MSc Proposal
Extrusion detection and network monitoring

Etienne Raymond Stalmans

The rapid growth of the internet and the ever connected nature of modern electronic devices has lead to the development of malicious software aiming to exploit this connectivity. An increasing number of services are moving in to the cloud with users able to do every day tasks such as banking, shopping and travel planning online. Malicious software, known as malware, aims to intercept this traffic and distribute it to unauthorised third parties. The last five years has seen the development and spread of advanced botnets. These botnets consist of thousands of infected computers that are under the control of an operator and used for attacks, malware distribution and email spam.

Traditional network monitoring tools are aimed outwards, looking at traffic coming into the network. This method of detection may work for standard attacks such as Denial of Service (DoS) and Spam. However, the attack surface of an organisation has expanded beyond this one external interface. Modern malware has multiple attack vectors available, with users introducing files into the system via USB devices, P2P file sharing, email and unauthorised external connections such as 3G mobile connections, resulting in traditional monitoring systems being unable to detect all incoming attacks. Looking at recent botnet infections such as Conficker and BredoLab (infecting an estimated 10 million and 30 million hosts respectively) the most used attack vector was USB device autorun vulnerability exploitation. Once a single host on the network is infected, the botnet is able to propagate freely through the network without being detected by traditional intrusion detection systems, as these monitoring systems look outward and not inward at the local network. Infected hosts include a “phone-home” functionality, which allows them to contact the botnet controller. The botnet controller is then able to send instructions to the botnet and perform tasks such as DDoS (Distributed Denial of Service) attacks, e-mail spam and click fraud.

This research project will focus on the development of a network level extrusion detection framework. This framework will aggregate data from multiple sources such as DNS servers, network monitors and host monitors focussing on outbound traffic. Through normalisation of the data it will be possible to detect network traffic patterns. Using pattern analysis and heuristics, the framework will classify traffic as potentially malicious, suspicious or safe. These classifications will be used in the development of network rules to filter traffic and identify infected hosts on the system. Currently network administrators make use of blacklists to block malicious traffic; these blacklists are updated by external sources once malicious traffic has been identified and are focused on filtering inbound traffic. Through the use of the proposed framework it will be possible to dynamically update traffic blacklists as malicious traffic is detected on the local network, eliminating the current delay between the infection detection and subsequent blocking/removal. Proactive blocking of malicious traffic will assist in preventing the leaking of personal data captured by spyware programs. The use of multiple monitoring techniques and pattern analysis will allow the detection of malicious activity, even though techniques such as fast-flux are used to hide the malicious activity.

The framework will provide an API, which will allow for the development of plugin modules that provide additional monitoring tools and traffic analysis tools, such as data visualisation and data mining. The extensibility of the framework ensures that detection techniques can be updated as malware evolves and new attack patterns are identified.