However, this infrastructure would be impossible without a rigid set of rules called “protocols” to control this crazy traffic.

Finally, the software behind these communications is split into two: user-side and server-side. They continuously communicate with each other via HTTP requests and the data is saved in a database where it is then retrieved on a users request.

All these components and more make up the backbone of the internet which is an essential part of our everyday lives. This poster will attempt to provide a simple, yet informative explanation of how the internet works. And, best of all, it will be interactive!

MSc student abstracts

Lifesaver or Heartbreaker? (4.01)

Avanthika Vineetha Harish, *Lancaster University*

Internet of Medical Things (IoMT) is a term relating to the network of inter-connected devices in hospitals. These devices aim to improve the quality of treatment and service, from sensors attached to the patient’s bed detecting bedsores, drug infusion pumps, through to lifesaving pacemakers implanted in patients. The range of IoMT devices is vast and improves the monitoring and treatment of many health conditions for patients both in and out of hospital. But have you ever thought about the security of a device implanted or connected to your body? In 2019, the US Food and Drug administration issued warnings that medical equipment such as Implantable Cardioverter-Defibrillators (ICDs) could be hacked due to lack of encryption and authentication, alongside unpatched vulnerabilities and incorrectly configured settings on devices and connected systems. Other vulnerabilities were raised about morphine infusion and insulin pumps that could be remotely controlled to overdose and potentially kill patients. Even the medical imaging systems like CT and MRI scan machines were found accessible to the attackers, altering images and manipulating scan results. All these connected devices and unpatched legacy systems leave hospitals and patients vulnerable to cyber-attacks.
With a little technical knowledge, there is the potential for attackers to do harm. In this poster, I will explore the cyber risks associated with the implanted IoMT devices like pacemakers and drug infusion pumps and look at solutions to mitigate them from different stakeholders’ perspectives (manufacturers, hospital authorities, doctors and patients)

Intelligent Assistive Navigating Device: A relationship between the features and enhanced usability (4.02)

Bokyung Lee, *University of Glasgow*

Devices to aid people with visual impairments have been developed as part of a drive to increase the availability of assisted devices for people with disabilities. This study examines how to enhance the usability of such devices when being used for navigation. To assess the usability of these devices, three features derived through the principles of universal design: Accessibility, Depth of Information and Obstacle Detection. The evaluation showed a positive relationship between the three features and enhanced usability. In order to judge usability, the previous work at Glasgow International College involved developing the essential characteristics: the system should be able to use in both indoor and outdoor area; the system should use tactile or acoustic sense but also need an accurate supplement of the disturbing conditions; the system should alert detailed information in real-time. Therefore, the possible suggestions to improve these intelligent assistive devices will be drawn in the poster especially in terms of the software perspective. I propose the improvement of human-computer interaction (HCI) for the devices, data analysis and machine learning for detecting obstacles while yet more studies are required in this field.

Gender Bias in Recruitment: Is Artificial Intelligence the Problem or the Solution? (4.03)

Delyth James, *Aberystwyth University*

Despite a growth in awareness of gender bias, and employment legislation which seeks to protect employees from discrimination, there are still industries where women are massively underrepresented. In 2018 only 26% of professional computing occupations in the U.S. workforce were held by women. A study of women in the tech industry in the same year found that over 50% of respondents felt that there was a visible bias in hiring for tech roles, and that almost 55% believed that blind hiring would help improve technical recruitment among women. Major companies increasingly use Artificial Intelligence in their recruitment process as an efficient method for sifting through large numbers of applicants and short listing those who are likely to be a good fit for the role. This method has however frequently been criticised for amplifying bias by using training data which reflects the already skewed gender balance within certain industries. But are we too quick to dismiss machine learning as a method to remove bias from recruitment? The machine itself cannot be biased; it can only be taught to perpetuate human bias. A machine can be trained to ignore gender entirely, something which is impossible for a human who will always have some level of unconscious bias. Rather than blaming Artificial Intelligence for causing gender bias in recruitment, should we look again at how we train a data driven model in order to create a level playing field for both male and female applicants?

Auditory and Haptic Feedback in a Socially Assistive Robot Memory Game (4.04)