Impact case study template (REF3b)

Title of case study: Securing Networked Systems

1. Summary of the impact

The Network & Information Security Technology Lab (NISTL) at Liverpool John Moores University (LJMU) conducts research in securing networked systems against the growing threat of cyber crime. The research has generated a correlated set of new security protocols, novel system composition methods and efficient digital forensic analysis schemes for more effective layered security protection. Their main impacts for the period 01/2008 – 07/2013 are highlighted below:

- *The text here has been redacted.*
- Thales (engaging in commercial secure system development) has continued collaboration with us to exploit our findings on system composition since 2008. This enabled Thales to deliver three invention disclosures and one security-enhanced commercial solution. The open source software version produced was downloaded 14,323 times since 04/2009.
- *The text here has been redacted.*
- Our research in forensic analysis led to the generation of a patent in 2009, which was later implemented by the lab into a software tool. Merseyside Police used the tool to enhance its efficiency in digital forensic analysis by 8.5 times.

In addition to the above direct impacts, our work is also beneficial to other organisations and even the general public, as they all require security techniques for information protection.

2. Underpinning research

The rapid development of networked systems has been constantly moving towards the provision of seamless, ubiquitous and intelligent services through system integrations. These integrated systems often process valuable, critical, confidential or private information that must be secured against unauthorised access and cyber crime. However, the increasing complexity of the systems poses serious challenges to their security protection and makes already very intricate security tasks much harder to handle. Consequently the systems become far more vulnerable to the growing quantity of cyber attacks.

To tackle the above problems, our NISTL lab has a long-term research goal of developing an integrated framework to systematically handle security issues at three important layers for preventing, detecting and investigating cyber attacks. The first layer addresses the research challenges of securing individual component systems. The second supports the secure composition of component systems based on their properties to form a larger networked system. The third layer deals with cooperation between a composed system and other security measures such as intrusion detection and forensic analysis for enhanced security protection.

This case study takes one example of the lab's work from each of the above three layers to illustrate the impact of our research. It includes a security scheme at the first layer, secure system/component composition at the second layer, and a forensic analysis method at the third layer. The key research findings from them are outlined separately below:

- The security scheme published in 2013 by Prof. Q. Shi, Prof. M. Merabti and Dr K. Kifayat (Lecturer since 09/2010) at LJMU together with Dr N. Zhang (Senior Lecturer at Manchester University) allows a node in a heterogeneous wireless sensor network to establish shared cryptographic keys with others in an authentic and resource-efficient manner to support secure communication [1]. A central novel outcome of the research is that the hierarchical clustering features of the network can be used to deliver vertical key shareability before sensor deployment to enable horizontal key shareability when needed after the deployment. The finding empowers the scheme with the ability to not only achieve strong authenticity and resilience against security threats, but also to offer better resource-efficiency, flexibility and scalability than related work.
- The early work published in 1998 by Dr Q. Shi (Lecturer at LJMU) and Dr N. Zhang (Lecturer at Manchester Metropolitan University) proposed a novel model for secure system

composition [2]. A key finding of the work revealed that it is possible for a composed system to obtain stronger security than some of its component systems by properly handling their security properties and interactions. The importance of this finding was that it laid down a theoretical foundation for the development of more applicable solutions to secure system composition, which were virtually non-existent at the time.

The above work was then exploited to secure an EPSRC research grant of £146k for advancing secure system composition techniques in the context of personal ubiquitous computing between 03/2003 – 02/2006 [7]. Prof. M. Merabti, Dr. Q. Shi (Principal Lecturer) and Dr. R. Askwith (Lecturer) at LJMU were the project investigators, and Dr. D. Llewellyn-Jones was employed as a RA to work on the project. One of the original research outcomes produced is a framework for protecting networked systems from code with security flaws by integrating direct code analysis with secure system composition [3]. The framework offers a practical and effective solution to system protection.

Since the successful completion of the project in 2006, the research has been continuing in partnership with Thales Research and Technology Ltd, with Dr B. Zhou employed as the first RA at LJMU for the research. One of the innovative results generated is a method for performing boundary checks to secure a system composition [4]. It has been exploited jointly to provide a simplified, effective and applicable way of ensuring the security of system composition. The method was published at IEEE SoSE 2010, winning the conference's best paper award due to the novel way it solves a practical and challenging problem.

Moreover, our research has been further boosted by a large EU FP7 project, ANIKETOS, with a total grant of €9.6m including €741k awarded to LJMU to develop secure and trustworthy composite services during the period 08/2010 – 01/2014 [8]. Prof. M. Merabti, Prof. Q. Shi, Dr. D. Llewellyn-Jones (Reader) and Dr. R. Askwith (Principal Lecturer) are the project investigators at LJMU. One of the main outcomes produced so far is a novel architecture with the capabilities needed at the platform level for managing trust, security and threats in relation to required services [5].

- The research conducted by Dr. J. Haggerty (Lecturer, left in 09/2009) and Dr. D. Llewellyn-Jones (Lecturer) at LJMU produced a novel method for the searching of malicious data stored in computers or networks for digital forensic investigation, which was first patented in 2009 [6]. The work focussed on the increasing complexity of systems and the consequence this has on the time taken for forensic analysis. The key finding from the method evaluation showed that it is feasible to efficiently and effectively detect large datasets of malicious data (millions of images) from large quantities of hard drive storage (hundreds of gigabytes of data). Such efficiency is important for expediting the forensic investigation process.

3. References to the research

Peer-reviewed Outputs

[1] Q. Shi, N. Zhang, M. Merabti & K. Kifayat, "Resource-efficient Authentic Key Establishment in Heterogeneous Wireless Sensor Networks", Feb. 2013, Journal of Parallel and Distributed Computing, Vol. 73, No. 2, pp. 235-249, DOI: 10.1016/j.jpdc.2012.10.004.

[2] Q. Shi and N. Zhang, "An Effective Model for Composition of Secure Systems", Nov. 1998, Journal of Systems and Software, Vol. 43, No. 3, pp. 233-44, DOI: 10.1016/S0164-1212(98)10036-5.

[3] D. Llewellyn-Jones, M. Merabti, Q. Shi and B. Askwith, "Buffer Overrun Prevention through Component Composition Analysis", July 2005, IEEE COMPSAC 2005, Edinburgh, UK, pp. 156-163, DOI: 10.1109/COMPSAC.2005.54.

[4] B. Zhou, O. Drew, A. Arabo, D. Llewellyn-Jones, K. Kifayat, M. Merabti, Q. Shi, R. Craddock, A. Waller and G. Jones, "System-of-Systems Boundary Check in a Public Event Scenario", June 2010, IEEE SoSE 2010, Loughborough, UK, pp. 1-8, DOI: 10.1109/SYSOSE.2010.5544013 (***won best paper award***).

[5] P.H. Meland, J.B. Guerenabarrena and D. Llewellyn-Jones, "The Challenges of Secure and Trustworthy Service Composition in the Future Internet", June 2011, IEEE SoSE 2011, Albuquerque, USA, pp. 329-334, DOI: 10.1109/SYSOSE.2011.5966619.

Patent and External Grants

[6] J. Haggerty and D. Llewellyn-Jones, “Method and Apparatus for Detection of Data in a Data Store”, Patent published in US in Nov. 2009 with number 12/152335 and extended in Sept. 2012 with number 8265428, and also in UK in Dec. 2010 with number PCT/GB2010/001103.
[7] M. Merabti, Q. Shi and R. Askwith, “Secure Component Composition for Personal Ubiquitous Computing”, EPSRC, 03/2003-02/2006, £145,888, Reference GR/S01634/01.
[8] M. Merabti, Q. Shi, D. Llewellyn-Jones and R. Askwith, “ANIKETOS: Secure and Trustworthy Composite Services”, EU FP7, 08/2010 – 01/2014, €741k for LJMU with a total project grant of €9.6m, Project Reference 257930.

Note that the above references 1, 2 and 6 best indicate the quality of our research.

4. Details of the impact

Cyber security is becoming ever more important as society increasingly relies on networked systems, while at the same time security threats to the normal operation of these systems grow in number. To counter such threats, it is important to develop effective tools to reduce security vulnerabilities, and train users for proper understanding and handling of security threats and tools for system protection. These activities are underpinned by the three areas of our research outlined in Section 2, with their impacts detailed separately below:

- *The text here has been redacted.*
- *Secure system composition*: Our lab’s research outcomes in this area were disseminated through publications in journals and at conferences. This attracted interests from Thales Research and Technology (UK) Ltd, which actively engages in secure system development. A joint on-going project was then initiated in 2006 to transfer the lab’s work on secure system composition outlined in Section 2 into security tools. During the period 01/2008 - 07/2013, the project resulted in three invention disclosures and an enhanced Secure On-Demand Architecture (SODA) solution to dynamic cascade vulnerability checks in real-world networks for Thales [a]. The collaboration is evidenced in joint publication [4] in Section 3. The work has benefited Thales in terms of better security solutions.

  In addition, the project enabled our lab to produce a software tool MATTS (Mobile Agent Topology Test System) for assessing composed system security. Some components of MATTS have been released by the lab as open source software [b]. This helps to promote its further development by other developers and to make the tool freely available for security improvement. Between 04/2009 – 07/2013, the released visualisation component of MATTS was downloaded 14,323 times (about 3,305 times per year) worldwide [c]. This has made a positive impact on the wide adoption of advanced technologies.

  The lab’s security research also received broad international recognition through the dissemination. This led to collaboration with 16 other partners across 9 EU countries to secure an EU FP7 grant of €9.6m for developing secure and trustworthy composite services between 08/2010 - 01/2014 (see [8] in Section 3). The lab is the third largest contributor with €741k. *The text here has been redacted.*

  The lab’s work on secure system composition outlined in Section 2 forms a core theme of the project. It has been integrated into the solutions and tools being exploited by the project’s 10 industrial partners for the development of secure composite services. The exploitation has benefited not only these companies through more advanced security techniques but also their customers through better-secured services. *The text here has been redacted.*

  The text here has been redacted.
- *Forensic analysis*: As described in Section 2, the lab produced a patent published in the US and UK in 2009 and 2010 respectively (see [6] in Section 3). A spinout company Forsigs [d] was created jointly with Tubedale Communications Ltd in 2008 with an investment of £120k to commercialise the patented technique for fast and accurate automated searching of illegal data stored in computing devices for forensic investigations. The product mainly aims at users from law enforcement organisations (e.g. police) and companies. It has been used by the Merseyside Police High Tech Crime Unit (MPHTCU) in real investigations [e]. The product demonstrated a speed improvement of 8.5 times that of the previous tool used by

the police with one case reducing a full analysis from 22 hours down to 19 minutes, which was measured between 10/2010 - 03/2011. This reduces investigation time and hence increases the police's efficiency in solving criminal cases. The use of the product also resulted in the development of a new triaging process at MPHTCU.

The lab also provided MSc-level computer forensics training for 3 policemen from MPHTCU (09/2009 - 09/2011), one of whom is now at the National Cyber Crime Unit, and a training course (04 - 05/2013) for 3 policemen for setting up Kuwait's first computer forensics unit.

5. Sources to corroborate the impact

[a] Chief Scientist, Thales Research and Technology (UK) Ltd.
[b] MATTS available at http://www.cms.livjm.ac.uk/nistl/?to=matts.
[c] https://sourceforge.net/projects/functy/files/stats/timeline?dates=2008-04-16+to+2013-11-13.
[d] http://www.cms.livjm.ac.uk/nistl/?to=forsigs.
[e] Police Officer, Merseyside Police High Tech Crime Unit.