**Project N1: Malicious Insider Threat Key Indicators and Dataset analysis.**

**Project Outline**

Insider threat issue is complex area for researcher community to address, and to deal with this kind of security breaches we have to think differently, as must of previous approaches address this problem from one aspect usually technical solution which applied to particular application or systems.

**Project Objectives**

The aim is to find out the main indicators that indicate the behaviors of any potential insider threat (Human Factor).

Objectives are:

* Review Insider threat incident cases.
* Identify the behavior of insider threat.
* Validate your indicators by analyses datasets (Data mining) to identify any malicious user. (Dataset will be provided)

**Prerequisite**

Programming skills.

Technical Requirements: YELLOW

**Expected Deliverables**

* Literature review of Insider Threat.
* Insider Indicators.
* A report on the design of the approach with the analysis and validation your results.

**Supervisor – Nebrase Elmrabit**

PhD Student (Insider Threat Prediction)

Loughborough University

E: n.elmrabit@lboro.ac.uk

**Project N2: Home Network Intruder Detection Alert Using Mobile Application.**

**Project Outline**

With the use of Internet of Things (IoT) nowadays, it is simple to connect any devices at home (e.g., mobile phone, tablet, gaming console, TV, network storage devises, printer, CCTV, sensor, and many more) to your Local Area Network. However, the need of developing an easy way for the home user to manage and monitor these connections is vital.

**Project Objectives**

The aim of this project is to create a mobile app solution to scan the private network for any unauthorised connection.

Objectives are:

* Develop a new mobile app that gives alarms for any discovered unauthorised access to your Private network (LAN or WLAN).
* Easy user interface to manage a whitelist of trusted devices which allowed to connect to your network using the app.
* Sending SMS notification.

**Prerequisite**

* Programming skills (Java).
* Android Studio.
* Good knowledge of TCP/IP
* Technical Requirements: YELLOW

**Expected Deliverables**

* Mobile app
* User manual

**Supervisor – Nebrase Elmrabit**

PhD Student (Insider Threat Prediction)

Loughborough University

E: n.elmrabit@lboro.ac.uk

**Project N3: Insider Threat --- Data Loss Prevention System.**

**Project Outline**

The increasing number of data breach carried by authorised users “Insiders”. And the urgent need to mitigate from such a threat. We can develop a control system that monitor data communication flow and prevent data leakages.

**Project Objectives**

The aim of this project is to mitigate the level of insider threats by:

* Develop DLP system using Squid proxy server “Linux”.
* Content filtering based on criteria.
* Writing java code and install it on the client computer that search on the bodies of website text (e.g., Hotmail) to compare it with the organisation’s intellectual property files. If similar text is found the proxy server will drop the packet and notify system administrator.

**Prerequisite**

* Programming skills.
* Linux.
* Technical Requirements: YELLOW

**Expected Deliverables**

* Literature review of existing approaches.
* Implementation of the DLP system for HTTP request and HTTPS is an advantage.
* Report.

**Supervisor – Nebrase Elmrabit**

PhD Student (Insider Threat Prediction)

Loughborough University

E: n.elmrabit@lboro.ac.uk