DOI: http://dx.doi.org/10.7551/978-0-262-31709-2-ch192

CARDINAL-E: AIS Extensions to CARDINAL for Decentralised Self-Organisation for Network Security

Peter Scully[1], Jingping Song[1,2], Jules Pagna Disso[3] and Mark Neal[1]

[1]Department of Computer Science, Aberystwyth University, Wales SY23 3DB
{pds7;jis17;mjn}@aber.ac.uk
[2]Software College, Northeastern University, Liaoning, China 110819
[3]Cyber Security Research Lab, EADS Innovation Works, Newport, Wales NP10 8FZ
julesferdinand.pagna@eads.com

Extended Abstract

This paper extends the CARDINAL architecture by Kim et al. (2005) to CARDINAL-E. CARDINAL-E keeps the innate immune system behaviour at every computer on the network and relocates the adaptive immune system behaviour to higher performance computers. Two paradigmatic shifts are achieved by this modification. First is the shift from standalone to supportive, otherwise considered as architecturally static to dynamic. This leads to an additional layer of homeostasis at a network-wide level. The intended effect is to leverage unused capacity on networks of heterogeneous machines. Secondly, the change represents a subtle granular shift from *"each computer has identical immune system components"* to *"the network (as a whole) carries all the immune system components"*. This is a synthetic network-wide "body" where organs (CARDINAL's Periphery and Lymph Node components) are finite and proportionate in quantity, and evolve their behaviour over time.

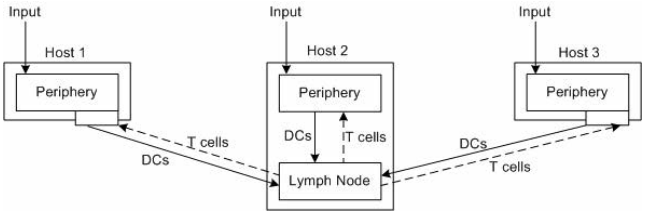

Figure 1: A simplified illustrative example of the CARDINAL-E architecture in a small network. Inputs are received at each host. Unknown inputs with danger signals are transferred to lymph nodes for further analysis. In larger networks $l < n \wedge l > 1$ is true, where l is the set of hosts with lymph nodes and n is the quantity of hosts. Host 2 illustrates a single CARDINAL host as proposed by Kim et al. (2005).

Problem

A problem for moderately sized real-time distributed applications is maintaining enough computational capacity for decision analysis. We are addressing the performance requirement for real-time security applications in industrial control system (ICS) network and supervisory control and data acquisition (SCADA) network scenarios. These networks commonly have combinations of legacy and new systems that need real-time protection. SCADA networks, by definition are remotely and sparsely located. Balancing computational effort is often a solution to the computation capacity problem. These same applications and networked computer systems are also targeted by hackers and malware. In this case the load balancing solution needs to be robust (no single point of failure) and adaptive to a number of compromised systems or disconnected network segments. Therefore, we need an architecture (like CARDINAL-E) that would support these application scenarios whilst requiring minimal computational resources.

Approach

To achieve these aims we worked toward a decentralised and fault tolerant framework and selected an immune system inspired approach. The CARDINAL framework against malicious worms by Kim et al. (2005) provided an artificial immune system (AIS) base for this self-organisation and the malware self-healing functionality. CARDINAL offered malleability to network-based decentralised decision making applications and embodied immunological danger theory, see Matzinger (1994). Our work employed the conceptual AIS framework in Stepney et al. (2005) to aid the complex (distributed) systems framework development. This led us to consider the decentralised self-management and self-organisation mappings to immune system flow and signalling regulatory mechanisms and other biological processes including cell potency and conscious awareness. We also considered these mappings to the engineered robustness of recent peer-to-peer botnet architectures particularly for their approaches to minimising their impact on network traffic, see Wang et al. (2010).

Method

In the proposed method, the key modifications to Kim et al.'s framework are the conditional removal of lymph node behaviour from *some* computers and periodic reorganisation of the behavioural roles. Figure 1 simplifies the proposed architecture. An engineered implementation of CARDINAL-

E will only accept the networked application with multiple Lymph Node components.

The reorganisation process proposed enables the reactive lightweight CARDINAL component (input sensor, signatures, etc.) to execute on all CARDINAL-E hosts and the heavier-weight analysis (diagnosis, etc.) to execute on fewer selected hosts. A reorganisation procedure of distributed system roles requires routines for initialisation, transfer of roles, periodic data analysis, historical data analysis, decentralised decision making, secure data transfer, etc. We expect suitable metrics for the role transfer decision to be CPU, memory, disk space and network load parameters recorded and averaged over given time periods. Further careful consideration of these routines will potentially lead to the occurrence of adaptive homeostasis and the emergence of regulatory network activity cycles for a given network.

Future Application

A future application of CARDINAL-E is to self-healing network security on industrial network types. This requires definition of the CARDINAL application. Kim et al.'s CARDINAL framework uses a population based model of dendritic cell and T-cell interactions to decide when to respond. The definitions of danger theory damage proposed by Kim et al. define bad or unwanted behaviour. The degree (severity and certainty) to which that unwanted behaviour has been experienced will determine the response category. CARDINAL leaves the definition of *strong* and *weak* responses, and response types open to the application designer. To close some of CARDINAL's open representations, Fu et al. (2007) introduced the MAAIS architecture as a derivative of CARDINAL. We intend to reuse Fu et al.'s following additions "length of attack time" to CARDINAL's damage certainty and severity factors; a two-tier damage threshold to decide whether attack analysis requests are handled locally (client) or remotely (server); a weighted equation to determine a damage value; and use of the ASK and TELL protocol for agent communications.

Furthermore, we describe the key representations of detection (antigen input vector), diagnosis (innate system damage decision vector) and experimental response. We represent antigen input as a statistically dimensionally reduced set of eight attributes from the KDD Cup '99[1] dataset. These attributes are {*protocol_type, service (port number), flags, src_bytes (received), dst_bytes (sent), count, diff_srv_rate, dst_host_same_src_port_rate*} which are collected over two second intervals. Appropriate attributes are summed over the interval using a connection identifier defined as <*src_ip*+*port*+*dst_ip*+*port*>. We represent Kim et al.'s damage (necrosis) signal as network packet latency (to local area and Internet hosts) and individual process loads (CPU and memory loads) where their values breach given thresholds. At this experimental stage, we use Kim et al.'s three effector T-cells to label responses. These are strong response ($CD8^+$ or cytotoxic T-cells), weak response (helper 2 T-cells) and assist a strong response (helper 1 T-cells), Kim et al. (2005).

[1]Computer Network Intrusion Detection DARPA Competition Dataset 1999, University of California, Irvine. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (Accessed: 27/02/2013)

Conclusion

This work leads toward a self-healing system against novel attacks and malware on ICS and SCADA network scenarios, such as dynamic military and defence computer networks and manufacturing industrial networks of various scales. Further work is required to define the CARDINAL-E reorganisation routines and the immune system inspired decentralised decision making, and the CARDINAL diagnosis and response mechanism for novel attacks must be explicitly addressed.

Acknowledgements

This work was supported by EPSRC I-CASE studentship EP/J501785/1 and EADS Innovation Works Program IW201339.

References

Fu, H., Yuan, X., and Wang, N. (2007). Multi-agents artificial immune system (maais) inspired by danger theory for anomaly detection. In *Computational Intelligence and Security Workshops, 2007. CISW 2007. International Conference on*, pages 570 –573.

Kim, J., Wilson, W., Aickelin, U., and McLeod, J. (2005). Cooperative automated worm response and detection immune algorithm (cardinal) inspired by t-cell immunity and tolerance. In *Artificial Immune Systems. ICARIS 2005. International Conference on*, pages 168–181. Springer.

Matzinger, P. (1994). Tolerance, danger, and the extended family. *Annu Rev Immunol*, 12:991–1045.

Stepney, S., Smith, R. E., Timmis, J., Tyrrell, A. M., Neal, M. J., and Hone, A. N. W. (2005). Conceptual frameworks for artificial immune systems. *International Journal of Unconventional Computing*, 1(3):315–338.

Wang, P., Sparks, S., and Zou, C. C. (2010). An advanced hybrid peer-to-peer botnet. *IEEE Transactions on Dependable and Secure Computing*, 7(2):113–127.