UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

DIPARTIMENTO DI INFORMATICA

PhD Program in Computer Science and Mathematics
34 **cycle**

Research Project

PhD Student: Joseph Ogochukwu Aneke

Supervisor: Prof. Carmelo Antonio Ardito

Coordinator: Prof. Maria F. Costabile

PhD student signature ______________________

Supervisor signature Carmelo Antonio Ardito

1. Research title: Towards more secure interaction in the Cyberspace

2. Research area: Cybersecurity and Human Computer Interaction

3. Research motivation and objectives

In todays connected world, everyone benefits from the increasing popularity of the use of online services such as web-based emails, social networks and blogs. While this is applauded, it has made them a popular platform for attackers. Cybercriminals leverage such services to spread spam, malware, and steal personal information from their victims. Cyberattacks endanger individuals and companies, as well as vital public services and infrastructures. Confronted with spreading and evolving cyber threats, organizations and individuals are falling behind in defending their systems and networks, and they often fail to implement and effectively use basic cybersecurity practices and technologies.

Successful security depends on systems, technology and people (users) collaborating to identify threats, weaknesses, and solutions. However, many initiatives today focus on systems and technology, without addressing well-known user-related issues. In fact, users have been identified as one of the major security weaknesses in today's technologies, as they may be unaware that their behavior while interacting may have security consequences. They are the weakest link in the security chain [10]. However, if users are to be considered one of the greatest risks to system security, they are also one of the greatest hopes for system security. In this perspective, Human–Computer Interaction (HCI) becomes a fundamental pillar for designing more secure systems. By considering the users — their peculiar characteristics (Biometrics), what they know, how they use the system (behaviour), and what their needs are —then designers will be better positioned to empower them in their digital security role and increase the usability of security solutions. The human biometrics has been very useful in developing systems which recognises a person having a specific physiological and or behavioral characteristic unique to her/him, e.g. finger prints, iris, facial, etc. This Biometric-based authentication has firmly established itself as one of the most reliable, efficient, and versatile tools for providing discretionary access control to a secure resource or system [8].

Ensuring safe and secure communication and interaction among users and, respectably, their on-line identities presents unique challenges to academics, as well as industry and the public. Presently at the University of Bari Aldo Moro, there is an ongoing work at the IBM lab on cybersecurity which is developing an integrated model called "the Hack Space" made up of four components: Knowledge, Organization, Skills & Tools, and Collaboration [2]. This is aimed at training and equipping cyber security professionals for the future to be ready to operate in real business world. As an extension, we propose in this project to integrate biometric features to this model to checkmate cyber-attacks.

The project is motivated by the research question: "*How can existing techniques and tools be improved and integrated to support the design of usable and secure systems?*"

This research question can be broken down to the following questions.

- RQ1: Which concepts/components from Human-Computer Interaction, Security, and Software Engineering can be harmonized to support the design of secure and usable systems?
- RQ2: What are the characteristics of tools supporting the design of secure and usable systems?
- RQ3: How can User-Centered Design techniques be improved to support the design of usable and secure systems possibly implementing biometrics security solutions?

4. State of the art

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes [3]. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

Cybercrime is a serious threat for Internet users. Miscreants infect their victim computers and control them to perform malicious activities, such as sending email spam [18] or phishing [4], stealing their victims' personal information [17], performing denial of service attacks [9], or mining digital currencies [11]. Cybercrime operations are a successful business, generating important revenues for attackers [6, 12]. To perform malicious activity on online services, such as online social networks, web based email services, and blog platforms.

There are different types of cybersecurity threats. The main one, which will be also addressed in this research are:

- ***Ransomware*** is a type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered or the system restored.
- ***Malware*** is a type of software designed to gain unauthorized access or to cause damage to a computer.

- ***Social engineering*** is a tactic that adversaries use to trick you into revealing sensitive information. They can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats listed above to make you more likely to click on links, download malware, or trust a malicious source.
- ***Phishing*** is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like credit card numbers and login information. It's the most common type of cyber-attack.

Before now, computer security research has focused on technical defences to safeguard systems. Obviously, it is now clear that technical measures are not enough: "People are the weakest link in the security chain." This statement by Bruce Scheiner [16] has been confirmed by reformed hacker Kevin Mitnick [14], who claims that the most effective and devastating means of attacking a system is through social engineering – an attack that targets authorized users of that system and attempts to trick, con or otherwise compel them to break security policy. Recent research efforts to address human factors in security have concluded that security mechanisms are too difficult to use [21], and that most users do not maliciously break security policies [1, 15, 19], but do so as a consequence of bad design, complex requirements or an inadequate security culture. The focus of Human-Computer Interaction in security (HCISec) research has been the improvement of user interfaces to security tools [5, 7, 13]. Central to HCI is the notion of usability, which some authors define as "…the ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component." [10]. Given this definition, a significant portion of HCI is concerned with user interfaces to software systems. While usability and user interface design can be said to be looking at the issues of making a given interaction easier, HCI design has come to develop a broader picture, which includes identifying and resolving conflicting goals in a socio-technical system consisting of the stakeholders and their activities. The design process must not only consider the characteristics of the immediate user, but their goals when interacting with the system, and the physical, social and cultural context in which that interaction takes place. Also central to the discipline of HCI is the concept of human factors and how these affect and shape how people react to computer systems. Human factors typically refer to the intrinsic properties of people, such as short-term memory, visual acuity, physical dexterity, etc. These properties can strongly influence the design of a system, most visibly at the interface level, but also at a more fundamental level such as the underlying model of operation of the system.

5. Problem approach

The focus of HCI is the investigation of relationships between computer technology, human activity and society. For this project, we are interested in the development of artefacts, services and systems that improve and make same available to software engineers for use in developing systems devices for use online.

The following research methodology will be used in this work:

1. Perform extensive literature research on cybersecurity
2. Perform extensive literature research on current HCI techniques
3. Identify weaknesses in current measures in place to checkmate cybercrime treat types which will cover ransomware, malware, social engineering and phishing.
4. Explore different Cybersecurity and HCI implementation approaches with a view to proposing suitable models for implementation

6. Expected results

A fundamental objective of HCI research is to make systems more usable, more useful, and to provide users with experiences fitting their specific background knowledge and objectives. The following are expected results:

1. A model for teaching and learning cybersecurity
2. A set of metrics for identifying abnormal user behaviors through recognition of their physiological and behavioral traits for real time access and protection.
3. Social biometrics as an additional security measure (new online traits harvested from social networks Twitter, Wikepedia, Facebook and LinkedIn social networks etc). will be integrated for real time access and protection

7. Phases of the project

S/N	ACTIVITY	EXPECTED OUTCOME
1	**1st year: Study of the literature, of the state of art and other basic research materials**	
1.1	Study of the state of the art regarding cybersecurity with particular Interest on their operation mode, types, and causes and effect	
1.2	Review of HCI objectives with a view to resolving feed backs from 1.1	
1.3	Attendance of courses and seminars included in the doctorate study plan	
1.4	Participation to international schools and conferences regarding topics relevant for the research theme and the goals planned.	
1.5	Review 1.1,1.2 and 1.3	Publish new findings if any
2	**2nd year: Development of methods**	
2.1	Study of the works produced by other researchers with the same goals;	
2.2	Presentation of research proposal for approval	
2.3	Amending the research proposal and developing data collection tools and sample size	
2.4	Data Collection, analyzing and filling of gaps (if there is any)	
2.5	Review 2.1,2.2, 2.3 and 2.4	Publish new findings if any
3	**3rd year: Implementation of findings and writing of the doctorate thesis**	
3.1	Comparison with other research groups works, both national and international, with possible stages in foreign universities or research centers.	
3.2	Analysis of the results obtained and implementation	
3.3	Writing of the doctorate thesis	Publish findings

8. Result evaluation

The results of this project will be subject to empirical evaluation and possible industry trials.

9. Possible reference persons external to the department

I hope to identify some possible reference persons external to the department, working in USA/European universities or research centers, during summer schools or during time spent abroad.

10. References

[1] Adams, A. & Sasse, M. A. Users Are Not The Enemy. Communications of the ACM. Vol. 42, No. 12 December 1999.

[2] Baldassarre M.T., Barletta V., Caivano D., Ragusco D. and Scalera M. (2019). Teaching Cybersecurity: The Hack-Space Intergrated Model. To appear in Proceedings of Italian Conference on Cybersecurity (ItaSec '19).

[3] Cisco.: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html. Last access on January 19, 2019.

[4] Desolda G., Di Nocera F., Ferro L., Lanzilotti R., Maggi P., Marrella A. (2019). Alerting Users about Phishing Attacks. To appear in Proceedings of International Conference On Human-Computer Interaction (HCII '19).

[5] Dourish, P. & Redmiles, D. (2002). An Approach to Usability Security Based on Event Monitoring and Visualization. In Proceedings of New Security Paradigms Workshop.

[6] Freiling F. C., Holz T. and Wicherski G. (2005). Botnet Tracking: Exploring a RootCause Methodology to Prevent Distributed Denial-of-Service Attacks. In Proceedings of European Symposium on Research in Computer Security (ESORICS '05).

[7] Fukuyama, F. Social Capital and the Civil Society (1999). In Proceedings of 2nd Conference on Second Generation Reforms.

[8] Gavrilova M. and Yampolskiy R. (2011). Applying biometric principles to avatar recognition Transactions on computational science XII, 140-158.

[9] Huang D. Y., Dharmdasani H., Meiklejohn S., Dave V., Grier C., McCoy D., Savage S., Weaver N., Snoeren A. C. and Levchenko K. (2014). Botcoin: monetizing stolen cycles. In Proceedings of Symposium on Network and Distributed System Security (NDSS '14).

[10] Institute of Electrical and Electronics Engineers (1990). IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries.

[11] Kanich C., Kreibich C., Levchenko K., Enright B., Voelker G., Paxson V. and Savage S. (2008). Spamalytics: An empirical analysis of spam marketing conversion. In Proceedings of ACM Conference on Computer and Communications Security (CCS '08).

[12] Kanich C., Weaver N., McCoy D., Halvorson T., Kreibich C., Levchenko K., Paxson V., Voelker G. and Savage S. (2011). Show Me the Money: Characterizing Spam-advertised Revenue. In Proceedings of USENIX Security Symposium.

[13] Ka-Ping, Y. (2002). User Interaction Design for Secure Systems. http://zesty.ca/sid

[14] Mitnick, K. D. & Simon, W. L. (2003). The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons Inc.

[15] Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link': a human-computer interaction approach to usable and effective security. BT Technical Journal, 19 , pp 122-131.

[16] Schneier, B. Secrets and Lies. (2000). John Wiley & Sons.

[17] Stone-Gross B., Cova M., Cavallaro L., Gilbert B., Szydlowski M., Kemmerer R., Kruegel C., and Vigna G. (2009). Your Botnet is My Botnet: Analysis of a Botnet Takeover. In Proceedings of ACM Conference on Computer and Communications Security (CCS '09).

[18] Stone-Gross B., Holz T., Stringhini G. and Vigna G. (2011). The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns. In Proceedings of USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '11).

[19] Weirich, D. & Sasse, M. A.(2001). Pretty Good Persuasion: A first step towards effective password security in the real world. New Security Paradigms Workshop.

[20] Yanushkevich S., Gavrilova M., Wang P. and Srihari S. (2007). Image Pattern Recognition: Synthesis and Analysis in Biometrics, World Scientific Publishers.

[21] Zurko, M. E. & Simon, R. T. (1997). User-Centered Security. New Security Paradigms Workshop.