Developing Robotic Systems with Security in Mind

Scott Gibb
scott.gibb.2016@uni.strath.ac.uk
University of Strathclyde

Networked Robotic systems require both safety issues and security issues to be dealt with. If the project were to be carried out, the work that would be carried out would argue that both safety and security are not entirely separate from one another and that when developing a robotic system, they both should be considered equally throughout the development process.

In recent years, robotic systems have been gaining in popularity, and are currently being increasingly used in surgical environments[1]. An example of a surgical robot that is currently in use is a robot known as the “da Vinci Surgical System” which can provide surgeons with robotic assistance for complex, sometimes long procedures[2]. This robot consists of four arms, which are controlled by a surgeon through a connected control panel. Not only does it allow the surgeon to have far more precise movements, it also allows the them to fully focus on the procedure and minimises the human resources required to undergo a surgery as less humans are needed in the surgical room. The system allows the surgeon to not only see the surgery, through a high definition camera held by of the arms, it can also allow the surgeon to see real time radiology images of the patient through the robot’s internet access[3]. Not only does it allow the surgeon access to more diagnosing techniques, during the operation, footage of the surgery can also be broadcasted to other observation rooms, allowing medical students or other professional surgeons to observe without being in the same room. Although surgical robots do have their benefits, they do however have their downfalls, how does the system cope with outside intrusion such as a malicious hacker? How is the system aware of each arms position ? How easy is it to modify this positional information? What happens if someone else gains control of the system? What happens if someone intercepts and modifies the video feed? Currently, robotic engineers develop their systems with physical safety in mind, whilst cyber security engineers develop their security overhead with digital security as their prime focus. This gap between these two fields is what this research held at the University of Strathclyde Computer Science department intends to focus on and by the end of it, bridge this gap. This work opens many avenues to unexplored security measures within robotics, as well as finding new development processes to which robotic systems can be made, processes that will allow the robots to be developed with the same functionality, but where the security threat is minimal.

The topic to be addressed is the development process of a robotic system. More specifically how to address these security issues within the development phase. The project will involve the creation of a robot that will perform as a basic “surgical” robot. This gives rise to more security issues with automatic updates during patient operation, as well but not limited to the issues with robotic systems being remotely accessed. To undergo this research project , the robot will consist of two robotic arms that are connected to each other via a network. Each robotic arm is essentially a node in the network and is controlled by another node in the same network. Essentially acting as a robotic network in a hospital. Since the robotic arms are acting as surgeon’s arms, they both also must be aware of each other’s movements as to not potentially damage the patient or each other. To do this, they must use the network to communicate with one another and, as such, the security risk of the system is increased. Due to this increased risk, security protocols will need to be developed for these interactions. Thus, highlighting the potential research that will be conducted in relation to building a secure robotic system.

The investigation will involve building this robot and researching into how to make it secure from simulated attacks on the same network. Primarily, the research will focus on first making the 'surgical' arms aware of each other but also having them simultaneously independent of each other. This is a very important aspect of it being a surgical robot as in practice they will be carrying out different tasks. Once this is achieved, the system will be redesigned with security being added to any and all communications within the system. The security implementation can then be rated against the robot's performance, as well as each implementations security risk. This will allow the different implementations to be investigated for both their short comings and corresponding benefits.

The research will initially be qualitive, focusing on the robotic security systems currently in place, at which point these systems will be rated and documented accordingly. This should then bring to light the different robotic system's efficiency versus its security. After this is completed, the development of the robotic arm protocols will begin, and once completed, the robotic arm nodes will be added to the node network, consisting of the two arms and a controller. The development of the communications network will then be started, and the network protocols established. At this stage the process will be focusing on both minimising the risk of the two arms missing each other's current location, whilst simultaneously keeping the network traffic low. Once most of the development has been completed, security measures will then be added, and the security risk and latency of the system will then be monitored and recorded. This will bring the project to its final chapter which involves test driven development in relation to developing the system to deal with simulated hacker events such as giving faulty or malicious data to the arms to deliberately try and cause harm to the system.

The results of this project are necessary for the future of the robotics industry, this industry is increasingly moving to the centre of innovative technology and, as such the risk to these robotic companies and their networked robotic systems from cyber-attacks increases. The project's results, such as its source code and statistical data, will be made available through the university's GitLab, allowing other research institutes to get involved with this new area of research. As well as making all this research open source, a poster will also be made for the Vacation Scholars Poster Competition which will show off the constructed robotic system and its achievements throughout the development process.

The work that I hope to carry out, if this project is accepted, will not only highlight issues within security in robotic systems but also shed light on some of the solutions that are already in place but also give rise to a development process to which robots are built with Security in mind.

References

[1] Vianney Gilard, Florent Marguet, Maxime Fontanilles, Stéphane Derre. 2019. *Stereotactic brain biopsy: evaluation of robot-assisted procedure in 60 patients*

[2] Mark A Talamini, S Chapman, S Horgan, and William Scott Melvin. 2003. *A prospective analysis of 211 robotic-assisted surgical procedures.*

[3] Shuji Shimizu, Ho-Seong Han, Koji Okamura, Naoki Nakashima, Yasuichi Kitamura, and Masao Tanaka. 2010. *Technologic developments in telemedicine: state-of-the-art academic interactions. Surgery*