



Institute of Technology

Ciência sem Fronteiras / Science Without Borders

Postgraduate Project Template

Institution:	Institute of Technology Blanchardstown
Title of Postgraduate Opportunity: (include level of study)	Information Security & Digital Forensics in Master and PhD levels
PI Name & Contact Details:	<p>Dr Anthony Keane Room 131, Block E Department of Informatics School of Informatics & Engineering Institute of Technology Blanchardstown Dublin 15, Ireland</p> <p>Phone: +353 1 885 1085 Fax: +353 1 885 1004</p>
Department/School:	Department of Informatics
Research Centre /Group:	Information Security & Digital Forensics (ISDF) Research Group
Research Centre/Group website:	http://www.digitalsecurity2020.com
<p>Brief Summary of PI research / research group /centre activity</p> <p>The Information Security & Digital Forensics (ISDF) research group was setup in 2007 at the Institute of Technology Blanchardstown (ITB). The group has evolved from the distributed systems and networks research activities in ITB in response to the widespread recognition of the serious and growing shortage of college post-graduates to meet industry and research demands in the areas of network security and computer forensics.</p> <p>The primary aims of the ISDF research group are:</p> <ol style="list-style-type: none"> 1. To attract students into full-time and part-time education and training, leading to BSc, MSc and PhD degrees 2. To facilitate college staff and local industry to engage in high level research 3. To address the set of challenges created by new security threats through expertise and research 4. Help information security companies to generate innovative solutions leading to lucrative Intelligent Property and patentable material 5. Help companies to be business compliant and to ensure their computer data is properly protected according to the requirements of the law 6. Have a centre of excellence at ITB that would help local companies with security requirements and knowledge 7. Provide graduate opportunities to create campus companies through the dedicated Industrial Innovation Centre in the LINC building 	

The **ISDF** research group run a Honeynet monitoring facility as part of the Irish Chapter of the **Honeynet Project** (<http://www.honeynet.org/>). The **ITB Honeynet** facility is used to conduct investigations into illegal activities on the Internet. The Honeynet is a network of vulnerable computers called Honeypots that are monitored for malicious activity from the Internet. Everyday we detect hundreds of attacks and some of these attacks have managed to infect the Honeypot computers.

ITB Honeynet - <http://honeyn3t.ie/>

Brief Description of Masters or PhD Project

Projects cover activities in Information Security & Digital Forensics such as Intellectual Property Theft, Electronic Discovery, Document Analysis, Email Forensics, Computer Misuse and Fraud Investigations.

Identification of Information Stealing and Spying Software

This project will consist of infecting ‘**sandbox**’ hard drives with various information stealing and/or spying malware. The general approach will be to use various forensically acceptable methods that are admissible in court, to detect and identify the malware on the hard drives. These methods will consist of searching the image of a hard drive for evidence of the malware using forensic investigation software like **Encase** and **FTK**. The analysis of the activity on the ‘**live**’ systems will be monitored and evaluated using software such as **Gargoyle** and other methods to identify the malware. The aim of the project is to use the test cases as a basis to determine which methods perform better and are the most reliable method of positively identifying malware on a computer. The project will focus on popular operating systems that are frequently targeted by malware. This type of project will be useful where there is a need to identify information stealing or spying software on **PC’s** in criminal or civil court cases and where intellectual property has been stolen.

Universal End-User Activity Tracker application

This project is building an application that can covertly display the timeline of activity of any user on any computer platform either locally or remotely.

Dynamic Multi-Tenant Security Awareness Profiling

This project is to build a framework and implement an application to detect attackers during their discovery phase and to neutralise the attacker before they can become an active threat.

Forensics in the Cloud

Cloud Computing offers new challenges for the forensics investigator in terms of recovery of evidence from remote storage and remote processing machines. New methodologies, tools and policies will be needed to ensure that data can be found and for the integrity of the evidence recovered.

Key Attributes of Project for Brazilian Postgraduate Students

The **ISDF** research group actively engages in partnerships with **SME** companies to cooperate and participate in **R&D** funded projects with mutual benefit to both **ITB** and the industrial partner. Research projects focus on real-world problems as presented by the SME companies and researchers work closely with the SME companies.

Name and contact details for project queries, if different from PI named above:

anthony.keane@itb.ie

Please indicate graduate disciplines which are eligible for application:

BSc in Computing

Alignment with Science Without Borders Priority Areas:

Please indicate the specific programme priority area under which the proposed postgraduate project fits – choose only one (tick box)

Engineering and other technological areas	
Pure and Natural Sciences (e.g. mathematics, physics, chemistry)	
Health and Biomedical Sciences	
Information and Communication Technologies (ICTs)	<input checked="" type="checkbox"/>
Aerospace	
Pharmaceuticals	
Sustainable Agricultural Production	
Green Chemistry	
Oil, Gas and Coal	
Renewable Energy	
Minerals	
Biotechnology	
Nanotechnology and New Materials	
Climate Change	
Biodiversity and Bioprospection	
Marine Sciences	
Productive Inclusion and Social Technologies	
Housing and Sanitation	