Peter Lotts

Part II Project Progress Report

Name:	**Peter Lotts [pml43@cam.ac.uk]**
College:	**Downing College**
Project Title:	**Adding network subsystem provenance collection to CADETS**
Director of Studies:	Dr R. Harle
Supervisor:	Dr G. Jenkinson
Overseers:	Prof J. Daugman & Dr D. J. Greaves

Timetable

The project remained on track for most of the Michaelmas Term, with one simplification to the plan being made in order to achieve this. During a project meeting with my supervisor, it was decided that it would be best not to fully instrument the TCP/UDP layer (usually referred to as layer 4) of the network stack, given the amount of time it had taken to inspect the implementation of the IP layer (layer 3) at that point. Sufficient instrumentation has since been added to associate packets with sockets at the top of these layers, meaning that the success criterion of the project is not affected. Despite falling behind schedule towards the end of term and into the Christmas Vacation, the project is now back on track with respect to the original plan.

Work Completed

DTrace has been investigated, and the network stack portion of the FreeBSD kernel source has been inspected to find relevant lines where memory allocation is performed within the IP layer. Trade-offs between the UUID generation methods available in the kernel were considered, and network performance was benchmarked to compare a baseline measure with a single call to each generation algorithm at the top of the IP layer's output side. This process lead to the UUIDv1 algorithm being chosen, and packet tagging was implemented using this.

DTrace's Statically Defined Tracing (SDT) provider was used to create probes to track the lifetime of packets travelling through the network stack, including structural changes which they undergo, such as IP fragmentation and reassembly.

Difficulties

As mentioned in the 'Timetable' section, inspection of the FreeBSD implementation of the IP layer took longer than expected (as long as had been anticipated for the full network stack), and this was mitigated by deciding to only instrument the IP layer fully initially, adding instrumentation to the TCP and UDP layers later if time permits.

One of the design goals of DTrace is to provide simple, low-cost (in terms of complexity) probes within the kernel in order to affect performance as little as possible, especially when these probes are disabled. This means that its language to define what it should do when a probe is reached, the so-called 'D' language, is simplistic and so is lacking some features which would be desirable for this application. DTrace has a concept of transformations which can perform simple type conversions to allow both kernel and D code to be simple. However, the type conversions required by this project are more complex and require execution of kernel functions, which is not supported. This means that, at present, type conversions must be performed prior to a DTrace probe firing. The result of this is that conversions are performed even when probes are disabled, which goes against DTrace's design goals. Some possible methods to shift work into DTrace from the kernel have been discussed with my supervisor, and progress is now being made to implement these and hopefully remove as much of the performance impact as possible.

Further Work

Work from this point will focus on producing a userspace application to visualise the data which is collected from the network stack, and to implement the alterations to DTrace which were referenced in the 'Difficulties' section. This should prevent inactive DTrace probes from having a significant performance impact on the system, bringing the new probes in line with existing DTrace probes. The userspace application will take priority in the first instance, as it is felt that this will make the project more useable and demonstrate the analytic power of what has been achieved. The DTrace alterations are not considered crucial to the project's success, so these will be implemented only once the visualiser is complete. Plenty of contingency time and time for additional work was left at this point in the project plan, so neither of these should present a threat to the project timeline.