

William M. Fitzgerald (Ph.D., M.Sc., B.Sc.(Hons))

CONTACT INFORMATION

Cork Constraint Computation Centre,
Department of Computer Science,
University College Cork,
Ireland.

E-mail: info@williamfitzgerald.net
Web: www.williamfitzgerald.net

AREAS OF SPECIALISATION

Network Access Control, Policy Analysis, Automated Reasoning, Ontologies, Formal Modelling.

RESEARCH INTERESTS

Inclusive of above: Threat & Vulnerability Management, Systems Security, Semantic Web.

EDUCATION

University College Cork, Cork, Ireland.
Ph.D., Computer Science.

Jan. 2006 - Aug. 2010

- Dissertation: “An Ontology Engineering Approach to Network Access Control Configuration”.
- Advisors: Dr. Simon N. Foley (Principle Advisor, UCC), Mr. Mícheál Ó Foghlú (WIT).

National University of Ireland, Maynooth, Kildare, Ireland.
M.Sc. Computer Science.

Sept. 2000 - Oct. 2002

- Dissertation: “Performance Analysis of Host Based Routing”.
- Advisor: Dr. Stephen Brown (N.U.I.M).

National University of Ireland, Maynooth, Kildare, Ireland.
B.Sc. (Hons) Science.

Sept. 1996 - June 2000

- Majoring in Computer Science and Mathematics.
- B.Sc. subjects in Computer Science: Computer Networks, Programming Paradigms, Artificial Intelligence, Advanced Computer Architectures, Software Engineering, Databases, Distributed Systems, Formal Methods, Automated Reasoning, Parallel Processing, Computer Vision, Complexity Theory, Operating Systems, Theoretical Computer Science, Neural Networks.
- Course also covered: Mathematics (3 years), Physics (2 years), and Chemistry (1 year).

PROFESSIONAL ACTIVITIES

Journal Reviewer:

- Journal of Network and Systems Management (JNSM), 2009.
- Computer Standards & Interfaces (CSI), 2008.

Conference Reviewer:

- ACM Symposium on Applied Computing (SAC), 2008.
- Autonomic and Trusted Computing (ATC), 2007.
- New Technologies, Mobility and Security (NTMS), 2007.
- Management of Multimedia and Mobile Networks and Services (MMNS), 2006.
- International Symposium on Wireless Communication Systems (ISWCS), 2006.
- International Conference on Pervasive Computing, 2006.
- Vehicular Technology Conference (VTC), 2006.

Workshop Reviewer:

- International Workshop on Security in Information Systems (WOSIS), 2009.
- New Security Paradigms Workshop (NSPW), 2007.
- IEEE International Workshop on IP Operations and Management (IPOM), 2006.

Guest Lecturer:

- “Hacker 101: Introduction to Security Auditing”, National University of Ireland Maynooth, April 2008.

PUBLICATIONS

Journal Papers:

W. M. Fitzgerald, S. N. Foley: “*Aligning Semantic Web Applications with Network Access Controls*”, Computer Standards & Interfaces, Elsevier, October 2009 (in Press).

W. M. Fitzgerald, S. N. Foley, M. Ó Foghlú : “*Network Access Control Configuration Management using Semantic Web Techniques*”, Journal of Research and Practice in Information Technology, Vol. 41, No. 2, May, 2009.

Conference Papers:

S. N. Foley, W. M. Fitzgerald: “*An Approach to Security Policy Configuration using Semantic Threat Graphs*”, 23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec’09), Concordia University, Montreal, Canada, July, 2009.

J. Clarke, Z. Dooley, W. M. Fitzgerald: “*SecurIST: Security & Dependability to Empower the Citizen in the 21st Century*”, 15th IST Mobile Summit, Myconos, Greece, June, 2006.

J. Clarke, Z. Dooley, W. M. Fitzgerald: “*SecurIST: The Application Security Initiative*”, IST Africa Conference, Pretoria, South Africa, May, 2006.

Z. Dooley, W. M. Fitzgerald, J. Clarke, “*SecurIST: Ensuring Secure, Dependable & Resilient European ICT Technologies to Empower the Citizen, Protect Critical Infrastructure & Provide Economic Growth*”, Euro-Atlantic Symposium on Critical Information Infrastructure Assurance, Switzerland, March, 2006

W. M. Fitzgerald, J. Clarke: “*SecurIST: Co-ordinating the development of a Strategic Research Agenda for Security and Dependability R&D*”, 39th IEEE International Carnahan Conference on Security Technology, Las Palmas de G.C., Spain, October, 2005.

J. Clarke, W. M. Fitzgerald: “*Strategic Research Agenda for Security and Dependability R&D*”, Information Security Solutions Europe, ISSE, Budapest, Hungary, September, 2005.

W. M. Fitzgerald, K. Doolin, F. Mahon, C. Hauser, A. Gomez-Skarmeta, S. Butler, P. Schlosser, B. Weyl: “*Daidalos Security Framework for Mobile Service*”, eChallenges, Ljubljana, Slovenia, October, 2005.

G. G. Mitchell, W. M. Fitzgerald: “*An Approach for Network Forwarding Systems Quality*”, Information Technology and Telecommunications (IT&T), Athlone, Ireland, pp 103-111, ISSN 1649-1246, September, 2001.

Workshop Papers: W. M. Fitzgerald, S. N. Foley: “*Management of Heterogeneous Security Access Control Configuration using an Ontology Engineering Approach*”, 2nd ACM Workshop on Assurable & Usable Security Configuration, Chicago, USA, October 4, 2010.

W. M. Fitzgerald, S. N. Foley, M. Ó Foghlú : “*Network Access Control Interoperation using Semantic Web Techniques*”, 6th International Workshop on Security in Information Systems (WOSIS), Barcelona, Spain, June, 2008.

S. N. Foley, W. M. Fitzgerald : “*Semantic Web and Firewall Alignment*”, 1st International Workshop on Secure Semantic Web (SSW), Cancun, Mexico, IEEE CS Press, April 7-12, 2008.

W. M. Fitzgerald, S. N. Foley, M. Ó Foghlú: “*Confident Firewall Policy Configuration Management using Description Logic*”, Proceedings of The Twelfth Nordic Workshop on Secure IT Systems, Short Paper, Reykjavik, Iceland, October, 2007.

S. N. Foley, W. M. Fitzgerald, S. Bistarelli, B. O’Sullivan, M. Ó Foghlú: “*Principles of Secure Network Configuration: Towards a Formal Basis for Self-Configuration*”, Springer LNCS, 6th IEEE International Workshop on IP Operations and Management, Volume 4268/2006, ISBN 978-3-540-47701-3, Dublin, Ireland, October, 2006.

IST EU Framework Programme 6 Reports:

Z. Dooly, J. Clarke, W. M. Fitzgerald, W. Donnelly, M. Riguidel, K. Howker, “*D3.3-ICT Security & Dependability Research beyond 2010: Final strategy*”, SecurIST, 2007.

CONFERENCE PRESENTATIONS

23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Montreal, Canada, 2009.

6th International Workshop on Security in Information Systems, Barcelona, Spain, 2008.

1st International Workshop on Secure Semantic Web, Cancun, Mexico, 2008.

12th Nordic Workshop on Secure IT Systems, Reykjavik, Iceland, 2007.

6th IEEE International Workshop on IP Operations and Management, Dublin, Ireland, 2006.

39th IEEE International Carnahan Conference on Security Technology, Las Palmas de G.C., Spain, 2005.

RESEARCH EXPERIENCE

Cork Constraint Computation Centre, Cork, Ireland.

Ph.D. Student Researcher

Jan. 2009 - present

Dissertation Abstract:

- Network access controls, such as firewalls and VPNs, are intended to reflect the business-level security policies of an enterprise. Running to many thousands of access-control rules, and potentially involving multiple subnets, their configuration is complex and error-prone. This can result in misconfigurations that are not compliant with the business-level security policies, resulting in unapproved access, or the denial of approved access, to network resources. Avoiding misconfiguration can largely be dependent on the expert-knowledge of a security administrator and drawing upon best practice.

The thesis of this dissertation is that this security knowledge can be modeled in terms of an ontology. This approach enables knowledge related to detailed network access control configurations, business-level security policies, and their relationships, to be represented and reasoned about

within a common framework. An advantage of an ontology-based approach is the Open World Assumption, whereby reasoning over an existing security ontology is easily extended to include further security ontologies. OWL-DL ontologies are developed for Linux iptables, TCP-Wrapper and threat-graph based business-level security policies.

Security administrators use firewall query and structural analysis techniques to help avoid mis-configuration. The security ontology permits the entire firewall rule to be used in this analysis, unlike many existing tools, which rely on a firewall model centered around a five-tuple rule of IP addresses, ports and protocols. For example, a structural analysis that considers stateful inspection can detect the presence or absence of shadowing that is not detected by the conventional five-tuple based model. The dissertation explores the effectiveness of ontology-based firewall analysis that considers stateful inspection, TCP flags, and logging actions, in addition to the conventional five-tuple.

The approach is evaluated by considering its effectiveness at modelling existing best practice for network access control configuration. Best practice approaches, including PCI-DSS for systems that process credit card information, NIST for secure Web-servers and Internet RFC's for anti-bogon are considered. These are encoded as an ontology of threat graph based catalogues which enable firewall configuration recommendations to be generated for given threats.

Academic years 4 & 5 were sponsored by Science Foundation Ireland under the *Federated, Autonomic Management of End-to-end Communication Services (FAME)* project, grant number 08/SRC/I1403.

Telecommunications Software & Systems Group (TSSG), Waterford, Ireland.

Ph.D. Student Researcher (Internship)

Jan. 2006 - Dec. 2008

Included Ph.D. research.

Academic years 1, 2 and 3 were sponsored by Science Foundation Ireland under the *Autonomic Management of Communication Networks and Services (AMCNS)* project, grant number 04/IN3/I404C.

Telecommunications Software & Systems Group (TSSG), Waterford, Ireland.

Applied Researcher

Sept. 2004 - Dec. 2006

SecurIST (IST-FP6).

- The SecurIST project (EU Framework Programme 6) delivered a Strategic Research Agenda for ICT Security and Dependability R&D for Europe beyond 2010. As a member of the Security Taskforce, I played a role in all the security roadmap initiatives with significant roles in Application Security Initiative (ASI) and Internet Infrastructure Security Initiative (IISI)

Daidalos (IST-FP6).

- Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services (Daidalos). I was involved in the security aspects of the project (WP1 and WP4 deliverables).

Additional Responsibilities:

- Collaborate and contribute to the writing of FP6, FP7, PASR and EI CFTD proposals.

Ericsson, Dublin, Ireland

Junior Research Scientist and Software Engineer

Jan. 2003 - March. 2004

Reputation and Cooperation in Ad-Hoc Networks.

- The research investigated a dynamic game theoretical model of node cooperation in ad-hoc networks, based on evolutionary game theory.

Ericsson OSS Security Architecture (Current State and Challenges Ahead).

- OSS-RC architecture, CORBA, Citrix, architecture vulnerabilities, federated network identity (Liberty Alliance).

National University of Ireland, Maynooth, Kildare, Ireland.

M.Sc. Student Researcher

Sept. 2000 - Oct. 2002

Abstract:

- “UNIX-based routers are an integral part of the Internet, so understanding their performance is important part of understanding network performance. In order to understand the execution times and behaviour of IP forwarding under Linux, a software tool (*KETTLe*): Kernel Event Tracing for Time & Logic was developed. Results from this tool and external performance measurements are presented along with an analysis of IP forwarding code path. In Today’s Internet, there is a high demand to forward datagram’s efficiently at speeds of gigabit, or even terabits per second. It is important to investigate the performance overheads that manifest themselves in current routers in order to develop new router technologies to cope with the exponential growth of the Internet.”

Research Included:

- Linux Kernel Coding, TCP/IP protocol stack, Router & Forwarding concepts, Network Performance Enhancers, Network Sniffers, QoS Traffic Shaping, implementation of *KETTLe*.

Kernel Event Tracing for Time & Logic:

- The tool monitors the internal datagram lifecycle through the router. This tool accumulates information on what mechanisms are executed and exactly how long each mechanism spent working on its task for a given datagram travelling through the forwarding IP stack within a router. Using *KETTLe*, one can accurately detect at what point bottlenecks occur.

National University of Ireland, Maynooth, Kildare, Ireland.

Software Engineer (short term contract)

June 2000 - Sept. 2000

Educational Tool: a guide to the theory of NP-Complete problems.

- The scope of the research project involved the *Travelling Salesman Dilemma*. The project goal was to develop an educational tool that helped undergraduate students to understand the complexity of NP-complete problems. It has been used at a number of the N.U.I.M Open Days to demonstration the type of problems that engineers and computer scientists attempt to solve. The tool was also exhibited on the N.U.I. Maynooth stall at the Irish Young Scientist Award (2000).

ACADEMIC
EXPERIENCE

University College Cork, Cork, Ireland.

Masters of Science Co-Supervisor

Sept. 2008 - May 2009

Co-supervised the following students with Dr. Simon N. Foley as part of the M.Sc. Software Development for Computer Networks degree:

- Cui, W.: “*Semantic Web Techniques for Intrusion Detection and Prevention*”.
- O’Neill, L.J.: “*Semantic Web Techniques for Network Discovery*”.

Assisted with the following:

- Weekly discussions providing constructive criticism as to how best to model and reason over the knowledge regarding network system & service discovery, and IDS.
- Working with the students to establish a realistic timetable for the completion of the various milestones to be achieved.
- Creating an environment in which the students found conducive to research and their own intellectual growth.

National University of Ireland, Maynooth, Kildare, Ireland.
Computer Laboratory Demonstrator

Sept. 2000 - June 2003

Laboratories demonstrated:

- Networks, Operating Systems (Solaris, Linux) and Programming Paradigms.

The position responsibilities included:

- Active collaboration with course lecturers.
- Ensuring all students have access to laboratory material.
- Ensuring laboratory material is completed in a timely fashion.
- Grading student laboratory examinations and managing student results.
- Identifying problem areas that students have and providing extra support where needed.

TEACHING
CERTIFICATION

JEB/EDI Teachers Diploma in Information Technology

Sept. 2007 - June 2008

Diploma¹ is composed of:

- JEB/EDI Level 3 Certificate in Education Principles and Practice
(Formerly JEB/EDI Certificate in the Principles of Teaching and Training)
- JEB/EDI Level 3 Certificate in Education Practice: ICT Skills
(Formerly JEB/EDI Teacher Trainer Certificate in IT Skills)

ADDITIONAL
CERTIFICATION

Occupational First Aid Certificate including Defibrillator Training in accordance with the 'Irish safety, health and welfare at work act 1993', 2007.

Fire Safety & Warden Training, 2007.

Irish FÁS Construction Site Safe Pass, 2002.

European Computer Driving Licence (EDCL), 2000.

REFEREES

References on demand.

¹Education Development International (EDI) is an accredited *awarding body* working in collaboration with industry, governments, universities and professional bodies internationally to ensure its qualifications and assessments are accredited, recognised and relevant. Web: <http://www.ediplc.com/>