INTERNATIONAL CONFERENCE RCIC'20
Redefining Community in Intercultural Context
Cluj-Napoca, 7-9 May 2020

COMMUNICATION IN THE TIMES OF GLOBALIZATION. SECURITY IN SMARTPHONE COMMUNICATION AT THE TIMES OF THE WEB 3.0

Guido ANCONA*

*Digital Security Expert, Adjunct Professor, University of Bari Aldo Moro, Bari, Italy

Abstract: *On the basis of a critical survey of the scientific literature and a wide range of quantitative and qualitative researches conducted in Europe, of great interest appears to be the study aimed at analyzing digital online environments starting from the daily practices that young people put into act to learn, communicate with the peer group, build their identity or exercise their citizenship rights in a multi-ethnic and globalized society (Fonasari, 2017). The main users of these new media are the so-called 'digital natives' (Prensky, 2001), or that new generation particularly inclined to use new technologies, but this does not mean that they have the appropriate responsibility, the critical sense and the right awareness to make the best use of it to avoid network dangers. In fact, mobile technologies in the past years have known a strong impact and a large diffusion. Within this new context of global explosion of new mobile technologies, an increasing concern is developing towards cybersecurity issues that, now more than ever, become current and perceived, even if not always in an appropriate manner, by users. The article presents an articulated critical reflection on the threats connected to communication via smartphones (the device most used by young people) focusing on the vulnerabilities of: the Android system, applications and connections and highlighting the need to help students build both digital skills (as explained in the context of the eight key European competences) and media education*

Keywords: *security, media; technologies; communication; media education*

1. INTRODUCTION

The *web* today is one of the main places of innovation, driving a rapid social change which easily ends up appearing disturbing or problematic to the eyes of adults. This concern may seem right and wrong at the same time: right because it represents awareness of how much the means of communication (understood as symbolic devices through which is produced and reproduced, on an everyday basis, the culture of a community and as socio-technical devices that redefine the conditions of personal interaction and social relationships) constitute a considerable part of the environment. Wrong because in a historical perspective it does nothing but renovate fears as old as the advent of the first mass media from comics to cinema to television, applying more or less faithfully the same discursive models and the same arguments to the role that internet plays in the experience of young people, forgetting both the groundlessness or partiality of many of those fears and the innovations introduced by digitalization. It happens paradoxically that those who, in an educational perspective, complained of the substantial passivity of the television medium compared to reading, today express their concern about the excess of network interactivity. This social change has affected how teenagers use the media to keep in touch and communicate with each other and with the whole world. One would say that almost all experiences for this generation, that not surprisingly has been defined ***always on*** (always connected) or digital, go through the media: from study to free time, to the relationship with friends near and far. The *new media* encourage the development of a particular type of intelligence that Gardner has defined "Relational intelligence" which is configured as an intercultural thought matrix.

This type of intelligence, in fact, opens up to something more significant than tolerance or acceptance; it introduces a flexible, mobile thinking, capable of operating inside of a multi-dimensional, dynamic, procedural culture; in other words to a culture that recognizes in its own birthplace the differences. As Turkle (2013) and De Kerckove (2016) had observed, mass media

have allowed teenagers unprecedented access to the adult world, blurring the boundaries between their respective cognitive experiences.

On the other hand, the contemporary affirmation of youth culture (minors under 18 represent about 20% of the population of developed countries and 50% of developing countries) suggests that teenagers, though wishing to broaden their knowledge, seem more motivated to experiment and put to the test their identity and relationships within the peer group, often inaccessible to the eyes of adults. For Gergen this shift from a vertical relationship (intergenerational) to a horizontal one (the peer group) is quite another thing with respect to the democratization process described by Giddens. It would rather result in an "overall devaluation of the profound dimension of relationships", since adolescents are increasingly absorbed by the effort to maintain a plurality of horizontal relationships with their network reference and less and less willing to develop those rich and intense bonds that characterize relationships with the significant and physically present adult groups around them.

What drives *online* communication on the move is the need for teenagers to stay connected with their peers anytime and anywhere, but does this communication always take place in security? Do young people have sufficient skills for the safe management of these devices and to deal with any network threats?

2. MEDIA AND SECURITY: VULNERABILITIES ON THE ANDROID PLATFORM

Mobile technologies over the past years have experienced a disruptive impact and an enormous propagation. The Internet is now constantly used within public places through free WI-FI connections which, together with a solid 3G and 4G coverage, always better guaranteed by the different telephone operators, has made it possible that smartphones are constantly used to carry out all types of activities. Within this new context of global explosion of mobile technologies, there is an ever growing concern towards cybersecurity issues, which now more than ever, have become relevant and are not perceived adequately by users. In particular, compared to the world of Personal Computers, there are some differences that make mobile devices even more attractive to hackers for the following reasons: smartphones almost always contain a large amount of confidential data. Contacts, text messages, calls and GPS position are just some of the information available from any mobile device, which can reveal confidential information about the individual using it; smartphones are designed to stay on throughout the day. The availability of an individual will depend on whether the device is active or not and consequently the time window in which a device can suffer an attack widens considerably; smartphones use the same operational systems and consequently the system in which the data is saved and stored is often known to hackers who are able to plan large-scale attacks using the same mechanism. For its nature of free software, but above all for its diffusion, Android has in a short time become the aim of targeted attacks to spread malware and exploit the vulnerabilities of the system. Android's vulnerabilities are essentially inherited from the structure of the operating system and from the applications installed on the device, which expose some components to a series of more or less critical threats (Gunasekera, 2012). In a more summary way we can say that on mobile devices it is possible to identify different types of threats: the communication channel network, applications or the market from which they are downloaded, user settings, improper use of the device but also the operating system itself. There are non-profit organizations such as the OWASP (Open Web Application Security Project) created to highlight the sometimes obscure aspects of computer security for web applications. These experts contribute daily to updating information on a field in which it is easy to be out of date and therefore be exposed to greater safety risks. OWASP, in 2016, drew up a ranking that highlights possible critical issues that may occur within the mobile devices: insecure data backup; low implementation of security protocols; insecure management of sessions and cookies; mechanisms of inefficient cryptography; disclosure of confidential personal information. These risks represent the fundamental level on which most of the vulnerabilities currently known for mobile platforms are based.

3. SYSTEM VULNERABILITY

There are some vulnerabilities that allow the user to obtain the so called root privileges inside the device. This operation is called in technical jargon *root or rooting* (understood as "root operation") of the mobile phone. Applications installed on the device cannot obtain this type of privilege and the Android application Sandbox serves to avoid this. In this regard, it wants to

protect the user from a series of threats which could compromise the functioning of the smartphone. At the same time, however, it happens that the users still want to root the devices for several reasons: a) eliminate customizations of the Provider from the phone: the telephone companies often sell smartphones in conjunction with tariff plans and promotional offers. The devices will be personalized in this way by the Carriers in order to allow the user to take advantage of some services which are often perceived by users as troublesome and not very useful. However, the user will not be free to delete the customizations except with the root; b) customization: a long series of operating system software components can be unlocked or customized only by root; c) access to blocked hardware features, such as the processor frequency control; d) to access and modify folders, system files and contents otherwise inaccessible. In order to obtain the root permissions of a device, the only method will be those to exploit a known operating system vulnerability, or flashing of the firmware. Both operations risk compromising the warranty of the device and are therefore largely discouraged for non-experts. Several operating system vulnerabilities have been found and exploited over the recent years. In particular, there are several exploits, almost always easily available on the web both in the form of source code and binary code, which can be used to root the device.

Each of these exploits will have its own target environment and will not work in operating system versions where the security flaw has been corrected. Sometimes it will not be Google Android to be vulnerable but the versions modified by some manufacturers. However, the fact remains that a device on which root privileges have been obtained, even voluntarily by the user, is more exposed to a series of attacks that could undermine its security. Furthermore, it is appropriate to specify how users who root their own device are not necessarily more 'advanced' than the average. In fact, it is quite easy to find a series of tutorials online that describe the correct procedure to be performed for each different phone model. This allows, even novice users, to root their device with all the associated security risks.

4. APPLICATION AND CONNECTION VULNERABILITIES

Applications for mobile devices have experienced a rapid diffusion in recent years, becoming extremely popular and representing the new frontier in the field of communication, like websites and social networks. App-level vulnerabilities are not always detectable mainly because most of the apps in the official Android store are created by amateur developers not always attentive to the implementation of a secure code (Jeff Six, 2011). Therefore the task of classifying every single error in a series of 'releases' of downloaded or unknown apps would be extremely complex and unproductive. A similar study would only make sense for apps whose traffic in terms of downloads are very high. Furthermore, it should be decided whether to also include in this particular selection the apps present outside the market, which are often perfectly legitimate and authoritative, but banned by Google for policy issues (e.g. applications from betting and gambling agencies).

There are also other authoritative markets, such as that of phone manufacturers or service providers. It often happens that in these markets there are top-apps not present in the Google Play Store, but extremely popular with users. In short, applications should also be filtered by the market in which they are available. In recent years, there has been no shortage of extremely famous application examples, within which, bugs and vulnerabilities have been found (Elenkov, 2014). We cite for example the case of extremely famous software such as Whatsapp, Messenger or Viber suffering from rather obvious security flaws that have been promptly repaired through updates released following the publication of the exploits by researchers, hackers and industry magazines. Application vulnerabilities jeopardize the integrity of users' personal data. A rather fitting example in this sense is represented by the bug that allowed the famous Viber messaging / VoIP application to unlock phones by circumventing the protection provided by the lock screen. However this is the proof that Sandbox and the permit mechanism do not always guarantee the total independence of the applications from system components, even when using certified libraries. In particular Android does not specify whether the type of connection used by the various applications that connect to external servers is safe or not, as happens instead when surfing the browser. It is therefore possible to see how a great number of the bugs present in the applications of the different Markets is attributable to bad code writing and/ or programming; the cause is attributable to inexperienced developers that often copy codes present on the internet without carrying out an accurate debugging or a correct analysis of the possible bugs present in it, but above all without performing any troubleshooting. Insecure connections are typical

vulnerabilities found in most of the Android applications developed by third parties.

The implementation of SSL / TLS protocols is often done improperly and this causes a possible unsafe exposure of data that could, therefore, be intercepted through simple MITM attacks. The fact remains that the security protocols mentioned above, although implemented in a correct way, do not guarantee the total security of the established connection. In 2017 a study conducted by some American experts in the field, detected that out of a sample of 13,500 applications downloaded from Google Play, about 8% of the apps examined contained codes potentially vulnerable to MITM-type attacks. Through simple tools like Wireshark, the data that is exchanged between a client and a server inside any node of the network utilized can be verified. In the development of client-server communications a secure set of connection instructions should always be implemented, especially for transactions involving sensitive data. In this sense, Android provides several APIs that make it possible to build a simple secure connection using the JAVA libraries that make good use of the object SSL Context. Sometimes the problem lies not so much in the implementation by the developers, but in the fact that safety certificates often have a price that cannot be sustained by those who create applications, especially if it concerns single individuals and not companies of a certain importance. Archiving files on the internal or external storage of the device is a fairly common operation for Android applications.

The use of hashing or cryptography protocols therefore represents a very important prerogative for any app that decides to take advantage of the storage media offered by the device. A first measure of security is actually offered by the Android Sandbox, which at least allows to isolate the content of a specific file stored inside the device from the other applications.

5. CONCLUSION

As emerges from this article, the digital skills of the 'generation always on' who often ignore the risks associated with surfing the net, are particularly fragile. If with the term Media Education (Buckingham, 2006) it intends, in fact, the set of educational and didactic activities aimed at informing young people and developing their critical understanding about the nature and use of the media, it is important to emphasize that in the contemporary schools these educational paths are not present. All this appears very serious in a media society, where young people live a good part of their school and social life online, constantly connected, which is why it is essential to put specific training activities into practice in order to provide all the necessary tools to allow us to live our contemporaneity in a safe, fair and ethical way.

BIBLIOGRAPHY

1. AA.VV. (2013). Android/ Introduction. *Wikibooks.* [online]. URL: http://en.wikibooks.org/wiki/Android/Introduction [Accessed on March, 2020].
2. Bornstein, David. (2020). Dalvik VM Internals. *Politechnika Łódza: Katedra Mikroelektroniki i Technik Informatycznych* [online]. URL: http://fiona.dmcs.pl/podyplomowe_smtm/smob3/Presentation-Of-Dalvik-VM-Internals.pdf. [Accessed on March, 2020].
3. Buckingham, D. (2006). *Media education. Alfabetizzazione, apprendimento e cultura contemporanea*. Milano: Erickson.
4. De Kerckove, D. (2016). *Un mondo condiviso.* Bari: Edizioni Laterza.
5. Dewdney, A.K. (1989). Computer Recreations: Of Worms, Viruses and Core War. *Scientific American*. Vol.260. 110-113.
6. Elenkov, N. (2014) *Android Security Internals: An In-Depth Guide to Android's Security Architecture.* San Francisco, CA:No Starch Press.
7. Fornasari, A. (2017). Social Privacy. Informare, comunicare, educare ai tempi del web 3.0. *Mondo Digitale*. Settembre 2017.
8. Gardner, H. (2013) *Formae mentis. Saggio sulla pluralità dell'intelligenza*. Translated by L. Sosio. Milano: Feltrinelli.
9. Goffman, E. (1956). *The Presentation of Self in Everyday Life.* Edingurgh: University of Edinburgh.
10. Gunasekera, S. (2012) *Android Apps Security.* New York: Apress.
11. Kerrisk, Michael. (2013). An introduction to Linux IPC. *linux.conf.au* [online]. URL: http://man7.org/conf/lca2013/IPC_Overview-LCA-2013-printable.pdf [Accessed on March, 2020].
12. Prensky, M. (2001). Digital Natives, Digital Immigrants. *On the Horizon*. Vol. 9 no. 5. 1-6.
13. Rusling, David A. (1999).Interprocess Communication Mechanisms. *The Linux Documentation Project* [online]. URL:

http://www.tldp.org/LDP/tlk/ipc/ipc.html. [Accessed on March, 2020].
14. Schreiber, Thorsten. (2011). Android Binder. Android Interprocess Communication. Bochum: University of Ruhr.
15. Shipman, M. (2012). Clickjacking Rootkits for Android: the Next Big Threat?. *The NC State University* [online]. URL: http://web.ncsu.edu/abstract/technology/wms-jiang-clickjack/. [Accessed on March, 2020].
16. Six, Jeff. (2011), *Application Security for the Android Platform.* Newton, MA: O'Reilly Media.
17. Turkle, S., (2013). *La vita sullo schermo*. Milano: Apogeo Education.
18. ***. (2012).Comparison of Dalvik and Java Bytecode. *Forensic Blog* [Online]. URL:: http://forensics.spreitzenbarth.de/2012/08/27/comparison-of-dalvik-and-java-bytecode/. [Accessed on March, 2020].
19. *** (2020). OWASP Mobile Security Project. *OWASP* [online]. URL: https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project__Top_Ten_Mobile_Risks. [Accessed on March, 2020].
20. ***. (2020). Common Vulnerabilities and Exposures - The Standard for Information Security Vulnerability Names. *CVE* [online]. URL:: http://cve.mitre.org/. [Accessed on March, 2020].