

Chapter 14

Security and Privacy in Next Generation Networks and Services

Panayiotis Kotzanikolaou
University of Piraeus, Greece

ABSTRACT

The deployment of Next Generation networks such as wireless broadband networks and wireless ad hoc networks, has lead to the proliferation of new mobile, pervasive and ubiquitous services, such as online social networks, location based services or cloud computing services. These new network paradigms and services raise serious privacy concerns. This chapter reviews security and privacy issues in Next Generation (NG) networking. Initially, a general categorization of various popular NG networks and services is presented. Then, the security and privacy threats identified for each category are examined, along with a brief review of the related security requirements and mitigation strategies described in the recent literature.

INTRODUCTION

Next Generation (NG) networks and services are already in the move to become mainstream technologies, as the users embrace new pervasive and mobile technologies. The main features that characterize NG networks and services are their ubiquitous and pervasive nature. Modern mobile networks allow users to have low cost, continuous and real-time network access, using mobile devices of adequate computing capabilities. Thus NG networks pave the way for NG services such as Cloud Computing, Online Social Networking,

Location Based Services, P2P communications and Internet-of-Things (IoT) communications. Pervasive computing environments consist of smart devices, able to connect to each other or to remote users/nodes, but also able to do context sensing and/or actuation operations pertaining, among others, to everyday human activity, health-care automation, smart homes, environmental monitoring and smart grids. The penetration of NG networks and services does not thus only involve typical customer-centric or user-centric services. The so-called critical infrastructures which used to be closed services in isolated networks, are already

DOI: 10.4018/978-1-4666-8732-5.ch014

interconnected through the Internet. The massive adoption of these new technologies from the users, the service providers as well as the public sector, has led to a massive exchange and processing of private and sensitive through on-line services.

As NG networks and services provide network connectivity everywhere and any time and online services provide new and fascinating communication channels, data are massively exchanged and stored through these services. In a typical scenario, mobile users use typical mid-range mobile devices (such as smartphones or tablets) that are connected to cellular mobile networks or to local wireless access points, in order to have continuous access to different services, anytime and anywhere (Weiser, 1991). In Figure 1, a description of some of the most popular NG networks and services is presented. Our analysis will be based on this categorization. Although this categorization is not meant to be an exhaustive description of NG technologies, it aims to capture the particularities of the next generation pervasive computing environments.

Due to the pervasive computing characteristics offered by NG technologies, such as user mobility, loose physical boundaries, interactions with devices or services of undefined trust, security will naturally be required as an inherent property by consumers and organizations. Privacy is related to a person's right to control how personal or sensitive data related with him/her are disclosed, managed, transferred or stored by third parties. These

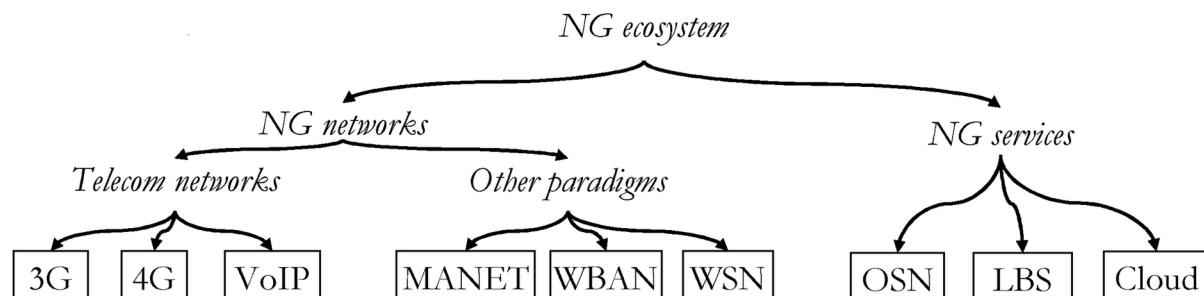
new computing paradigms of NG networks and services increase the exposure of data to privacy and security threats and they also introduce new privacy threats. In this chapter we will describe the privacy threats which are raised by the use of various NG networks and services. We emphasize on the privacy and security requirements that are necessary to provide adequate protection of private data, when using or deploying NG networks and services. We also discuss open problems related with privacy in NG computing environments.

SECURITY AND PRIVACY IN NEXT GENERATION NETWORKS

Telecommunication Networks

Next generation telecommunication networks include various new technologies and protocols, apart from the traditional Public Switched Telecommunication Network (PSTN), such as the 3G Unified Mobile Telecommunication System (UMTS), the 4G Long Term Evolution (LTE) and mobile WiMAX and the forthcoming 5G networks. In addition, internet-based communication protocols such as the Session Initiation Protocol (SIP) and the Voice over the Internet Protocol (VoIP) have been developed. The telecommunication networks also provide a major underlying infrastructure for the proliferation of TCP/IP, and more recently IPv6 packet networks.

Figure 1. Popular Next Generation Networks and Services



17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/security-and-privacy-in-next-generation-networks-and-services/136566

Related Content

Analytical Study of a Dual Pointer Based Strategy for Location Update Using Node B Sojourn Time in UMTS Networks

Samir K. Sadhukhan, Chayanika Bose, Debashis Saha and Asis Chattopadhyay (2018). *International Journal of Business Data Communications and Networking* (pp. 44-70).

www.irma-international.org/article/analytical-study-of-a-dual-pointer-based-strategy-for-location-update-using-node-b-sojourn-time-in-umts-networks/204456

Exploiting Scalar Effect in Wireless Access Networks: A Case Study and Research Directions

Rongrong Qian and Yuan Qi (2014). *Broadband Wireless Access Networks for 4G: Theory, Application, and Experimentation* (pp. 171-182).

www.irma-international.org/chapter/exploiting-scalar-effect-in-wireless-access-networks/99338

Optimal Green Virtual Machine Migration Model

Noah Sabry and Paul Krause (2013). *International Journal of Business Data Communications and Networking* (pp. 35-52).

www.irma-international.org/article/optimal-green-virtual-machine-migration-model/95722

High-Performance Solutions for Adaptive and Customizable Streaming of Interactive Content to Mobile Devices

Gianluca Paravati, Fabrizio Lamberti, Andrea Sanna and Cesare Celozzi (2012). *Multimedia Services and Streaming for Mobile Devices: Challenges and Innovations* (pp. 154-180).

www.irma-international.org/chapter/high-performance-solutions-adaptive-customizable/58703

The Media Gatekeeping Model Updated by R and I in ICTs: The Case of Wireless Communications in Media Coverage of the Olympic Games

Vassiliki Cossiavelou, Philemon Bantimaroudis, Evangelia Kavakli and Laura Illia (2011). *International Journal of Interdisciplinary Telecommunications and Networking* (pp. 49-74).

www.irma-international.org/article/media-gatekeeping-model-updated-icts/60240