An Analysis of Emerging Security Threats in 3G/4G Cellular Network Deployment in Pakistan

Muhammad Ahmad*, Munam Ali Shah, Manzoor Ilahi Tamimy
Department of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan
*Email: mahmad.comsats [AT] gmail.com

***Abstract*—The advancements in wireless communication are increasing tremendously. The transition from legacy cellular networks to 3rd Generation (3G) cellular networks and 4th Generation (4G) cellular networks has globally taken place.The Government of Pakistan has announced the deployment of 3G/4G technology in the country. In this paper, we investigate the emerging security threats to 3G/4G cellular network in Pakistan. Our contribution is twofold. Firstly, we highlight modern security attacks that can hinder the smooth delivery of mobile phone services and secondly, we conduct a survey questionnaire about the emerging security threats to mobile users in Pakistan. The results obtained from the survey reveals some interesting facts which will help the stake holders of 3G/4G networks in Pakistan to take appropriate security measures in time.**

Keywords—3G/4G cellular network; security threats; attacks.

I. INTRODUCTION

Currently, cellular companies are providing second generation (2G) and 2.5G cellular services in Pakistan. The telecommunication industry has shown a mixed behavior towards 3rd Generation (3G)/4th Generation (4G). Though, 2G and 2.5G have well-served the end-users and have shown efficient results of cellular network performance in Pakistan, the 3G/4G network deployment is still showing a nervous behavior towards its evolution in Pakistan. Due to major security weaknesses in 2G and 2.5G networks [1] and to enable data, voice and video transmission at higher rates, the 3G/4G networks are successfully deployed in the country. There is no doubt that 3G will boom the telecom industry and mobile market of Pakistan because of its salient features such as quality of service (QoS), better coverage and higher data rates.

It is also believed that when something new is introduced then society adopts it in both positive and negative aspects. 3G can also negatively impact the market by abusing the best features of 3G networks such as video calling which may badly impact our social lives. As far as services are compared, 3G offers Universal Mobile Telecommunication System (UTMS) [2]. This is a new locality dependent service which promises faster voice and video calling services, fax and non-stop Internet, mobile applications and multimedia content [3]. 4G networks provide a unique environment where different wireless technologies are merged to form an IP based core network. This technology also provides continuous services to their consumer with improved quality of service (QoS) fast Internet and mobile TV [4][5]. Other applications of 3G/4G technology are video conferencing, online examination and consultancy by a doctor, and banking industry [6]. Online tutoring, online lecture and quickly tracking student and teachers performance are some of the other exciting features of 3G/4G networks[7][8]. In addition to the technical reasons, the service providers must make sure that their infrastructure and services are resilient against all kinds of security threats and vulnerabilities. It is very important for service providers to protect their network communication not only for successful commercialization of their services but also for improved users' experience. Before we further explore the modern security threats to 3G/4G networks we briefly review some key features of this technology.

A. Seamless Verified Handover

3G/4G offers intra-and-inter technology handover. This is the characteristic of a base station in 3G network which ensures service connection with zero or minimum disturbance, and with no notable failure in service quality. This function provides nonstop visible protection of active service instances and addition of various types of access technologies, from Wi-Fi to Orthogonal Frequency-Division Multiple (OFDMA)[8][9].

B. Selection and Detection of Network

The characteristics of mobile terminal with multiple radio technologies allow access to multiple networks simultaneously [10]. It improves call quality within cellular networks[9].

C. Key Management

The main security vulnerability in 2G networks has been addressed in 3G networks. For improved security measure, authentication and key agreement (AKA) [1] method has been developed. The main advantages of AKA are: long authentication keys; stronger hash function; support of mutual authentication[11];support for signaling message data; massage encryption and user data encryption[12].

D. Quality of Service and Support for Multiple Applications

4G networks are specially designed to support multimedia applications. The developed scheduling algorithms for 4G networks provide improved QoS to the end-user[13].4G also provides support for unicast and multicast services and applications. Enforcement of service level agreements (SLA) offer strong confidentiality for multiple applications [8].

Table 1: Salient Features of 1G to 4G Cellular Networks

Emerging Technology	1G	2G	2.5G	3G	4G
Services	Analog voice	Digital Voice	Higher Capacity, Packetized	Higher Capacity, broadband data up to 2mbps	Completely IP based, speed up to hundreds of MBs
Standard	NMT, AMPS, Hicap, CDPD, TACS, ETACS	GSM, iDEN, D-MPS	GPRS, EDGE etc.	WCDMA, CDMA 2000	Single standard
Data Bandwidth	1.9 kbps	14.4 kbps	384 kbps	2 Mbps	200 Mbps
Multiplexing	FDMA	TDMA, CDMA	TDMA, CDMA	CDMA	CDMA
Core Network	PSTN	PSTN	PSTN, Packet Network	Packet Network	Internet

We briefly reviewed some of the key features of 3G/4G networks. Table 1 summarizes a comparison of different features of 1G, 2G, 2.5G, 3G and 4G cellular networks. In this paper we investigate security threats and vulnerabilities to 3G/4G deployment in Pakistan and based on survey results, we present appropriate security measures that can be set up for secure and efficient usage of 3G/4G cellular networks. The rest of the paper is organized as follow. Section II reviews related studies. Section III analyzes emerging security threats in Pakistan. Section IV presents summary and findings and the paper is concluded in Section IV.

II. Related Studies

The security threats and vulnerabilities to 3G/4G cellular networks have been intensively investigated. In this section, we provide an overview of different security aspects in 3G/4G networks.

A. User identity

Maintaining user individuality during transmission is very crucial. As sending user identity in plain text can allow an eavesdropper to intercept the communication and to track the subscriber cell locality by means of user International mobile subscriber identity (IMSI) impersonation and relay of user message [14].

B. Wi-Fi security

The open environment and less secure behavior of wireless LAN has created many security threats. It is very important to secure the Wi-Fi networks in public areas[15]. Different solutions have been proposed, e.g., [16]. To summarize, the security of Wi-Fi has made significant improvements in recent. However, the new security threats [16][17]are still a challenge for researchers and developers.

C. WiMAX security

WiMAX use bothPhysicallayer and Link layer, so thesecurity attacks can be at variance depending on which method is applied. Currently, WiMAX is using the IEEE 802.16 standard composed of IEEE 802.16-2004 and 802.16e-2005 [16] for fixed and mobile architecture. IEEE 802.16-2004 defines confidentiality key managing protocol by which mobile station is authorized from the base station [18]. However, in IEEE 802.16-2004 a variety of weaknesses were

discovered such as access vulnerability, weak encryption key and lastly denial of service (DoS) attacks. The WiMAX IEEE 802.16-2005 addresses all the weakness of IEEE 802.16-2004. However, it still suffers from few security weaknesses. Similarly in case of Wi-Fi, it is important to deploy better security protocols to address all possible known attacks and weakness.

D. Possible Threats on 4G.

Due to the open nature of 4G, a number of security risks have emerged. New end-user equipment can also become a cause of DoS[19]. One type of attack is VoIP spam. It is similar to spam in inbox email. Due to the unlocked nature of VoIP, it has become easy for an attacker to transmit VoIP Spam over Internet Telephony (SPIT). The VoIP threats include the eavesdropping of confidential or private conversation, attacks on user names, password, confidential key, credit card and social security number and compromise on bank accounts [20].

E. Social Aspects of 3G/4G.

The 3G/4G technology provides high speed Internet access to the end-user to use Internet services on cell phone and computer[21]. Fast Internet speed means a new concern for security threats. The capability of 3G mobile communications could make a criminal and terrorism activity convenient. The development of social networks has exploded over the last 4years [22].According to Facebook website pages, the site has over 200 million active users, of

which over 100 million log on every day [23]. Majority of people use Internet and Facebook in positive way but these are also used for destructive activities.In European countries, the high speed Internet connectivity has given birth to many dating websites [24] where people meet online with each other. However, this feature should not be encouraged in Islamic Republic of Pakistan as it can give birth to cyber crimes. It has been reported that major targeted killings and kidnappings in Karachi were done via Facebook[25]. Another security vulnerability of high speed Internet access is the more we connect to the Internet, the more prone we are to be attacked. A person creates his account on social network like Facebook [25], MySpace [26], Twitter[27], Tagged[28] etc., and a hacker send a fake page to the user and user logs-in to that page. Thus, unknowingly sends his information to the hacker which could be usedforany harmfulactivity. Same applies to computers which has increased the potential of viruses, Trojanhorses and spam attacks[29]. Hackers can easily access the remote computer and can contaminate a whole network within seconds with the high speed of 3G/4G network [30].

III. An Analysis of Emerging Security Threats of 3G/4G Cellular Network in Pakistan

In this section of the paper, we conduct a survey questionnaire. The purpose is to ask the respondents about their security concerns related to 3G/4G deployment and then to analyze emerging security threats and to propose appropriate measures. The respondents are categorized into students, IT-professionals, academic staff and non-IT/other persons. Figure1 below shows the relation between age groups and number of respondents.

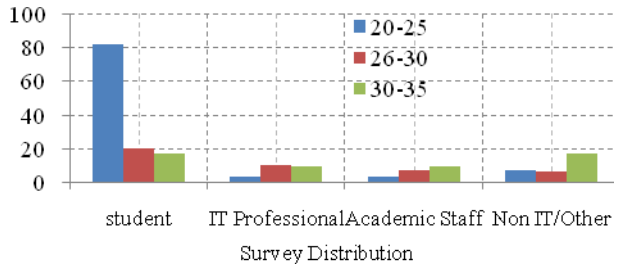

Figure 1. Relationship between the age factor and categories of respondents

In our survey, we have also considered gender and age group. Table 2 shows the division based on gender and age group.

Table-2 Relationship between gender and their ages

Gender	Age in years			Total
	20-25	26-30	30-35	
Male	33	7	13	53
Female	62	41	44	147
Total	95	48	57	200

Our first question was about the awareness of respondents regarding 3G/4G deployment in Pakistan and their eagerness to use the new technology. The results obtained are plotted in Figure 2. It could be observed that 70% of the respondents know about the launch of this technology and are willing to use the services. It is also observed that the respondents of age 20-30 years are more conscious about 3G/4G services.

We then asked the respondents about their motivation to switch from legacy 2G/2.5G cellular network to state of the art 3G/4G technology. The respondents were given four options: i.e., enrich their mobile phone experience (calls only); enrich their multimedia experience (voice, video, and data); high speed Internet access or all three options. The respondents were asked another question about the authentication technique they use in their smart phones. The survey results obtained are plotted in Figure 3 which reveals some interesting facts. Most of the users want to use 3G/4G

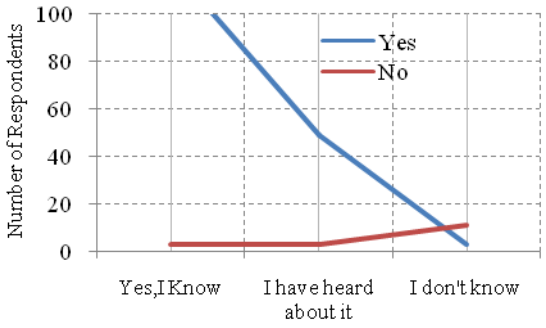

Figure-2 Relationship between using 3G/4G services and awareness

services because they want to enrich their voice, video call experience and they want to access the Internet on their mobile phones at very high speed. It was also revealed that the most commonly used authentication technique amongst the users of smart phone is PIN code which is used by approximately73% of the respondents.

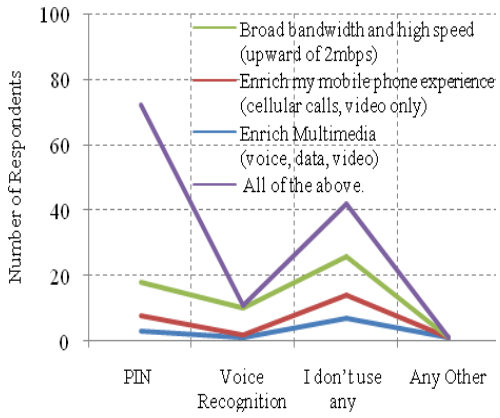

Figure 3. Motivation of respondents to use 3G/4G cellular services and their preferred authentication technique on their smart phone.

The respondents were asked how much they are concerned about the security features in the 3G/4G technology and what measures they will take to incorporate more security. It can be seen in Figure 4 that regardless of the salient features of 3G/4G technology, most of the people are concerned about the security provision mechanism in 3G/4G networks. All the respondents are willing to take all possible measures in order to achieve high security while using the new technology on their smart phones.

The respondents were asked which brand of smart phone and what type of operating system they feel can provide better security. Some very interesting facts are revealed which have been plotted in Figure 5.

It can be inferred that despite the fact Android is an open source platform and is more vulnerable to security threats, people feel secure while having Android operating system installed in their smart phones. One reason behind the usage of Android security is achieved by utilizing memory management unit (MMU) [21]. While iOS security model is different with Android operating system [2]. Though, both operating systems provide security by first checking every application before downloading but still, users are confident about security mechanism in their installed operating system. Another interesting fact that has been revealed is that most of the users are using Samsung brand handset which shows that there is much market potential for Samsung handset products.

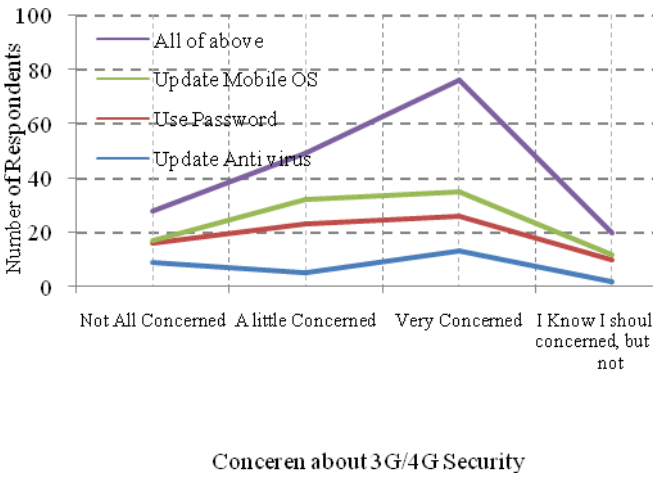

Figure 4. Security concerns amongst the userandpreferred measures to ensure techniques to update security

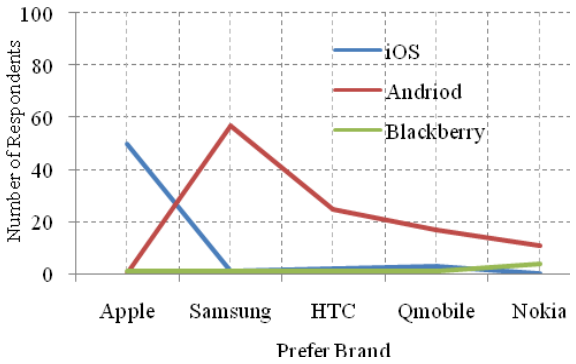

Figure 5.Users' preferred brand and preferred operating system

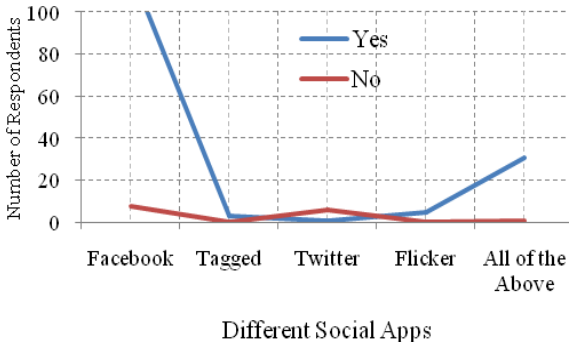

Figure-6 Comparison between different social apps and its uses

While using 3G/4G network, social network circle will be more increased and users will be spending more time on social media. This fact was revealed when the respondents were asked the question which social networking app they will be using more. Almost, all the respondents are agreed that their social networking experience will be enriched (Figure 6). It could be inferred that the more time user spend on social networking application, more will be they are exposed to threats and vulnerabilities specifically, chances become high for breach of confidentiality.

Lastly, the respondents were asked what kind of service(s)they will be using more often. The survey results obtained for this question are plotted in Figure 7. It can be seen that users will be enhancing their cell phone experience by using different types of services such as video call, mobile TV, high speed Internet access, content download, location aware services, online ticketing and multi-user

online gaming. The respondents are excited that they will be 3G/4G network. Respondents also revealed that all the data in their smart phone is important for them.

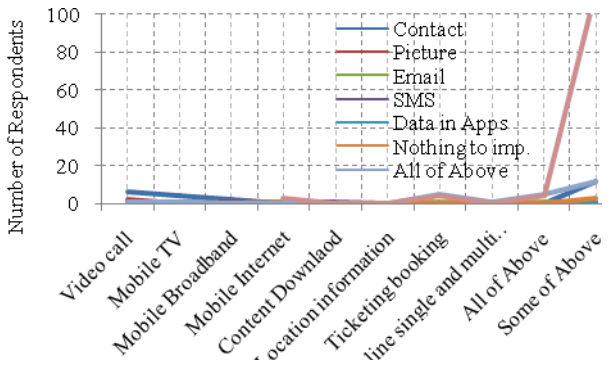

Figure 7. Usage of different types of services in 3G/4G and the important data.

IV. Summary and Findings

Pakistan is a developing country but when it comes to adopting a technology, Pakistan is in front line to compete the rest of the world. From smart phones to smart TVs, as the gadget is launched, the citizens of Pakistan not only adopt its current version instantly but they always remain curious about the upcoming technologies. These facts were revealed when most of the respondents in our survey questionnaire already knew about the launch of 3G/4G technology in Pakistan. Undoubtedly, the 3G/4G technology is mostly awaited by the young citizens of age 20-30 years. It is also inferred that the users of 3G/4G cellular networks in Pakistan want to enrich their mobile phone experience by having access to high speed Internet and facility of voice and video conversation on the go. The social lives of the respondents will also be improved as they will remain connected to the world at very low and affordable prices. However, despite numerous salient features of 3G/4G technology, users are concerned about the security of their data in their mobile devices. It is believed that the more they are connected, the more they are prone to security threats and vulnerabilities. The existing security techniques for authentication and authorization of the legitimate users need to be enhanced further.Now its up to the manufacturers and the developers of the smart phone and 3G/4G technology to ensure maximum security against the modern security threats so that the users' personal data remain secure all the time.

V. Conclusions

In this paper, we studied emerging security issues for 3G/4G cellular networks in Pakistan.We conducted a survey and asked different questionnaire which revealed some interesting facts. People are anxiously waiting to get benefitted from the state of the art technologies but meanwhile, they are also very cautious about their sensitive data in their smartphones. Currently, cellular users in Pakistan face traditional security threats and vulnerabilities of 3G/4G networks. It is anticipated that there will be new kind of security attacks to the users of 3G/4G networks in Pakistan. These new attacks could relate to locations, culture linguistics or ethnicity. In future, we aim to investigate these threats and vulnerabilities and their solutions. 3G/4G network are still growing in Pakistan while relevant threats will be increases. We would be concentrating on solutions for the emerging security issues for 3G/4G networks users in Pakistan.

References

[1] R. Aiash, M.Mapp, G.Lasebae, A. Phan, "Providing Security in 4G Systems: Unveiling the Challenges," *Telecommun. (AICT), 2010 Sixth Adv. Int. Conf.*, pp. 439–444, 2010.

[2] G. Delac, M. Silic, and J. Krolo, "Emerging Security Threats for Mobile Platforms," pp. 1468–1473, 2011.

[3] W. Li and A. Joshi, "Security Issues in Mobile Ad Hoc Networks - A Survey," pp. 1–23.

[4] "3G Migration in Pakistan," 2009.

[5] F. D. Issues, M. Ajana, E. Khaddar, H. Harroud, M. Boulmalf, M. Elkoutbi, and A. Habbanil, "Emerging Wireless Technologies In E-Health," 2012.

[6] W. Liu and E. K. Park, "e-Healthcare Security Solution Framework," *2012 21st Int. Conf. Comput. Commun. Networks*, pp. 1–6, Jul. 2012.

[7] B. B. Muvva, R. Maipaksana, and M. N. Reddy, "4G and Its Future Impact : Indian Scenario," vol. 2, no. 4, pp. 497–499, 2012.

[8] I. Shah, S. Shukla, R. Shrotriya, N. Mehta, N. Mehta, and S. Bakliwal, "Comparative Study of 4G Technology , Applications and Compatibility in Prevailing Networks," vol. 2, no. 6, pp. 287–291, 2012.

[9] B. Bhattacharyya and S. Bhattacharya, "Emerging Fields in 4G Technology , its Applications & Beyond-An Overview," vol. 3, no. 4, pp. 251–260, 2013.

[10] A. K. Jain, D. Shanbhag, and T. C. Services, "Addressing Security and Privacy Risks in Mobile Applications," no. October, pp. 28–33, 2012.

[11] J. Al-saraireh and S. Yousef, "Extension of Authentication and Key Agreement Protocol (AKA) for Universal Mobile Telecommunication System (UMTS)," vol. 1, no. 1, pp. 109–118, 2006.

[12] "Entity Authentication and Key Agreement."

[13] M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 1, pp. 446–471, 2013.

[14] R. C. Phan and D. J. Parish, "Analysis and Design of Security for Next Generation 4G Cellular Networks," 2012.

[15] H. Peng, "WiFi network information security analysis research," *2012 2nd Int. Conf. Consum. Electron. Commun. Networks*, pp. 2243–2245, Apr. 2012.

[16] Y. Park and T. Park, "A Survey of Security Threats on 4G Networks," *2007 IEEE Globecom Work.*, pp. 1–6, Nov. 2007.

[17] K. Scarfone, M. Sexton, and C. Tibbs, "Guide to Securing WiMAX Wireless Communications Recommendations of the National Institute of Standards and Technology."

[18] L. Yi and K. X. Miao, "WiMAX-WiFi unified network architecture, security, and mobility," *2010 IEEE 12th Int. Conf. Commun. Technol.*, no. 2, pp. 324–327, Nov. 2010.

[19] R. M. Needham, "Denial of service" University of Cambridge," pp. 151–153.

[20] S. Mcgann and D. C. Sicker, "An Analysis of Security Threats and Tools in SIP-Based VoIP Systems."

[21] L. Giripunje and S. Nimbhorkar, "Survey on Security Systems for Mobile Network," vol. 2, no. 1, 2013.

[22] A. Beach, M. Gartrell, and R. Han, "Solutions to Security and Privacy Issues in Mobile Social Networking," *2009 Int. Conf. Comput. Sci. Eng.*, pp. 1036–1042, 2009.

[23] S. Mahmood, "New Privacy Threats for Facebook and Twitter Users," *2012 Seventh Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput.*, pp. 164–169, Nov. 2012.

[24] "beautifulpeople," 2014. [Online]. Available: http://www.beautifulpeople.com/en-PK. [Accessed: 02-Dec-2014].

[25] "FaceBook," 2014. [Online]. Available: www.facebook.com. [Accessed: 02-Dec-2014].

[26] "myspace," 2014. [Online]. Available: https://myspace.com/. [Accessed: 02-Dec-2014].

[27] "twitter," 2014. [Online]. Available: https://twitter.com/. [Accessed: 02-Dec-2014].

[28] "Tagged," 2014. [Online]. Available: http://www.tagged.com/. [Accessed: 02-Dec-2014].

[29] V. K. Gunjan, A. Kumar, and S. Avdhanam, "A survey of cyber crime in India," *2013 15th Int. Conf. Adv. Comput. Technol.*, pp. 1–6, Sep. 2013.

[30] V. Saini and A. K. Saini, "3G Widens the Scope for Cyber Crime in India," vol. 12, no. 4, 2012.