A. Nieto, and J. Lopez, "Security and QoS relationships in Mobile Platforms", *The 4th FTRA International Conference on Computer Science and its Applications (CSA 2012)*, Lecture Notes in Electrical Engineering vol. 203, pp. 13-21, 2012.
http://doi.org/10.1007/978-94-007-5699-1_2
NICS Lab. Publications: https://www.nics.uma.es/publications

Security and QoS relationships in Mobile Platforms

Ana Nieto and Javier Lopez

Computer Science Department
University of Malaga, Spain
{nieto, jlm}@lcc.uma.es

Abstract. Mobile platforms are becoming a fundamental part of the user's daily life. The human-device relationship converts the devices into a repository of personal data that may be stolen or modified by malicious users. Moreover, wireless capabilities open the door to several malicious devices, and mobility represents an added difficulty in the detection of malicious behavior and in the prevention of the same. Furthermore, smartphones are subject to quality of service (QoS) restrictions, due to users' needs for multimedia applications and, in general, the need to be always-on. However, Security and QoS requirements are largely confronted and the mobility and heterogeneous paradigm on the Future Internet makes its coexistence even more difficult, posing new challenges to overcome. We analyze the principal challenges related with Security and QoS tradeoffs in mobile platforms. As a result of our analysis we provide parametric relationships between security and QoS parameters focusing on mobile platforms.

Keywords: Security, QoS, Tradeoffs, Mobile Platforms.

1 Introduction

Security risks in mobile platforms are increasingly a customer concern. In particular, the theft of personal data is a widely discussed issue. As a consequence, some mobile platforms have begun to develop specific solutions to avoid the theft of private data from mobile terminals. Indeed, threats in mobile platforms open up a new market for anti-virus providers, whose products have been adapted to protect mobile platforms (e.g. McAfee Mobile Security). These new services are of particular interest in corporate environments, where personal devices can inadvertently introduce malware into the system. In addition, from a commercial point of view, new emerging technologies (e.g. NFC) open the door to new ways to trick the user.

Furthermore, the widespread use of multimedia applications does necessitate the presence of mechanisms to ensure the quality of service (QoS), and more generally the quality of experience (QoE). These applications have the added difficulty of being deployed in resource-constrained devices, so more requirements have to be taken into account apart from those concerned with improving the multimedia capabilities. Therefore it is not only the network parameters that must to be controlled. In mobile platforms the QoS mechanisms have to integrate network parameters (e.g. bandwidth) and device parameters (e.g. battery power). Furthermore, as user's satisfaction is closely related with the success of the platform, it is fundamental to add QoE

measurements to the quality study. However, security mechanisms can damage the user's opinion [13]. In fact, security mechanisms tend to consume network and local resources and can easily affect the normal performance of devices.

The main objective behind the approach presented here is to provide an analysis about security and QoS tradeoffs in mobile platforms where the aforementioned concepts will be widely exposed. Indeed, although such concepts are separately analyzed in several papers, in the end they have to coexist in the same environment. Thus, understanding these relationships previous to running it on the architecture is fundamental to savings in cost and ensuring better security and performance. As a result, we provide a parametric relationship scheme between security and QoS, which also considers the effect that such dependencies have on the user perception.

The remainder of the paper is organized as follows: Section 2 provides an analysis on the current challenges related with Security and QoS. In Section 3, an analysis of Security and QoS tradeoffs in mobile platforms is shown. Finally, Section 4 discusses related work and Section 5 concludes the paper.

2 Security and QoS challenges

Fig.1 shows a simplified diagram with the main Security and QoS challenges identified based on the current literature. We consider three sections: commercial purposes, development and communication.

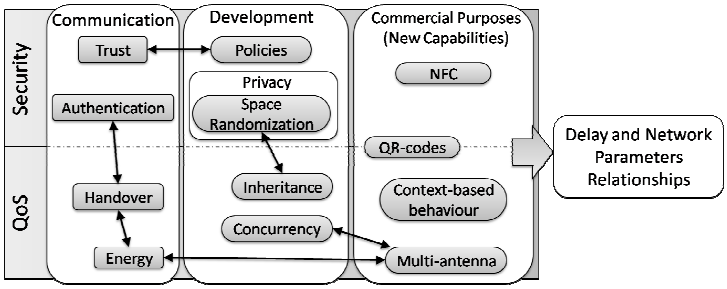

Fig. 1. Security and QoS challenges.

Commercial Purposes. Identifies popular characteristics developed with the aim of improving functionality of personal devices to be more attractive for the user. For example, in the QoS context, the use of multiple radio antennas allows better transmission services at higher speeds and also offers the possibility for early detection of collisions, among other things [12], but increase the complexity of the system[2][21]. Regarding security, NFC allows secure e-payment, and can be built in the device as it is anti-tampering, but it can also affect the system's overhead by increasing the transaction time and therefore the response time [5]. To the contrary, QR-codes can be used (like tokens) in authentication mechanisms to reduce the response time [18]. However, both NFC and QR-codes open the door to new threats [19] and ways to trick the user [5] [10]. We also note that context-based services are

also of growing interest [22], because they allow a more realistic behavior based on knowledge.

Development: Takes into account the security risks due to a wrong implementation of security requirements [9] [20]. Related with it, [14] highlights the importance of establishing different users' permission levels to prevent that, once the attacker finds a bug in the system, it can take absolute control. Also it is necessary to pay attention to problems caused by incompatibility of functions. For example, privacy mechanisms based on space randomization (e.g. ASLR) can be unusable when inheritance-based mechanisms (e.g. Zygote) are used to allow two processes to share the same memory space to reduce the overhead [17]. Note that privacy is becoming a major issue, because user participation in mobile platforms requires it. But, privacy is being continuously threatened. For example, in [8], the authors show that it is possible to recover information from mobile platforms even though it has been deleted.

Communication: Considers the requirements and mechanisms to protect network communication at a low cost. From a QoS point of view, solutions to provide end-to-end QoS guarantees should consider local QoS requirements, such as memory, or energy consumption. The last one is critical, not only to improve the QoE, but also because without it the device is useless. Traditional QoS requirements and energy consumption tradeoffs are studied in [1], [3] and [21]. In particular, [1] provides a solution based on predicting the behavior of the system, which is not always a feasible option. From a security point of view, trust mechanisms are fundamental to ensure the survival of a communication platform based on the interaction between entities through the Internet. However, it implies in several cases the use of certificates or complex authentication schemes that are not supported on mobile phones.

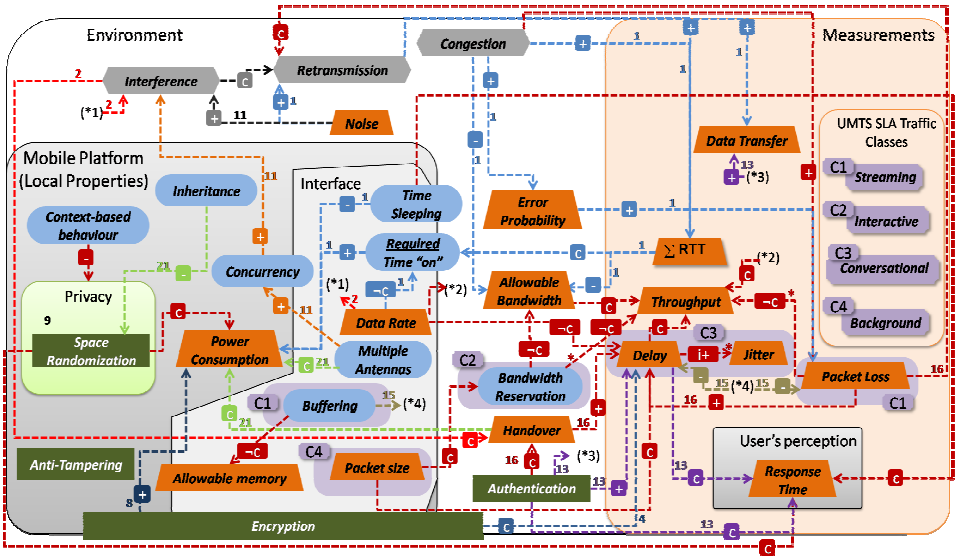

Fig. 2. Security and QoS Parametric Relationships in Mobile Platform

3 Parametric relationships on mobile platforms

This section analyses the dependencies between Security and QoS parameters illustrated in Fig.2. Below, the mathematical definition of each relation is described.

3.1 Mathematical Definition

In our previous work [16] we defined a set of dependency relationships between parameters (1,2,5,6). However, we need to add new equations to the current formulation to express the specific dependencies on mobile platforms. Below, we work with a formulation based on basic expressions (1-4) in order to clarify the dependencies diagram (Fig. 2).

Basic expressions		Complex expressions (based on 1-4)	
$D^{+} :: aD^{+}b \Rightarrow (\Delta a \rightarrow \Delta b)$	(1)	$D^{c} :: (\Delta a \rightarrow \Delta b) \wedge (\nabla a \rightarrow \nabla b) \equiv aD^{+}b \wedge aD^{-+}b$	(5)
$D^{-} :: aD^{-}b \Rightarrow (\Delta a \rightarrow \nabla b)$	(2)	$D^{t} :: aD^{c}b \wedge bD^{c}a$	(6)
$D^{-+} :: aD^{+}b \Rightarrow (\nabla a \rightarrow \nabla b)$	(3)	$D^{-c} :: (\Delta a \rightarrow \nabla b) \wedge (\nabla a \rightarrow \Delta b) \equiv aD^{-}b \wedge aD^{--}b$	(7)
$D^{--} :: aD^{-}b \Rightarrow (\nabla a \rightarrow \Delta b)$	(4)	$D^{i+} :: (\Delta a \rightarrow \Delta b) \wedge (\nabla a \rightarrow \Delta b) \equiv aD^{+}b \wedge aD^{--}b$	(8)
		$D^{i-} :: (\Delta a \rightarrow \nabla b) \wedge (\nabla a \rightarrow \nabla b) \equiv aD^{-}b \wedge aD^{-+}b$	(9)

In order to get a basic set of equations, we add to the formulation in [16] the equations (3 and 4), corresponding to inverse positive and negative respectively. $D^{\neg+}$ (3) means that the decrement of the first parameter causes the decrement of the second parameter, while in $D^{\neg-}$ (4) the decrement of the first parameter causes the increment of the second parameter. Moreover, complex equations are obtainable from basic equations by adding to the formulation in [16] the equations 7, 8 and 9, corresponding to inverse complete, independent positive and independent negative respectively. $D^{\neg c}$ (7) means that both parameters are related negatively (D^{-}) and inverse negatively ($D^{\neg-}$). The independent relationships (8 and 9) have been added to reflect the dependencies in which regardless the change of value in the first parameter the result is always the increasing (D^{i+}) or decreasing (D^{i-}) of the second parameter. This happens, for example, with the relationship between parameters Delay and Jitter, as we shall see.

3.2 Dependency relationships diagram

Fig.2 shows the dependency relationships diagram that we will now explain. Each dependency is marked with the dependency symbol corresponding to the dependency relationship (+,-,¬ +,¬ -, c, t, ¬ c, i+, i-) and the reference to the article where it appears. However, some of them are based on known formulations for the calculation of some parameters, specifically 10, 11 and 12. These last dependencies have been highlighted with the symbol *. There are also some dependencies that are explained in the text, and that appear without being referenced in any paper previously mentioned

here. Moreover, the diagram also integrates the SLA traffic classes named in [15], which are: Interactive, Background, Streaming and Conversational.

$$\text{Delay} = \#\text{bits}/\text{DataRate} \tag{10}$$

$$\text{Jitter} = |\text{Delay}T_0 - \text{Delay}T_1| \tag{11}$$

$$\text{Throughput(per user)} = \text{DataRate}/\#\text{Users} \tag{12}$$

As we can see, delay, throughput and power consumption are highly influenced by the rest of parameters and characteristics. On the one hand, delay severely affects network performance. As we can see in Fig.2, both streaming and conversational traffic are affected whether delay increases or not. Note that buffering can help to minimize the delay if the data can be pre-processed while it is in the buffer, and also helps to decrease packet loss when an adequate buffer size is defined. However, the buffering technique demands memory in order to work. We also observe that the handover increases the delay, as do the authentication mechanisms. Moreover, although increasing data rate can decrease the delay (13), it is important to note that it also may cause interferences because high speeds introduce noise. In addition, long packet size can increase the delay because it introduces more data to be sent in the same packet (15).So, depending on the intermediary communication mechanisms, it can require a greater amount of time to be processed (e.g. decode/coding data). In addition, when the receptor fails, the entire packet has to be sent again.

$$(\Delta DataRate \rightarrow \nabla Delay) \wedge (\nabla DataRate \rightarrow \Delta Delay) \equiv DataRateD^{-c}Delay \tag{13}$$

$$(\Delta \#bits \rightarrow \Delta Delay) \wedge (\nabla \#bits \rightarrow \nabla Delay) \equiv PacketSizeD^{c}Delay \tag{15}$$

On the other hand, although increasing the packet size means the delay increases, when the packet size is very small it may cause throughput degradation because each packet requires that a header is sent, increasing the volume of data to be sent. Therefore, header content is not considered as useful data for communication at service level, and thus the throughput decreases. However, if the packet size is too big then the throughput can be damaged too. For example, if the packet size is static and the data to be sent is less than the packet size, then the packet has to be completed with garbage data to achieve the total size, and such data cannot be counted as useful data. The problem is greater if bandwidth reservation mechanisms are static. In such cases, the bandwidth that has been previously reserved is unusable for other devices. As a consequence, the greater the packet size the higher the bandwidth reservation, decreasing the network's resources.

Note that, when the delay increases then the throughput decreases because the channel is probably saturated. Contrarily, when the delay decreases the throughput can be increased because there are more available resources for data transmission and fewer errors are likely to occur. If the throughput is poor, the service is not receiving sufficient data to work properly. This can damage the user's perception of the service, which is also affected when the response time increases. Packet loss affects both; throughput and delay. When packet loss is high (e.g. due to congestion or the high error probability), the delay increases and, contrarily, the throughput decreases (in the case that the re-send data is not considered for throughput calculation). Indeed, if the

packet loss increases, then the number of retransmissions also increases, thus increasing the data transfer and also the power consumption.

Regarding the power consumption, it is strongly decreased by the time that the antennas are active (required time-on). Thus, although local security mechanisms increase the computational requirements, the power consumption is increased mainly due to those operations related with data transmission. Note that, by decreasing the required time-on, the power consumption can also decrease if the network interface is disabled in such situations. Indeed, if the data rate increases, then the required time-on decreases, but it is possible that noise appears when speed increases. LTE, one 4G technology, requires ICIC techniques to avoid interferences, precisely due to high speeds. However, it does not mean that, because of this, LTE terminals consume less energy. On the contrary, LTE technology is able to use multiple antennas, improving performance in communications, but also requiring more energy for transmission. Besides, multiple antennas also increase the complexity of the terminal, where concurrent operations can coexist increasing the interference probability.

Finally, in general, security mechanisms increase the response time. It is particularly true when additional messages to establish a secure communication channel are required. The rising amount of data to be sent inevitably affects power consumption, but also causes delay, which increases as a consequence of the growing traffic. Cryptographic techniques also affect power consumption, but sent data requires even more energy than that. Therefore, when authentication mechanisms have to be performed during the handover, the overall performance of the network can be severely damaged. Indeed, the handover process involves several operations to be effective (message interchange between entities), and, therefore, it also increases the power consumption by itself. Lastly, privacy mechanisms based on space randomization (e.g. ASLR) provide local security for user's data. However, context-based services require the storing of the user's preferences in the mobile platform or sending it to an external server in order to work. In both cases the user's privacy is affected.

4 Related Work

There are some papers related with the study of Security and QoS tradeoffs, although they have been developed within a specific scenario. Therefore they do not provide a general view of the current state of the art in mobile platforms. For example, [13] analyzes how the authentication mechanisms affects delay, and how it affects the user's perception. Moreover, the end-to-end secure protocol proposed in [7] for Java ME-based mobile data collection also considers the balance between flexibility, efficiency, usability and security. In said work, the effect that different encryption algorithms (e.g. AES, RSA) have on performance has been studied. Moreover, [4] propose SECR3T, a secure communication system over 3G networks that considers QoS restrictions. For example, the paper shows the effect that encryption protocols have on delay (minimum and maximum), and how it affects different types of data (audio and video). Power consumption is also considered, and the authors conclude that it greatly depends on the implementation of the protocol

used (e.g. TLS, ECDH). Moreover, as we have seen, in [18] the advantages of using QR-codes for authentication in Cloud computing environments in order to increase the performance are highlighted, and in [5] the impact of NFC technology on delay and computation time is shown.

5 Conclusions

In this paper we have seen how several studies have focused on both security and QoS concepts, although with different aims, deploying mechanisms or defining models to solve specific problems. We have carried out an analysis of such mechanisms and also detected further challenges to be addressed. Moreover, we have grouped this knowledge in a comprehensive dependency relationship map, in order to enable the future development of tools to support developers in the development of secure and efficient services for mobile platforms. The final diagram shows that delay, throughput and power consumption are highly influenced by the rest of the parameters and characteristics. Note that, in this paper we provide several examples where security and QoS tradeoffs are present. However, in such papers the tradeoffs are very specific, mainly focusing on a particular problem or scenario and are not considered together. This lack of abstraction makes the complete understanding of security and QoS tradeoffs in mobile networks more difficult. The novelty of this paper is therefore, precisely, in providing such a global vision where, in addition, parametric relationships are provided within an understandable logic.

Acknowledgment

This work has been partially supported by the Spanish Ministry of Economy and Competitiveness through the projects SPRINT (TIN2009-09237) and IOT-SEC (ACI2009-0949), being the first one also co-funded by FEDER. Additionally, it has been funded by Junta de Andalucia through the project PISCIS (TIC-6334). The first author has been funded by the Spanish FPI Research Programme.

References

1. G. Anastasi, M. Conti, E. Gregori, and A. Passarella. Balancing energy saving and qos in the mobile internet: an application-independent approach. In System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on, pages 10–pp. IEEE.
2. D. Aziz and R. Sigle. Improvement of lte handover performance through interference coordination. In Vehicular Technology Conference. IEEE 69th, pages 1–5. IEEE, 2009.
3. P. Bellasi, S. Bosisio, M. Carnevali, W. Fornaciari, and D. Siorpaes. Constrained power management: Application to a multimedia mobile platform. In Design, Automation Test in Europe Conference Exhibition (DATE), 2010, pages 989 –992, march 2010.
4. A. Castiglione, G. Cattaneo, G.D. Maio, and F. Petagna. Secr3t: Secure end-to-end communication over 3g telecommunication networks. In Innovative Mobile and Internet

Services in Ubiquitous Computing (IMIS), 2011 Fifth International Conference on, pages 520 –526, 30 2011-july 2 2011.
5. G. V. Damme and K. Wouters. Practical experiences with nfc security on mobile phones. Katholieke Universiteit Leiden, 2009.
6. Dai Zovi and Dino A. Apple ios 4 security evaluation. Trail of Bits LLC, 2011.
7. S. Gejibo, F. Mancini, K. Mughal, R. Valvik, and J. Klungsøyr. Challenges in implementing an end-to-end secure protocol for java me- based mobile data collection in low-budget settings. Engineering Secure Software and Systems, pages 38–45, 2012.
8. William Glisson, Tim Storer, Gavin Mayall, Iain Moug, and George Grispos. Electronic retention: what does your mobile phone reveal about you? International Journal of Information Security, 10:337–349, 2011. 10.1007/s10207-011-0144-3.
9. M. Grace, Y. Zhou, Z. Wang, and X. Jiang. Systematic detection of capability leaks in stock android smartphones. NDSS, 2012.
10. Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, and Edgar Weippl. Qr code security. In Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia, MoMM '10, pages 430–435, New York, NY, USA, 2010. ACM.
11. S. Kiminki, V. Saari, V. Hirvisalo, J. Ryynanen, A. Parssinen, A. Immo- nen, and T. Zetterman. Design and performance trade-offs in parallelized rf sdr architecture. In Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), 2011 Sixth International ICST Conference on, pages 156–160. IEEE, 2011.
12. S.P.S. Kumar and S.V. Anand. A novel scalable software platform on android for efficient qos on android mobile terminals based on multiple radio access technologies. In Wireless Telecommunications Symposium (WTS), 2011, pages 1 –6, april 2011.
13. C. Lorentzen, M. Fiedler, H. Johnson, J. Shaikh, and I. Jorstad. On user perception of web login - a study on qoe in the context of security. In Telecommunication Networks and Applications Conference (ATNAC), 2010 Australasian, pages 84 –89, 31 2010-nov. 3.
14. C. Miller, J. Honoroff, and J. Mason. Security evaluation of apples iphone. Independent Security Evaluators, 19, 2007.
15. S. Mohan and N. Agarwal. A convergent framework for qos-driven social media content delivery over mobile networks. In Wireless Com- munication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on, pages 1–7. IEEE, 2011.
16. A. Nieto and J. Lopez. Security and qos tradeoffs: Towards a fi perspective. In Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on, pages 745 –750, march 2012.
17. Joh Oberheide. A look at aslr in android ice cream sandwich 4.0. The Duo Bulletin, 2012.
18. Dong-Sik Oh, Bong-Han Kim, and Jae-Kwang Lee. A study on authentication system using QR code for mobile cloud computing environment. In Future Information Technology, volume 184 of Communications in Computer and Information Science, pages 500–507. Springer Berlin Heidelberg, 2011.
19. M. Roland, J. Langer, and J. Scharinger. Security vulnerabilities of the ndef signature record type. In Near Field Communication (NFC), 2011 3rd International Workshop on, pages 65 –70, feb. 2011.
20. N. Seriot. iphone privacy. Black Hat DC, page 30, 2010.
21. M.M.Uddin,S.Haseeb,M.Ahmed,andA.-S.K.Pathan.Comprehensive qos analysis of mipl based mobile ipv6 using single vs. dual interfaces. In Electrical, Control and Computer Engineering (INECCE), 2011, International Conference on, pages 388 –393, june 2011.
22. K. Wac, A. van Halteren, and D. Konstantas. Qos-predictions service: Infrastructural support for proactive qos-and context-aware mobile services (position paper). In On the Move to Meaningful Internet Systems,OTM 2006 Workshops, pages 1924–1933. Springer.