Royal Academy of Engineering

End of Secondment Report
Reliable approaches to gathering evidence and intelligence from network sources

Main (public) report

Secondee: **Phil Brooke**

School of Computing, Teesside University

pjb@scm.tees.ac.uk

Host organisation: **Cleveland Police**

P.O. Box 70, Ladgate Lane, Middlesbrough, TS8 9EH

2 July 2014

Introduction

I describe a secondment to the cybercrime area of Cleveland police. My normal employment is as a Reader in Computer Science at Teesside University's School of Computing.

I applied for a secondment having worked full-time in academia for over a decade. My previous non-academic employment was in the Civil Service in a research and development role. As my academic interests have steadily shifted from formal methods to information security and the use of computers in crime, it seemed appropriate to apply for a formal secondment to a police or similar agency.

As I already had some engagement with Cleveland Police and knew that this was an area of significant interest to them, it was clear that this would be a valuable secondment to myself, the police and the university.

This report necessarily omits some details due to their sensitivity. To aid dissemination of the secondment results, I provide a protectively-marked annex to this report for police and other law enforcement agencies.

"Housekeeping"

Cleveland Police underwent some structural changes between my application for the secondment and starting the secondment. This was anticipated in the original application, although the final structure was not known at that point.

I was located at police HQ in Middlesbrough. This was convenient geographically, given that I opted for a part-time secondment (three days per week at the police over ten months) so that I could retain some teaching and other university engagement. I was provided with desk space and computing facilities immediately opposite the newly in-post Cybercrime Officer. I adopted the same hours of work as the officers and staff in that area.

The university, as part of the normal workload management process, adjusted some of my duties. I retained teaching duties of modules that were of interest. One, *Information Systems Security,* was particularly relevant to this secondment and experiences from the secondment were incorporated this academic year. To prevent distractions between the roles, it was agreed that I would not be contactable by the university during my secondment days; in particular, I did not read or respond to emails those days. In hindsight, this was vital to ensure sufficient concentration on the secondment.

Secondment objectives

The overall aim of the secondment was to make better use of computer technology to collect evidence and intelligence from Internet resources for policing purposes.

The police as a whole could be expected to derive benefits from my considerable computer science expertise. This related directly to the gathering of intelligence and evidence, but also to broader issues such as the use of computers generally and information security.

The benefits to the university were expected to derive from my increased expertise, and the potential to develop new modules and courses.

In terms of my expertise, the work plan was structured around one major strand and two minor strands. The major strand concerned network-derived evidence and intelligence, also known as *cybercrime*, and was to be the main bulk of the secondment. The minor strands were complementary: the computer forensics strand concerned traditional computer "box" forensics, and the information security (infosec) strand to develop my experience of practical infosec issues.

From the outset, my plan accepted that flexibility was needed. For example, the reorganisation placed my office on the same corridor as the infosec officer, meaning that allocating blocks of time was unnecessary. In any case, the cybercrime agenda increasingly touched on infosec issues meaning that I was able to pursue this strand of work concurrently.

Secondment content

My reporting structure involved the cybercrime officer, the Detective Sergeant (DS) for that team, and above the DS, a Detective Inspector and a Chief Inspector. Latterly I was also reporting to a Detective Chief Superintendent in terms of some advice around technical issues.

The major cybercrime strand of my secondment operated on an agile model. My aim, as described in my plan, was to devise tools and techniques to improve the reliability and automation of these investigations.

My tasks were grouped into two: reactive taskings around police functions, where I took on some work from the cybercrime officer; and development tasks where I autonomously worked on software development based on the requirements derived from the reactive tasks. Some work overlapped the two areas, where a specific policy or technique was requested.

As I already held a formal volunteering role within Cleveland Police, it was easy to take on some aspects of the work. After an initial period of observing investigations and carrying out my own tasks (including live investigations), I started operating some rapid development cycles. Each cycle considered which aspects of the prior investigations had been time-consuming, difficult or

otherwise problematic due to computing, or technical issues, and then attempt to develop or enhance some software to mitigate those issues. Subsequently, the following investigations would test the updated software and identify issues for the next cycle. Other matters during the initial periods involved discussing existing practice with the computer forensics staff, and regulatory and authorisation issues.

This is the first time in recent years that I have had opportunity to devote a considerable amount of time to developing substantial software that had real application. A more formal feature-driven development process may have helped in terms of structuring the development process, although as I was the sole author of the software, it would not likely have saved time.

Secondment results

To a large extent, the secondment is successful in terms of tasks set and objectives required. Techniques have been developed, software written and a number of policy issues addressed. Feedback from “clients” – e.g., major crime team detectives – is that the outputs have been valuable in detecting and convicting offenders. As the software has developed, this has become less time-consuming and more reliable in terms of process. This allows investigatory effort to concentrate more on the issues in the case rather than low-level computer issues.

There have been obstacles during the secondment. There are outside agencies who are directly and inextricably linked to the criminal justice process and it has been very difficult to obtain necessary feedback. More positively, software has been made available and announced on a closed forum. An abstract to a police-related conference in September will be submitted in July.

The period of secondment has been sufficient to obtain a good working knowledge of the problems and issues, and to make substantial contributions. It would be possible to spend a large amount of time making further improvements and contributions. Inevitably, software can always be developed further, although I have identified a small number of tasks that would be particularly valuable. There are also new and evolving targets and services on the Internet, and these require further work. Sometimes, writing new software is not the best approach to a problem, and use of a range of tools to extract and process data has been efficient of time and resource.

The impact directly on me as the secondee has been positive. I have been able to apply a range of techniques from computer science and software engineering, and consider how my use of them might be improved further. I have spent a sustained period of time considering both requirements and risk, then implementation details. I am also involved with the QAA review of the subject benchmark statement, and some of my views on this are informed by the secondment.

Cleveland Police have benefited from the secondment during this period: the secondment was timely in that it occurred during a time of national and local interest in developing the cybercrime agenda. Thus I have been able to contribute to Cleveland Police's development of their cybercrime capability as well as assisting on specific tasks.

The university has received some benefit already in terms of fresh material for an undergraduate module (delivered during the period of secondment). I have discussed cross-school collaborations with other colleagues, and there is some possibility of developing new modules and courses. It remains to be seen whether or not these are developed to the point of recruiting students.

In the current public funding environment, future funding appears difficult to obtain and this is a matter of concern. The dissemination is aimed at national organisations such as the College of Policing and the National Crime Agency in the hope that ongoing support can be obtained.

Meeting the objectives

The overall aim of the secondment was to make better use of computer technology to collect evidence and intelligence from Internet resources for policing purposes. I believe this has been achieved in the narrow sense of the secondment, although much should be done in developing this line of work.

The individual strands of work have been generally successfully. The major strand has resulted in documented processes and techniques, new software and contributions to policy development. The minor strand on information security is more nebulous in terms of specific outputs, although the opportunity to identify and discuss infosec issues within the police has been valuable and the major strand of work increasingly required infosec matters to be addressed. The computer forensics strand was, in part, shorter than planned, but then much longer in terms of developing a specific tool in response to some particular requirements.

Conclusions

At the time of writing, the national impact is hard to assess, but will likely improve as the dissemination activities take effect. I have discussed a number of matters with national organisations, and hope that I can continue my involvement. There are specific remarks in the police annex concerning national guidance.

The secondment has given me opportunity to apply techniques and methods from computer science and software engineering, including programming, project management and requirements capture. Some concurrency techniques have been used, for example, to model and debug problems in concurrent applications. I have had ample opportunity to practice risk assessment in terms

of technological, process and regulatory risks. Not everything has worked perfectly, but the lessons learned in terms of technical and process issues have been valuable to me. As the secondment draws to a close, I am applying for my Chartered Engineer status.

On reflection, it is clear that those undertaking higher tiers of cybercrime roles need much stronger computing experience and education than is previously appreciated. It is possibly easier to train computer specialists as investigators than to train investigators as computer specialists. For example, solid understanding of the technology underpinning the process where a server delivers information to a web browser that itself renders the data into a view for the end user is sometimes necessary for contentious issues. Another example concerns analysis around the technical risks involved in these investigations, which is intrinsically related to traditional computer science. Finally, bespoke automation requires at the very least some skills with scripting.