blockchain and X-tee technology to secure the communication system including hospital and third-party health data networks, physical layer security for securing the wireless interface in access networks, physical unclonable functions, and a trusted execution environment for securing end-user devices. We propose the adoption of network slicing for isolating health systems from other 5G industry verticals. We define system domains that are used to identify security threats and propose mechanisms to mitigate these threats.

Keywords: mHealth; 5G; security architecture; network slicing; Blockchain; X-tee

Introduction

Mobile health (mHealth) has the potential to mitigate the negative impacts of disease globally. The main drivers for the adoption of mHealth include improvements in information and communication technologies; the need to address global healthcare and social care challenges; the shift from hospital- and practitioner-focused care to distributed and virtualised patient-centred care; and the emergence of the fifth generation of wireless systems (5G) (5G-IA, 2015). mHealth systems implemented using 5G will allow provision of healthcare in locations where it has not been possible to do so before. While current 4G technologies have enabled delivery of mHealth services, 5G is expected to improve the reach and quality of healthcare due to the expected 100% network coverage including rural and remote areas and service that is superior to 4G. The performance and capability requirements defined for 5G provided in the third-generation partnership project (3GPP) technical specification 3GPP TS 22.261 (3GPP TS 22.261, 2019), differ substantially from those of earlier mobile technologies. Capabilities that will drive increased adoption of mHealth systems include network slicing, multiple access technologies, quality of service monitoring, device positioning and service prioritisation. 5G network performance requirements include high data rates and traffic densities, ultra-reliable low latency communications, enhanced mobile broadband, and massive machine type communications. Where these are not achieved, 5G is expected provide service that is superior to that of 4G. Table 1 summarises the key differences between 4G and 5G and the benefits of 5G to mHealth (5G Americas).

Table 2 shows the performance requirements for the new mHealth/telemedicine services, i.e. augmented/virtual reality, assisted surgery and remote medication control, in terms of latency and positioning accuracy (Marabissi et al., 2019). While some mHealth services may be available in 4G, 5G aims to make the services available in all areas, including rural and remote; and improve the services where they are being delivered over 4G. The underlying technologies enabling high performance on the wireless segment of the mobile network, i.e. between mobile phones and base stations, include massive multiple-input multiple-output (MIMO) for increased spectral efficiency and efficient network coverage, millimetre wave (mmW) for Gbps data rates and small cells for improved network coverage (Wu et al., 2018). Software defined networking (SDN) and network functions virtualisation (NFV) technologies are being proposed to enable dynamic service provisioning on the 5G system, while mobile edge computing (MEC) is expected to bringing content closer to users for higher data rates

*Corresponding author: bessie.malila@uct.ac.za and lower latency. Network slicing will enable flexible and scalable network partitioning into different virtual service segments. SDN and NFV are used to realise the distributed 5G core and network slicing (Ordonez-Lucena, 2017).

Table 1. Comparison of the performance requirements defined for 4G and 5G systems (5G Americas, 2018).

Parameter	**4G**	**5G**	**5G benefits for mHealth**
Download speed	300Mbps to 1Gbps	1Gbps to 10Gbps	Transfer of large data files, high quality image and high-quality video and augmented/virtual reality services
Latency	<50ms	<1ms	Near-real-time video and augmented/virtual reality services
Operating frequencies	800MHz, 1.8GHz, 2.6GHz	2,3GHz, 3.4GHz, 3.6-3.8GHz, >24GHz (mmW)	Wide operating bandwidths for improved network coverage and quality of service
Technologies		Network slicing, software defined networking, cloud-based, network function virtualisation, small cell base stations, mobile edge computing	Agile, scalable, flexible and dynamic healthcare service provision
Coverage	Based on commercial viability	100% or superior to 4G	100% or superior healthcare coverage

Table 2. Performance requirements for mHealth use cases (3GPP TS 22.261, 2019).

Parameter	**mHealth use case**	**Guideline**
Latency	Real-time video	100ms end-to-end
	Assisted surgery	
	Telepresence/augmented reality	
	Real-time command and control for remote medication and surgery	10-100ms end-to-end
Positioning accuracy	Remote healthcare and remote assisted surgery	1-10meters

In 5G, user devices will have multi-connectivity capabilities, i.e. LTE, WiFi and new radio frequencies, offering more flexible and reliable connections. Artificial intelligence and machine learning tools are expected to aid in the use of network generated data and allow network operators to adapt to evolving traffic patterns, security risks and user behaviour. Adoption of these technologies and tools in 5G will allow healthcare services such as asset and intervention management in hospitals, robotic surgery, real-time remote monitoring of health, and smart medication (5G IA, 2015).

The benefits of 5G systems come with increased security risks due to the large number of deployed devices, the open nature of 5G networks, an elevated use of virtualisation and cloud services, and a broader multifaceted security attack surface (Han et al., 2017). These security risks pose a significant barrier to the adoption of 5G-enabled healthcare services. Inability to protect the privacy and security of patient data has both social and economic consequences (Burns & Johnson, 2015; Alibasa et al., 2017). For example, a breach in the integrity of patient data can result in misdiagnosis, mistreatment and possibly death. Violation of the confidentiality of health data has social consequences such as inability to access health or life insurance.

The security threat surface in 5G is expansive and challenging (5G Americas, 2018). The Internet of things (IoT) threat surface can be attributed to the large number of devices that may be difficult to account for and will reside in exposed and vulnerable environments. IoT devices have the risk of resident data and operating system software and firmware being tampered with. Most health sensing medical devices fall in this category, and thus are open to the same security risks. Transport networks allow connectivity between different network nodes in different network domains. The identification and authentication of the nodes need to be guaranteed. Subscriber or end user privacy is also a challenge in 5G due to threats such as tracking and stealing of personal information. The inclusion of external data networks in the network architecture presents another security threat to 5G systems, since the networks become a potential source for launching security attacks on mobile networks.

In view of the anticipated increase in the adoption of mHealth services and applications, governments are putting in place rules and regulations to ensure the protection of patient data in digital health systems. Examples include the Protection of Patient Information Act in South Africa (Dala & Venter, 2016), the Health Insurance Portability and Accountability Act (HIPAA) in the USA, (Luxton et al., 2012; Cohen and Mello, 2018) and the Data Protection Guide in the UK (Carey, 2018). To address the security challenges and meet regulatory requirements, new security mechanisms need to be developed for mHealth systems.

Security architectures

To address the security challenges in 5G, 3GPP has published a generic security architecture which outlines the security features, mechanisms and procedures for 5G systems (3GPP TS 33.501, 2019). However, details of security mechanisms to achieve the security goals are not specified. Thus, implementation to address security threats in specific service networks such as mHealth is still an open research area. In this paper, we propose a security architecture for mHealth systems implemented on 5G networks. The proposed architecture is based on the latest version of the 3GPP 5G security architecture and designed to address the security requirements for digital health systems, i.e. mHealth and eHealth.

Arfaoui et al. (2018) present a security architecture for 5G networks which is defined by 5G-ensure (2017). The architecture builds on the 4G security architecture (3GPP TS 33.401, 2019) and extends it to cover some of the aspects in the 5G security threat landscape. However, the architecture does not capture some of the aspects defined in the latest version of the technical specification TS 33.501 of 2019 (3GPP TS 33.501, 2019). For example, authentication of non-3GPP access networks such as WiFi and Bluetooth and the security edge protection perimeter (SEPP) that protects messages sent over different mobile network domains are not included the 5G-ensure architecture.

A number of security solutions for eHealth have been proposed (Zriqat and Altamimi, 2016). However, they do not provide end-to-end security guarantees for health data. Alibasa et al. (2017) proposed a security architecture that focuses on the data storage network domain. The architecture separately stores identifiable and non-identifiable patient data on servers. Folly (2013) proposed an end-to-end security architecture for mHealth systems with several use cases described. However, the architecture is based on earlier mobile systems and therefore does not address security threats resulting from the introduction of network slicing, MEC and non-3GPP user devices and access networks in 5G networks. An end-to-end mHealth security framework is proposed by Simplicio (2014). However, emerging 5G security challenges are not addressed. Hussain et al. (2018) describe a security architecture for mHealth apps deployed on Android devices. The framework uses security checks and policies to ensure user and device authentication and thus focuses on device security, excluding other domains involved in the delivery of the healthcare service. The IoT Foundation is currently developing security architectures and policies for IoT devices and networks (IoT Foundation, 2018). However, the architectures are specific for IoT devices connected in wired local area networks and do not address wireless and mobile networks. Furthermore, addressing security issues on this segment of the system may potentially create interoperability issues if connected to the 5G system.

The security architecture proposed in this paper addresses the end-to-end security requirement for 5G systems and identifies technologies that can be used in realising the security mechanisms. The 3GPP 5G security architecture identifies security domains that enable secure exchange of information between the 5G system domains. The proposed mHealth security architecture builds on this architecture by identifying security domains in mHealth systems, defining the security requirements and threats specific to mHealth services and applications whose adoption is driven by 5G performance capabilities. We review the 3GPP 5G system and highlight the key system domains and present an mHealth system based on 5G technologies. This approach gives security system designers an understanding of the processes and components of the system to be protected, without which the system cannot achieve its purpose (DCMS, 2018). We discuss the security requirements for, and potential threats to, the 5G mHealth system, and explain how the proposed mHealth security architecture meets the defined security requirements.

Overview of proposed mHealth security architecture

Since the 3GPP does not prescribe the technologies to be used to achieve 5G security goals in different use cases such as mHealth, in this paper we identify emerging security technologies that may be implemented to address the security threats in 5G mHealth systems. Physical unclonable functions (PUF) are a proposed means of authentication and identification of low-power devices, for which limited processing and battery power make them unable to deal with cryptographic algorithms usually used to achieve this purpose (Anagnostopoulos et al, 2018). While this technology has been in use, its application to medical devices, especially Internet of Things for medical devices (IoMD), is still limited. We propose trusted execution environments (TEE) (Mukhopadhyay, 2016) and trusted platform modules (TPM) (Bajikar, 2002) for authenticating and guaranteeing the integrity of software, firmware and data resident on connected mobile and medical devices. As is the case with PUF, application of TEE and TMP in IOMD is still limited. To guarantee the authenticity, integrity and confidentiality of data exchanged between network nodes on the access, core and external networks, we propose to adopt keyless signature infrastructure blockchain (KSIBC). KSIBC is currently under investigation for securing eHealth systems (Mannaro et al., 2018). A new security feature in the 3GPP architecture is the SEPP node, whose function is to mitigate the security vulnerabilities that occur during inter-exchange/roaming between networks of different mobile network operators. To provide the services of the SEPP node, we propose to use X-tee technology (previously known as X-Road) (Cybernetica, 2015), for securing mHealth information as it traverses different healthcare systems. X-tee is a distributed integration layer between information systems, which allows organisations to exchange information securely over the Internet and has successfully been used to secure communication network infrastructures including digital health networks (Cybernetica, 2015). X-tee and KSIBC also address the interoperability between security tools of different stakeholders involved in the end-to-end delivery of healthcare services and is expected to provide a flexible and scalable end-to-end security solution. While X-tee is already being used in eHealth systems, its application is limited to health information systems and to the best of our knowledge, interconnecting the health systems to mobile networks has not been considered. We therefore propose to extend X-tee to secure health data traversing mobile networks, thus providing the required end-to-end security guarantees for health data.

Our main contribution is the proposal of a structured approach to designing and developing an mHealth security architecture based on the 3GPP 5G security architecture design principles and guidelines. To the best of our knowledge, this is the first end-to-end security architecture aimed at addressing security challenges in mHealth systems implemented over 5G networks that covers all the network domains involved in the delivery of a healthcare service.

5G system architectures

Our proposed security architecture is based on the architectural domains of 5G networks. This section gives an overview of the 5G system and presents an mHealth system based on 5G network design architecture.

The generic 5G system

Figure 1 illustrates a 5G system architecture (Zhang et al., 2017). Access networks will consist of both 3GPP and non-3GPP technologies and these are commonly referred to as heterogeneous access technologies (Peng et al., 2014). The access networks connect sdata acquisition devices for IoT and provides network access to device-to-device (D2D) and machine-type-communication (MTC) networks. For mHealth, data acquisition devices would include mobile phones, video cameras, head mounted displays for virtual reality visualisations, medical imaging modalities, wearable sensor devices and other diagnostic devices.

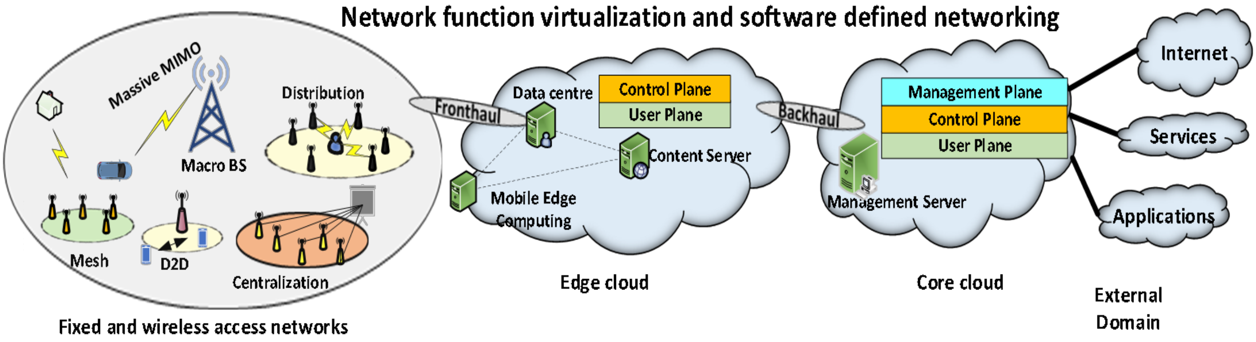

Figure 1. A generic 5G system architecture (adapted from Zhang et al. (2017)). The architecture can be demarcated into four domains. The external domain is owned by third parties with network infrastructures for hosting storage and processing servers. Third parties can also own user devices for accessing network services.

The edge cloud is realised through MEC and consists of some of the network elements from the core in 4G networks (Mao et al., 2017). MEC allows for running applications and related processing tasks closer to the users. This eases network congestion and improves application performance, resulting in superior quality of experience for the user. The core cloud provides important control, management and mobility functions of the mobile network. Management functions also include mechanisms for enforcing security on the network and creation of network slices (Ordonez-Lucena et al., 2017).

The 5G mHealth system

Using existing literature on mHealth systems and the available 5G network architecture, we define five network domains for a 5G mHealth system. This is illustrated in Figure 2. The data acquisition domain consists of mobile phones and medical devices used for acquisition of healthcare information. Medical devices with ZigBee, Bluetooth or WiFi capabilities (Rayanchu, 2011) connect to the mobile networks through a mobile phone used as a hotspot or through WiFi access points, which have gateways into the 5G core. The access and core network domains provide the same services as in the generic 5G system. The storage and processing network domain hosts the servers where health data is stored. Processing servers host algorithms that are used for processing the raw data from patient-owned diagnostic devices, for example vital signs monitoring data and data from image acquisition modalities from remote and rural healthcare facilities (Kumar and Rakesh, 2011). Third party cloud servers are also used for storing raw or processed health data for access by hospitals and third parties such pharmacies, insurers etc. The communication network provides a channel for exchange of health data between patient mobile phones and medical devices, and healthcare systems and other interested stakeholders, such as ministries of health. As such, we have included the data retrieval network domain. End-user devices in this domain include mobile phones, tablets, or personal computers which can access data via wireless or wired networks.

Security requirements of mHealth systems

The primary security requirements for mHealth systems are confidentiality, integrity and availability. Secondary requirements include authentication, accountability and non-repudiation (Fang et al., 2018; Arfaoui et al., 2018). These requirements are briefly described in the following paragraphs.

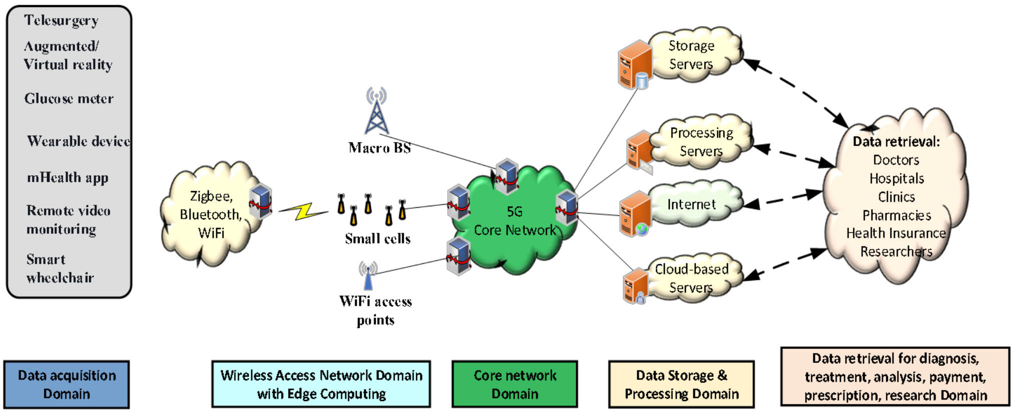

Figure 2. 5G mHealth network showing the different segments of the system. Mobile, wearable and non-wearable devices acquire health information from patients in real-time or non-real-time. Local area technologies and body area networks use gateways to connect the devices to the mobile network base stations. The base stations use high-speed fibre connections or high capacity microwave links to connect to the core network, which transfers the data to storage servers. The links between the core network and external data networks inter-connecting the servers are assumed to be high-speed fibre links. Authorised entities retrieve the data.

Confidentiality

There are two aspects of confidentiality i.e. data confidentiality and data privacy (Arfaoui et al., 2018). Data confidentiality protects transmitted data by limiting access and disclosure to intended users only. Privacy prevents the controlling and influencing of information related to legitimate users. Attacks on confidentiality include eavesdropping, data alteration and traffic analysis. In such attacks, unauthorised eavesdroppers can read some or all the data on a communication link without the legitimate parties noticing it. Traffic patterns obtained during traffic analysis can lead to disclosure of sensitive information such as patient location, health condition, diagnosis and treatment. Encryption has been used to ensure data confidentiality (Arfaoui et al., 2018). However, the traditional methods used assume that attackers have limited computing power, which is no-longer the case. New methods ensuring data confidentiality are therefore required.

Integrity

Integrity protects data from unauthorised duplication or modification and is violated when attackers inject new information or modify the data (Arfaoui et al., 2018). Modification of patient health information can lead to life-threatening situations due to misdiagnosis or inappropriate treatment. The 5G deployment strategy increases the surface for security attacks, making medical devices more vulnerable to integrity attacks. When attackers have valid device identities, it is difficult to detect the attacks. The problem of validating entity identity can be addressed using authentication, which is described below.

Authentication

There are two types of authentication, i.e. message authentication and entity authentication. Entity authentication ensures that an entity is what it claims to be, and message authentication ensures that the information being used for treatment or diagnosis contained in the message is as it was created, transmitted, stored or retrieved. Mobile phone authentication in 4G networks has been addressed (Ferrag et al., 2018). However, in 5G, medical and IoT devices form D2D and MTC networks and are not authenticated on mobile networks (Al Hadidi et al., 2017). Mechanisms are therefore required for authenticating messages, devices and users in these networks before they communicate with 5G mHealth systems.

Accountability and non-repudiation

Accountability and non-repudiation ensure that authorised individuals cannot deny changes that they effect on data. For mHealth, this may include patients not denying changes to data acquired and stored on their devices. However, unauthorised individuals can gain access to devices by impersonating authorised persons.

Availability

Availability defines the degree to which data is accessible to legitimate users whenever, wherever and however requested, and how robust a system is when facing various security attacks (Arfaoui et al., 2018). Availability attacks include denial of service (DoS) and jamming. For mHealth systems, availability of services or network resources is critical since failure to send or retrieve data when needed can lead to delayed diagnosis and treatment, or even death.

Security threats to mHealth systems

The discussion on security threats addresses system domains illustrated in Figure 2.

Security attacks on the data gathering segment

Human users as potential target for security breach: Human end-users have access to mobile phones, medical devices and health-related information. User authentication and data integrity can be violated when users share their device passwords and wittingly or unwittingly release data to unauthorised users via email or other forms of communication. Burns & Johnson (2015) found that 41 percent of people in the health sector have no passwords on their mobile device. Furthermore, 53 percent of the users admitted using their devices on unknown networks.

Mobile applications: Mobile applications are vulnerable to self-installation by malware which can obtain, damage or send stored patient health information to untrusted entities. Poorly implemented applications are therefore potential points for security attacks for mHealth systems. Target locations for the attacks can be data stored on unsecured locations such as server logs, mobile app logs or device browser history (Goncalves et al., 2013). Application owners may also violate patient health information confidentiality by obtaining and keeping records of who has downloaded their apps.

Mobile and medical devices: Mobile devices with no password protection become vulnerable to unauthorised usage if left unattended or are stolen. Furthermore, if unencrypted data is stored on devices, confidentiality can be violated. The data can also be deleted, impacting on data availability. Damage to devices can lead to data loss and compromise the availability requirement. mHealth devices that use Bluetooth are vulnerable to an attack called external device mis-bonding (Naveed et al., 2014) which allows external devices to steal data or insert fake data into the original application, thus compromising data confidentiality and integrity. Implantable medical devices are vulnerable to information harvesting, patient-tracking, impersonation and denial of service (Rathore et al., 2017).

Elkhodr et al. (2011) proposed six features to ensure the authentication of the device, user and environment: secure username, subscriber identification module (SIM) serial number, international mobile identity number, and device longitude and latitude. Naveed et al. (2014) recommended applying encryption to patient health information stored on mobile devices. While this may work for smart phones, medical devices operating in the IoT realm may have limited battery power, storage space and processing capability to apply encryption algorithms. Tan et al. (2012) recommended restricting the capabilities of smartphones used for mHealth applications by advising users to remove unnecessary applications and avoiding installing new applications. They also recommend authenticating both users and devices. PUF can be used to authenticate small medical devices since there is no need to run encryption algorithms; it is already being proposed for IoT (Deutschmann et al., 2018).

Security attacks on the mobile wireless network segment

Eavesdropping and traffic analysis are passive attacks used by attackers to intercept information and are hard to detect since they do not affect normal operations (Wu et al., 2018). Traffic analysis is used to reveal the location and identity of a user even when the data is encrypted. Eavesdropping allows the attacker to monitor a communication link and obtain access to the data. Data encryption is normally used to mitigate the attack. However, with the current increase in computing, hackers can now more easily decipher some cryptographic codes. Physical layer security (PLS) is a robust and flexible approach currently being investigated to mitigate active and passive eavesdropping in 5G wireless systems (Wu et al., 2018). However, the massive deployment of D2D, IoT and MTC technologies presents technical challenges when using PLS techniques (Wu et al., 2018). Virtual private networks (VPN) and the onion router (TOR) technologies have been proposed to minimise eavesdropping and traffic analysis attacks (Borgaonkar, R., 2008). However, VPNs lack scalability, while TOR does not protect the privacy of user location.

Jamming is a denial of service attack (see below) where the attacker transmits high power signals to disrupt communications with the aim of depleting the wireless resources on the communication channel and rendering them inaccessible (Swamy et al., 2013). Direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) have traditionally been used to mitigate the attacks. However, these techniques are not suitable for use in 5G due to massive device deployments. New techniques are currently under investigation, making this an open research area (Adem et al., 2015; Labib et al., 2015).

Denial of service (DoS) and distributed denial of service (DDoS) attacks involve flooding a device or network domain with service requests using a single device or multiple illegitimate devices, respectively. This results in legitimate users being unable to access services, or the devices or network being unable to respond to service requests. Currently DoS or DDoS is prevented via detection. However, in 5G it is difficult to detect points of attack due to the large attack surface (Ahmad, 2018). For mHealth systems, DoS and DDoS can result in patients and healthcare practitioners being unable to access healthcare services. While solutions are being proposed to address DoS for communication networks (Li et al., 2011), the solutions are fragmented and focus on specific network segments. For mHealth networks, a holistic approach to DoS attacks on all segments of the system is therefore required.

Security attacks on the storage and processing segment include unauthorised access, eavesdropping, DoS, and data manipulation (Wang & Wang, 2010), which violate data confidentiality, integrity and authentication. Forms of attack used to violate the confidentiality and integrity of encrypted data include chosen-cyphertext, chosen-plaintext, known-plaintext and rubber hose. For the first three attacks, the attacker uses cryptoanalysis tools to obtain cryptographic keys on the data. For the rubber hose attack, an individual is forced to divulge the secret keys (Wang & Wang, 2010). Cloud-based storage services are vulnerable to an attack called HX-DoS (Chonka & Abawayjy, 2012). The attack involves two or more machines flooding the storage device with service requests to the point that the system totally collapses and becomes inaccessible to legitimate users, thus violating data availability. For mHealth systems, data gathered by wearable devices or obtained through mobile applications is sent to cloud or hospital or third-party servers for storage or processing. As explained above, inability to access the information can lead to life-threatening situations.

Security attacks from data retrieval devices

Security attacks on this segment affect devices used by patients, physicians and healthcare workers to access data for diagnosis, treatment or patient monitoring purposes. In traditional healthcare systems, the storage devices are located in hospitals or other medical facilities. In mHealth systems, storage devices can also be in the cloud or at other institutions, and this opens security vulnerabilities similar to those on the data gathering and access network segments, i.e. DoS attacks and non-repudiation. Furthermore, data alteration becomes a security problem since third parties have access to patient health information. This creates the need for establishing trust zones (Han et al, 2017) in 5G mHealth systems.

Proposed 5G mHealth security architecture

In this section, we present the proposed mHealth 5G security architecture and discuss its key security goals. We then describe how the proposed mHealth security architecture aligns with the principles and guidelines for the design of security architectures for 5G systems. Using the 5G mHealth system domains, we analyse how the proposed architecture meets the security requirements of mHealth systems.

Proposed security architecture

The proposed mHealth security architecture is illustrated in Figure 3. We assume that the mHealth system is a network slice created over a 5G physical network infrastructure. The network slice is realised using NFV and SDN technologies and spans from the data acquisition domain, depending on the capabilities of the device being used for data acquisition, through to the core network. We assume that the network would be separated physically in third party domains, hence there is no network slicing in this domain. Slicing can also be implemented in the data retrieval domain. Since network slicing is key to implementation of 5G mHealth systems, an implementation of the technology on the mHealth system domains is given in the next section.

To address the requirements for an end-to-end security architecture and the distributed nature of mHealth systems, we propose implementation of TEE, KSIBC and X-tee technologies. Publicly connected medical devices and mHealth applications pose a security risk to the patient health information. We propose to use TEE, whose specification is publicly available from the Global Platform, to isolate patient health information from other device-resident applications (Secure Technology Alliance, 2018). Isolation of device-resident applications has been realised by dedicated hardware in current devices, but it can also be realised with TEE. When applications are isolated from the client-side execution environment, this is referred to as a rich execution environment in common processors. The TEE is emerging to be a robust and widely available solution for protecting the confidentiality and integrity of sensitive data on IoT devices. It is employed in smart cards and embedded secure elements. TEE can also provide remote attestation for mHealth devices and applications, i.e. using a secure protocol to convince a remote verifier of specific properties such as the state of the software on the device.

X-tee is a decentralised system for enabling secure exchange of information between organisations (Cybernetica, 2015). The main design goals of the system are: allowing organisations to exchange information securely with no intermediaries; retention of data ownership by the owner; high assurance of system availability; use of data as digital evidence and implementation of communication as service calls; no requirement for organisations to implement security-related functionality; and handling of authentication and access control at organisation level. However, end user authentication is left to the organisation. X-tee is a suitable technology for the mHealth security architecture as it can provide security services between mobile networks. The logical architecture, which implements a security server at the edge of each network domain, can perform the same function as the SEPP node proposed in the 3GPP security architecture. The system can be used to allow third parties outside the mobile network system to securely exchange patient health information.

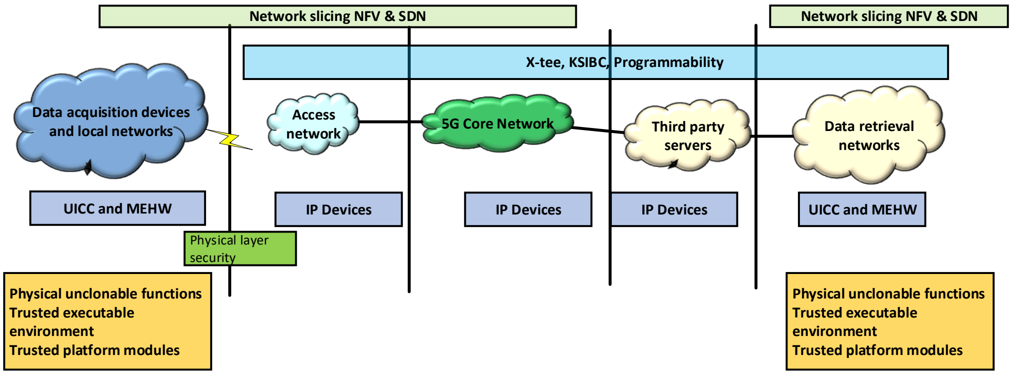
Network slicing NFV & SDN
Network slicing NFV & SDN
X-tee, KSIBC, Programmability
Data acquisition devices and local networks
Access network
5G Core Network
Third party servers
Data retrieval networks
UICC and MEHW
IP Devices
IP Devices
IP Devices
UICC and MEHW
Physical layer security
Physical unclonable functions
Trusted executable environment
Trusted platform modules
Physical unclonable functions
Trusted executable environment
Trusted platform modules

Figure 3. The proposed mHealth security architecture. The architecture is segmented into five domains. This reflects the domains defined in the mHealth system above. The domains provide a structured way of identifying security threats and defining the required solutions.

KSIBC combines two security technologies; Blockchain (BC) and keyless signature infrastructure (KSI). KSI is a globally distributed system for providing time-stamping and server-supported digital signature services and is an alternative to the traditional public key infrastructure (PKI) (Mylrea et al., 2018). The technology uses keys for authentication. However, the validity of signatures can be verified reliably without assuming the continued secrecy of the keys. Keyless signatures solve the problem of time-stamping in PKI by separating the functions of signer identification and evidence of integrity. Signatures are therefore implemented as multiple signatures (Buldas, 2013). BC is a distributed public record of public events which appends records of events where each event is cryptographically linked to the previous (Mylrea et al., 2018). New entries are created using a distributed consensus. KSIBC overcomes two challenges of BC. Firstly, BC transactions grow linearly with the number of transactions, on the other hand, KSIBC grows linearly with time, and is therefore independent of the number of transactions. This is important in our proposed architecture where a massive number of devices need to be authenticated and the integrity of the exchanged data guaranteed. Secondly, in crypto-currencies where BC is widely used, the number of participants is unlimited, whereas KSIBC limits the number of participants. This eliminates the need for Proof of Work algorithms implemented in BC and ensures settlement can occur within one second. This is critical in delay-sensitive applications and services in mHealth. Furthermore, for battery-powered devices with limited processing power, running of algorithms in security implementations must be minimised.

To address the need for flexibility and scalability, we incorporate programmability of security mechanisms, which can be achieved using machine learning techniques.

For mHealth systems, many devices will not connect directly to the mobile network. This means their security cannot be guaranteed by mobile network operators. Technologies such as PUF, TEE and TPM have been proposed to provide device authentication and ensure the integrity and confidentiality of data generated, stored on devices or sent from the devices. The technologies eliminate the need to implement cryptographic algorithms, commonly used in network devices, on battery-operated IoT, D2D and MTC mHealth devices which also have limited processing power due to their small sizes.

As explained above, mMIMO, mmW, MTC and IoT present new security challenges which require more efficient and secure transmission schemes that exploit the propagation characteristics of the wireless channel in the physical layer. We propose the use of PLS technology in conjunction with blockchain technology as part of the mHealth slice security mechanisms on the access network segment. Wu et al. (2018) give a detailed review of the technology and its possible integration with BC technology to address the new security challenges of the 5G wireless system.

mHealth network slice

Following 5G vertical industries implementations, we assume that the mHealth system is a network slice implemented on the physical domains of a 5G system and realised using NFV and SDN technologies. Figure 4 illustrates how an mHealth network slice can be implemented over the 5G system domains. Slicing in the user equipment domain allows more than one application to run on the same user device. Different radio access technologies (RATs) will allow creation of different network slices on the access network domain. This caters for the different performance requirements of services and applications; for example, virtual reality services may require low latency and high bandwidth for transmission of high-quality images, whereas vital signs data from a wearable device would require reliable but low bandwidth links. In this case, the virtual reality service slice can be implemented over a mmW RAT, whereas the vital signs monitoring service can be allocated resources in legacy RATs which offer low bandwidth and reliable connection. In the core network domain, different industries are separated into different slices, for example health, energy, smart cars and smart city. The network slices can also be separated into sub-slices, allowing a slice to serve more than one service with different performance requirements. For example, the vital signs monitoring, and augmented reality services belong to the health slice but different sub-slices. There is no network slicing in the third party and service provider domains as these are individually owned networks, for example hospitals, pharmacies and health insurance providers. Resources for services can therefore be provided as and when required. This leveraging of the dynamic configurability capability of slicing allows efficient, cost-effective and flexible use of network resources.

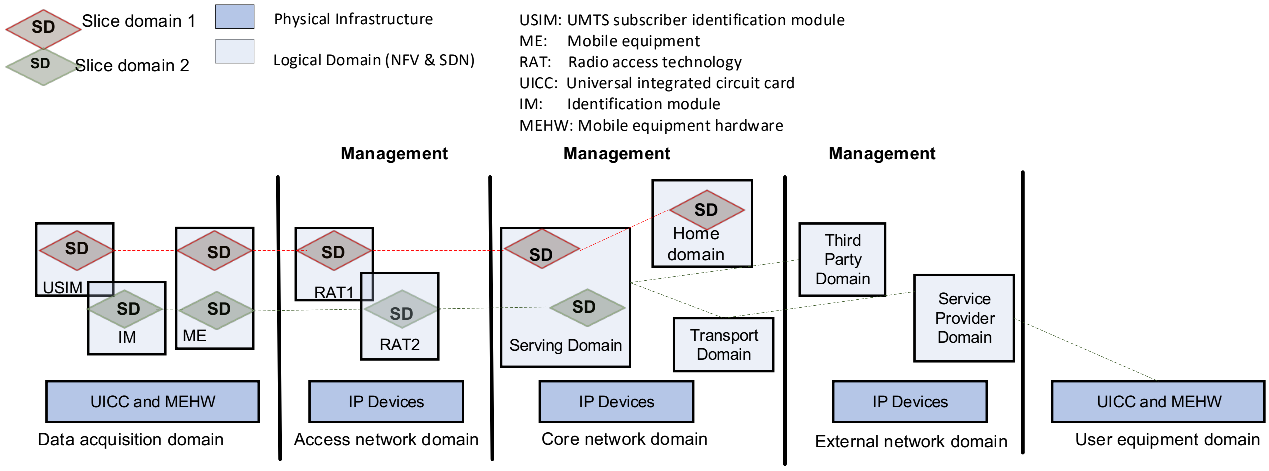

Figure 4. mHealth network slice domains super-imposed on the 5G domain architecture (adapted from Arfaoui et al. (2018)). Network slicing is implemented in the data gathering, access network and core network domains. We assume that in third party and service provider networks, the services are already defined hence traffic is directed to the appropriate services upon leaving the network operator domain. The management function in the network domains is necessary for slice creation and service implementation, monitoring and termination.

Aligning the 5G mHealth and 3GPP 5G security architectures

The 3GPP 5G security architecture includes four new modules in the core network. These include (3GPP TS 33.501, 2019): the authentication and server function, which stores data for authentication of UEs; the authentication credential repository and processing function, which selects an authentication method based on the identity of a subscriber and their configured policy, and computes the authentication data and keying algorithms; the subscriber identifier de-concealing function, which de-conceals a subscriber concealed identifier to obtain the long-term identity, i.e. the subscriber's permanent identifier; and the security anchor function, which is located in a serving network and intermediates authentication between a UE and its home network.

These new security features are designed to address the new security challenges in 5G systems. The new security features include increased home control for authentication of massive IoT devices, unified authentication of both 3GPP and non-3GPP access networks, the security edge protection proxy SEPP node which implements application layer security for all application information exchanged between different mobile networks, and mitigation of bidding attacks (making the UE and base station believe that one does not support the security feature of the other), and guaranteed subscriber privacy. The architecture highlights the different domains that must be secured and the interfaces between these domains. Table 3 maps the 5G security domains and the corresponding domains used in our proposed security architecture. This mapping allows development of security mechanisms that are also aligned to 5G security networks, to realise the architecture.

Table 3. Mapping the security domains for the 3GPP and those of the proposed 5G mHealth security.

3GPP 5G mHealth domains	5G mHealth domains
Mobile equipment (ME), USIM, user application	Data acquisition domain
3GPP access network (AN) and 3GPP AN	Access network domain
Serving network (SN) and Home environment	5G core network
Provider application	Data storage, processing and retrieval

Aligning the 5G mHealth security architecture to standardised design principles and guidelines

Arfaoui et al. (2018) summarise the standard design principles and guidelines for developing security architectures for networks. For an mHealth system, a distributed end-to-end security architecture is required to address the distributed nature of healthcare services. A hierarchical approach to the development of mHealth security architecture is adopted to allow the development of the security solution in layers (Zhu et al., 2011). A similar approach is used in a smart grid security architecture, where a six-layered architecture has been proposed (Zhu & Basar, 2012). In our proposed architecture we divide the mHealth system into five domains as illustrated in Figure 3. The recursive design approach to a security system involves designing subsystems of the system and validating and improving each subsystem until the whole system is secured (Kondakci, 2008; Zhu et al., 2011). Our proposed security architecture achieves this by breaking the network domains into several subsystems where security solutions can be implemented and tested repeatedly until the security objective is achieved. For example, in the data gathering domain, security threats on mobile phones will be different from those on medical devices. In the storage and processing domain, the different servers may have different security threats which can be addressed differently.

5G system design concepts incorporate flexibility and scalability due to the heterogeneous nature of the system and the diversity of services requiring different performance guarantees. This objective is achieved through softwarisation, virtualisation and network slicing. These concepts are incorporated into the design of the mHealth security architecture by introducing mHealth network slices. We propose to include self-organising capabilities, virtualisation of security modules and dynamic security orchestration, to achieve flexibility and scalability of the proposed security architecture. This can be done through open programming interfaces in the management domain. In addition to flexible network implementation, network slicing will help isolate mHealth systems from other network services, hence reduce the security threats from other 5G vertical industries. A scalable security architecture allows for extending the security mechanism to new devices as they connect onto the mHealth system and new services and applications are activated. This will allow the security system to protect medical devices as and when they are deployed on the network. Regulatory compliance is key as new regulations to protect personal health information emerge, violation of which has legal and social consequences. However, a detailed discussion on regulation is beyond the scope of this paper.

Addressing the security requirements for mHealth systems

This section describes how the proposed security architecture addresses the security requirements of the mHealth system.

Securing the data acquisition domain

The security requirements for this domain are user and device authentication and ensuring the integrity and confidentiality of the collected information. The mHealth system should allow only authorised users, applications and devices to send information over the network. Mobile applications can be protected by implementing application specific protocols, and this is the responsibility of application developers. PUF technology is currently being used to provide low-cost authentication of IoT devices (Mukhopadhyay, 2016). The technology can be used for providing digital fingerprints of medical devices such as body sensors, which have limited processing power and storage space. TEE technology is used to secure devices in mobile environments such as Android OS and can be used in medical devices with adequate resources to implement the technology. These could include image rendering modalities such as X-ray machines. PUF and TEE technologies therefore allow all devices to provide credentials when they connect on the network, directly or indirectly. To guarantee the confidentiality and integrity of the credentials stored on the devices, the universal integrated circuit card and TEE technologies have been widely used in mobile phones. These can also be used on medical devices with mobile connectivity capabilities (Sheperd, 2019). Biometric user authentication using fingerprint, voice, or iris is currently being used in many security systems for authentication and identification of individuals (Grindrod et al., 2018), and biometric authentication such as voice recognition can be used for user authentication on the mHealth data gathering domain.

Securing the access network domain

For the access network segment, the security requirements are authentication and identification of network devices including base stations. Security mechanisms for 4G and earlier technologies have worked well. However, the introduction of small cell base stations, wireless body area networks, other local health networks and WiFi access points which connect directly onto mobile network platforms, creates security vulnerabilities since these are located in customer premises and hence out of the control of mobile network operators. In other cases, mobile devices will be used as gateways for medical devices and this creates the need to provide more security mechanisms for these devices. Power restrictions on small cell base stations, smart phones, and WiFi access points may limit the heavy authentication algorithms implemented in base stations. While PUF is being proposed for IoT devices, the root of trust capability can be used to support TEE implementation (Mukhopadhyay, 2016). Furthermore, the benefits of TEE can be used to implement TPM. KSIBC can be used for authentication of network devices and ensuring trust among different service providers on the shared infrastructure technology. While the use of BC on the radio access network has recently been processed (Ling et al., 2019), the authors use the concept of Proof of Work, which can introduce latency on the network, affecting application performance. We propose to use KSIBC to mitigate this limitation (Mylrea et al., 2018). PUF technology can also be used for providing fingerprints of some of the small mobile network devices such as small cell base stations with limited power and processing capabilities.

Core and external network domains

The main security threat on the core and external networks is availability. The mHealth traffic is isolated from other traffic by network slicing. By dedicating resources to specific slices, the attacks on some slices may not impair traffic on others. Infrastructure providers may also use SDN techniques to quarantine disturbing traffic before it compromises traffic on the mHealth network slice. Furthermore, as in the case on the access network domain, we propose using KSIBC (Mylrea et al., 2018) for authenticating network devices as well as protecting the integrity and confidentiality of information. We propose adoption of X-tee for our proposed security architecture. For mHealth systems, trust and assurance in the external network domains become security concerns (Forgerock, 2015). Trust in the hardware and virtual machines can be based on TPM (Bajikar, 2002). Secure booting can also be used to ensure that only operator accepted software is running on the network devices on this domain to ensure that no devices can be taken control of by attackers and used to launch DoS attacks (Arfaoui et al., 2018).

Conclusion

5G systems promise to revolutionise the delivery of healthcare through mHealth systems, however, full realisation of the benefits of mHealth will be hampered by the inability to ensure the security and privacy of patient health information. Using 3GPP security architecture design principles, we propose a security architecture for mHealth systems implemented over a 5G mHealth network. We define system domains that are used to identify security threats on the network, i.e. the data acquisition, access network, core network and external network domains. We further identify the security threats in each of the domains and propose security mechanisms for mitigating the security threats.

Acknowledgements

This research is supported by the National Research Foundation of South Africa.

References

3GPP TS 22.261. 2019. *Service requirements for the 5G system*. Available: https://www.3gpp.org/ftp/Specs/archive/22_series/22.261

3GPP TS 23.501. 2019. *System architecture for the 5G system*. Available: https://www.3gpp.org/ftp/Specs/archive/23_series/23.501.

3GPP TS 33.401. 2019. *Security architecture (Release 15)*. Available: https://www.3gpp.org/ftp/Specs/archive/33_series/33.401/.

3GPP TS 33.501. 2019. *Security architecture and procedures for 5G system*. Available: https://www.3gpp.org/ftp/Specs/archive/33_series/33.501

5G Americas. 2018. *The evolution of security in 5G*. Available: http://www.5gamericas.org/files/8815/4092/3086/5G_Americas_5G_Security_White_Paper_Final.pdf

5G-ensure, 2017, Deliverable D2.7: Security architecture (final). Available: http://www.5gensure.eu/sites/default/files/5G-ENSURE_D2.7_SecurityArchitectureFinal.pdf

5G IA. 2015. *5G and e-Health*. 5G Infrastructure Association. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-eHealth-Vertical-Sector.pdf

Adem, N., Hamdaoui, B. & Yavuz, A. 2015. Pseudorandom time-hopping anti-jamming technique for mobile cognitive users. In 2015 *IEEE Globecom Workshops* (pp. 1-6). IEEE. DOI: 10.1109/GLOCOMW.2015.7414043

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M. & Gurtov, A. 2018. Overview of 5G security challenges and solutions. *IEEE Communications Standards Magazine*, 2(1), pp.36-43. DOI: 10.1109/MCOMSTD.2018.1700063

Al Hadidi, M., Al-Azzeh, J.S., Tkalich, O.P., Odarchenko, R.S., Gnatyuk, S.O. & Khokhlachova, Y.Y. 2017. ZigBee, Bluetooth and Wi-Fi Complex Wireless Networks Performance Increasing. *International Journal on Communications Antenna and Propagation* 1(48):1-48. DOI: 10.15866/IRECAP.V7I1.10911

Alibasa, M.J., Santos, M.R., Glozier, N., Harvey, S.B. and Calvo, R.A. 2017. Designing a secure architecture for m-health applications. In *2017 IEEE Life Sciences Conference* (pp. 91-94). IEEE. DOI: 10.1109/LSC.2017.8268151

Anagnostopoulos, N.A., Arul, T., Fan, Y., Hatzfeld, C., Lotichius, J., Sharma, R., Fernandes, F., Tehranipoor, F. & Katzenbeisser, S. 2018. Securing IoT Devices Using Robust DRAM PUFs. In *2018 Global Information Infrastructure and Networking Symposium* (pp. 1-5). IEEE. DOI: 10.1109/GIIS.2018.8635789

Arfaoui, G., Bisson, P., Blom, R., Borgaonkar, R., Englund, H., Félix, E., Klaedtke, F., Nakarmi, P.K., Näslund, M., O'Hanlon, P. & Papay, J. 2018. A security architecture for 5G networks. *IEEE Access* 6:22466-22479. DOI: 10.1109/ACCESS.2018.2827419

Bajikar, S. 2002. *Trusted platform module (tpm) based security on notebook pcs*. Available: http://ogobin.de/TCPA/Trusted_Platform_Module_White_Paper.pdf

Borgaonkar, R. 2008. TOR and Onion Routing: Protecting your privacy. Available: http://www.cse.hut.fi/en/publications/B/4/netsec08-proceedings.pdf#page=33

Burns, A.J. & Johnson, M.E., 2015. Securing health information. *IT professional* 17(1):23-29. DOI: 10.1109/MITP.2015.13

Carey, P. 2018. *Data protection: a practical guide to UK and EU law*. Oxford University Press, Inc.

Chonka, A. & Abawajy, J., 2012. Detecting and mitigating HX-DoS attacks against cloud web services. In *2012 15th International Conference on Network-Based Information Systems* (pp. 429-434). IEEE. DOI: 10.1109/NBiS.2012.146

Cybernetica. 2015. *X-Road Architecture Technical Specification*. Document ID ARC-G. Cybernetica

Dala, P. & Venter, H.S. 2016. Understanding the level of compliance by South African institutions to the Protection of Personal Information (POPI) Act. In *Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists* (p. 13). ACM. DOI:10.1145/2987491.2987506

DCMS. 2018. *5G Network Architecture and Security*. Available: https://uk5g.org/media/uploads/resource_files/5G_Architecture_and_Security_technical_report_-_04Dec18.pdf

Deutschmann, M., Iriskic, L., Lattacher, S.L., Münzer, M., Stornig, F. & Tomashchuk, O. 2018. *Research on the Applications of Physically Unclonable Functions within the Internet of Things*. Technikon. Available: https://technikon.com/download/White-Paper-on-PUF-Applications-in-IoT.pdf.

Elayoubi, S.E., Bedo, J.S., Filippou, M., Gavras, A., Giustiniano, D., Iovanna, P., Manzalini, A., Queseth, O., Rokkas, T., Surridge, M. & Tjelta, T. 2017. 5G innovations for new business opportunities. In *Mobile World Congress*. 5G Infrastructure Association.

Elkhodr, M., Shahrestani, S. & Cheung, H. 2011. Enhancing the security of mobile health monitoring systems through trust negotiations. In 2011 *IEEE 36th Conference on Local Computer Networks* (pp. 754-757). IEEE. DOI: 10.1109/LCN.2011.6115545

Fang, D., Qian, Y. & Hu, R.Q. 2018. Security for 5G mobile wireless networks. *IEEE Access* 6:4850-4874. DOI: 10.1109/ACCESS.2017.2779146

Ferrag, M.A., Maglaras, L., Argyriou, A., Kosmanos, D. & Janicke, H. 2018. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications* 101:55-82. https://DOI.ORG/10.1016/J.JNCA.2017.10.017

Folly F. 2013. Mobile health: Architecture, Applications and Security. *Africa Internet Summit*. Available: https://meeting.afrinic.net/afrinic-18/sites/default/files/Farell.pdf.

Forgerock, 2015, *The 5G Trust Equation*. Forgerock. Available: https://www.forgerock.com/app/uploads/2017/10/FR-WhitePaper_5G-Trust-Equation.pdf.

Gonçalves, F., Macedo, J., Nicolau, M.J. & Santos, A. 2013. Security architecture for mobile e-health applications in medication control. In *21st International Conference on Software, Telecommunications and Computer Network*s (pp. 1-8). IEEE. DOI: 10.1109/SOFTCOM.2013.6671901

Grindrod, K., Khan, H., Hengartner, U., Ong, S., Logan, A.G., Vogel, D., Gebotys, R. & Yang, J. 2018. Evaluating authentication options for mobile health applications in younger and older adults. *PloS One* 13(1):e0189048. https://DOI.ORG/10.1371/JOURNAL.PONE.0189048.

Han, B., Wong, S., Mannweiler, C., Dohler, M. & Schotten, H.D. 2017. Security trust zone in 5G networks. In 2017 24th International Conference on Telecommunications (pp. 1-5). IEEE. DOI: 10.1109/ICT.2017.7998270

Hussain, M., Al-Haiqi, A., Zaidan, A.A., Zaidan, B.B., Kiah, M., Iqbal, S., Iqbal, S. & Abdulnabi, M., 2018. A security framework for mHealth apps on Android platform. *Computers & Security* 75:191-217. https://DOI.ORG/10.1016/J.COSE.2018.02.003

IoT Foundation. 2018. IoT security architecture and policy for the enterprise – a hub and policy the enterprise – a hub-based approach release 1. IoT Foundation. Available: https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Security-Architecture-and-Policy-for-the-Enterprise-a-Hub-Based-Approach.pdf.

Kondakci, S. 2008. A recursive method for validating and improving network security solutions. In *Proceedings of the International Conference on Security of Information and Networks* (pp. 74-83).

Kumar, T.S. and Rakesh, P.B. 2011. 3D reconstruction of facial structures from 2D images for cosmetic surgery. In *2011 International Conference on Recent Trends in Information Technology* (pp. 743-748). IEEE. DOI: 10.1109/ICRTIT.2011.5972446

Labib, M., Ha, S., Saad, W. & Reed, J.H., 2015, December. A colonel blotto game for anti-jamming in the internet of things. In *IEEE Global Communications Conference* (pp. 1-6). IEEE. DOI: 10.1109/GLOCOM.2015.7417437

Li, Y., Kaur, B. & Andersen, B., 2011. Denial of service prevention for 5G. *Wireless Personal Communications* 57(3):365-376.

Ling, X., Wang, J., Bouchoucha, T., Levy, B.C. & Ding, Z. 2019. Blockchain Radio Access Network (B-RAN): Towards Decentralized Secure Radio Access Paradigm. *IEEE Access* 7:9714-9723. DOI: 10.1109/ACCESS.2018.2890557

Mannaro, K., Baralla, G., Pinna, A. & Ibba, S. 2018. A blockchain approach applied to a teledermatology platform in the Sardinian region (Italy). *Information* 9(2):44. https://DOI.ORG/10.3390/INFO9020044.

Mao, Y., You, C., Zhang, J., Huang, K. & Letaief, K.B. 2017. A survey on mobile edge computing: the communication perspective. *IEEE Communications Surveys & Tutorials* 19(4):2322-2358. DOI: 10.1109/COMST.2017.2745201

Mukhopadhyay, D. 2016. PUFs as promising tools for security in Internet of things. *IEEE Design & Test* 33(3):103-115. DOI: 10.1109/MDAT.2016.2544845

Mylrea, M., Gourisetti, S.N.G., Bishop, R. & Johnson, M. 2018. Keyless Signature Blockchain Infrastructure: Facilitating NERC CIP Compliance and Responding to Evolving Cyber Threats and Vulnerabilities to Energy Infrastructure. In *IEEE/PES Transmission and Distribution Conference and Exposition* (pp. 1-9) IEEE. DOI: 10.1109/TDC.2018.8440380

Naveed, M., Zhou, X.Y., Demetriou, S., Wang, X. and Gunter, C.A., 2014. Inside Job: Understanding and mitigating the threat of external device mis-bonding on Android. Available: https://www.ndss-symposium.org/wp-content/uploads/2017/09/03_5_0.pdf

Ordonez-Lucena, J., Ameigeiras, P., Lopez, D., Ramos-Munoz, J.J., Lorca, J. & Folgueira, J. 2017. Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges. *IEEE Communications Magazine* 55(5):80-87. DOI: 10.1109/MCOM.2017.1600935

Peng, M., Li, Y., Zhao, Z. & Wang, C. 2014. System architecture and key technologies for 5G heterogeneous cloud radio access networks. *arXiv preprint*: 1412.6677. DOI: 10.1109/MNET.2015.7064897

Rathore, H., Mohamed, A., Al-Ali, A., Du, X. and Guizani, M., 2017, June. A review of security challenges, attacks and resolutions for wireless medical devices. In *13th International Wireless Communications and Mobile Computing Conference* (pp. 1495-1501). IEEE. DOI: 10.1109/IWCMC.2017.7986505

Rayanchu, S., Patro, A. & Banerjee, S. 2011. Airshark: detecting non-WiFi RF devices using commodity WiFi hardware. In *ACM SIGCOMM Conference on Internet Measurement* (pp. 137-154). ACM. https://DOI.ORG/10.1145/2068816.2068830

Rost, P., Banchs, A., Berberana, I., Breitbach, M., Doll, M., Droste, H., Mannweiler, C., Puente, M.A., Samdanis, K. & Sayadi, B. 2016. Mobile network architecture evolution toward 5G. *IEEE Communications Magazine* 54(5):84-91. DOI: 10.1109/MCOM.2016.7470940

Secure Technology Alliance. 2018. Trusted Execution Environment (TEE) 101: A primer. Available: https://www.securetechalliance.org/wp-content/uploads/TEE-101-White-Paper-FINAL2-April-2018.pdf

Shepherd, C., Arfaoui, G., Gurulian, I., Lee, R.P., Markantonakis, K., Akram, R.N., Sauveron, D. & Conchon, E. 2016. Secure and trusted execution: Past, present, and future-a critical review in the context of the internet of things and cyber-physical systems. In *IEEE Trustcom/BigDataSE/ISPA* (pp. 168-177). IEEE. DOI: 10.1109/TrustCom.2016.0060

Simplicio, M.A., Iwaya, L.H., Barros, B.M., Carvalho, T.C. & Näslund, M. 2015. SecourHealth: a delay-tolerant security framework for mobile health data collection. *IEEE Journal of Biomedical and Health Informatics* 19(2):761-772. https://DOI.ORG/10.1109/JBHI.2014.2320444

Swamy, M.K., Deepthi, M., Mounika, V. & Saranya, R.N. 2013. Performance analysis of DSSS and FHSS techniques over AWGN channel. *Development (IJECIERD)*, 3(2): 7-14.

Tan, C.C., Bai, L., Mastrogiannis, D.S. & Wu, J. 2012. Security analysis of emerging remote obstetrics monitoring systems. In *IEEE 14th International Conference on e-Health Networking, Applications and Services* (pp. 329-334). IEEE. DOI: 10.1109/HEALTHCOM.2012.6379431

Wang, Y. & Wang, H., 2010. On key authentic degree of cryptosystem. In *2nd IEEE International Conference on Information Management and Engineering* (pp. 301-304). IEEE. DOI: 10.1109/ICIME.2010.5477578

Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K.K. & Gao, X. 2018. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE Journal on Selected Areas in Communications* 36(4): 679-695. https://DOI.ORG/10.1109/JSAC.2018.2825560

Zhang, H., Liu, N., Chu, X., Long, K., Aghvami, A.H. & Leung, V.C. 2017. Network slicing based 5G and future mobile networks: mobility, resource management, and challenges. *IEEE Communications Magazine* 55(8):138-145. https://DOI.ORG/10.1109/MCOM.2017.1600940

Zhu, Q. & Basar, T., 2012. A hierarchical security architecture for smart grid: From theory to practice. In *Proceedings of the Smart Grid Communications and Networking*, E. Hossain, Z. Han, and H. V. Poor, Eds., Cambridge University Press, Cambridge, U.K.

Zhu, Q., Rieger, C. & Başar, T. 2011, August. A hierarchical security architecture for cyber-physical systems. *In 4th International Symposium on Resilient Control Systems* (pp. 15-20). IEEE. https://DOI.ORG/10.1109/ISRCS.2011.6016081

Zriqat, A. & Altamimi, M. A. 2016. Security and privacy issues in eHealthcare systems: towards trusted services. *International Journal of Advanced Computer Science and Applications* 7(9). http://dx.doi.org/10.14569/IJACSA.2016.070933