

Long Term Visit and Collaboration Report

Julie Greensmith (& Justin Balthrop) - Los Angeles, 20/08/05 - 12/08/05

University of Nottingham

Following my attendance at this years ICARIS conference in Banff, I travelled to Los Angeles, CA, to work with a former colleague and research associate at UNM, Justin Balthrop. We both work in research relating to using AIS for intrusion detection systems (IDS). The purpose of this trip was to understand in detail his work in IDS and to combine elements of both our work. This work was performed with a view to producing a paper in addition to expanding the system Justin developed as part of his Masters degree. In this trip report I outline the work performed during my visit and outline details of our ongoing collaboration.

Work Performed

My colleague, Justin, recently developed an extension of the Lisys IDS (developed by Hofmeyr at UNM), which includes active (not passive) responses to the detection of an intrusion, known as RIOT. My initial task was to scrutinise the thesis he produced as a result of the systems development. This was done in order for me to understand the differences between RIOT and Lisys, and to get a feel for how to develop an AIS based intrusion detection system. As opposed to doing this work sat at my desk, I benefited from performing this with Justin readily available. As a result I was able to ask many questions and get satisfactory answers as and when they arose. As a result of this I have produced a report on the RIOT system, how it works as an IDS and any problems encountered during the implementation and testing of the system. This report is complete with snippets of information and clarification of certain points not present in the thesis itself. This information was often crucial to understanding the system which was obtained through questioning Justin as we went through it. This report will shortly be available as a technical report published through my university.

In addition to understanding RIOT, we felt that it was important to combine our respective research efforts. Certain elements of the RIOT system may have implications for the system that we are producing as part of the Danger Project. This includes an adaptive way of training thresholds needed by detectors. This may be useful for the signal processing aspect of our work i.e. when an actual signal is translated into a danger signal. I have also been able to see a number of potential problems with implementing a real-time anomaly detection system. For example, how to perform parameter tuning when your data is real-time. Justin overcame this problem by developing a simulator which takes care of the packet generation and capture, so data could be replayed for analytical purposes. The

techniques used here may help up when it comes to the tuning and testing of our large system.

RIOT is a system which was developed to slow the spread of high connection rate attacks such as a large number of worms which have been seen over the last couple of years. We held lengthy discussions regarding my work (adding context signals to system call analysis) and the basics of my recently developed Dendritic Cell Algorithm (outlined in my ICARIS paper). We both felt that adding a second signal' to RIOT would expand the scope of the attacks which could be detected and reacted to. We derived a number of ideas as to what a suitable signal would be and stated exploring how this signal could be incorporated into RIOT. Perhaps this signal could also reduce the amount of false positives generated by the system, though as discovered through examination of the thesis the rate of false positives is difficult to ascertain given the current implementation. The basic context signal that we are initially experimenting with is incorporating information regarding the activity of the user on the machine. If a user is not actually sat at the machine, the detection system will behave differently as if the user was active, perhaps through keystroke frequency analysis. Other signals we looked at included a number of attributes such as ratio of packets in to packets out, and a number of meta-information contained in actual TCP packets. The applicability of context signals for RIOT and ideas to be borrowed/lessons learned will also be written up and published as a technical report through my institution.

Our Continuing Collaboration

Justin and I work well together, and as a result, we are keen to continue our collaboration. As we have decided to include an extension to RIOT based on elements of my work, we are hoping to meet again in November (thankfully he will be doing the travelling) to finish the implementation and perform testing of the second signal' component. We hope to investigate the suitability of this as a signal, and if not, find a signal that may be of more assistance. Supplemental to furthering our own knowledge, we aim to submit a joint paper to GECCO 2006 (January deadline), including new results in addition to describing the basics of the RIOT system and the premise of adding context signals (the incorporation of Danger Theory in a basic form). This work is also relevant to the related work section of my thesis (to be written within the next 6 months) and to IDS in general - not many systems take the context of the host machine into account.

And Finally...

I'd like to thank the ARTIST network for continuing to support collaborations with the UK- AIS community. I hope you feel that my work performed during my time in California was worthwhile. I certainly feel that I have benefited positively

from this experience. We both look forward to continuing our so-far successful collaboration for the near future.