1. Abstract of Research Work

Digital Identity

When we access to Internet site as a social network, uploading pictures there, or registering our travel information by example, we are making visible to other people our preferences like interests, locations, friends; leaving information and footprints that characterize our identity, preferences and behavior.

Government systems actually are harvesting data about us, like taxes, police and migration records, also records obtained from credit cards or shopping invoices, moreover they concentrate medical or records of documents as identification, passport, driver license, or social security number by example. All information could be interchanged across the Internet, putting in risk our privacy, sharing these confidential data.

When we associate our personal information in a global context en Internet, taking our data from government systems, social networks, banking records, shopping records as buying preferences, Internet navigation preferences, and more; we are constructing a Digital Identity of an individual person.

The goal of this research project consists in a proposal of a technical approach to solve the problem related before.

The research project will contain the study, analysis and technical proposal with the following aspects:
- Systematic review of the work made before.
- Proposal of privacy solution
- Architecture of the reference model
- Interoperability reference model for Digital Identity

Keywords: Digital Identity, Privacy, Confidential Data, Information harvesting, Data Interchange

2. Field of Study: Information Security

Information security is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Information assurance is the responsibility of IT security specialist and is the act of ensuring that data is not lost when critical issues arise.

Some of the most common threats today to avoid information assurance are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

Identity theft, related to extortion by example, is the attempt to act as someone

else usually to obtain that person's personal information or to take advantage of their access to vital information.

Governments, military, corporations, financial institutions, hospitals and private businesses harvests and saves a great deal of confidential information about their employees, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

For the individual, information security has a significant effect on privacy, which may concern CIA (confidentiality-integrity-availability) principles:
- Access control: Access to protected information must be restricted to people who are authorized to access.
- Identification: is an assertion of who someone is.
- Authentication: is the act of verifying a claim of identity.
- Authorization: After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform.

Keywords: Data security, Crime prevention, Information Security, CIA principles

CONGRESS

Congress #1
Name: 2015 SRI Security Congress
Acronyms: SRI Security Congress
URL: http://conferences.secau.org
Paper submission deadline: 30 September 2015
Submission procedure:
- Implies the authors' willingness to register and present the paper at the conference.
- In the case of papers with multiple authors, at least one author is required to register, pay the conference registration fee and attend the conference to present the paper. Other co-authors of the same paper should register separately and pay the applicable registration fee, only if they also plan to attend the conference
- An accepted paper will only be published in the proceedings if at least one author has addressed the reviewer's feedback, registered and paid the appropriate fees to attend the conference to present the paper and completed a copyright declaration form (see link below for copyright form
- Authors submitting paper(s) to the 2015 SRI Security Congress are required to submit using the online submission system – https://cmt.research.microsoft.com/SRISC2015
- The registration fee covers publication of up to two accepted papers

Papers must:
- Adhere to the maximum word limit of 3500 words including the abstract and text, but excluding the references
- Include a 200 word abstract and keywords identifying the paper's area of research
- Be submitted prior to 30 September 2015
- Camera Ready Papers conform to the 2015 Congress Academic Paper Format Guidelines (see links below to paper format guidelines and paper format template). Papers that do not conform will be returned to the author(s) for corrections

Best Paper Awards will be given for:
- Best paper in each conference
- Best paper overall (selected from the 5 best papers awarded in each conference)

Best Paper Awards will be announced at the Congress Dinner.

Organization:
- Edith Cowan University. Security Research University
- Australian Security Magazine
- Australian Computer Society
- CISCO

Congress #2
Name: World Congress on Internet Security
Acronyms: WorldCIS-2015
URL: http://www.worldcis.org
Paper submission deadline: 01 June 2015
Submission procedure:
The conference registration fee includes luncheons, refreshments, workshops, industrial presentation and one copy of the conference proceedings in electronic format (CD). At least one author must attend the conference to present the paper. (Participants will incur £250.00 for additional proceedings. Therefore, if you do not need additional proceedings, please ignore this option during the registration).

The submissions should be in Adobe Portable Document Format (PDF) or Word Document Format (DOC) only.
The following style files and templates are available for users of LaTeX and Microsoft Word.

Types of Submission:
Research Paper
Completed research paper. A total of 4 to 6 A4 pages for a paper including all figures, tables, and references not more than 20 references.
Extended Abstract (Work in Progress)
The extended abstract should not exceed 2 pages (including introduction, body of knowledge and conclusion, supported by not more than 10 references). Please submit your extended abstract in PDF format at **extendedabstract@worldcis.org**
Camera Ready Paper
After applying the reviewers' feedback, the camera ready paper needs to be emailed to **final_paper@worldcis.org**
IEEE Copyright
The IEEE Copyrigth form is available as a **Word File** and in **PDF** (Please sign, scand and email it to **copyright_form@worldcis.org**).

Abstract and Extended Abstract (Work in Progress) Submission Date	June 01, 2015
Notification of Abstract and Extended Abstract (Work in Progress) Acceptance/Rejection	June 20, 2015
Research Paper, Student Paper, Case Study, Report Submission Date	June 20, 2015
Notification of Research Paper, Student Paper, Case Study, Report Acceptance /Rejection	July 10, 2015

Organization:
- IEEE UK/RI Computer Chapter

JOURNALS

Journal #1
Name: International Journal of Information Security Science
Acronyms: IJISS
URL: http://www.ijiss.org/ijiss/index.php/ijiss/index
Paper submission deadline: NA
Submission procedure:
The scope of IJISS comprises original research on all aspects of security science, engineering and technology. Original research results, scientific reviews and short communication notes in various fields of security science and technology are considered for publication. The publication language of the journal is English.

IJISS is published 4 times in a year. Original research results, applications, implementations, scientific reviews and short communication notes in information security science and technology are considered for publication.
Manuscripts previously published in another journal are not accepted. Manuscripts with a suitable balance of practice and theory, pure theory or applications are accepted.

A review article is expected to give in-depth information and satisfying evaluation of a topic supported with an extensive list of sources.
Short communication notes are also accepted to share the first outcomes of researchers' on-going original research work.
The IJISS currently has an acceptance rate of 32%. EBSCO, DOAJ, Index Copernicus, Google Index have indexed the IJISS.

Each of submitted manuscripts is reviewed at least two reviewers. The period of revisions is at most two months.

As part of the submission process, authors are required to check off their submission's compliance with all of the following items, and submissions may be returned to authors that do not adhere to these guidelines.
- The submission has not been previously published, nor submitted to another journal for consideration (or an explanation has been provided in Comments to the Editor).
- The submission file is in PDF, OpenOffice, Microsoft Word, RTF, or WordPerfect document file format.
- Where available, URLs for the references have been provided.
- The text is single-spaced; uses a 12-point font; employs italics, rather than underlining (except with URL addresses); and all illustrations, figures, and tables are placed within the text at the appropriate points, rather than at the end.
- The text adheres to the stylistic and bibliographic requirements outlined in the Author Guidelines, which is found in About the Journal.

If submitting to a peer-reviewed section of the journal, the instructions in Ensuring a Blind Review have been followed**.**

Organization: GAZI UNIVERSITY

Journal #2
Name: Journal of Information Security
Acronyms: JIS
URL: http://www.scirp.org/journal/jis
Paper submission deadline: NA
Submission procedure:

Papers submitted to Scientific Research Publishing must contain original material. The submitted paper, or any translation of it, must neither be published, nor be submitted for publication elsewhere. Violations of these rules will normally result in an immediate rejection of the submission without further review.

Contributions should be written in English and include a 100-300 words abstract. SCIRP's journals usually welcome the following types of contributions:

• Original research articles
• Review articles, providing a comprehensive review on a scientific topic

All manuscripts and any supplementary material should be submitted via SCIRP's Paper Submission (and Manuscript Tracking) System (PSS) at http://papersubmission.scirp.org/. Please follow the instructions given on this site.

General Peer-Review Process
In short, all manuscripts submitted for publication in our journals are strictly and thoroughly peer-reviewed. The review process is single blind. If the manuscript is accepted for full review, it will be reviewed by a minimum of two external reviewers.

Submitted manuscripts will undergo a detailed initial check including a Plagiarism Check in the Editorial Office. An Editor – usually the Editor-in-Chief or a board member of the journal – together with the Editorial Office takes charge of the peer-review process. It starts with a Preliminary Review by the Editor (finished no more than 10 days after manuscript submission).

After a manuscript is accepted for full review, the Editor will collect at least two review comments and prepare a decision letter based on the comments of the reviewers (finished no more than 4 weeks after preliminary review). The decision letter is sent to the Corresponding Author to request an adequate revision (peer-reviewed again whenever necessary). The author will be asked to format the manuscript according to SCIRP's template before it goes into typesetting and proofreading with the publisher. The author will receive the paper in PDF produced by SCIRP for checking before it is published online. The Generic SCIRP Peer Review Process visualizes this.

Organization: Scientific Research