



**SCONE**

**Towards  
Excellence in  
Scotland**

## Details

**Meeting:** SCONE, 25/02/2010

**Place:** Room H.18, Merchiston Campus, Edinburgh Napier University.

**Details:** Sandwiches, Tea and coffee from 12pm, Session starts 1:10pm

**Chair:** Prof Bill Buchanan

## Objectives

This SCONE event aims to showcase the excellence in the research built around the SICSA Next Generation Internet theme. The programme covers a wide range of research topics, but with a special focus on presentations on the areas of security and trust. For this the SICSA Next Generation Internet theme outlines the development of the Internet towards a ubiquitous infrastructure, of which key research targets are related to security and trust. Without these the Internet will not truly scale to encapsulate every aspect of our lives, and leave threats to the future economy and to our own personal integration with the Internet.

## Schedule

These timings are likely to change, and are just in a draft form.

- 1:10pm Social Network Security and Privacy: The Good, the Bad and the Ugly, Mike Just (University of Edinburgh)
- 1:30pm SecureAngle: Improving Wireless Security with Angle-of-Arrival, Kyle Jamieson (UCL)
- 1:50pm Knowledge sharing for systems engineering and the Internet of Things, Paola Di Maio (University of Strathclyde)
- 2:10pm Social Roles for Opportunistic forwarding, Greg Bigwood (University of St. Andrews)
- 2:30pm Novel Information Sharing Architecture between the Police and their Community Partners, Omair Uthmani (Edinburgh Napier University)
- 2:50pm Coffee
- 3:00pm 1-N OT Algorithms in Privacy-Preserving Investigations, Zbigniew Kwecka (Edinburgh Napier University)
- 3:20pm Profiling Normal Network Behaviour for Robust Anomaly Diagnosis, Angelos Marnierides (Lancaster University)
- 3:40pm Understanding Tidal Fading on Rural Long Distance Over-Water Wireless Links, Alex Macmillan (University of Edinburgh)
- 4:00pm Intrusion Detection and Response in Open Multi-agent Systems, Shahriar Bijani (University of Edinburgh)
- 4:20pm Cross Layer Neighbourhood Load Routing for Wireless Mesh Networks, Liang Zhao (Edinburgh Napier University)
- 4:40pm Virtual Worlds, Real Traffic: Interaction and Adaptation, Iain Oliver (University of St Andrews)
- 5:00pm Security Challenges for Learning in 3D MUVE – Our Experiences, Indika Perera (University of St Andrews)

## Overview

### **Social Network Security and Privacy: The Good, the Bad and the Ugly, Mike Just (University of Edinburgh)**

While creating new opportunities for users to communicate, collaborate and share information, social networks (e.g., Facebook) also introduce some interesting challenges for both security and privacy. In this talk, I will review recent work in this area and discuss some of the outstanding research challenges.

### **SecureAngle: Improving Wireless Security with Angle-of-Arrival, Kyle Jamieson (UCL)**

Wireless networks play a key role in our business and personal lives, but make the network vulnerable to attack from a comfortable distance. Attackers circumvent security protocols such as WEP and WPA with impunity, allowing them to break into the network and resulting in disastrous consequences for organisations. The result is an ongoing competition between new exploits and better wireless security protocols. To fundamentally change this status quo, we propose SecureAngle, an approach to wireless security designed to operate alongside and strengthen existing wireless security protocols. SecureAngle uses cutting-edge multiple antenna signal processing to profile the directions at which a client's signal arrives at the access point and thereby construct signatures that uniquely characterise each client. In this talk, I will explore some potential uses of SecureAngle's signatures: virtual fences, to disallow wireless connections from outside a building or conference hall; address spoofing protection, to prevent malicious clients from masquerading as trusted clients; and a number of more speculative future applications.

### **Knowledge sharing for systems engineering and the Internet of Things, Paola Di Maio (University of Strathclyde)**

Systems Engineering as it is taught and practiced today, often does not account for the strategic importance of knowledge sharing and knowledge exchange. This can contribute to some poor understanding and consequent sub optimal systems architectures and configuration. Security and trust are a key inhibitors or promoters of knowledge sharing and exchange. In my research I look at future scenarios, which I refer to broadly as *networks of things*. I will share with the audience some of the underlying research questions, and speculate what will knowledge exchange look like in the age of embedded intelligence.

### **Social Roles for Opportunistic forwarding, Greg Bigwood (University of St. Andrews)**

Opportunistic networks exploit human encounters to enable new mobile networked applications. Efficient routing for these types of networks relies on utilising encounters between nodes so that messages are moved closer to their destination. Previous work has looked at using encounter-based social network data for routing, including schemes using social network analysis to identify communities or to find metrics that can be used to identify favourable routes. In this work we look at the potential of classifying nodes using social roles to find nodes with equivalent connections that can be used for forwarding.

### **Novel Information Sharing Architecture between the Police and their Community Partners, Omair Uthmani (Edinburgh Napier University)**

The exchange of information between the police and community partners forms a central aspect of effective community service provision. In the context of policing, a robust and timely communications mechanism is required between police agencies and community partner domains, including: Primary healthcare (such as a Family Physician or a General Practitioner); Secondary healthcare (such as hospitals); Social Services; Education; and Fire and Rescue services. Investigations into high-

profile cases such as the Victoria Climbié murder in 2000, the murders of Holly Wells and Jessica Chapman in 2002, and, more recently, the death of baby Peter Connelly through child abuse in 2007, highlight the requirement for a robust information-sharing framework. This presentation presents a novel syntax that supports information-sharing requests, within strict data-sharing policy definitions. Such requests may form the basis for any information-sharing agreement that can exist between the police and their community partners. It defines a role-based architecture, with partner domains, with a syntax for the effective and efficient information sharing, using SPoC (Single Point-of-Contact) agents to control information exchange. The application of policy definitions using rules within these SPoCs is inspired by network firewall rules and thus define information exchange permissions. These rules can be implemented by software filtering agents that act as information gateways between partner domains. Roles are exposed from each domain to give the rights to exchange information as defined within the policy definition. This work involves collaboration with the Scottish Police, as part of the Scottish Institute for Policing Research (SIPR), and aims to improve the safety of individuals by reducing risks to the community using enhanced information-sharing mechanisms.

#### **Privacy-Preserving Data Retrieval Framework, Zbigniew Kwecka (Edinburgh Napier University)**

Surveys show that the invasion of privacy is among the things people fear the most from the coming years. These fears seem to be justified, in the light of a number of cases where user data has leaked or has stolen from large databases of public institutions, retail network and social networking sites. New technologies allowed for fast digitalisation of operational procedures used by many organisations. These also affected the way public authorities conduct their investigations. Organisations such as Police, HMRC, and Home Office need to request information from third-parties on regular basis. Depending on the way these are performed human and natural rights of the researched data-subject can be neglected and/or investigation can be jeopardised. This presentation gives an insight on how the Privacy Enhancing Technologies (PETs) can be used to enhance investigative data retrieval to protect against possible negative outcomes for data-subjects or for investigations. Techniques discussed will include use cases for private matching and private equijoin algorithms, as well as novel technique for retrieval of data based on privacy protected database queries.

#### **Network Anomaly Detection, Angelos Marnierides (Lancaster University)**

In recent years, network anomaly detection has become an important area for both commercial and academic interests. The diverse and dynamic characteristics of the Internet which consists of heterogeneous networked systems pose a great challenge in identifying and classifying abnormal traffic patterns. An initial objective for efficient anomaly detection is to set a stable statistical metric known as the normal behaviour model, which subsequently acts as a reference scheme for observing deviations referred to as anomalies. In this talk we will discuss the current trends in anomaly detection and elaborate on our findings from employing a particular timeseries model (ARIMA) that enables forecasting with the usage of certain network flow features. We will show and compare the different outputs that certain features produce on real pre-captured network traces.

#### **Understanding Tidal Fading on Rural Long Distance Over-Water Wireless Links, Alex Macmillan (University of Edinburgh)**

#### **Intrusion Detection and Response in Open Multi-agent Systems, Shahriar Bijani (University of Edinburgh)**

Intrusion detection is a popular issue in the network security domain, but in open Multi-agent systems, which share knowledge amongst (unknown) peers, is quite a forgotten subject. In these systems because of the very openness and the dynamic interaction protocols, traditional security mechanisms are not suitable, so we should interpret conventional security concepts into this new

domain.

### **Cross Layer Neighbourhood Load Routing for Wireless Mesh Networks, Liang Zhao (Edinburgh Napier University)**

Wireless Mesh Network (WMN) has been considered as a key emerging technology to construct next generation wireless communication networks. It combines the advantages of both mobile ad-hoc network (MANET) and traditional fixed network, attracting significant industrial and academic attentions. In WMN, the load balancing becomes a hot topic in enhancing the QoS provision as a load balanced WMN exhibits low delay and high quality communications. Although there are a number of proposals on using load-aware routing metrics in WMN, the neighbourhood load has not been considered within the context of load balancing and QoS aware WMNs. In this paper, we propose a Neighbourhood Load Routing scheme to further improve the performance of the existing Routing protocol such as AODV in WMN. We have conducted extensive simulation experiments. Our results confirm the superiority of our proposed scheme over its well-known counterparts, especially in grid topologies.

### **Virtual Worlds, Real Traffic: Interaction and Adaptation, Presenter: Iain Oliver (University of St Andrews)**

Metaverses such as Second Life (SL) are a relatively new type of Internet application. Their functionality is similar to that of online 3D games but differs in that users are able to construct the environment their avatars inhabit and are not constrained by predefined goals. From the network perspective metaverses are similar to games in that timeliness is important but differ in that their traffic is much less regular and requires more bandwidth. The relationships between application functionality, SL's traffic control system and the wider network environment has been investigated. Two sets of studies have been carried out: one of the traffic generated by a hands-on workshop which used SL; and a follow up set of controlled experiments to clarify some of the findings from the first study. The interplay between network latency, SL's traffic throttle settings, avatar density, and the errors in the client's estimation of avatar positions are demonstrated. These insights are of particular interest to those designing traffic management schemes for metaverses and help explain some of the oddities in the current user experience.

### **Security Challenges for Learning in 3D MUVE – Our Experiences, Indika Perera (University of St Andrews)**

3 Dimensional Multi User Virtual Environments (MUVE) are becoming a mainstream education methodology. They are particularly appropriate for educational use due to their alignment with the concept of experiential learning within a collaborative environment. We have used the MUVEs SecondLife® and OpenSim in teaching modules. Being a proprietary system, SecondLife® does not allow required freedom that educationalists look for, whilst the open source counterpart – The Open Simulator project, has yet to prove it is a reliable and trustworthy learning platform. Moreover, none of these systems have been developed with the prime motive to facilitate learning processes, resulting in difficulties when customizing them for learning requirements. This talk is about security challenges that we have experienced with two case studies of 3D MUVE based HCI assignments. Our experiences indicate the need for research focus on security challenges within 3D MUVEs, such as we do with social networks and Web 2.0, at present. However, the solutions to these security issues should not hinder user collaboration and system usability, to sustain the benefits of MUVE.

### **Integrating Security, Digital Forensics and Cybercrime research around Scotland, Prof Bill Buchanan.**

## Attendees

- Abdesslem, Fehmi Ben (University of St Andrews)
- Al-Dubai, Ahmed (Edinburgh Napier University)
- Allison, Colin (University of St Andrews)
- Bernardi, Mino (University of Edinburgh)
- Bhatti, Saleem (University of St Andrews)
- Bigwood, Greg (University of St Andrews)
- Bijani, Shahriar (University of Edinburgh)
- Calder, Matt (University of Edinburgh)
- Strowes, Stephen (University of Glasgow)
- Di-Maio, Paola (University of Strathclyde)
- Dimatteo, Savio (University of St Andrews)
- Ellis, Martin (University of Glasgow)
- Espi, Jorge (University of Strathclyde)
- Fan, Lu (Edinburgh Napier University)
- Farshad, Arsham (University of Edinburgh)
- Fayed, Marwan (University of Stirling)
- Graves, Jamie (Edinburgh Napier University)
- Harvey, Paul (University of Glasgow)
- Henderson, Tristan (University of St Andrews)
- Jamieson, Kyle (UCL)
- Johnston, Stuart (Inmon)
- Just, Mike (University of Edinburgh)
- Koliouisis, Alexandros (University of Glasgow)
- Kriara, Lito (University of Edinburgh)
- Kwecka, Andrew (Edinburgh Napier University)
- Kwecka, Zbigniew (Edinburgh Napier University)
- Macfarlane, Richard (Edinburgh Napier University)
- Macmillan, Alex (University of Edinburgh)
- Magill, Evan (University of Stirling)
- Marina, Mahesh (University of Edinburgh)
- Marnierides, Angelos (Lancaster University)
- Miehlung, Mathew (Edinburgh Napier University)
- Mooney, Graham (University of Glasgow)
- Musolesi, Mirco (University of St Andrews)
- Oliver, Iain (University of St Andrews)

- Panchen, Sonia (Inmon)
- Parris, Iain (University of St Andrews)
- Pathivada, Sandeep (University of St Andrews)
- Pediaditaki, Sofia (University of Edinburgh)
- Perera, Indika (University of St Andrews)
- Perkins, Colin (University of Glasgow)
- Pezaros, Dimitrios (University of Glasgow)
- Rehunathan, Devan (University of St Andrews)
- Richardson, Chris (Lancaster University)
- Romdhani, Imed (Edinburgh Napier University)
- Schnetler, Hermine (UK Science and Technology)
- Sinclair Neil (University of Strathclyde)
- Tauber, Markus (University of St Andrews)
- Ul-Amin, Riaz (University of Glasgow)
- Uthmani, Omair (Edinburgh Napier University)
- Wiegel, Valeri (Edinburgh Napier University)
- Yu, Yi (University of St Andrews)
- Zhao, Liang (Edinburgh Napier University)