Adaptive Anomaly Discovery by Learning Software Models

Proposal for CASE PhD Studentship with BT

David Aspinall, Prof. Software Safety & Security, Informatics
Alex Healing, Chief Researcher, Security Futures Practice, BT Research & Innovation.
Mark Shackleton, Chief Technologist, BT Research & Innovation.

Project outline

Cyber Security relies on a range of defensive techniques, including sophisticated intrusion detection systems and firewalls that try to detect and prevent attacks against software subsystems. But it is challenging for in-the-large anomaly detection to cope with the scale of network traffic and the churn of normal, non-anomalous behaviour through regular software updates or the addition of new devices such as IoT sensors and actuators. Current tools raise too many warnings that must be manually investigated, and are also overly difficult to configure.

This project will combine methods from machine learning and formal verification, to automatically learn precise semantic models of software and devices which describe *normal* traffic patterns and logging behaviours. Then anomalous, potentially *malicious* behaviours stand out as being different to these learned behaviours. Malicious behaviours can indicate a security intrusion, data exfiltration, or the presence of an Advanced Persistent Threat.

Program analysis methods for describing simplified annotated call graphs as restricted forms of automata (similar to security automata) will be used with methods for learning languages from examples, using a mix of supervised and semi-supervised techniques. The result is a collection of sub-automata, equivalently, logical formulae, which (roughly) correspond to rules used in present day application-level firewalls. At the current state of the art, such firewalls are complex to configure and maintained mostly manually. The operation of changing firewalls and ensuring similar protection remains is a practical one facing BT security engineers in their Managed Security Services operations.

Our recent research on Android malware [1,2] in the App Guarden project [3] has shown that malware models constructed at a semantic level are more robust against changing malware than signature-based classifiers. By "semantics level", we mean features that relate to the precise program semantics rather than surface syntax or binary patterns, which are more fragile (especially across increasingly sophisticated polymorphic malware instances). The proposed PhD research aims to test this idea in an entirely new setting, where programs may not be available, but models can be reconstructed from the external effects of programs including captured traffic, log files, and other sources.

For test and training data to develop the methods, the PhD project can make use published datasets such as the CTU-13 malware [4], which has already been used by BT in their research, as well as other public or restricted datasets which are available through various sources (including, we expect, the National Cyber Security Centre and Alan Turing Institute).

The PhD project requires a mix of theory and applied Computer Science skills: an ability to conduct practical experiments with data and machine learning tools, as well as an ability to conceptualise and design the fundamental process using tools from program analysis, logic and semantics. It fits within the EPSRC and UK priority areas for cyber security research.

1. Wei Chen, David Aspinall, Andrew D. Gordon, Charles A. Sutton, Igor Muttik: *On Robust Malware Classifiers by Verifying Unwanted Behaviours*. In Proceedings Integrated Formal Methods, 12th International Conference, IFM 2016, LNCS 9681, Springer, pp 326-341. 2016.
2. Wei Chen, David Aspinall, Andrew D. Gordon, Charles A. Sutton, Igor Muttik: *More Semantics More Robust: Improving Android Malware Classifiers*, in Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, WiSec '16, pp 147-158. 2016.
3. App Guarden EPSRC project EP/K03266/1 (2013-16).
David Aspinall, PI. See http://groups.inf.ed.ac.uk/security/appguarden/. A project funded in the UK Cyber Security Research Institute for Automated Program Analysis and Verification, see http://verificationinstitute.org.
4. Stratosphere IPS project, CTU University of Prague. CTU-13 Dataset. See https://stratosphereips.org/category/dataset.html.