PRIVACY AND SECURITY CONFERENCE 2018

PRIVACYANDSECURITYCONFERENCE.PT

Proceedings of the Digital Privacy and Security Conference 2018

17 January 2018 *Porto, Portugal*

Editors
Carla Cordeiro and Hugo Barbosa

UNIVERSIDADE LUSÓFONA DO PORTO

COPYRIGHT

1st Edition 2018

Editors: Carla Cordeiro and Hugo Barbosa

Proceedings Design: Hugo Barbosa

Graphical Design/Website: Hugo Barbosa

E-mail: hugo.barbosa@ulp.pt

Conference Website: http://www. privacyandsecurityconference.pt

Universidade Lusófona do Porto
Rua Augusto Rosa, nº 24
4000-098 Porto – Portugal
Telephone: +351 222 073 230

FOREWORD

ORGANIZING AND SCIENTIFIC COMMITTEES

Digital Privacy and Security Conference 2018 organization and Scientific Committees welcome you to the first conference. The main goal of a scientific event is to discuss, disseminate and create knowledge. Organizing this conference proved to be a challenging opportunity for us to achieve this goal. Regardless of its small size, it demanded our commitment and hard work but also delivered the proudness of seen the successful concretization of our plans. We take this knowledge for our future and believe that every person enrolled with this conference has improved its knowledge.

We are currently living in an information society constantly updated where we believe that hope and more knowledge come from wiser people. In this sense, young students that devote themselves to research deserve our praise for their efforts in the search of new knowledge and better intellectual and technical skills.

Persistence and strong motivation constitute the driving force which stimulates students of Supplementary Networking Course, Informatics Engineering degree, from the Lusofona University of Porto (ULP), to the creation of scientific papers related to this field of study, to the promotion of research, and to the knowledgeable discussion and practical demonstration on a variety of issues addressed, particularly in the context of computer science and computer networks. This has proven to be an exciting challenge. This challenge, which takes the shape of a book, is the natural result of these principles put into practice.

We would like to thank all those authors whose participation in this endeavor contributed to its success, hoping it will promote a better understanding of the issues that were addressed.

Porto, January 2018

Carla Cordeiro and Hugo Barbosa

Conference Committees

ORGANIZING COMMITTEE

Carla Moreira Cordeiro

Hugo Azevedo Barbosa

SCIENTIFIC COMMITTEES

Hugo Azevedo Barbosa

Óscar Ferreira Ribeiro

José Lobinho Gomes

Pedro Strecht Ribeiro

Telmo Silva Morais

Contents

SESSION 1 - Security in Digital Health

Privacy and Security in the Era of Digital Health: Case mHealth..…..…. page 6
Leandro Mendes

Cybersecurity of Social Media: Case in Health Area……...…. page 14
Susana Dias

Privacy and Security Control in E-Health…….…. page 20
Paulo Moura

SESSION 2 - Secure Data Storage

Secure Data Storage of Health Information …….…. page 28
Miguel Fonseca

Securing Data Storage of Cloud Storage...……...…….…. page 34
Diogo Oliveira

Secure on Site Caching of Encrypted Cloud Storage...…….…. page 40
Rui Oliveira

Information Gathering through Image Leaking...…….…. page 45
Rodolfo Matos and Telmo Morais

SESSION 3 - Data Encryption Application

A Data Encryption Application: Development Proposal
Encrypt and Decrypt Several Types of Data ……...…..…. page 52
Nuno Cunha

A Data Encryption Application: Development Proposal
Implementation of the Algorithm AES in an Android Application…...…. page 61
Eduardo Carneiro

SESSION 1
SECURITY IN DIGITAL HEALTH

Privacy and Security in the Era of Digital Health: Case mHealth

Leandro Mendes

Cybersecurity of Social Media: Case in Health Area

Susana Dias

Privacy and Security Control in E-Health

Paulo Moura

Privacy and Security in the Era of Digital Health: Case mHealth

Leandro Mendes

Lusofona University of Porto, Portugal
leandromiguel-@hotmail.com

Abstract. These papers give an overview about the state of health and relation with technology. Then approach digital health and its promises and how privacy and security integrates with it. We then get more specific talking about mHealth. First, we explain how mHealth integrates with digital Health and then we give some suggestion for a successful mHealth implementation, giving implementations examples, relating it again with privacy and security and some possible threats and attacks. We then finish it with some steps on how to protect our data and an overall conclusion of the information contained in the paper.

Keywords: Digital Health, Privacy, Security, Implementation, mHealth, Threats, Attacks.

1 Introduction

The emergence of the computer chip and the rapid technological advances that ensued has enhanced industrialized societies' ability to work and play. Indeed, in the 1970s, technology was hoped to promote a 4-day work week by reducing the physical strain of labor, thus providing more time for leisure. Personal computers (PCs) began to enter homes in the early 1980s, and ownership has increased steadily, nearly 8 of 10 Americans now own a PC. Video game console ownership paralleled PC ownership in homes in the 1980s, and in 2011 approximately €14,5 billion euros was spent on video game hardware. In the mid-1990s, 2 of 10 Americans had personal access to the developing Internet. Now, 7 of 10 Americans have access to the Internet in their homes. However, it is the once-humble cell phone that is now ubiquitous worldwide. In 2011, there were 6 billion cell phone subscriptions worldwide - enough for 87% of the world's population. [1]

Smartphones have a number of characteristics which give them an advantage over other technologies, such as portability, constant internet connectivity, enough computing power to run complex applications and the simple fact that the majority of doctors have one in their pocket. In June 2011, the penetration of wireless devices amongst the United States population was recorded at 102%, meaning that there were more wireless devices than the total population. Whilst smartphones do not account for all wireless devices, it is estimated over 75% of medical staff use a smartphone. [2]

Researchers, practitioners and consumers alike are increasingly embracing mobile technology, cloud computing, broadband access, and wearable devices-effectively removing the traditional perimeter defenses around sensitive data. As a result, security measures to protect this information must be initiated at the source and maintained until the information reaches its intended endpoint-whether it be sensors, apps, research databases, websites, electronic health records (EHR), a patient, or a general population. Health care providers and researchers are now

working with a digital ecosystem of tools, enabled by the Internet, loosely coupled and easy to deploy, that provides powerful capabilities for care delivery and analysis, but along with this comes formidable challenges in protecting the privacy and security of individuals and their information. [3] A new phenomenon we call digital health, and define as the cultural transformation of how disruptive technologies that provide digital and objective data accessible to both caregivers and patients leads to an equal level doctor-patient relationship with shared decision-making and the democratization of care, initiated changes in providing care and practicing medicine. [4] Along in this paper we will get to know more about digital health and privacy and security related to it while getting a bit more specific of matters inside it.

2 Privacy and Security in Digital Health

According to [5], health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data. Security refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.

Digital health is an area of growing interest for physicians, patients, and technology companies alike. It promises the ability to engage patients in their care, before, during, and after an emergency department visit. [6]

It is defined as the convergence of digital technologies and healthcare, is widely promoted for patient engagement. Some digital health tools, such as websites, mobile applications, and personal health monitoring devices, have demonstrated efficacy at improving medication adherence, management of chronic conditions, and patient safety. Studies suggest that digital health is most often used by patients seeking additional information or support. [7]

Most adults are confident in the privacy and security of their medical records, many express concerns regarding sharing of information between providers; a minority report withholding information from their providers due to privacy and security concerns. Whether individuals thought their provider was using an EHR was not associated with negative privacy/security perceptions or withholding, suggesting the transition to EHRs is not associated with negative perceptions regarding the privacy and security of medical information. However, monitoring to see how this evolves will be important. Given that positive health care experiences and higher information efficacy were associated with more favorable perceptions of privacy and security, efforts should continue to encourage providers to secure medical records, provide patients with a "meaningful choice" in how their data are shared, and enable individuals to access information they need to manage their care. [5]

3 Mobile Health

Digital health, including the utilization of mobile health (mHealth) apps and devices, has become popular in the everyday practice of medicine. It has the potential to promote improved patient health outcomes, support care coordination, and improve communication. [8]

3.1 mHealth implementations

The technology aspect of offering mobile apps is usually viewed as a major challenge. However, in practice, technology is most likely to be the least challenging. While confidentiality of data can be addressed through proper regulation and policies, challenges such as market volatility and information technology are of a more serious concern. For a successful implementation, payers should focus on:

User adoption of apps

Access via multiple devices

Identification of user needs

Measurement of user satisfaction

Offering mobile business-to-consumer (B2C) healthcare solutions requires payers to understand consumer mobile devices and mobility habits, and how they change. Healthcare payers must first focus on identifying member needs and goals, and select apps that drive expected outcomes. [9]

For implementation examples are mHealth Clinic Appointment PC Tablet and Frontline health workers.

mHealth Clinic Appointment PC Tablet: The iPad Mini high-definition, 5 mega-pixel, forward-facing built-in camera allows patients to take and send a picture or video to health professionals for assessment (e.g., of an IV site, ostomy site, or other problematic wound or fistula site requiring professional evaluation). The data plan for each iPad Mini is provided at no cost and the iPad Mini is loaned to patients during the study. This data plan provides real-time interactive videoconferencing Polycom RealPresence among multiple health professionals from their offices with IV patients and their family members at home. The iPad Mini has the screen space to accommodate up to six participants simultaneously with each in a “windows,” so all are visible to one another. [10]

Frontline health workers (FHW): Forty-two studies were included in this review. With adequate training, FHWs were able to use mobile phones to enhance various aspects of their work activities. Training of FHWs to use mobile phones for healthcare delivery ranged from a few hours to about 1 week. Five key thematic areas for the use of mobile phones by FHWs were identified as follows: data collection and reporting, training and decision support, emergency referrals, work planning through alerts and reminders, and improved supervision of and communication between healthcare workers. Findings suggest that mobile based data collection improves promptness of data collection, reduces error rates and improves data completeness. Two methodologically robust studies suggest that regular access to health information via short message service (SMS) or mobile-based decision-support systems may improve the adherence of the FHWs to treatment algorithms. The evidence on the effectiveness of the other approaches was largely descriptive and inconclusive. [11]

3.2 Privacy and security challenges of mHealth technology

Mobile health technology has shown the potential to optimize the management of Cardiovascular Disease (CVD) and other chronic diseases by empowering patients through

better health self-monitoring and education. However, several challenges are present when patient's data are utilized and monitored in the healthcare setting. A common issue is the privacy and security of health information. A robust framework and guidelines are already established and utilized in software development for electronic medical record (EMR) systems. For example, the Health Insurance Portability and Accountability Act (HIPAA) guidelines need to be observed when handling healthcare data. HIPAA provides patients with rights to access health information and restrict its use and disclosures. In addition, the Health Information Technology for Economic and Clinical Health (HITECH) act was created to increase the scope of privacy and security protections under HIPAA and to enforce legal liability for non-compliance. [12]

Next we focus on the privacy and security challenges of mHealth technology. Health IT systems face daunting security and privacy challenges due to six recent trends, according to [13]

The locus of care is shifting as the healthcare system seeks more efficient and less expensive ways to care for patients, particularly outpatients with chronic conditions.

Strong economic incentives to keep patient populations healthy, rather than caring for patients only when ill, are motivating healthcare providers to purse innovative prevention plans and treatments of chronic conditions that entail more continuous patient monitoring outside of the clinical setting.

Mobile consumer devices like smartphones and tablets are quickly being adopted by patients, caregivers, and healthcare providers for health and wellness applications in addition to their many other uses, making it difficult to protect sensitive health-related data and functions from the risks posed by general-purpose devices connected to the Internet.

Significant emerging threats target health IT systems, while new regulations strive to protect medical integrity and patient privacy.

Rapid technology advances that enhance mobile devices' utility - for example, computational models that convert wearable-sensor data into measures of addictive behaviors such as cocaine use or smoking - increase the range of potentially private events that can be inferred from seemingly innocuous sensor data.

Healthcare organizations lack the technology and expertise to adequately secure patient data; according to a recent survey, 69 percent of clinicians said their organization did not address demonstrated cyber vulnerabilities in medical devices approved by the US Food and Drug Administration (FDA). [13]

These challenges represent an important part on the security and privacy, and if they are not overcome, some may open doors to attacks and threats.

4 Possible Attacks and Threats

If we don't take privacy and security in mHealth in a serious way there is going to be consequences and irreversible damage. Here it's shown some of the possible attacks and threats that can affect and create a bad impact in mHealth.

Resource depletion (RD) attack: A RD attack attempts to exhaust resources of a mHealth device, such as, battery, bandwidth and storage. This is similar to denial of service (DoS) attacks on the internet, which cause a service or network resource to become unavailable to the intended users. An RD attack can reduce the effective standby time of the glucose sensor from several months to a few hours, which may have serious consequences. To mitigate an RD attack, a mHealth device may adopt a limited authentication protocol instead of an on-demand based communication strategy.

Replay attack: A replay attack attempts to spoof the sensor readings to induce the users or other mHealth devices to make wrong decisions. One way to avoid replay attacks is to introduce timestamps within the message, where one mHealth device only accepts the message from the other device if the timestamp in the received message is within a reasonable time tolerance range.

External Device Mis-Bonding (DMB) attack: A DMB attack targets the mobile gateway running the Google Android Operating System (OS). To tackle this type of threat, an OS-level safeguard mechanism is needed, which require an Android system update from Google, App improvement by developers, as well as mHealth device manufacture enhancements. [14]

Cross-site scripting - XSS: Is a common vulnerability present in web applications. An android user interacts with a Web app through Webview components as graphical user interface. Webview is vulnerable to attacks with malicious code.

SQL Injection: An intruder inserts new SQL keywords into a SQL instruction. Consequently, the instruction logic changes.

Hijacking and Spoofing Intents: This vulnerability occurs when a malicious service intercepts intent meant for a legitimate service. Consequently, in order to steal data supplied by the user (i.e., phishing), it leaves a connection between the application and the malicious service.

Sticky broadcast tampering: This vulnerability is characterized by persistent intents of communication from legitimate mobile apps that can be accessed and removed by malicious mobile apps.

Freak - SSL/TLS vulnerability: Is a weakness in some implementations of SSL/TLS.

Heartbleed Bug: Is the most popular OpenSSL library vulnerability that enables to steal protected information that is encrypted under SSL/TLS protocols.

Insecure storage: Stored data without digital encryption and that is accessible from a mobile application can be converted in an objective for the attackers.

SSL - stripping: Is a type of vulnerability that enables to an intruder performs an attack man in the middle. [15]

5 How to Protect Mobile Data

There’s never too much we can do when we are talking about protecting our data, especially when it comes to health-related matters. They are some measures we can take to make sure our information doesn’t go to wrong hands and compromise other people’s life’s, here we focus more on mobile.

One of the easiest steps you can take to protect your health information on your phone is using a password or pin to unlock it, and making sure it auto locks after some period of inactivity. You can also add fingertip authentication to make the process even more complex. These options are located on the security tab, view figure 1.

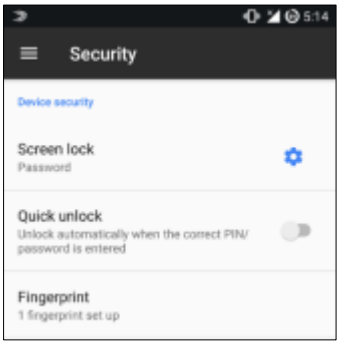

Fig. 1 - Screen lock and fingerprint example

A second step you can take is to encrypt the data on the mobile phone (figure 2), in that way you make sure the data is not viewed by other people. Most phones have and in-built option that allows to do the process as shown on my phone. Once again, this option appears in the security tab.

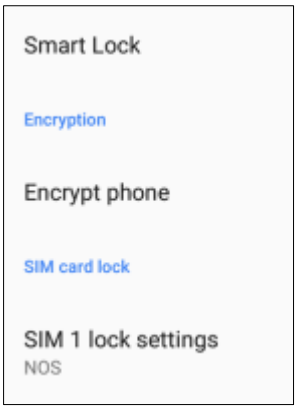

Fig. 2 - Encryption example

You can also lose your phone making the data inside it vulnerable. Some phones come with inbuilt apps that allow you to see remotely where your phone is and even block it with another pin and erasing all the data inside it (figure 3). Below is a picture of the desktop browser for my phone that allows me to find me device, after clicking it I can do all the options referred above and even making it play an alarm, so I can hear it if it's close to me.

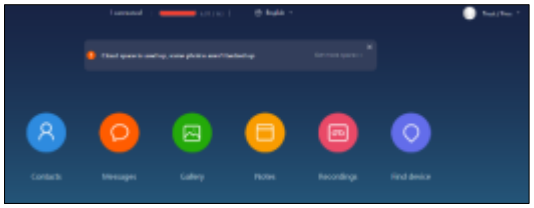

Fig. 3 - Remote access example

We should never use password free/unsecured networks to access our health data as other people connected can see it. When using public networks, we should use a VPN or a secure browser connection to make sure our data is not accessed by others (figures 4 and 5).

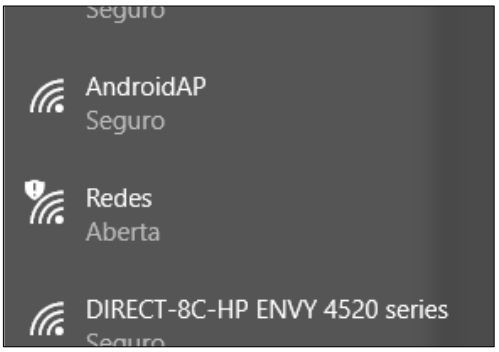

Fig. 4 - Unsecured Network example

Fig. 5 - VPN Example

6 Conclusions

The world is in constant shifting and in a few years, we will become more advanced and create more devices capable of satisfying our needs, we conclude that more technology will be part of our health-related information. Most aiming to make that information more user friendly easier to access but we can see that by doing that we are put our information more exposed to others. Digital health promises to make that connection, but it also needs to promise to that our privacy and security isn't always put at risk. There's the need of creating pilot projects or other type of ideas such as experimental studies that can test and show us the venerability of certain systems before they get in use and compromise the information.

Mobile health comes as a part of digital health and includes all the problems referenced above, showing that there's all the need of knowing the type of threats and attacks we can face, as that's the best way to create a defense.

All of this needs to be take in consideration not only by companies making apps and services to accommodate people but also by the user itself, because in the end he's the one that gets the most damage out of all this.

In this moment in time people always need to ask themselves if they want their life easier by compromising information that can put their life at risk. And if that's not the case they should get to know how they can protect their data, by self-initiative or by following the tips I gave in this paper, or any other mean such as dedicated lectures on the matter that can help them keep their information save.

References

1. Gradisar, M.; Wolfson, A. R.; Harvey, A. G.; Hale, L.; Rosenberg, R.; Czeisler C. A.: "The Sleep and Technology Use of Americans: Findings from the National Sleep Foundation's 2011 Sleep in America Poll", Journal of Clinical Sleep Medicine, vol. 9(12), pp. 1291-1299, (2013).
2. Perera, C.: "The Evolution of E-Health - Mobile Technology and mHealth", Journal MTM vol.1(1), pp.1-2, (2012).
3. Filkins, B. L.; Kim, J. Y.; Roberts, B.; Armstrong, W.; Miller, M. A.; Hultner, M. L.; Castillo, A. P.; Ducom, J. C.; Topol, E. J.; Steinhubl, S. R.: "Privacy and Security in the Era of Digital Health: What Should Translational Researchers Know and do About It?", American Journal of Translational Research, vol.8(3), pp. 1560-1580, (2016).
4. Meskó, B.; Drobni, Z.; Bényei, E.; Gergely, B.; Győrffy, Z.: "Digital Health is a Cultural Transformation of Traditional Healthcare", mHealth, vol.3(38), (2017).
5. Patel, V.; Beckjord, E.; Moser, R. P.; Hughes, P.; Hesse, B. W.: "The Role of Health Care Experience and Consumer Information Efficacy in Shaping Privacy and Security Perceptions of Medical Records: National Consumer Survey Results", JMIR Medical Informatics, vol.3(2), (2015).
6. Birnbaum, F.; Lewis, D. M.; Rosen, R.; Ranney, M. L.: "Patient Engagement and the Design of Digital Health", Academic Emergency Medicine Journal, (2015).
7. Ranney, M. L.; Duarte, C.; Baird, J.; Patry, E. J.; Green, T. C.: "Correlation of Digital Health Use and Chronic Pain Coping Strategies", mHealth, vol.2(35), (2016).
8. Ichikawa, D.; Kashiyama, M.; Ueno, T.: "Tamper-Resistant Mobile Health Using Blockchain Technology", JMIR Mhealth Uhealth, vol.5(7), (2017).
9. Modi, K.; Mohanty, R.: "M-Health: Challenges, Benefits, and Key to Successful Implementation", Infosys.com, India, (2017).
10. Smith, C. E.; Spaulding, R.; Piamjariyakul, U.; Werkowitch, M.; Yadrich, D. M.; Hooper, D.; Moore, T.; Gilroy, R.: "mHealth Clinic Appointment PC Tablet: Implementation, Challenges and Solutions", Journal of Mobile Technology in Medicine, vol.4(2), pp. 21-32, (2015).
11. Agarwal, S.; Perry, H. B.; Long, LA.; Labrique, A. B.: "Evidence on Feasibility and Effective Use of mHealth Strategies by Frontline Health Workers in Developing Countries: Systematic Review", Tropical Medicine & International Health, vol.20(8): pp. 1003-1014, (2015).
12. Lobelo, F.; Kelli, H. M.; Tejedor, S. C.; Pratt, M.; McConnell, M. V.; Martin, S. S.; Welk, G. J.: "The Wild Wild West: A Framework to Integrate mHealth Software Applications and Wearables to Support Physical Activity Assessment, Counseling and Interventions for Cardiovascular Disease Risk Reduction", Progress in Cardiovascular Diseases, vol.58(6), pp. 584-594, (2016).
13. Kotz, D.; Gunter, C. A.; Kumar, S.; Weiner, J. P.: "Privacy and Security in Mobile Health: A Research Agenda", Computer (Long Beach Calif) Journal, vol.49(6), pp. 22-30, (2016).
14. Machado, L.O.; Wang, S.; Wang, X.; Iranmehr, A.; Jiang, X.: "Privacy, Security, and Machine Learning for Mobile Health Applications", American Association for the Advancement of Science, (2017).
15. Cifuentes, Y.; Beltrán, L.; Ramírez, L.: "Analysis of Security Vulnerabilities for Mobile Health Applications", International Journal of Health and Medical Engineering, vol.9(9), (2015).

Cybersecurity of Social Media: Case in Health Area

Susana Dias

Lusofona University of Porto, Portugal
susana.filipa.dias@hotmail.com

Abstract. Cybersecurity has become a prime concern in the present society. Social media has emerged as a newer form of media through which people can communicate with each other's. The impact of social media now a day is extremely significant. Therefore, the same is being used in almost every walk of life. Though, it provides so much ease to the users but it also needs to be controlled. The monitoring of social media has become significant especially when people do not understand the repercussions of their acts. It has been observed recently that people have started using social media for malicious activities too. Scores of criminal acts have been registered which was done with the help of social media. Therefore, monitoring or scrutiny of what people are doing on social media has become indispensable. This article aims to deliberate and discuss the topic of cybersecurity and social networks, properly referring to information destined to the senior's rehabilitation with regard to an essential case in health.

Keywords: Cybersecurity, Social Media, Rehabilitation, Health

1 Introduction

Currently in society, the concept of social networks makes us realize the configuration of the interpersonal relational degree itself and contributes to recognition as a subject, to the construction of identity, to the feeling of well-being, belonging and autonomy. [1]

The priority is social reintegration and strengthening the union of users, offering support and encouragement in the search for the construction of autonomy and citizenship. [2]

The electronic social networks based on the Internet represent models of this type of expression of the subject involved by the contemporary hypermodern, since in them the transformations are developed, involving, as an example, the simultaneity of the experiences that characterized the collective uses of the electronic networks before the rise of as shown in figure below. [3]

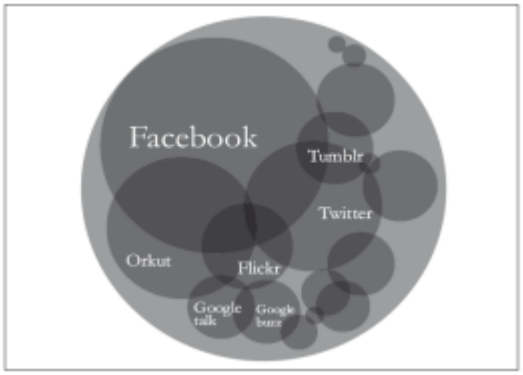

Fig. 6 - Model of interactions between users and social networks

With the Internet as a means of connecting us globally as never before in history, privacy, image rights, and other precautions are crucial. It is always recommended that social network users be aware of the risks they are having when they disclose too much information about themselves. These risks include exposure to identity theft, blackmail; loss of rights over shared content, and, in extreme cases, risks of harassment or physical assault. [4]

Protection against these hazards is essentially the safest form of disclosure of personal data. Any information that identifies the person (address, place of work, school or contact) should be restricted to the smallest number of users. [5]

This is why society is finding itself increasingly dependent on communication and information technologies, the space created by these technologies known as cyberspace. [6]

2 Cybersecurity in Industries

Throughout the history of mankind man has continuously adapted his way of life in function of the technology that he has, as defined "man is man and his circumstance". [7]

As civilization evolves to grow increasingly connected through the inevitable ubiquity of technology, securing systems, networks and data on which we rely on has become paramount. Cybercrime is a major threat for economics, individual safety and even the public in general, as it is a primary medium for terrorism. [8].

In fact, the 2016 Internet Organized Crime Threat Assessment by Europol, reports an increasing acceleration of cyber criminality to such a level, that for some EU countries, it has surpassed traditional crime. Assisting a growing range of threats, from human trafficking to terrorism. [9]

Day by day, more and more devices gain access to it, including Wi-Fi in restaurants, coffees, buildings, schools, hospitals, transports. The more development we see, the more unsafe we are.

In order to avoid being attacked one must initially understand the enemy, identify him and analyze the way he attacks. Then reduce existing vulnerabilities, constantly improving defensive barriers and finally be ready to take the initiative in counter-offensive actions. [5]

Therefore, as a form of communication between computers and other servers, it is fundamental to understand how all information is recorded, for processing and analyzing the final results. The so-called computer networks have become, say, the "roads" of information for the way of information exchange and sharing of information. [10]

As one of the objectives submitted within social networks, we have the use and sharing of information, depending also on its severity and in turn, the capacity of individuals, groups and organizations of sharing, leading to mobilization and collective action in social networks. [10]

2.1 Social network as communication channel

Faced with the processing and transfer of information, the impact on the web influences the process of cognition where they create, divulge and share impostures and not truths. Faced with this reality, it is important to reflect on the limits of information technologies, that is, when they cease to act for the benefit of individuals, causing them problems, transforming them into objects. [11]

The social network, Facebook, is experiencing a vertiginous growth already counting on 1.32 billion active users, who make use of it at least once a month. Of this significant number, 62.2% access the social network daily, which corresponds to 829 million logins. For these data it is possible to affirm that we are facing a society of real-life commentators who, with the popularization of mobile phones, should increase these values considerably. [11]

The first piece of information presented to those surveyed has as a reference: Three investigators of the 9/11 attacks died on the same day. This rumor surfaced in February 2015 three journalists who would be involved in the investigations into the attacks on the Twin Towers in the United States, realizing that they would have died with a few hours difference and the causes of the deaths would not have been disclosed.

The result obtained on this information which is false is recorded in the table below. [12].

About the above news you evaluates how:		If you found this new in your Facebook Timeline:	
True new	**45,5%**	enjoy	**14,9%**
		comment	**7,1%**
False new	**45,5%**	share	**9,7%**
		ignore	**68,2%**

Tab. 1 - Result obtained on false information

Observed that a value of 45.5% evaluates the news as true and 9.7% would share the false information, while 14.9% would enjoy it and 9.7% would comment. Although little more than half of people have agreed that it was more false information spread on a social network and most would ignore such information, it is noted that there is a high number of people who have it as true.

In the face of what has been revealed, what causes concern is that, unlike other times, today information sharing is immediate, turning social networks into a "heap of falsehood." The information, sometimes untrue and futile, is internalized and shared by its users without the process of reading, understanding and contextualization and in-depth research. In this sense, the debate on the role of information technology must be resumed since the role of the issuer in some cases is no longer to modify the structure of a receiver's image to change society. [12].

3 Health Area: Rehabilitation Example

The number of elderly people in the world's population is increasing significantly. The number of people 60 years of age and over has been projected to reach approximately 700 million by 2009 and 2 billion by 2050. [13]

Rehabilitation is a set of measures that help individuals achieve and maintain optimal functioning in the interaction with their environments. "Sometimes a distinction is made between habilitation, which aims to help those who have acquired congenital or early life impairment to develop maximum functioning; and rehabilitation, where those who have experienced a loss of function are assisted to regain maximum functioning. [14]

For this main reason, the elderly are people with increasing difficulty in debilitation, in the actions of their daily life, no one lives and grows to new.

Thus, rehabilitation can be understood as a process of optimizing health and safety opportunities for individuals, with the simple aim of improving their quality of life. Thus, it aims at helping to improve physical, mental and financial health up to the most advanced years, with a reasonable support for political powers, with a concern for the elderly part of society. [15]

Rehabilitation provided over a range of care time, from hospital care to community rehabilitation [15], can improve health outcomes, reduce costs by reducing hospital needs [16], reduce disability, and improve quality of life. [17]

3.1 Cybersecurity in the technologies of the rehabilitation process

Global cybersecurity has been increasing in our society, and represents a variety of threats at the level of companies, individuals or governments. The evolutions of the technologies have led to an increase of the social networks, accentuated in recent times as a result of the development of the technology.

In the United States, a study has shown that users of assistive technologies, such as mobility aids and personal care equipment reported, have less need for support services [16].

The areas of processing and manipulation of digital images are increasingly used by individuals or criminal organizations, involving illegal activities related to the falsification of documents, mainly security documents. There are many different digital techniques to produce fake documents, for example, rewrite, copy, paste. [18]

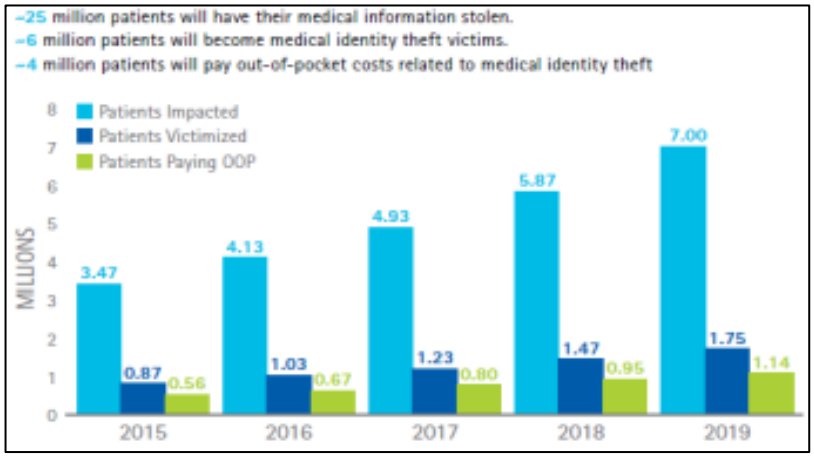

Fig. 2 - Data of medical and personal information theft due to healthcare provider data breaches

According to the Ponemon Institute[1], these financial losses may take several forms. Not fully understanding their medical bills, some victims have unwittingly paid bills run up by others. Some have had to reimburse their insurers for healthcare services obtained fraudulently. Many have incurred substantial legal costs as they have sought to unravel the cybercrimes perpetuated

[1] Ponemon Institute conducts independent research on privacy, data protection and information security policy.

against them. In fact, 65 percent of victims of medical identity theft pay Out-of-pocket (OOP2) costs at an average of $13,500 per victim, and are patients after 60 years. Accenture projects that 25 percent of patients impacted by healthcare provider data breaches between 2015 and 2019.

More than 6 million people will subsequently become victims of medical identity theft. Sixteen percent of impacted patients, more than 4 million people, will be victimized and pay out-of-pocket costs totaling almost $56 billion over the next 5 years. [19]

Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. This vulnerability increases as medical devices are increasingly connected to the Internet, hospital networks, and to other medical devices. [19]

It's important the relevance the way health services advocate seniors' patients care and guidance, suggesting the implementation of policies for early intervention in their way physical behavior is established within the organization. [20]

Security, privacy, and attack-free communication can lead to an optimal and realistic healthcare system. To ensure attack-free communication in remote healthcare systems, there must be some countermeasures to protect the data and detect any intrusions in the human personal data during wireless communications in healthcare systems. Similarly, the physiological values also change in the case of an emergency. There should be some measure or technique to detect these changes in the physiological values during an emergency to provide an early response to the user of the system. [20]

Healthcare providers will pay a heavy price for cyber security complacency. A case study revealed almost half of seniors' patients said they would find a different provider if they were informed that their medical records were stolen. Taking into account the estimated lifetime economic value of a patient, Accenture analysis shows that healthcare providers are at risk of losing billions in cumulative lifetime senior's patient's revenue over the next years due to patients switching providers because of medical identity theft and shared data between patients. [21]

To prevent revenue loss on this scale, healthcare providers must prioritize improvements of their cybersecurity in order to thwart attacks that aim to steal patient data from clinical and financial systems. [22]

4 Conclusion

The proximity of technologies to rehabilitation has been accentuated in recent times as a result of technological development. Today our society is in transformation, with the growing influence of existing technology. People increasingly focus their attention on new technologies, exposing themselves by sharing personal information and confidential data, making them more and more accessible to attack. After you connect to the Internet, you lose your 100% safety humanity evolves rapidly as the growth of public accessible knowledge has been greatly nurtured and facilitated.

The contribution of this paper depicts several studies referring to resources and information that currently people are constantly attacked, more precisely a case in the area of health

rehabilitation of older people, namely sharing of data between patients and therapists, or even falsification of medical processes.

The various existing studies as new contributions are intended to be a medical platform capable of supporting the safe and effective communication between patient and the patient to care in the medical process, facilitating a better rehabilitation with evolution data, without lack of security. By searching more, you collect more info, and you also can protect yourself even more, because like we defend, you are never safe.

References

1. Sluzki, C. E.: "A Rede Social na Prática Sistêmica: Alternativas Terapêuticas", São Paulo (1997).
2. Lancetti, A.: "Contrafissura e plasticidade Psíquica", São Paulo, Hucitec, (2015).
3. Scolari, C.: "Hacer Clic: Hacia una Sociosemiótica de las Interacciones Digitales", Barcelona, Gedisa, (2004).
4. CERT Homepage, accessed on December (2017).
5. Tzu, S.: "The Art of War: e-artnow", 2nd edn. Publiser, (2012).
6. Tornatzky, L. G; Fleischer, M.: "The Process of Technological Innovation", Lexington Books, (1990).
7. José Ortega y Gasset, Book, Madrid (1967).
8. Wenke L.; Rotoloni, B.: "Emerging Cyber Threats, Trends and Technologies", Technical Report, Institute for Information Security and Privacy, (2016).
9. Europol: "Internet Organized Crime Threat Assessment", Technical Report, Europol, (2016).
10. Tanenbaum, A. S.; Steen, M. V.: "Distributed Systems Principles and Paradigms", Pearson International Edition, (2007).
11. Toutain: "Designing Fictions: Literature Confronts Advertising", Montreal, (2007).
12. Canaltech, Homepage, accessed on December, (2017).
13. Department of Economic and Social Affairs: "World Population Prospects The 2008 Revision" vol.1: "Comprehensive Tables", New York, NY, (2009).
14. The National Board of Health and Welfare: "Swedish disability policy: services and care for people with functional impairments: habilitation, rehabilitation, and technical", Stockholm, (2011).
15. Stucki, G.; Reinhardt, J. D.; Grimby, G.: "Organizing Human Functioning and Rehabilitation Research into Distinct Scientific Fields", vol.2: "Conceptual descriptions and domains for research, Journal of Rehabilitative Medicine", European Board of Physical and Rehabilitation Medicine, (2007).
16. Rauch, A.; Cieza, A.; Stucki, G.: "How to Apply the International Classification of Functioning Disability and health (ICF) for Rrehabilitation Management in Clinical practice", European Journal of Physical Rehabilitation Medicine, (2008).
17. Davies, E. J.: "Exercise Based Rehabilitation for Heart Failure", Cochrane Database of Systematic Reviews, Online, (2010).
18. Farid, H.: "Image Forgery Detection", in IEEE Signal Processing Magazine, pp. 16-25, March (2009).
19. Schwartz, S. B.: "FDA's Role in Medical Device Cybersecurity" (October 31, 2017).
20. Jansen, M. D.: "Mental Health and Family Structure Master's Dissertation", Institute of Psychology, (2007).
21. "Companyewsroom Portugal", accenture.com, accessed on November, (2017).
22. "Company News Release Accenture Security Study", accenture.com, accessed on November (2017).
23. Malan, D.: "Sensor Network Infrastructure for Emergency Medical Care", International Workshop on Wearable and Implantable Body Sensor Networks, pp. 12-14, April (2004).

Privacy and Security Control in E-Health

Paulo Moura

Lusofona University of Porto, Portugal
teigal@hotmail.com

Abstract. Privacy and security control in electronic health is a complex process. In the course of the article, advantages and disadvantages will be presented regarding user registration methods (traditional and electronic) and additional information about Electronic Patient Record (EPR). To protect patient data and ensure patient privacy, it is necessary to create protection mechanisms. Communication between institutions should be done using international standards in order to create a general understanding on both sides as well as the Health Level 7 (HL7) standard. However, just like everything connected to the Internet, there are several security holes on the platforms regarding patient data records.

Keywords: Privacy, Security Control, E-Health, Authentication, Privacy Policy, EHR, EPR, HL7.

1 Introduction

With the passing of the years, technologies are increasingly developed and complex, there is an increasing need to use these technologies since they provide certain advantages and make various tasks more practical in people's daily lives.

In the health sector, technology is increasingly a fundamental and indispensable factor to perform several necessary actions and greatly facilitates the work of health professionals. Nowadays, with the emergence of intuitive operating systems and interfaces, there has been an exponential growth of computer applications in the health sector, such as EHR, where health information is stored electronically, in other words, there is no traditional paper method and pen. This platform has many advantages over the previously used method, but clinical information systems must guarantee: Confidentiality, integrity, privacy and authenticity through the protection mechanisms.

However, these electronic health systems need security / protection mechanisms, since sensitive information circulates in order to protect users' data. In order to have interoperability between health information systems, international standards have been defined, such as: HL7, CEN TC251, CorbaMed, DICOM (Digital Imaging and Communications in Medicine), OpenEHR (Open Electronic Health Record) and the TISS (Supplementary Health Information Exchange), in order to create an organized communication through a set of rules in each standard.

Security at EHR is a crucial concern, confidentiality, integrity and availability are second-only information security attributes, however there are flaws in this platform. [1] [2]

2 Traditional Method Data Record

Nowadays, with the development of new technologies, the traditional method of registration of users has been increasingly set aside. Over the years, different methods of registration have been adopted, from the paper and pen method to the computer method with the aim of improving the health care provided to the citizen, increasing the productivity of professionals in the area, reducing administrative costs and service, however, it is necessary to ensure the privacy and integrity of your clinical data. [3]

In the traditional method there is a greater disorganization since the records of a patient were made in different sheets and there is also a greater probability of loss of information and fragility of the paper. With this method there was a bad use of time of the consultation due to the delay in the filling of the papers and sometimes with incorrect fillings; the information was difficult to access, unscientific and incomplete. Finally another problem of this method is the illegibility of the records, due to the calligraphy of health professionals and data redundancy.[2][4]

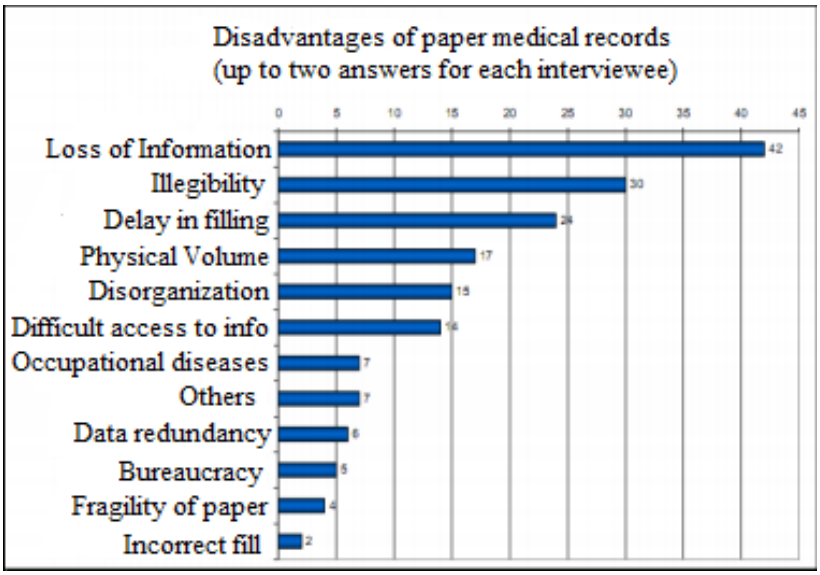

Fig. 1 - Disadvantages of traditional method [7]

3 Electronic health record systems

With the emergence of the Internet, Health Information Systems (SIS) has undergone changes that have improved some functionalities and ways of using them. These include telemedicine, which helps rural communities to have specialized medical care.Another improved aspect is the exchange of information between professionals about a particular patient. However this system may have privacy and interoperability failures due to lack of standards.

Given the way information is shared and its type, we can classify Electronic Health Record Systems (EHRS) into four categories [2]:

EPR - this is the main part of any category of EHRS, which covers simpler systems and is directed only to medical record per se.

Electronic Medical Record (EMR) - in addition to the EPR, contains features aimed at managing administrative information.

EHR - this is a complement to the EMR as it adds communication functions between health institutions.

Personal Health Record (PHR) or Personal Health Systems (PHS) - the information present in the EPR for users is made available online. Medical information is the responsibility of each patient.

We can define EPR as a computerized record of the patient's health and illness where all the information (personal data, previous illnesses, allergies, life habits, family history, used medications, immunizations, etc.) will be integrated into a support system the decision.

EPR increases the quality of health care in the course of new applications and resources and also helps with physician follow-up. However, in spite of the advantages it also presents some disadvantages which will be enumerated in the following table: [2]

Benefits	Disadvantages
Comprehensiveness	Need for large investments (hardware, software)
Remote and simultaneous access	Poor training of EPR users
Legibility	System failures
Patient data security	Difficulty in collecting complete patient information
Confidentiality of patient information	Reduced mobility, since paper files can be transported anywhere
Integration with other Information Systems	Less freedom in the style of the report
Continuous data processing	Requires specific training
Research assistance	Increase in the working time of professionals
Constant updating of data	Negative impact on the patient-physician relationship
Rapid access to patient history	Fear of professionals exposing their clinical behavior / Loss of autonomy
Improvement in the quality of care	Misuse compromises the reliability and safety of patient data
Systematic, clear and objective organization of information	Maintenance of data confidentiality

Tab. 1 - Advantages and Disadvantages of EPR [2] [5]

3.1 Mechanisms of protection

Since user's information is circulated through a variety of platforms, it is necessary to protect user's personal data in a way that guarantees privacy. There is a sharing of resources and data across the network between various institutions hence the importance of ensuring a set of security features in the communication and sharing of data between health systems, such as[2][3]:

Confidentiality: method of protecting data / information so that it is not viewed indiscriminately - guaranteeing professional secrecy.

Authentication: method of verifying the identity of a person - use of passwords and periodical exchanges within a maximum period of 60 days.

Authorization: consists in granting an identity authorization to a list of rights, privileges, or access areas.

Audit: method of ensuring that the activities of an identity are properly registered and can be reviewed to detect suspicious events / errors - information system must have log of events.

Integrity: how to ensure that information / data are not altered by unauthorized identities.

Non-repudiation: process of when someone cannot deny the authenticity of a document, its signature and its sending. Availability: corresponds to the availability of the system for the authorized identities. Backup: should be performed every 24 hours - backup.

It is necessary to ensure these safety features as there is an exposition of sensitive information in health systems, focusing on global security policies that offer a willingness to reduce risks and promote the availability of clinical information, integrity and confidentiality. More technically, the use of strong authentication mechanisms such as biometric techniques should be induced. As such, the use of a smart card as a professional ID card helps with regard to the level of access control: so the card would be non-transferable and cancellation of the card could be done at any time; if for some reason the user left his job, he would have to be accompanied by his card, so logout would be inevitable and automatic. The Professional Identification Card would also have to cover RFID (Radio Frequency Identification) technology, so as to make its use extremely pleasant since the health professional would not need to remove it from its attachment site. In terms of infrastructure, the use of strong cryptographic systems, firewalls and organizational measures such as continuous training of users, user profiles, permissions management and access rules) would increase confidence in the security of the system. It is also recommended to double the central equipment (redundancy mechanisms) and periodic inspections (electrical, physical and computer). [6]

Fig. 2 - RFID technology

The privacy and security of medical informatics include other methods such as: implement access controls based on roles and privileges so that only a few employees have access to relevant patient information; encrypt the databases to ensure that third parties do not access the information and ensure minimum sharing and disclosure by means to ensure that only necessary information is shared and shared. [7]

3.2 International standards

According to the International Standards Organization (ISO), the standard is defined as: a document established by consensus and approved by a recognized group that establishes, for general and repeated use, a set of rules, protocols or process characteristics, with the purpose of ordering and organizing activities in specific contexts for the benefit of all. [2]

In order to facilitate communication among the various identities that have access to information, it was necessary to define a common vocabulary for registration and also to make the communication obey a set of rules shared by all, especially in the area of health that is where it exists vocabulary and concepts.

With the existence of standardization there is a greater facility in obtaining information for epidemiological studies and definition of health policies; an improvement in communication between various entities; an ability to perform cost-benefit analysis of investments in health; a possibility of comparison and analysis of institutional performance and an automatic transfer of information in the network. Currently some of the existing standards in the health area are: HL7, CEN TC251, CorbaMed, DICOM, OpenEHR and TISS. [2]

3.2.1 HL7

In order to exchange information, a common set of rules is necessary, but a middleware that uses an international standard is designed to enable interoperability between health systems.

HL7 is a system that adopts the client-server architecture, in other words, there is a server that is named HL7Server and a group of clients.

The HL7Server is the system responsible for handling health information and has competencies such as: processing instructions, performing operations in the database; sending an HL7 message with the processing response performed and receiving HL7 messages over the Intranet / Internet.

Regarding the part of the customers, these are represented by desktop and also medical devices that send messages according to the HL7.

According to this standard, to send messages, a client system must carry out the following steps:

- Compose an HL7 message with the desired request (add in an XML file the data that must be retrieved or sent according to the HL7 standard specification);
- Send the message to the server (HL7Server) via computer network;
- Wait for a reply message;
- Extract the information from the message returned by the HL7Server.

Through the exchange of messages used by the middleware, it is possible to share patient information in order to improve security in the Telemedicine Portal System. [1]

This standard has many advantages, namely:

• Established syntax and vocabulary;
• Developed messaging standards;
• Supports communication protocols such as TCP (Transmission Control Protocol) / IP (Internet Protocol) and HTTP (Hypertext Transfer Protocol);
• Data sharing security;
• ANSI Standard (American National Standards Institute);
• Many medical devices may receive or transmit information through the HL7 standard; and
• Use of the standard in most health applications.

Tab. 2 - Advantages of HL7

3.3 EHR security breaches

Security in EHR is an important issue; however there are several incidents of security breaches. Some examples of failures: a hacker infiltrated the University of Washington computer medical center and stole at least 5000 patient records on cardiology and rehabilitation medications; patient records at the University of Michigan Medical Center were left exposed to the public on the Internet because the server was supposed to be password protected; a Florida public health official brought home a hard drive bearing the names of 4,000 people with HIV (Human Immunodeficiency Virus) and sent the names to two Florida newspapers; and a hacker exposed the vulnerabilities of the computer system because he was able to enter a medical center in New York and another in the Netherlands.

If a patient's information is disclosed accidentally or involuntarily, it may establish a privacy violation, ruin the patient's career, terminate the job and even financial loss. [8]

4 Conclusion

The privacy and security of information in electronic health is a dynamic issue as the pace of technological change continually creates challenges for security policies. However, there is a need to protect the privacy of the patient and he / she must trust the institutions he / she attends and keeps his or her personal data.

Just like any system that is connected to the Internet, it is not possible to say that a certain health system is totally safe; there will always be possibility of attacks even with constant updates of safety standards and norms. But an important aspect that must also be taken into account is the physical security of the system's equipment in order to make the system as safe as possible.

References

1. Petry, K.: “Modelos para Interoperabilidade de Sistemas Hospitalares Utilizando Padrão HL7”, Federal University of Santa Catarina (2005).
2. Vanderlei, I.: “Um Modelo para Controle de Privacidade em Sistemas de Registo Eletrônico em Saúde”, Federal University of Pernambuco, Doctoral Thesis (2014).
3. Bezerra, S.: “Prontuário Eletrónico do Paciente: Uma Ferramenta para Aprimorar a Qualidade dos Serviços de Saúde”, vol.1(1), pp. 73-82 (2009).
4. Leal, M.: “Avaliação da Qualidade do Registo Clínico Eletrónico”, University of Minho, Master's Dissertation (2013).
5. Canêo, P.; Rondina, J.: “Prontuário Eletrônico do Paciente: Conhecendo as Experiências de sua Implantação”, Journal of health informatics, vol.6(2), pp. 67-71 (2014).
6. Araújo, S.: “Segurança na Circulação de Informação Clínica”, Faculty of Engineering, University of Porto, Master's Dissertation (2007).
7. Policy Engagement Network: “Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations”, pp. 1-28 (2010).
8. Win, K.: “A Review of Security of Electronic Health Records”, Health Information Management, vol.34(1), pp. 13-18 (2005).

SESSION 2

SECURE DATA STORAGE

Secure Data Storage of Health Information

Miguel Fonseca

Securing Data Storage of Cloud Storage

Diogo Oliveira

Secure on Site Caching of Encrypted Cloud Storage

Rui Oliveira

Information Gathering through Image Leaking

Rodolfo Matos and Telmo Morais

Secure Data Storage of Health Information

Miguel Fonseca

Lusofona University of Porto, Portugal
miguelfonseca9626@gmail.com

Abstract. In this work, we have an examination of the evolution of the health information and how its data storage is done now. It addresses some questions about health information privacy, security and data confidentiality rules. We talk about the current storage information systems, as well as the possibility of storing health information data in the cloud. We also show some important rules to keep safe the health information data and some requirements that lead to the good practice of safe data information storage. We talk about nowadays storage information systems as well. We understand that with the evolution of technologies and for the good of the population it's important to continue finding new solutions every day to keep the health information safe. Another reason to keep creating new solutions is the fact that population is increasing, and the new generation deals with technology every day.

Keywords: Health Information, Privacy, Security, Data Confidentiality, Data Storage.

1 Introduction

The adoption of health information systems is seen worldwide as one method to mitigate the widening health care demand and supply gap. [1] As healthcare organizations continue the path toward total digital operations, a topic often raised but not clearly understood is that of computer security. The reason for this is simply the vastness of the topic. Computers and networks are complex, and each service offered is a potential security hole. [2]

To understand the complexities of the emerging electronic health record system, it is helpful to know what the health information system has been, is now, and needs to become. The medical record, either paper-based or electronic, is a communication tool that supports clinical decision making, coordination of services, evaluation of the quality and efficacy of care, research, legal protection, education, and accreditation and regulatory processes. It is the business record of the healthcare system, documented in the normal course of its activities. The documentation must be authenticated and, if it is handwritten, the entries must be legible. [3]

In the past, the medical record was a paper repository of information that was reviewed or used for clinical, research, administrative, and financial purposes. It was severely limited in terms of accessibility, available to only one user at a time. The paper-based record was updated manually, resulting in delays for record completion that lasted anywhere from 1 to 6 months or more. Most medical record departments were housed in institutions basements because the weight of the paper precluded other locations. The physician was in control of the care and documentation processes and authorized the release of information. Patients rarely viewed their medical records. A second limitation of the paper-based medical record was the lack of security. Access was controlled by doors, locks, identification cards, and tedious sign-out procedures for authorized users. Unauthorized access to patient information triggered no alerts, nor was it known what information had been viewed. [3]

The personal health information contained in the patient record, regardless of its form, requires adequate protection. Empirical, anecdotal evidence and survey results demonstrate that security incidents are increasing even as organizations progressively invest in technology-based solutions. These incidents are controlled through security measures operating within an information security management system. However, the user is key. The security of healthcare data does not only involve the application of technical controls and procedures. Healthcare professionals, as the users, are the most significant threat, who due to their ignorance or mistakes may jeopardize this data. They are aware of the importance of being security compliant but do not practice it. [4]

The author [5] gave a lecture on the past, present, and future of hospital information systems. In the meantime, there has been a tremendous progress in medicine as well as in informatics. One important benefit of this progress is that our life expectancy is nowadays significantly higher than it would have been even some few decades ago. This progress, leading to aging societies, is of influence to the organization of health care and to the future development of its information systems.

1 Privacy, Security and Data Confidentiality

Most people are familiar with common types of computers security breaches - those caused by computer viruses, Internet hackers, and the loss or theft of laptops containing sensitive data. But concerns about security also extend to the computers embedded in sophisticated medical devices, which have become increasingly complex and often rely on intricate software and extensive automated functionality. Many devices perform complex analyses, have sophisticated decision-making capabilities, store detailed personal medical information, and communicate automatically, remotely, and wirelessly. These features have provided improved care and quality of life for millions of patients, but they also have created a susceptibility to security breaches that could compromise the performance of such devices and the safety and privacy of patients. Appropriate security of medical devices should ensure reliable, secure communication and continued functionality while preserving patients' safety, confidentiality, and data integrity. Though there is nearly universal agreement on the importance of security for personal health information and electronic health records, there is disagreement over the security requirements for medical devices, and the manufacturers have a legal responsibility to be vigilant and responsive to security threats. [6]

There is discordance between an information security culture and the medical culture. There appears to be a lack of understanding about the importance of security. It is pertinent to understand an information security culture and its antecedent, information security behavior. Information security behavior is viewed from a variety of perspectives. It is seen by many authors as a function of organizational culture which is extended, by a variety of interventions, to become an information security culture. Currently, there are few studies on user information security behavior. These security components influence the users who exhibit information security behavior. This security behavior evolves and becomes the de facto organizational behavior which cultivates an information security culture. There exists a reciprocal relationship between behavior and culture. Academic research studies typically address the deterrence and punishment factors of controlling user security behavior. Others address establishing an Information Security Awareness culture by changing the organizational culture using learning, training or knowledge or with strengthening it through the Information Security Policy. [4]

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, commonly known as HIPAA, is an attempt to update the health sector and insurance recordkeeping to bring more accountability and better protection of consumer rights. Besides regulating the insurance industry, one of HIPAA's significant effect is to mandate the confidentiality and integrity of medical information. The privacy rule of HIPAA requires the organization to ensure that they have taken reasonable steps to ensure the confidentiality of healthcare records and communication with individuals. [7]

The Privacy Rule of HIPAA protects individuals PHI (Protected Health Information) by dictating how and when a person's PHI may be disclosed and for what reasons. It grants individuals more involvement by allowing them specific rights to access their medical records and to request amendments, to authorize or restrict the disclosure of their information in certain circumstances, to be informed of the way in which their information is shared with others, and to be informed of their rights relating to privacy. [8]

The Security Rule of HIPAA specifically addresses PHI in electronic form. It mandates that PHI, electronically stored or transmitted, must be kept confidential and protected against unauthorized users and threats to its security or integrity. The Security Rule establishes a minimum "floor" of security that all covered entities must ensure. It does not, however, set standards for computer applications functional abilities. HIPAA establishes behavioral standards and requires covered entities to develop practices that adhere to these behavioral standards. [8]

Organizations outsourcing some of their record management tasks must ensure that the third-parties also comply with HIPAA. Each organization must have established internal audit procedures for medical records. All records must be disposed of in a trustworthy manner at the end of their retention period. Access to hardware and software should be limited to properly authorized individuals. Data integrity must be ensured by means of checksums, message authentication, or digital signatures. Each entity is responsible for ensuring that data within its systems have not been erased or tampered with. [7]

2 Data Storage

In the past few years, a collection of multiple technologies has given rise collectively to the concept of cloud computing. In cloud computing, a client does not own storage and server sat their physical site, rather they lease capacity (either computational, storage, or both) from providers over the Internet, trusting that said providers can scale without limit and have high reliability. By doing so, a client is freed from the responsibility of maintaining large numbers of servers and storage arrays but is increasingly dependent on their liability of a fast and large bandwidth network connection to their cloud provider. [9]

The data needed for immediate patient care should not be subject to the risks of a slow network. But, it certainly is reasonable to consider placing research data (or patient data after the patient leaves the medical center) on a remote site until it is needed later. If the need can be predicted, it is a simple matter to recall it during overnight pre-fetch operations to a local cache. There are also some new complications once the data leave the physical boundaries of the medical center. First, patient privacy must be protected. This is most simply accomplished by encrypting the data files before transmission to the cloud. The simplicity stems from the fact that encryption algorithms exist that are symmetric and can work on any data without knowing what it is. [9]

The development of cloud technology and the emergence of the Database as a Service (DaaS) model provide possibilities for innovative venues of data storage. Although the traditional relational database can allow users to manage, store, and retrieve data and have been successfully applied in many services, some limitations exist, such as the difficulty in expansion according to the number of users. Compared to traditional relational database services, a DaaS can serve more users. A DaaS service should have a good flexible expansion that can provide long-term service for many users, a balanced load on the system composed of multiple servers, and security and backup of private data. [10]

As cloud environment consists of heterogeneous servers and each server may have different types of access policy structures and security approaches so synchronization among these should be ensured for the overall performance of the cloud. But for synchronization purpose, the QoS and security approaches are sometimes hampered. So, cloud providers should manage and collaborate the access policy among the servers in a way so that no security breaches are occurred. [11]

3 Requirements to Storage Systems

On the following part, we discuss the main requirements that storage systems would need to adhere to, for compliance purposes, including data confidentiality, record integrity, and availability, as well as secure retention, deletion, and migration mechanisms.

3.1 Confidentiality, access control and authentication

As health-care records contain sensitive information, the storage systems must ensure their confidentiality. Moreover, only authorized personnel should have access to confidential medical records. Consequently, to ensure confidentiality, storage systems must deploy strong encryption in both the actual storage and the data pathways leading to and out. Moreover, in the case of storage media re-use or disposal, the confidentiality of records previously stored in such media should be ensured [7].

All access to the storage system should be logged in a trustworthy manner. HIPAA mandates recording all medical record access information. Many of the regulations require extensive logging to record the movement of records between systems, and the access and modification history. Consequently, the storage system must provide verifiable audit trails and the maintenance of provenance information on the chain of records custody. [7]

3.2 Integrity, availability and performance

The storage system must ensure the integrity of medical records [7]. Integrity assures that the data is accurate and has not been changed. This is a broad term for an important concept in the electronic environment because data exchange between systems is becoming common in the healthcare industry. Data may be collected and used in many systems throughout an organization and across the continuum of care in ambulatory practices, hospitals, rehabilitation centers, and so forth. This data can be manipulated intentionally or unintentionally as it moves between and among systems [3].

If the system is hacked or becomes overloaded with requests, the information may become unusable. To ensure availability, electronic health record systems often have redundant

components, known as fault-tolerance systems, so if one component fails or is experiencing problems the system will switch to a backup component [3]. Medical records are frequently expanded, and patients may also ask for correction of records [7].

Timely access to medical records would require indexing techniques. However, regular indexing schemes such as keyword index can breach privacy as the mere existence of a word in a document can leak information. For example, if the keyword “Cancer” is present in a medical, then an adversary can assume that the patient might have Cancer. So, the index itself must be trustworthy, and confidential [7].

3.3 Support for long retention and secure migration

Many of the regulations require long retention periods for certain types of health-care records. The storage system must can provide long term retention guarantees. Since it is conceivable that the failure of storage servers, as well as obsolescence of technology and formats will require migration of records, the storage system must provide trustworthy and verifiable migration mechanisms. [7]

3.4 Encryption for privacy

The goal of encryption is to perform some mathematical transformation to a "clear text" and produce a "cipher" text that cannot be read [3]. A significant early step in any protocol used for the establishment of a secure connection is the agreement of the server and client on the type of encryption to use. Modern cryptographic systems rely only on the security of the key. It assumed that an attacker will obtain knowledge of the cryptographic algorithm and the protocol. There are two major types of encryption currently in use: symmetric key and public key, each has strengths and weaknesses. In practice, most protocols use a combination of both types, relying on the strengths of both [12].

The basic protocol used by both systems is straightforward. The message, also termed plain text, is encrypted via a mathematical method into ciphertext. The ciphertext then is transmitted over a channel and then decrypted (vŸ) an inverse mathematical method back into the original plaintext message. [12]

In a symmetric key encryption system, there is only one key used for both the encryption and decryption of a message. The strength of this method is the relatively fast speed of the encryption and decryption algorithms. This makes the use of symmetric key encryption attractive for bulk transfers of information. [12]

The public key method relies on an asymmetric application of two different keys. For example, agent Y produces two keys (y and y'). The private key (y) is known only to Y and is never transmitted across a network. In contrast, the public key (y') is freely sent to all of Y's associates--perhaps even posted on Y's Worldwide Web page. When X wishes to communicate privately with Y, he/she encrypts the message with Y's public key and then sends the message across an insecure network with the knowledge that only Y has the private decoding key [3].

There must exist strong backup and restore operations. The backup copies should be in a separate off-site location to ensure survival in case of fire or natural disasters. [7]

4 Conclusion

In this work, we tried to explore major health information systems regulation nowadays, as well as the little knowledge of the actual population about the importance of the secure information, or even more important, the security and privacy of health information data. This data can be used in our favor to find solutions to diseases by data standards or to help doctors follow our health information.

We approached some of the most important rules to keep all the health information safe and some of the storage requirements.

As we refer to the abstract, the amount of health information tends to increase and it's important to create new solutions to support the huge amount of data and keep it all safe.

References

1. Doucette, J.; Ludwick, D.: "Adopting Electronic Medical Records in Primary Care: Lessons Learned from Health Information Systems Implementation Experience in Seven Countries", International Journal of Medical Informatics, vol.78(1) (2009).
2. Laurinda, B.; Cathy, A.; Bond, K.: "Electronic Health Records: Privacy, Confidentiality, and Security", American Medical Association Journal of Ethics, vol.14 (9), pp. 712-719 (2012).
3. Langer, S.; Stewart, B.: "Aspects of Computer Security: A Primer.", Journal of Digital Imaging, vol.12(3), pp. 114-131 (1999).
4. Boxa, D.; Pottasa, D.: "Improving Information Security Behaviour in the Healthcare Context", Conference on Enterprise Information Systems, Centeris (2013), International Conference on Project Management, Projman (2013), / International Conference on Health and Social Care Information Systems and Technologies, HCIST (2013).
5. Haux, R.: "Health Information Systems - Past, Present, Future", International journal of medical informatics, vol.75 (3) (2006).
6. Maisel; William, H.; Kohno, T.: "Improving the Security and Privacy of Implantable Medical Devices", N. Engl. J. Med., vol.362, pp. 1164-1166 (2010).
7. Hasan, R.; Winslett, M.; Sion, R.: "Requirements of Secure Storage Systems for Healthcare Records", Proceedings of the 4th VLDB conference on Secure data management 2007, Willem Jonker and Milan Petković (Eds.). Springer-Verlag, Berlin, Heidelberg, pp. 174-180 (2007).
8. Young, B.; Kathleen, E.; Joshua, S.; Meredith, M.: "Challenges Associated with Privacy in Health Care Industry: Implementation of HIPAA and the Security Rules", Journal of Medical Systems, vol.30(1), pp. 57-64, (2006).
9. Langer, S.: "Challenges for Data Storage in Medical Imaging Research", Journal of Digital Imaging, vol.24(2), pp. 203-207 (2011).
10. Chang; Hsien-Tsung; Lin, T.: "A Database as a Service for the Healthcare System to Store Physiological Signal Data", Ed. Houbing Song. Plos One (2016).
11. Onik, F.; Anam, K.; Rashid, N.; Salman, S.: "A Secured Cloud based Health Care Data Management System", International Journal of Computer Applications, pp. 24-30 (2012).
12. Michael, A.; Michael, S.; William, P.; Stephen, T.; Wong; Nicholas, J.: "Security for the Digital Information Age of Medicine: Issues, Applications, and Implementation". Journal of Digital Imaging, pp. 33-44 (1998).

Securing Data Storage of Cloud Storage

Diogo Oliveira

Lusofona University of Porto, Portugal
diogo_baguinho@hotmail.com

Abstract. Cloud services are growing fast and today many companies are migrating their data to cloud-based storage services. In this paper we have a summary of cloud services plus cloud types. This is important because without it we cannot understand cloud security, more accurately data security in cloud services, including how to ensure its security. Here we study some possible techniques to secure information on them, and analyze also an example of data encryption, as one of the techniques.

Keywords: Cloud Storage, Cloud Computing, Cloud Security, Securing Data, Encrypt Data.

1 Introduction

With the extremely fast growth of the information technologies nowadays, a brand-new machine can become obsolete in a period of two or three years, and with the thousand terabytes of information stored in the world every day, it's important for any company to have a way of flexible increasing processing and storage power in a way of coping with this demand to stay ahead of its game and beat the competition in a very demanding industry. A solution is found called Cloud Computing, which according to the National Institute of Standards and Technology (NIST) can be defined as "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" [3]. From this definition it's possible to conclude that the cloud is capable of a broad network access (access anywhere from any device with some processing capabilities and network access), On-demand service (a user can have access to computational resources with the only need of connecting to its cloud service provider), resource pooling (the resources of the service provider are shared among its clients, and these resources can be adjusted to suit the clients request without apparent changes), elasticity (the client can request, for example, additional 50GB of storage capacity to its cloud service and the service provider can provide him with these storage capacities anytime) and a measured service (The service provider uses a pay-per-use mechanism where the client only pays for what he uses, which means the provider optimizes automatically the use of these resources). With the increasing use of the cloud computing, immense quantities of data are being moved daily between the clients and the Cloud Service Providers meaning, like everything in the information Technology universe, that these data might be the target of any threat for many reasons, so all roads lead back to one important word - Security. So the main topic of this paper is Cloud Security and techniques to secure data in the cloud. It's also very important to know how the cloud works and how its models and architecture are based, so it's easier to understand how the security methods work. In section 1 there's a brief on how this cloud concept works, the models and types of cloud are found in section 2, security aspects in section 3 and in section 4 there´s an example of data encryption in the cloud. [1]

2 Cloud Computing Architecture

In this section is given an overview on the cloud architecture, services and types of clouds.

2.1 Service models for cloud computing

Clouds offer services that can be grouped into three categories: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). [2]

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings [3].

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. A well-known example is the Google Apps Engine [3][4].

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls) [3].

2.2 Types of cloud

Cloud deployment models have been discussed in the literature, however the most significant in the literature are described below. [5]

Private Cloud: In this model, the cloud provider provides cloud infrastructure to a single organization that has many consumers. This infrastructure is to be used exclusively for their use and need. The owner, manager, and operator of this cloud could be the organization itself, a third party, or the organization and third party together. This private cloud could be on premises or off premises. [5]

Community Cloud: In this model, the cloud provider provides cloud infrastructure to many organizations that forms community that shares mission, security requirements, compliance consideration, or policy. This infrastructure is to be used exclusively for their uses and needs. The owner, manager, and operator of this cloud could be one of organizations, a third party, or the organization and third party together. This Community cloud could be on premises or off premises. [5]

Public Cloud: This model differs from the previous model in that it is open for the public; it is not private and not exclusively for community. In this model, a public cloud can be provisioned for public to use it to satisfy their needs. The owner, manager, and operator of this cloud could be a government, private organization, a business or academic organization, and sometimes many of them can be in one cloud and get the service from the same provider. [5]

Hybrid Cloud: This model comprises two or more deployment models (private, community, or public). The cloud infrastructure can be combination of those models. Data center within an organization, private cloud, and public cloud can be combined in order to get services and data from both in order to create a well-managed and unified computing environment. A cloud can be considered hybrid if the data moves from a data center to a private cloud or public cloud or vice versa. [5]

Five Essential Characteristics	● On demand self-service ● Broad network access ● Resource pooling ● Rapid elasticity ● Measured Services
Three Service Models	● Software as Service (SaaS) ● Platform as Service (PaaS) ● Infrastructure as service (IaaS)
Deployment Models	● Public Cloud ● Private Cloud ● Hybrid Cloud ● Community Cloud

Tab. 1 - Cloud Architecture

3 Cloud Security

Key references such as CSA's (Cloud Security Alliance) security guidance and top threats analysis, ENISA's (European Network and Information Security Agency) security assessment and the cloud computing definitions from NIST (National Institute of Standards and Technology) highlight different security issues related to cloud computing that require further studies for being appropriately handled and, consequently, for enhancing technology acceptance and adoption. Emphasis is given to the distinction between services in the form of software (SaaS), platform (PaaS) and infrastructure (IaaS), which are commonly used as the fundamental basis for cloud service classification. However, no other methods are standardized or even employed to organize cloud computing security aspects apart from cloud deployment models, service types or traditional security models.

Aiming to concentrate and organize information related to cloud security and to facilitate future studies, in this topic were identified the main problems in the area and grouped them into a model composed of seven categories, based on the aforementioned references. [6]

- Network security
- Interfaces
- Data security
- Virtualization
- Governance
- Compliance
- Legal issues

In this paper the main theme is the data security, so the techniques to secure the data in the cloud are given on the next topic.

3.1 Techniques to secure data in cloud

There are many techniques to secure data in the cloud, in this topic some techniques are given.

Authentication and identity, authentication of users is performed by various methods, but the most common is cryptography. One problem with using traditional identity approaches in a cloud environment is faced when the enterprise uses multiple cloud service providers. In such a use case, synchronizing identity information with the enterprise is not scalable. Other problems arise with traditional identity approaches when migrating infrastructure toward a cloud-based solution. [7]

Data encryption, having passwords and firewalls is good, but people can bypass them to access your data. When data is encrypted it is in a form that cannot be read without an encryption key. The data is totally useless to the intruder. It is a technique of translation of data into secret code. If you want to read the encrypted data, you should have the secret key or password that is also called encryption key. [7]

Information integrity and privacy, cloud computing provides information and resources to valid users. Resources can be accessed through web browsers and can also be accessed by malicious attackers. A convenient solution to the problem of information integrity is to provide mutual trust between provider and user. Another solution can be providing proper authentication, authorization and accounting controls so the process of accessing information should go through various multi levels of checking to ensure authorized use of resources. [7]

Availability of information (SLA), non-availability of information or data is a major issue regarding cloud computing services. Service Level agreement is used to provide the information about whether the network resources are available for users or not. It is a trust bond between consumer and provider. A way to provide availability of resources is to have a backup plan for local resources as well as for most crucial information. This enables the user to have the information about the resources even after their unavailability. [7]

Secure information management, it is a technique of information security for a collection of data into central repository. It is comprised of agents running on systems that are to be monitored and then sends information to a server that is called “Security Console”. The security console is managed by admin who is a human being who reviews the information and takes actions in response to any alerts. As the cloud user base, dependency stack increase, the cloud security

mechanisms to solve security issues also increase, this makes cloud security management much more complicated. It is also referred as a Log Management. [7]

4 An example of a client side Data Encryption

Everyone should secure data in the cloud because people with bad intentions can try to obtain your data and can have access to all your confidential information.

In this section I'll encrypt data in the cloud, which is one of the techniques given under section 3, to ensure that no one can access my data.

I'm going to use Boxcryptor to encrypt my data in the Dropbox. So when I put a file in the Dropbox, using Boxcryptor, I can encrypt that file, by clicking in the right button of the mouse in the file and encrypt the same as shown in figure 1.

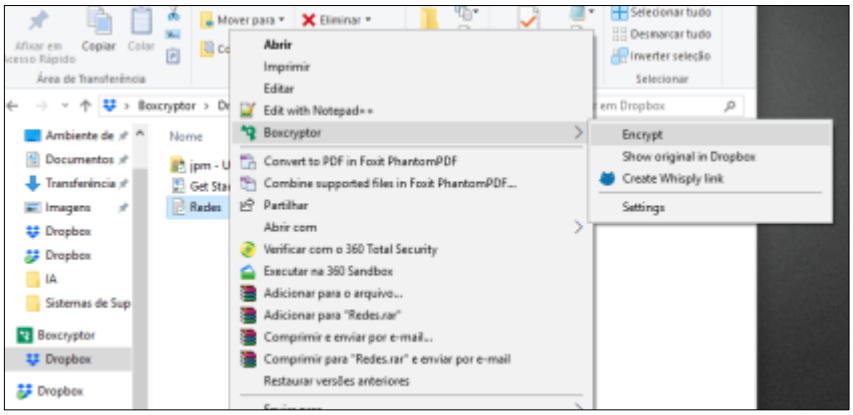

Fig. 1 - Encrypt file in Dropbox

Before being encrypted, my file in Dropbox it will appear like shown in figure 2. That is, as the file has not yet been encrypted it´s possible to see the content inside the file.

Fig. 2 - File contents preview

After encrypting a file with Boxcryptor (figure 1), it's possible to observe that is no longer possible to see the contents of the file that is in the Dropbox, as we can see in figure 3.

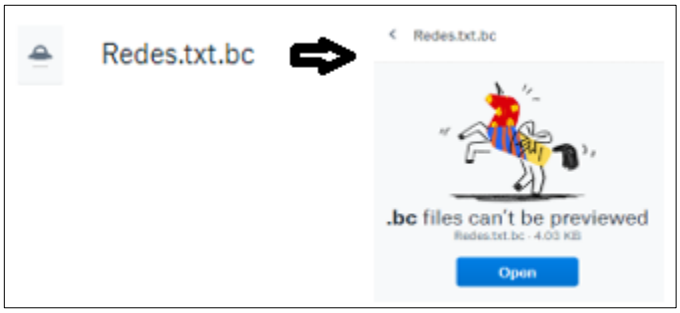

Fig. 3 - Encrypt File Contents preview.

To see what is inside our file, we have to enter Dropbox through the Boxcryptor, otherwise, we can't see the contents of the files, as they are encrypted.

It is possible to encrypt our data in the cloud in a simple way, as the example just shown.

From this simple example we can infer that the data was encrypted before it was sent to Dropbox, therefore as dropbox as no access to the encryption key used to encrypt the file, the file contents can't be correctly preview, as such increasing the data security and privacy.

5 Conclusion

With the evolution of cloud computing, new security challenges have been created, security in the cloud has started to be one of the biggest concerns to take into account, because people who want to change their data to a cloud want them to be safe, without others having access not authorized to the information in the cloud.

Throughout this essay, we have introduced the term cloud, to understand a bit more about this concept, the major cloud security issues were identified furthermore since the main topic of the paper was data security, the techniques for securing data in the cloud were mentioned.

At the end, we demonstrated how to encrypt data on the client side, before uploading it to the cloud, and by this simple act, we manage to improve the security of data transferred to the cloud.

References

1. Silva, R.: "Cloud Computing and its Security Technics", High Performance Networks Studies, Hugo Barbosa and Telmo Morais (Eds.) pp. 22-31 (2016).
2. Zhang, Q.; Cheng, L.; Boutaba, R.: "Cloud Computing: State-of-the-Art and Research Challenges", Journal Internet Serv Appl, vol.1, pp. 7-18 (2010).
3. Mell, P.; Grance, T.: "The NIST Definition of Cloud Computing", National Institute of Standards and Technology (2011).
4. Joshi, K. C.: "Cloud Computing: In Respect to Grid and Cloud Approaches", International Journal of Modern Engineering Research (IJMER), vol.2 (3), pp. 902-905 (2012).
5. Aldossary, S.; Allen, W.: "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solution", International Journal of Advanced Computer Science and Applications, vol. 7(4) (2016).
6. Gonzalez, N.; Miers, C.; Redígolo, F.; Simplício, M.; Carvalho T.; Naslund, M.; Pourzandi, M.: "A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing", Journal of Cloud Computing: Advances, Systems and Applications, Heidelberg, vol.1 (2012).
7. Gupta, G.; Laxmi, P. R.; Sharma, S.: "A Survey on Cloud Security Issues and Techniques", International Journal on Computational Sciences and Applications (IJCSA), vol.4 (1) (2014).

Secure on Site Caching of Encrypted Cloud Storage

Rui Oliveira

Lusofona University of Porto, Portugal
rui.oliveira97@live.com.pt

Abstract. This paper has the purpose to show the importance of security on cache cloud storage that are provided online, and for that there will be shown some type of attacks that can happen to anyone that uses cloud services, also there will be shown some types of ways to prevent them or at least minimize them. And to that effect a new device that entered the market is presented in this paper. This device shows that it is possible for everyone to protect their photos, important and personal files more easily and also improve the usage of cloud storage services provided online.

Keywords: Cloud, Security, Storage, site caching and SMiD.

1 Introduction

In the days that we live in cloud storage has become more and more popular in the business industry and off curse with the average public. In a more general way, cloud storage is a service provided online that can be used as a safer method to stash personal and important files, it is good to be used as backup mechanism, and easies to access from every device that as an internet connection [1]. Such as cloud storage services are so much in use [1], the companies that provide that, have to find a way to increase the speed of response of the site, so that the user continues to put into use their services, and that is what cache site is [2], in a more simple way. With the new appearance of new approaches to increase the yield, it is also necessary to coexist some process of security, which can protect them. For that purpose, this paper presents some examples of attacks to show the importance of security, mostly on online services. At the time that new technology is developed and presented to the public, some concerns appear, mainly when the technology involves the personal data of the users. And the way these concerns are answered is the first step to the development of technology itself [3]. In this particular case, the using of page caching in cloud storage apps.

2 Site Caching and Security on Encrypted Cloud Storage

The speed of download of a website it's an important factor. Many users are impatient and don't want to wait for the page to load, so if the upload speed is low, some of the users may stop using the service. Beyond that Google and other search engines keep a track and show the speed response of your website. Caching is the process that allows the loading speed to be higher. The process is simple: the subpages of the website are temporarily storage in the cache of the main page, son when a client calls them, they come in a form of cache. The advantage is to avoid consulting the data base which takes too much time to be complete. For example, you can turn your initial page cache being updated once a day, if later on you change it, the other users will only see them when the cache of the page update automatically in the next day or you update it

manually. To access to the settings of the page caching you must first: Access to the administration area, then select settings, and finally general configurations; after that select caching page. [4]

2.1 Cloud Storage Privacy

A widespread concern about the privacy of user's activities on the World Wide Web is what needs to have a big focus on. When a user visits the pages on the internet a list is created, and list sometimes storage detailed information about the user's family, financial or health situation. Therefore, users sometimes consider their Web browsing history to contain private information that they don't want others to know about. Obviously, from the first time the user enters a Website it leaks right away some information to that site, but off course users would like some assurance that the information about their visit to the site isn´t available to third parties. Unfortunately, some implementation bugs in browser have given opportunities for unwanted personalities to gather information without user knows about. Sadly, these bugs can´t be easily fixed once they are not caused by the browser.

These types of Web caching attacks can be anticipated by turning off Web caching. In other hand this can have a big penalty in performance, since caching has a major effect in the performance on several Websites, such as their response speeds. Even Web caching is turned off, an attacker can exploit other types of caching, such Domain Naming System (DNS) [5] caching, to get on his hands the user´s activities. [6]

3 Countermeasures

In this topic will be presented some potential ways to counter these types of attacks, despite the reality that it's presumed the impossibility to protect any information online by its total. Has it can assumed that the only way to protect a system is by unplug it from the power. [7]

Turning off caching, the first countermeasure that everyone thinks first is to simply turn off caching. The authors [6] say, this will certainly prevent the attacks, but cause a big impact on the Website performance.

Turning off first-level caching, instead of turning off caching in is total, we could try to turn only the first-level caching and count on the department-scale second-level caching. How-ever this still has a big importance in the performance, and grants intruders to collect information.

Implications of transparent caching, this type of caching gives the user some help and tykes the "work" of turning on web caching. Transparent caching can be installed in any network components like routers, and as before it increases the performance of the web, but this time the user doesn´t need to configure or interact with the system, he just needs to use it as he wants. Unfortunately, transparent caching can´t be turned off at the client, so the client alone, may not have the knowledge to avoid using caching. [6]

Altering hit or miss performance, another way of countermeasures depends on the performance of cache hits, in a try to make them harder to differentiate from the misses.

Attackers will be able to capture important information from the cache content, as long as hits are slightly faster than misses. But as it's easy to understand, if hits are made slower as misses, the attackers will lose their advantage, but in this case it's easier to turn off the website caching.

Seeing from another point, if a hit is reasonable faster than a miss, then the attacker will still be able to see it as a hit, in other hand if it's not easily recognizable as faster, it will be seen as a miss. Summing it up, this approach essentially converts randomly chosen hits into misses, but reducing the performance, once again. The authors [6] say, the more hits we wish to disguise, the more performance will suffer.

Turning off java and javascript, the last countermeasure is to turn off java and javascript. By doing this, the attacker lose their most accurate measurement tools, as lowering is measurements accuracy. Unfortunately, the attacker can still do precise measurements as the data presented by figure 1 demonstrates. And also, java and javascript are so intelligently used on websites that just seems impractical to ask the common user to turn them off. [6]

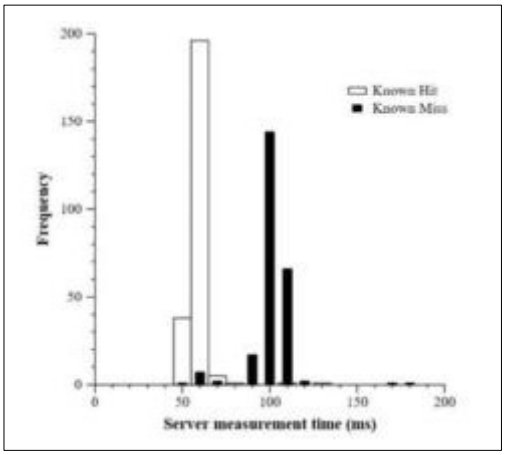

Fig. 1 - Distribution of access times for known cache hits and known cache misses [6]

4 New Ways of Encrypting Data

Since nowadays, only a small part of the world population doesn't use cloud services for storage there documents, new ways of encrypting enter the market, in addition to the cloud service encryption. As an example, there will be used the SiMD Cloud [8]. SMiD Cloud is a company that focus on protecting the data of cloud storage user's, as they say cloud storage ensures our information will be intact, but… Who sees your data on the cloud end – and what they do with it – is not under your control, we also FEAR the cloud [8], and because of that, they have come up with a device that encrypts all the data before it goes online, to the cloud storage provider that the user chooses.

The way it works its simple, the device only needs to be plugged in the computer, and with the personal encryption key, the user and only him can encrypt and decrypt the data. So if someone else tries to decrypt it, he will only see unusable files.

Fig. 2 - Equipment to encrypt and decrypt data [8]

4.1 How to use SMiD

In three simple steps anyone can set up is own SMiD: Connect the SMiD, insert the startup key into SMiD and connect it to the local network. Add your providers, type "smid" in the browser and follow the wizard to set up user accounts and cloud providers. For now the services only can support DropBox, Amazon S3, Google Drive, Box, Microsoft Azure, FTP and WebDAV, and it´s being improved to include more. Save your settings, perform a SMiD safeguard to be able to regenerate the SMiD in the case of damage to the device. [8]

Fig. 3 - How SMiD cloud System provides security to the data [8]

The following images show a practical usage of SMiD system, has it's possible to understand, SMiD assumes the function of a bridge between the user and the cloud, more like a toll, that encrypts the data before going online. Showing in the end the differences between the decrypted and encrypted file.

Fig. 4 - Plugging in and starting the SMiD device [8]

Fig. 5 - Recognition of the device in the computer [8]

Fig. 6 - Log in of the user [8]

Fig. 7 - Data to be transferred to the cloud [8]

Fig. 8 - Files to be transferred to the cloud [8]

Fig. 9 - File decrypted [8]

Fig. 10 - The file encrypted [8]

5 Conclusion

As described in the paper, the system cache on cloud storage websites, still has some security issues. This may be a big reason for potential users still prefer the "old" and physical methods of storaging data, such as using several hard drives, instead of using only one or two physical devices, and one cloud system. However, there are ways of protecting data, which are being constantly improved to better pro-tect the so much important personal data, so that the common user feels safer using this kind of services. Nevertheless, there are plenty of cloud storage services available online, so there is a great leach of possibilities to storage our data in a safely, more efficiently and prac-tical way. Of course doubts can arise, but the data, ounce online, it can never be truly erased from it. It will always be on cache, and it's true, but it's where the security systems, or encrypting data systems appear. They come in two formats, there being by hardware or soft-ware. By software, this type of security measure, is already included in the cloud storage service provider. Software used to encrypt the da-ta that stays on cache, but can be easily decrypted ounce it's online. In other hand, by using some external device, such as SMiD, hardware device, the data can be encrypted before going online, which makes it safer for the user, and even though the data stays on cache, it can only be access by the creator of that data. So, knowing this, it's possible to consider using external services to encrypt our personal data so that, we can fill safer using, and trust more in the services provided online to storage.

References

1. Wu, J.; Ping, L.; Wang, Y.; Fu, J.: "Cloud Storage as the Infrastructure of Cloud Computing", International Conference on Intelligent Computing and Cognitive Informatics, Kuala Lumpur, Malaysia (2010).
2. Subashini, S.; Kavitha, V.: "A Survey on Security Issues in Service Delivery Models of Cloud Computing", Journal of Network and Computer Applications, vol.34 (1), pp. 1-11 (2011).
3. Sengupta, S.; Kaulgud, V.; Sharma, V. S.: "Cloud Computing Security- Trends and Research Directions", Editor, F., Editor, S. (eds.) Conference, DBLP, IEEE World Congress (2011).
4. Amen.pt Homepage, "O que é o caching de páginas e como usá-lo", a dada brand, accessed (2017).
5. Albitz, P.; Liu, C.: "DNS and BIND", third ed. O'Reilly and Associates (1998).
6. Felten, E. W.; Schneider, M. A.: "Timing Attacks on Web Privacy", ACM Digital Library, Athens, Greece (2000).
7. Hon, W. K.; Millard, C.; Walden, I.: "The problem of Personal Data in Cloud Computing: What Information is Regulated? - The Cloud of Unknowing", International Data Privacy Law, vol.1 (4), pp. 211-228 (2011).
8. SMiD Homepage, accessed (2017).

Information Gathering through Image Leaking

Rodolfo Matos
University of Porto
Porto, Portugal
rodolfo@uporto.pt

Telmo Morais
University of Porto
Porto, Portugal
telmo.morais@gmail.com

Abstract. Nowadays, footprints from casual Internet users are widely spread. Having access to a mere face image that has been identified or tagged somewhere in the past, will make it possible for anyone to almost instantly and automatically gather a range of information. This can be done by using technologies available to the common user. Such information, which used to be considered private a few years ago, is now freely accessed by anyone and if used for the wrong purposes, establish connection between scattered content. This can then be used in order to establish someone's full digital identity.
This paper will demonstrate some of the methods currently available, and which can be easily found, used for this purpose.

Keywords: Privacy, Social Networks, Digital Footprint, Image Leaking, Information Gathering.

1 Introduction

A considerable number of the world's current population has access, to at least, some resources available online. Access to online resources has become so fundamental, it has, in fact, been considered a human right by the UN [1]. Nonetheless, we have to acknowledge that a user's digital footprint allows the automatic gathering of information. This can be done to such an extent that it will reveal a considerable high number of someone's activities. Therefore, we have access to information, made available online, that would have been difficult for police task forces of former totalitarian regimes, such as Stasi or Gestapo to obtain [2].

Up until recently, there was a somewhat heated debate about the legality, or lack of, of the Portuguese citizen's card. According to the Portuguese Constitution [3], article 35, clause 5: "The attribution of a unique national number to its citizens is forbidden.". The strict definition of "number" implies that a digital representation of the following numbers: fiscal, social security and health care number, can be considered as a sole number, since the several numbers have, each, a fix set of bits, which are always arranged in the same order.

Furthermore, we can look at the way in which the number of a credit card is presented, for example. Even though there is a space among groups of figures, the set of numbers can be interpreted as a single number. Moreover, as the definition is not explicit with regards to which base a number should be represented (binary or decimal), we can consider all the numbers present in the Portuguese Citizen's Card as a unique, single number.

This can lead to an interpretation in which these numbers are a possible violation of the rights established by the Portuguese Constitution [4].

However, the benefits and convenience of having a single system, within a democracy, make it possible for the general population not to realize they are giving up on their rights. This regarding the way their personal data are treated, and which have been established as a fundamental right. [5]. This perception is immediately altered and expanded when the population suffers the consequences of an oppressive regime [6], such as the one of the concentration camps of years past, which in fact was one of the reasons [4] it has not been adopted in Portugal.

Within the advent of social media and all the technology and services that sprang around the Internet, users started to be less worried about what they really shared online. It is clear that general concern with privacy has been decreasing [7]. People got used to giving up on their privacy, which is extremely easy to demonstrate. All it takes is to compare the amount of personal data available before the advent of the Internet in general and of social media in particular, and the one currently available [7].

To the providers of services such as social media, the amount of data available in a user's digital profile is a core business with monetary value. Its price varying according to where one lives [8] Even though these systems include a significant number of users, economy of scale means the profile of a European user is sold for little over a dozen euros. This should be taken into account by the user, when considering the cost-benefit relationship really obtained. Privacy is lost and the amount and quality of the information given out, is done so, at a very low price.

The Data Selfie [9] is a tool that can give us a glimpse of what Big Data really is, and of how corporations such as Facebook use it. They do so to extract information regarding digital footprints from users, and to understand the content and type of information they are gathering. Given these datasets dimensions, processing is generally sped by using distributed computation technologies, such as Hadoop, Spark or Storm[11] among other.

A corollary of this growing acceptance of the loss of privacy is how careless exam frauds are carried out whenever exams take place using a computerized form [12]. We have increasingly noticed [13] [14] that students - when using computerized assessment - do not realize that all actions that are carried out can be saved, and then used as evidence of intent of fraud in disciplinary action processes [12] [14] [15].

We can, therefore, state that by resorting to technology available to everyone, it is possible, with a minimum set of private information or metadata, to compile another set of information which can be quite detailed [4]. Even a conscientious user of the Internet and its services, who cares about safeguarding their privacy, will hardly succeed in becoming invisible. It is always possible, through digital footprints that are left behind, to recreate a digital profile, based on someone's path and network services use. The main goal of this paper is to demonstrate this hypothesis.

2 Facial recognition

Facial recognition is a key problem and a popular matter for research in computer vision for several reasons. First, it allows the structuring of well defined problems, since individuals are correctly identified by their name. Secondly, even though it is well defined, it is an impressive example of classification, because the variation of two images within a class (images of one

person only) can surpass that among images of different classes (images from two different people).

However, this task is easily carried out by human observers, as they deal with awkward variables, such as different poses and facial expressions, while still maintaining its focus on traits that really are important for a correct identification.

Finally, non-verbal recognition is extremely relevant for the human socialization process. Besides the basic ability to identify other human beings, the ability to assess a third party's emotional status, identifying their attention focus, as a survival tool, are all critical resources for successful social interaction. For all these reasons, facial recognition has become an area of intense studies for the community which studies systems of computer vision [16].

3 Methodology

Is it possible to create a digital profile from a simple photo extracted from a free, public access information system with only technologies available to anyone?

To find an answer to this hypothesis, we created a small dataset with well known images taken from the information system of a Portuguese university, whose access was free and public at the time it was created. These are passport-sized pictures, often with low resolution - 72 dpi or less - with high compression rates - which means in some of them, it is not even possible to see eye color - but which will allow to unmistakably identify at least, some facial traits.

To carry out with the automatized extraction of these images, a small script in BASH was designed, so that each organic unit in the target institution accessed students' profile sequentially. The image used for this process would have a public user photo. These represent under 10% of the tested profiles. Even so, in just 10 minutes - after which the gathering process was interrupted, so as to simulate possible access limitations - it was possible to obtain a small dataset with about 2000 pictures, which were saved using the following format:

<organic unit>-<school ID number>.jpg

These pictures were stored in a folder called “known” in the computer used for the experiment.

Fig. 1 - Building the dataset with known images

This computer has Linux Mint operating system, which is a variation of the Ubuntu distribution. Since the hardware used for this experiment does not have a GPU (which would allow the speeding of the calculation process), the instructions found for installing the facial recognition system [17] could be strictly followed, without any considerable changes.

For the creation of a testing set with subjects to be identified, Facebook pictures were used. These had been published at public social events and are somehow related to the university from where the above mentioned pictures had been extracted.

In all cases tested, and given the reduced size of the dataset, it took only a few seconds to correctly identify the people involved. There were two situations in which the answer was not unmistakable, producing, in a particular case, six (6) results as having the same degree of similarity. However, even so, the correct answer was part of the group of solutions obtained.

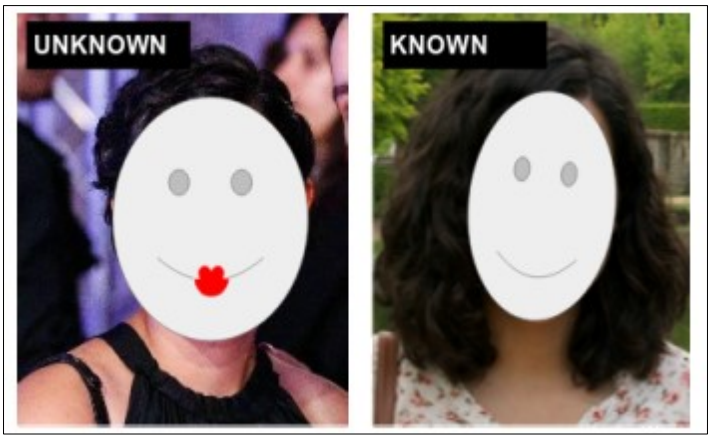

Fig. 2 - Example of the correspondence between the known dataset and image unknown.

From the moment the student's ID number was found, it was also quite easy to find their full name within the school information system itself, even without resorting to public access indexing systems (even though there is one available that we could have used). This process was always carried out without resorting to any sort of vulnerability, or privileged access to the mentioned systems. At the time we started collecting the data, anyone could replicate these stages.

With someone's full name, it is possible to find information about debts to the tax department [18], social security debts [19], in some cases even their phone and address [20], their fiscal information number, and in several cases, their private email.

With this sort of information available and having, for example, access to the list of 1.4 billion passwords that was recently found in the Dark Web [21] it is expectable that it will be fairly possible to hack into at least some of these accounts, which in turn would allow someone to commit several other cybercrimes [22].

4 Conclusion

With this work, it has been shown that gathering automated information about digital ID is, currently, at the reach of the mere user. All it takes is for them to choose the right combination of the existing tools.

The easiness with which people publish personnel information, not only on social media, but also in different sites and services, inadvertently will lead to a track which can be easily traced in an automated way.

It is up to the population, as Internet users, to mind the following before filling in any form:

Why this form exists;

Which information and how relevant it is;

Who will have access to it;

The need to do so.

If these elements are neglected, unnecessary risks can be taken, which in turn can have adverse consequences.

Acknowledgments

We would like to thank Sandra Luna for translating this paper.

References

1. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank R.: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. Retrieved on 15 Jan 2018.
2. Mass surveillance in East Germany, https://en.wikipedia.org/wiki/Mass_surveillance_in_East_Germany. Retrieved on 15 Jan 2018.
3. Artigo 35 da Constituição da República Portuguesa, https://www.cnpd.pt/bin/legis/nacional/ARTIGO_35_CRP.pdf . Retrieved on 15 Jan 2018.
4. Conferência Prós e Contras da aplicação do Artº 35º da Constituição, http://www.apdsi.pt/uploads/news/id183/relato.pdf . Retrieved on 15 Jan 2018.
5. Regulamento Geral de Proteção de Dados, http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=PT . Retrieved on 15 Jan 2018.
6. In China, Social Ranking social will list the good and bad citizens, https://www.publico.pt/2018/01/15/tecnologia/noticia/quantos-pontos-vale-a-sua-vida-1798308 . Retrieved on 15 Jan 2018.
7. Teens, Social Media, and Privacy, http://www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf . Retrieved on 15 Jan 2018.
8. How much are you worth to Facebook?, https://www.theguardian.com/technology/2016/jan/28/how-much-are-you-worth-to-facebook. Retrieved on 15 Jan 2018.
9. Hack Your Own Facebook Data with This Spooky Tool: http://bigthink.com/david-ryan-polgar/hack-your-own-facebook-data-with-this-spooky-tool. Retrieved on 15 Jan 2018.
10. Big Data, https://en.wikipedia.org/wiki/Big_data . Retrieved on 15 Jan 2018
11. Morais .T, “Survey on Frameworks for Distributed Computing: Hadoop, Spark and Storm” em Proceedings of the 10th Doctoral Symposium in Informatics Engineering - DSIE’15, 94-104.
12. Matos, R., Torrão, S., Vieira, T., Moodlewatcher: Detection and Prevention of Fraud when using Moodle Quizzes, https://www.academia.edu/12068691/MOODLEWATCHER_DETECTION_AND_PREVENTION_OF_FRAUD_WHEN_USING_MOODLE_QUIZZES
13. Teixeira A.A.C.; Rocha M.F. (2010) "Academic misconduct in Portugal: results from a large scale survey to university economics/business students", Journal of Academic Ethics, Springer, 8(1): 21-41.
14. Matos, R., Carvalho, F., Torrão, S., Vieira, T., Moodlewatcher: One Year Experience of Detecting and Preventing Fraud When using Moodle Quizzes,

https://www.academia.edu/12256231/MOODLEWATCHER_ONE_YEAR_EXPERIENCE_OF_DETECTING_AND_PREVENTING_FRAUD_WHEN_USING_MOODLE_QUIZZES
15. Matos, R., Barber, J., Moodlegate:Securing Computer Driven Exam Environments,https://www.academia.edu/12256283/MOODLEGATE_SECURING_COMPUTER_DRIVEN_EXAM_ENVIRONMENTS
16. Labeled Faces in the Wild: A Survey: https://people.cs.umass.edu/~elm/papers/LFW_survey.pdf . Retrieved on 15 Jan 2018.
17. Face Recognition: https://github.com/ageitgey/face_recognition#face-recognition . Retrieved on 15 Jan 2018.
18. Dívidas ao fisco, https://static.portaldasfinancas.gov.pt/app/devedores_static/de-devedores.html . Retrieved on 15 Jan 2018.
19. Dívidas segurança social, http://www.seg-social.pt/lista-de-devedores-na-seguranca-social . Retrieved on 15 Jan 2018.
20. Páginas Brancas, http://www.pbi.pai.pt . Retrieved on 15 Jan 2018
21. File With 1.4 Billion Hacked And Leaked Passwords Found On The Dark Web, https://www.forbes.com/sites/leemathews/2017/12/11/billion-hacked-passwords-dark-web/#3207801a21f2 . Retrieved on 15 Jan 2018.
22. Breda F., Barbosa H., Morais T., “SOCIAL ENGINEERING AND CYBER SECURITY”, em Conference: International Technology, Education and Development Conference.

SESSION 3

DATA ENCRYPTION APPLICATION

A Data Encryption Application: Development Proposal

Encrypt and Decrypt Several Types of Data

Nuno Cunha

A Data Encryption Application: Development Proposal

Implementation of the Algorithm AES in an Android Application

Eduardo Carneiro

A Data Encryption Application: Development Proposal

Encrypt and Decrypt Several Types of Data

Nuno Cunha

Lusofona University of Porto, Portugal
Porto, Portugal
nunorafael_6@hotmail.com

Abstract. This paper focuses on an application designed to encrypt and decrypt several types of data such as text, sound files, images, pdfs, software, zipped folders, virtually everything the server machine can handle. It is also focused on the process of encryption and decryption, techniques, methods, and software used to carry out the project. Encryption and decryption methods will be demonstrated with only two or three lines of code and the operation of these methods is clearly explained. Some results of encryption and hashing will also be exposed.

Keywords: Data Encryption, Cryptography, Security, Privacy, Application.

1 Introduction

As computer security increased, there was a need to improve records protection and maintenance practices. The encryption comes to protect the data so that it can only be accessed by authorized people. [1]

When analyzing data encryption, there are two points to consider: the first point is that data encryption makes the information difficult for an unauthorized person to discover, the second point concerns the key management of data encryption (encryption key distributions must be strong enough to stop an attack). Currently, data encryption tools are powerful and evolved to increase the degree of security to minimize information theft, exposure, and manipulation of data. [2]

This paper will report the development of an application to encrypt/decrypt any type of data that the user wishes. The methods and processes used for development and encryption will also be exposed. The goal is to ensure greater security and privacy of data between two users.

2 Cryptography

According to [3], cryptography is the science that provides information security. That is, to improve the security of information a process that converts readable information into unreadable is required. There are three types of cryptography, symmetric key cryptography, asymmetric key cryptography and hashing.

2.1 Symmetric key

In symmetric key cryptography, there is only one key, which is the necessary component for encoding and decoding information shared between two machines. These two machines must have the same key and this key must be kept as a secret between the two. The symmetric key usage process is as follows: the machine that intends to send information encrypts the message with an encryption algorithm (symmetric key cryptography algorithm) and a secret key (private key and equal on both machines), the originating message by this algorithm, is sent and when received by the receiving machine, it will decrypt the encrypted message through the corresponding decryption algorithm using the same private key. The result will be a communication system that depends on the private key.

A great advantage is the ease of use of this type of encryption and the speed of execution of the algorithms, of encryption and decryption.

The biggest disadvantage is that, as has been said previously, the system only depends on a key and that key is the same for encrypting and decrypting. And for the key to be the same on both machines, it must be shared between them. During this sharing, it is possible for someone to interleave the key, so it is essential that the key is distributed through another means of communication or any other secure means of sharing keys. [4]

2.2 Asymmetric key

According to [4], in the asymmetric key model (also called public key) the two machines have two different keys, which in pairs complement each other. The two keys are a private key and a public key. It is important that the private key is kept secret even though the public key is shared for any machine that wishes to perform the exchange of messages with this model. The public key is used by the sender to encrypt the message, and the corresponding private key is used by the receiver to decrypt the encrypted message.

The main advantage of this model is the great security and privacy because only the original message can be read by who owns the private key. Unlike the symmetric key model that depends only on a key, this model relies on four keys (two private and two public keys) if the communication is between two machines.

The disadvantage of the asymmetric key model is that it is a complex system of implementation and development. [4]

2.3 Cryptographic hash

Another form of cryptography is the hash. According to [5], a hash is a one-way cryptographic function, that is, when passing information through a hash function, it will be very unlikely to discover the original information. This method is used to verify the integrity of files (it is confirmed the hash of the original file and the hash of the received file), it is also used when it is necessary to store passwords in a safe way (instead of saving the password, the hash of the password is stored) and digitally sign a document. [5]

2.4 Cryptography in this application

The developed application is divided into two parts: hashing and encrypt/decrypt. In the first part will be presented several hash functions that the user can verify the result. The displayed hash functions are: md5, sha-256, RIPEMD-160, Whirlpool. In all these algorithms the input data will be treated as UTF-8 encoding and the output will be in hexadecimal.

In the second part of the application will be then encrypted/decrypted various data types whether it is plain text as well as files of any extension. This encryption process is done with symmetric key algorithm 'AES-256'. The symmetric key cryptography was chosen due to the ease of key sharing between two users. Since this model only requires a key that is private among users, they will use the key as if it were a password, and only those who know the password and have the encrypted content can discover the original message/file.

3 Development

Before starting development, it was decided that the proposed application would be a website since anyone could use it anywhere in the world as long as it had an internet connection. We should consider that this website is based on the client-server architecture and, according to Microsoft, for greater privacy and integrity [6] between the two machines, this should have the use of SSL / TLS protocol that is not given much value in this article, because the focus is the application and the process used in encryption. At the time of writing this article, it is possible to explore the web application developed that will be exposed in the domain https://dataencryption.ml.

3.1 Software and tools

The programming language used on the server side was JavaScript in the Node.js environment. The Node.js Foundation defines the Node.js as "the JavaScript runtime built on Chrome's V8 JavaScript engine". This environment was chosen for its "event-driven, non-blocking I / O model that makes it lightweight and efficient." [7] On the client side, jQuery is used to perform requests to the server.

Another tool that gave a lot of help in the development of this application was the npm. Npm is a tool that helps JavaScript programmers, this software lets you share code between programmers, so application development will be faster due to reuse of code. Each piece of code that is shared is given the name of packages or modules. Throughout this article will be shown which modules are used in the application development [8].

To conclude it is necessary to say that since it is a web application and due to its focus is the data encryption, it was decided to use a free HTML template. [9]

3.2 Application development

The first step in developing the application was to make modifications to the HTML template provided. There is only one page, which is divided into three sections: Introduction, "Hashing" and "Encrypt / Decrypt".

In the introduction section, the user is informed about the features that this web application has. The "Hashing" section is divided into four subsections, one for each hashing algorithm. Each subsection contains a text box so that the user can write the desired information and another text box that, by clicking on "Hash", shows the hash of the information given by the user by the respective algorithm, as we can analyze in figure 1.

Fig. 1 - Example of subsection of SHA-256

The "Encrypt / Decrypt" section is also divided into two subsections, using the same algorithm (AES-256), the user can encrypt and decrypt their messages or files. For this, there exists in each subsection a text box where the user writes the key (password). In the case of the subsection of text, there are two more text boxes, one to write the original message and another to the encrypted message that as soon as the user clicks "Encrypt" the original message will be converted to unreadable information and vice versa to the button "Decrypt." In the case of the sub-section of files instead of two text boxes will be two areas for uploading files, one for an encrypted file and the other for a decrypted file. When the user clicks on "Encrypt," he can choose to download the encrypted file or share it with someone via email as Figure 2 demonstrates. To decrypt, just place the encrypted file in the second upload area and then press the button and the user downloads the original file. If the message/file is shared by email or any media, it is important that the key to decrypt this content is shared by a media other than the encrypted information was.

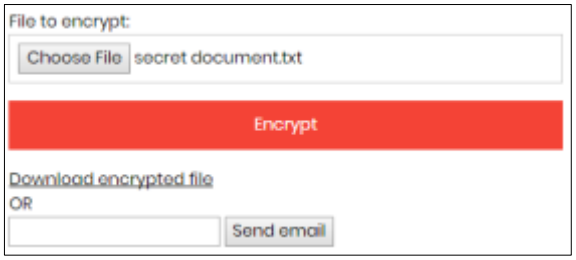

Fig. 2 - Encrypt secret file

The user interface needs to perform requests to the server to calculate the hash, encrypt, decrypt. Sending several types of information to the server is done through HTTP methods such as GET and POST (this topic will not be covered in this paper). And since the connection between the client and the server is private due to the SSL / TLS protocol, there is not much concern about

sending files and information to the server. Example of an accomplishment of a request for a hash function is as follows:

```
$.post(
  "/hash/md5",
  {data: inputData},
  function (result) {
    document.getElementsByName(
      "md5-data-encrypted"
    )[0].value = result;
  }
);
```

Fig. 3 - Example of a request for a hash function

A request is made to the "/hash/md5" path through the POST method to the server, it will return the result of the corresponding hash function and the response is placed in the text box where the user waits for the hash of their information. On the server side, there are two main modules that help us receive this request, the 'https' module to always have the server listening for a client and to create an SSL / TLS protocol connection with the client [10] modulo 'express' to define the routes of the requests for the functions that must be executed [11].

For other application features, such as other hashing algorithms, text or file encryption, sending the request to the server is similar, only the path and the data sent are changed.

Continuing in the previous example, the server receives a POST request for the path "/hash/md5" and it will receive, with the request, a variable 'data' with the value of the original information that the user placed in the first text box of the subsection md5. Now that the server has the information of the user, it will perform the hash of the information with the help of the module 'crypto', which is one of the most important modules to achieve the objectives of this application. The 'crypto' module contains several encryption functions including generating a hash, figure 4.

```
var md5Hash = crypto.createHash('md5').update(data).digest("hex");
```

Fig. 4 - Crypto module functions

First, we have to create an object (crypto.createHash('md5')) of type Hash given the algorithm we want (this module supports all algorithms available in the OpenSSL version of the node.js platform that is being used), in this case, we use the algorithm md5. We then update the contents of the object (.update(data)) with the information received by the client-side request and it is the variable data that contains this information. Finally, the hash of this information in

hexadecimal encoding (.digest("hex")) is calculated, although it is possible to use various types of encoding such as 'latin1' and 'base64'. [12]

After the hash is calculated, the result is returned to the customer in response to your request.

For the encryption of text, as said before will be used the algorithm 'AES-256' which is a symmetric key cryptographic algorithm. In this functionality, the server will receive two variables with the request: the key and the text to encrypt, figure 5.

```
var cipher = crypto.createCipher('AES256', key);
var textEncrypted = cipher.update(textToEncrypt, 'utf8', 'hex');
textEncrypted += cipher.final('hex');
```

Fig. 5 - Key and the text to encrypt

We initially created the object (crypto.createCipher('AES128', key)) that will use the algorithm chosen and the key given by the user, this is an object of the type Cipher. Then the content to be encrypted is updated (cipher.update(textToEncrypt, 'utf8', 'hex')), this is set to ' UTF8 ' input encoding and the result will be hexadecimal. In the end it is necessary to make sure that all the encrypted content is returned (textEncrypted += cipher.final('hex')). After this operation the ' textEncrypted' variable will have all the encrypted information. [12]

The file encryption process is more complex, because for each file it is necessary to reserve space on the server and the result (encrypted file) must be virtually impossible to be decrypted by any identity other than this application, on the other hand It also has to be possible to be converted to the original file with the same name, properties, and content. Figure 3 demonstrates the process that the server does to encrypt the file so that the previous conditions are possible.

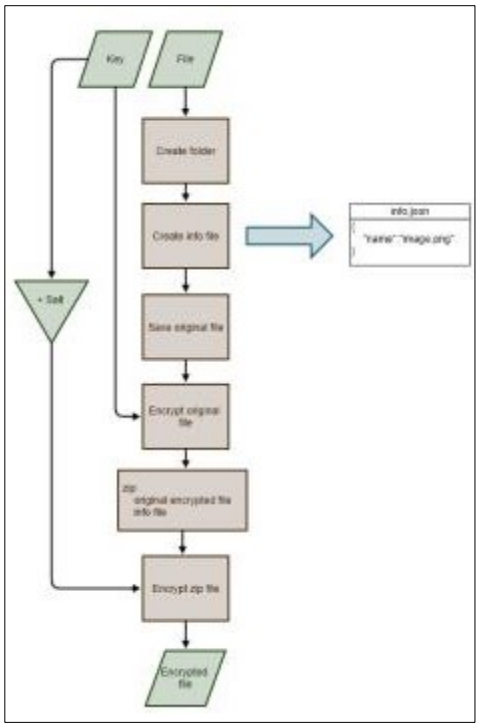

Fig. 6 - Encryption Diagram

As with text encryption, the server receives two variables with the request: The key and the content (file). After receiving the file, a folder is generated so that the original file, the encrypted file and all the auxiliary files are temporarily saved. This folder will name the hexadecimal hash resulting from the sha256 algorithm of the file name concatenation with the date/time of the moment, as shown in figure 7.

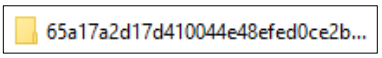

Fig. 7 - Generated Folder

The next step is to create an auxiliary file that saves the name of the original file, so that in the decryption step you can reset the name to the original file.

Only then the file that is allocated on the server is ready to be treated because until here was in a temporary location.

When the file is on the server, it is already possible to perform the encryption with the functions of the 'file-encryptor' module. The function of this module that we use for encrypting the file requires the location of the file to encrypt, the location to save the encrypted file, the key that the user chose, the name of the algorithm to be used, and a function Callback To be able to detect errors:

```
encryptor.encryptFile(
  newFilePath + file.name, newFilePath + 'encrypted.dat',
  key, {algorithm: 'aes256'},
  function (err) {…});
```

Fig. 8 - Function encryptFile

The result of the function (.encryptFile(…)) should be a file named 'encrypted.dat' which is the encrypted file [13]. But with this process the name of the original was lost, which is why we have saved the original name in a file apart.

At this point in the encryption process we already have two files: what contains only the original encrypted name and the encrypted file. For the user to only receive a single file, we put these two together in a zip file, once again we will have the help of a module that deals with archiving these files. The 'node-zip' module lets us do this process of archiving, we give as argument the names of the files and this generates the zip file. [14]

The encryption process is not finished yet because if this is the final file, an intruder when decompressing this zip will know the name of the original file and may have an idea of its contents. For this scenario not to be possible, we once again use the function to encrypt files, only this time the input file is the zip file and the key, which for greater security is different from the first encryption key. This key is the concatenation of two Strings: The original key and a hash of the set of a secret server key with the original key. For less confusion let's look at Figure 5 below. To simplify the implementation the server key is static, that is, it is the same for all files to encrypt.

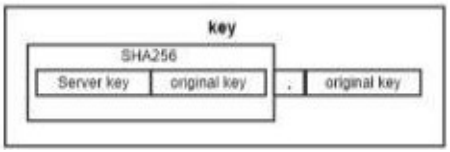

Fig. 9 - Generate key to encrypt zip file

After generating the final key, it is then encrypted the zip file. The encrypted final file name has the same process as the source of the folder where it is stored, but because the date/time is different, due to the milliseconds, the names will be different. Files that are encrypted in this process have the extension '. dat ' because they are generic data files.

At the end of this long process, the files (except the final encrypted file) are all eliminated so that neither the system administrator can discover the information that the user has uploaded. When the user downloads the file or sends it by e-mail, the final encrypted file and the folder where the files were stored will be deleted from the server.

The text decryption system is very similar to the encryption and, so it will not be explained in such detail. For decryption, instead of creating an object Cipher, we create an object Decipher which also receives the same choice of cryptographic algorithm and should receive the same key. We have a block try{} catch(){} in case the key is incorrect to be able to warn the user of the error occurred. In the decryption process the encoding is swapped, the input encoding is hexadecimal, and we want the result to be ' UTF8 ' to be readable for the user. [12]

To decrypt the file, it is necessary for the user to give the correct key and the encrypted file. This process to decrypt the file can be thought of as the encryption process, but in reverse. We can analyze Figure 10 and conclude that the steps performed in the decryption process are like those of encryption.

The server when receiving the requests with the key and with the encrypted file, generates the folder, through the same method used in the encryption process, to allocate the files that will be saved temporarily and save the encrypted file in that same folder.

To decrypt this file we use the same module (‘fileencryptor’), and by placing the location of the encrypted file, the location of the decrypted zip file, the key and the algorithm, the decryption function of the module used (.decryptFile(…)) will decrypt the file sent by the user [13]. We note that this first decryption requires, not from the original key given by the user, but from the second key as shown in figure 9.

After this step we can extract, with the help of the module ' node-zip ' [14], the original encrypted file of the sender and the file containing only the name of the original file.

We finally decrypted the original encrypted file with the original key, with the same function we used to decrypt the zip file. At the end of this process, the original file is renamed to its original name and is ready for the end user to download that file.

As in the previous process, all files on the server will be deleted due to the security reasons explained earlier.

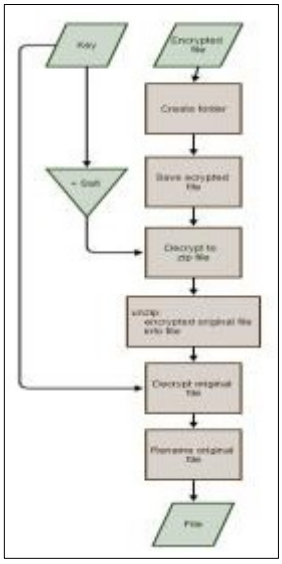

Fig. 10 - Decryption diagram

4 Conclusion

It was concluded that cryptography in general is critical to privacy among users. When it is necessary to make a private file share there must always be a safe method for this share to be reserved between the two entities. This article portrayed a possible solution for data encryption and private file sharing. The main objectives of the proposed application have been successfully completed and well demonstrated. An application was developed, and the encryption and decryption processes of this application were focused on this paper.

With this work it was possible to intensify the knowledge about cryptography in general and how it is possible to develop an application for data encryption in JavaScript, using several modules of node.js.

References

1. Cruz, B. F.; Domingo, K. N.; Guzman, F. E.; Cotiangco, J. B.; Hilario, C. B.: “Expanded 128-bit Data Encryption Standard”, International Journal of Computer Science and Mobile Computing, vol.6 (8), pp.133-134 (2017).
2. Branstad, D. K.: “Computer Security and the Data Encryption Standard”, Governm. Print. Off., Washington, D.C. (1978).
3. Microsoft: “What Is Cryptography?”, accessed (2017).
4. Oliveira, R. R.: “Criptografia Simétrica e Assimétrica: os Principais Algoritmos de Cifragem”, Revista Segurança Digital, Brasília, vol.2(3), pp. 21-24 (2012).
5. Friedl, S. J.: “An Illustrated Guide to Cryptographic Hashes”, accessed (2017).
6. Microsoft: “What is TLS/SSL?”, accessed (2017).
7. Node.js Foundation, “Report Node.js issue“, accessed (2017).
8. npm, Inc: “What is npm”, accessed (2017).
9. W3schools, html template, accessed (2017).
10. Node.js: “Node.js v9.3.0 Documentation – HTTPS”, accessed (2017).
11. Express: “Express - Basic Routing”, accessed (2017).
12. Node.js: “Node.js v9.3.0 Documentation – Crypto”, accessed (2017).
13. npm, Inc: “File-Encryptor”, accessed (2017).
14. npm, Inc: “Node-Zip”, accessed (2017).

A Data Encryption Application: Development Proposal

Implementation of the Algorithm AES in an Android Application

Eduardo Carneiro

Lusofona University of Porto, Portugal
eduardo.mcarneiro@hotmail.com

Abstract. In this paper is discussed the importance of Cryptography, the implementation of the cryptographic algorithm Advanced Encryption Standard (AES) in an Android application, as well as the difficulties faced during the development process. It was chosen the AES algorithm due to its efficiency, security and its easy implementation.

Keywords: Cryptography, AES, Encryption, Decryption, Android, Application.

1 Introduction

Over the years, technology has been improving at a large pace. Every day we depend more and more on our smartphones and computers to do everyday tasks, whether they are personal or for our company, where emails with sensitive data are sent and received and online banking transactions are made from our devices. This makes necessary the use of safety measures to ensure that out data isn't accessed by someone without the proper authorization. That's where cryptography comes in.

Cryptography is described by the author [1] as a branch of mathematics that is based on the transformation of data and can be used to provide several security services: confidentiality, data integrity authentication, and source authentication, and also to support non-repudiation.

There are several methods one can improve the safety of information. The one I chose to use is an Android application, the Text Safe application. In this paper, I will speak about the its development as well as encrypting and decrypting text using the cryptographic algorithm AES.

2 Advanced Encryption Standard

The cryptographic algorithm AES, was developed by Joan Daemen and Vincent Rijmen and was announced by the Federal Information Processing Standards Publica Publications (FIPS PUBS) in November 26, 2001. As described in the Federal Information Processing Standards Publication 197 [2], The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information". In this same publication [2], encryption and decryption are described as encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.

For the encryption and decryption of plaintext, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192 and 256 bits. [2].

2.1 Encryption key

For this application, I chose to let the user choose his/her own password when encrypting plaintext. The user has to create a password, the stronger the better, to be able to encrypt the plaintext. If the user wants to share the encrypted text, the user has to let the person know what password was used for the encryption. The most secure method is delivering verbally the password in person.

This application uses SHA-2, Secure Hash Algorithm 2, which is a cryptographic hashing function that, given an input, a 20 byte hash value known as a message digest.

3 Android Application

In this application it is possible for a user to encrypt plaintext, decrypt ciphertext and share the encrypted or decrypted plaintext. There is also a load file button.

To encrypt plaintext in this application, the user enters a password of his/her choosing, them enters the plaintext the user wants to encrypt and to finish, the user just needs to press the encrypt button. The encrypted text appears below the buttons.

To decrypt ciphertext, the user must enter the password used to encrypt the original text, enter the ciphertext and then press the decrypt button. If the wrong password is used, the user gets a message saying wrong password. When the correct password is used, the decrypted text appears below the buttons.

To share the encrypted or decrypted text, the user must first encrypt or decrypt something, or else it is shown to the user a message saying you need to encrypt/decrypt something. Once that has been done, the user gets several methods to share the message. The methods depend on what application the user has on the smartphone that allow him/her to share content.

The load file button shows a not yet available message. Due to some errors related with the application not being able to read a text file, this functionality is not available.

Fig.1 - Example of Encrypting Plaintext.

In the figure 1, we can see how using the password “hello” to encrypt the plaintext “test” we get the ciphertext “rnuUI1aZGxYwmd0tErZl7w”. If we were to change just a single letter from the text to encrypt, the result would be completely different.

3.1 Creating the application

To create this Android application, I used Java programming language. The AES algorithm used in the application to encrypt and decrypt was provided by [3]. Some changes were made by me to best suit the objective of the application. In the figures below can be seen the functions and code used in the application. Those functions are encrypt(), decrypt(), setKey() and share().

```
public static void setKey(String myKey){
    MessageDigest sha = null;

    try {
        key = myKey.getBytes( charsetName: "UTF-8");
        sha = MessageDigest.getInstance("SHA-1");
        key = sha.digest(key);
        key = Arrays.copyOf(key,  newLength: 16);
        secretKey = new SecretKeySpec(key,  algorithm: "AES");
    }catch (NoSuchAlgorithmException | UnsupportedEncodingException e) {
        e.printStackTrace();
    }
}
```

Fig. 2 - Function setKey().

```
public static byte[] encrypt(String strToEncriptal, String secret){

    try {
        setKey(secret);
        Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
        cipher.init(Cipher.ENCRYPT_MODE, secretKey);

        byte[] array=  cipher.doFinal(strToEncriptal.getBytes( charsetName: "UTF-8"));
        flag=1;

        return Base64.encode(array,  flags: 1);

    }catch (Exception e) {
        System.out.println(e.toString());
    }

    return null;
}
```

Fig. 3 - Function Encrypt().

```
public byte[] decrypt(String strToDecrypt, String secret){
    try {
        setKey(secret);
        Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5PADDING");
        cipher.init(Cipher.DECRYPT_MODE, secretKey);
        byte[] teste=  cipher.doFinal(Base64.decode(strToDecrypt.getBytes( charsetName: "UTF-8"),  flags: 1));
        flag=2;

        return teste;
    }catch (Exception e) {
        Context context = getApplicationContext();
        Toast toast = Toast.makeText(context,  text: "Wrong Password.", Integer.parseInt( s: "1"));
        toast.show();
    }
    return null;
}
```

Fig. 4 - Function decrypt().

In this functions we can see the AES algorithm that is being used as well as the message one gets when the application isn't used properly, as is shown in the decrypt() function as a "toast" that reads "Wrong Password" when the wrong password is used.

Fig. 5 - Example to Decrypt Ciphertext

Fig. 6 - Example of Wrong Password

In figure 5 we can see what happens when the correct password is used. The text we encrypted using the password "hello" appears in the area below the buttons. In figure 6 we can see what happens when the wrong password is used. A message is shown to the user saying "Wrong Password", as shown in the code of the figure 4.

```
public void share (View v){
    TextView text_done= (TextView) findViewById(R.id.text_done);
    String frase_original= text_done.getText().toString();
    EditText pass= (EditText) findViewById(R.id.password);
    String secretKey= pass.getText().toString();

    Log.i( tag: "Send email",  msg: "");

    String[] to= {""};
    String[] cc= {""};

    Intent textIntent= new Intent(Intent.ACTION_SEND);
    textIntent.setData(Uri.parse("to:"));
    textIntent.setType("text/plain");

    textIntent.putExtra(Intent.EXTRA_EMAIL, to); //Para quem se quer enviar
    textIntent.putExtra(Intent.EXTRA_CC, cc); //Quem está a enviar
    textIntent.putExtra(Intent.EXTRA_SUBJECT,  value: "TOP SECRET message");//Assunto

    if(flag==1){
        textIntent.putExtra(Intent.EXTRA_TEXT,  value: "The following message is Encrypted: \n\n"
                + frase_original + "\n\n  To Decrypt the text above, use the app " +
                "Encriptação AES."); //Mensagem
    }else if(flag==2){
        textIntent.putExtra(Intent.EXTRA_TEXT,  value: "The following message is Decrypted: \n\n"
                + frase_original + "\n\n  To Encrypt the text above use the app" +
                "Encriptação AES."); //Mensagem
    }

    if(flag==0 || secretKey.matches( regex: "")){
        Context context = getApplicationContext();
        Toast toast = Toast.makeText(context,  text: "You need to Encrypt/Decrypt something.",
                Integer.parseInt( s: "1"));
        toast.show();
    }else{
        try {
            startActivity(Intent.createChooser(textIntent,  title: "Send mail..."));
            finish();
            //Log.i("Finished sending email...", "");
        } catch (android.content.ActivityNotFoundException ex) {
            Toast.makeText( context: layout_2.this,
                    text: "There is no email client installed.", Toast.LENGTH_SHORT).show();
        }
    }
```

Fig. 7 - Function share().

In figure 7 we can the code used so that the user can share the text he/she encrypted or decrypted. As shown, there are several messages the use can be shown if the application is not used correctly.

4 Conclusion

The Advanced Encryption Standard algorithm is of simple implementation whether it is used for an Android application or a computer program. Even though the application isn't capable to do everything that was planned in the beginning, I still believe it is a good use of the cryptographic algorithm AES due to its speed and reliability.

With this project I learned how to understand cryptography, as well as the several methods one can use to protect his/her information, as well as sharing information in a way that others can't use, even if they have access to the encrypted text.

References

1. Barker, E.: "Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms", NIST Special Publication 800-175B, Computer Security, National Institute of Standards and Technology (2016).
2. Federal Information Processing Standards Publications (FIPSPUBS): "Announcing the Advanced Encryption Standard" (2001).
3. Gupta, L.: "AES Java algorithm", accessed (2017).

Papers in alphabetical order

A Data Encryption Application: Development Proposal
Encrypt and Decrypt Several Types of Data……..…… page 52

A Data Encryption Application: Development Proposal
Implementation of the Algorithm AES in an Android Application……..…. page 61

Cybersecurity of Social Media: Case in Health Area……..…. page 14

Information Gathering through Image Leaking……..……..…. page 45

Privacy and Security Control in E-Health…….…. page 20

Privacy and Security in the Era of Digital Health: Case mHealth..……..…. page 6

Secure Data Storage of Health Information …….…. page 28

Secure on Site Caching of Encrypted Cloud Storage...……..…….…. page 40

Securing Data Storage of Cloud Storage...……...……. page 34

Authors in alphabetical order

Diogo Oliveira..……..……. page 34

Eduardo Carneiro ….....…. page 61

Leandro Mendes.….....…. page 6

Miguel Fonseca …….....……..…. page 28

Nuno Cunha …….....……...…… page 52

Paulo Moura…….....……..…. page 20

Rodolfo Matos...…….....……. page 45

Rui Oliveira..…….....……. page 40

Susana Dias …….....……...…. page 14

Telmo Morais...…….....……. page 45

PRIVACY AND SECURITY CONFERENCE 2018

PRIVACYANDSECURITYCONFERENCE.PT