Dr. Ultan Neville (B.Sc., M.Sc., Ph.D.)

Cork City,
Ireland.
https://ultan-neville.github.io/

Current Position

October 2017 – Present **Senior Engineer - Global Product Security Engineering & Innovation Services**, Johnson Controls, Cork, Ireland.

Ultan is a Senior Cyber Security Engineer specializing in Product Security and Enterprise Application Security. His remit includes:

- Security testing involving penetration testing orchestration
- Security architecture design
- Security standards & compliance auditing
- Secure Software Development Life-cycle best-practice

He reports to the Director of Global Product Security, Technical Services division, where he leads the ongoing development of an automated Red Teaming ecosystem for the Global Product Security Technical Services team - a best-in-class scalable system for internal security assessment and pen-testing capabilities, applied to various product lines at JCI.

Education

2012 – 2017 **Ph.D., Computer Science (specializing in Cyber Security)**, University College Cork (UCC), Ireland.

Title *"Reasoning About Firewall Policies Through Refinement and Composition"*

2010 – 2011 **M.Sc., Software and Systems for Mobile Networks**, University College Cork, Ireland.

Title *"Smartphone Firewall Configuration management"* (major dissertation)

2006 – 2010 **B.Sc. (Hons.), Computer Science**, University College Cork, Ireland.

Summary of Experience

– 7+ years experience in Cyber Security R&D.

Industry Senior Cyber Security Engineer at JCI, Fortune 500.

Worked previously as an independent Cyber Security Consultant (pen-test vendor).

Developed integral soft-skills as part of previous and current industry positions.

Ethical hacking Various competencies, such as working with Kali Linux and pen-testing frameworks and tools, for example Metasploit, Nessus, OpenVAS, nmap, Nessus&Tenable.io, Netsparker, ThreadFix, and others, including an understanding of various vulnerability databases, for example ICS-CERT, NVD and exploit-db.

Research Post-Doctoral Researcher in the Mobile and Internet Systems Laboratory (MISL), and Ph.D. Internship in Cork Constraint Computation Centre (4C) and the Insight Centre for Data Analytics: the Department of Computer Science, UCC.

Researching in computer security, specialization in network security.

Expert skills in both theoretical and practical IT security.

Strong background in formal modeling.

Strong background in systems.

Rebuilt and flashed kernels to add extra capabilities to Android research test-bed.

Constructed OpenStack research test-bed on a USB.

Teaching Delivered lectures and tutorials, and demonstrated in security labs for undergraduate and postgraduate Cyber Security modules.

Proposed and co-supervised B.Sc. and M.Sc. Cyber Security student projects.

Software Development Developed a number of PoC prototypes as part of M.Sc. and Ph.D. research, and worked as part of a team in an SFI-funded project developing a software deliverable during Ph.D. Internship. Developing an automated app-sec pipeline as part of current position.

Awards

2014 **Best Student Presentation** – Award received at the Cyber Network Exploitation and Defence (NED) Forum's inaugural cyber security and resilience strategy conference.

2010 **UCC College Scholar** – Awarded the title of College Scholar for performance in undergraduate exams.

Research

Publications

1 U. Neville and S.N. Foley. Reasoning about firewall policies through refinement and composition. *Journal of Computer Security (JCS) 26(2): 207-254, 2018.*

2 U.J. Neville. Reasoning About Firewall Policies Through Refinement and Composition. *PhD thesis, University College Cork, Ireland, 2017.*

3 U. Neville and S.N. Foley. Reasoning About Firewall Policies Through Refinement and Composition. In *Data and Applications Security and Privacy XXX: 30th Annual IFIP WG 11.3 Conference, DBSec 2016, Trento, Italy, July 18-20, 2016. Proceedings*, 2016.

4 S.N. Foley and U. Neville. A Firewall Algebra for OpenStack. In *2015 IEEE Conference on Communications and Network Security, CNS 2015, Florence, Italy, September 28–30, 2015, pages* 541–549. IEEE, 2015.

5 W.M. Fitzgerald, U. Neville, and S.N. Foley. MASON: Mobile Autonomic Security for Network Access Controls. *Journal of Information Security and Applications (JISA)*, 18(1):14–29, 2013.

6 W.M. Fitzgerald, U. Neville, and S.N. Foley. Automated Smartphone Security Configuration. In *Data Privacy Management and Autonomous Spontaneous Security, 7th International Workshop, DPM 2012, and 5th International Workshop, SETOP 2012, Pisa, Italy, September 13–14, 2012. Revised Selected Papers*, pages 227–242, 2012.

Ph.D. Research

Title *Reasoning About Firewall Policies Through Refinement and Composition*

Supervisor Dr. Simon N. Foley

Examiners Prof. Joaquín García-Alfaro (external) & Dr. John Herbert (internal)

Description The thesis of the dissertation is that *a firewall policy should be anomaly-free by construction, and as such, there is a need for a firewall policy language that allows for constructing, comparing, and composing anomaly-free policies.* An algebra is proposed for constructing and reasoning about anomaly-free firewall policies. Based on the notion of refinement as safe replacement, the algebra provides operators for sequential composition, union and intersection of policies. The effectiveness of the algebra is demonstrated by its application to anomaly detection, and standards compliance. The effectiveness of the approach in practice is evaluated through a mapping to/from Linux iptables. The evaluation shows that the approach is practical for large policies. The effectiveness is also evaluated through a mapping to OpenStack network and host-based access controls, and the development of a policy management framework for the Android OS.

M.Sc. Research (1H - First Class Honors)

Title *Smartphone Firewall Configuration Management* (Major dissertation)

Supervisors Dr. Simon N. Foley & Dr. William M. Fitzgerald

Description Developed a prototype application for the Google Android mobile platform that can automatically manage the configuration of the underlying Linux iptables firewall on behalf of the non-expert end-user in different network environments. The firewall configurations are based on a compliance-driven threat-model. A catalogue of firewall best practice countermeasures, with which to mitigate known network-based smartphone threats was developed. This catalogue is based upon best practice standards, for example Internet RFC's that mitigate anti-bogon threats, and guidelines from the National Institute of Standards and Technology on firewalls, firewall policy and information security. Performance analysis of the smartphone firewall, in conjunction with best practice standards, was also used to determine suitable firewall countermeasures. For example, one may be willing to sacrifice some security in a particular network environment in order to reduce battery consumption.

Presentations

- *Reasoning About Firewall Policies Through Refinement and Composition.* Presented at the 30th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2016), June 2016.
- *A Firewall Algebra for OpenStack.* Presented at the 1st IEEE Workshop on Security and Privacy in the Cloud (SPC 2015), September 2015.
- *Autonomic Security Control Reconfiguration.* Presented at the NED Forum's inaugural cyber security and resilience strategy conference, November, 2014. See also, Awards section.

Other Relevant Experience

Researcher

Jul 2017 – Oct 2017 **Post-Doctoral Researcher – Cyber Security**, University College Cork (UCC), Ireland.
Ultan was a Post-Doctoral Researcher at the Mobile and Internet Systems Laboratory (MISL) under the CHIST-ERA DYPOSIT project. His research is focused primarily on autonomic security control reconfiguration, and the problem of large, shared Cyber-Physical System infrastructures under attack.

Jan 2012 – Dec 2016 **Ph.D. Researcher – Cyber Security**, University College Cork (UCC), Ireland.
Ultan worked as a researcher as part of the SFI-funded FAME and CTVR/CONNECT projects, where he obtained a Ph.D. in Computer Science, specializing in Cyber Security.

Teaching

Jan 2012 – Mar 2014 Teaching assistant, lab demonstrator, tutor, for undergraduate System Security and Network Security modules, and postgraduate Mobile Systems Security at Department of Computer Science, UCC.

Undergraduate and Postgraduate Cyber Security Project Supervisor

Co-supervised the following B.Sc. degree final year projects with Dr. Simon N. Foley:

2016 O'Riordan, J.: **Location-based permissions manager for Android**
2016 McDonald, C.: **Anomaly analysis of OpenStack firewall polices**
2015 Barrett, E.: **WYSIWIP for Android: What you see is what is permitted**
2014 O'Keefe, D.: **E-client Enforcement of Chinese Wall policies in Openfire**
2014 Hanley, S.: **Anomaly analysis of Openfire packet filter polices**

and the following taught M.Sc. degree project:

2012 Li, X.: **Botnet Analysis and Detection for the Smartphone**

Conference & Workshop Reviewer

2014 Served as a nominated peer-reviewer of scientific publications for the European Symposium on Research in Computer Security (ESORICS).

Software Developer (Cyber Security Prototypes)

Jan 2012 – Dec 2013 Ultan worked as part of the SFI-funded Federated, Autonomic Management of End-to-end communication services (FAME) Strategic Research Cluster (SRC). His primary contribution to the FAME SRC was the Java implementation of an autonomic, peer-to-peer, SAML-based agent. Asynchronous messaging was utilized to distribute Trust Management authorization/delegation credentials. This allowed for the dynamic reconfiguration of the network access controls on the XMPP servers in the test-bed, and permitted safe (secure) federation between collaborating agents.

Jan 2015 – Dec 2015 As part of his Ph.D. research, Ultan developed a Python implementation of the firewall policy algebra described in the Ph.D. Research section for iptables. The prototype was developed following a model-driven engineering approach, and experiments have been conducted on policy operators. Overall, the results are promising and have been reported in publications [1-3].

Oct 2017 – Present Ultan is utilizing a number of different technologies, including the Python programming language and a given set of RESTful APIs, to develop an automated app-sec pipeline as part of the remit of his current position.

Cyber Security Consultant (pen-test vendor)

Oct. 2014 – Dec. 2014 Ultan performed a security audit of the server, web app and Android application for **Froblem**, a small company based in Cork, involved in fault-reporting systems for buildings. He worked closely with the lead-developer throughout the consult, and upon completion, furnished a full report on his findings with recommendations. He also provided remediation assistance, thereby helping to implement the fixes outlined in the final report.

Interests

Music Ultan enjoys playing the button accordion and has various associated achievements, including first-place All-Ireland medals for competing at Fleadh Cheoil na hÉireann in both junior and senior Grúpa Cheoil competitions.

Other Astronomy, films, reading, gardening.

Referees

Available on request.