RESEARCH INSTITUTE IN AUTOMATED PROGRAM ANALYSIS AND VERIFICATION

UK's second academic Research Institute in Cyber Security, funded as part of the UK's national cyber security programme.

Host Institution: Imperial College London • Director: Professor Philippa Gardner

ABOUT US

We represent the UK research in automated program analysis and verification, in particular with its application to cyber security, both in the UK and internationally.

Modern society is critically dependent on computer software. However, we cannot yet guarantee what software does. Our understanding has not kept pace with its complexity. There is a clear and pressing need to improve cyber security by providing greater understanding, proving correctness of programs and identifying potential weaknesses of our software.

Mathematical analysis and verification techniques are just beginning to reach industrial scale, achieving guarantees of correctness, safety and security. The Institute has world leading researchers in the UK who are working in fields such as mathematical logic, programming languages, and program analysis and verification. It is a collaboration between six universities:

- University of Edinburgh
- Imperial College London
- University of Kent
- The University of Manchester
- Queen Mary University of London
- University College London

Funded by a £4.5 million grant, the Institute has been established by GCHQ in partnership with the Engineering and Physical Sciences Research Council (EPSRC) through the Research Councils UK (RCUK) Global Uncertainties Programme and the Department for Business, Innovation and Skills (BIS).

ADVISORY BOARD

Mike Gordon • Professor of Computer Assisted Reasoning, University of Cambridge, UK

Mike St John-Green • Independent Cyber Security Consultant, UK

Joshua Guttman • The MITRE Corporation, USA

Daniel Kroening • Professor of Computer Science, University of Oxford, UK

Xavier Leroy • INRIA, France

Brad Martin • USA Government, USA

Greg Morrisett • Professor of Computer Science, Harvard University, USA

Peter O'Hearn • Facebook, UK

Fred Schneider • Professor of Computer Science, Cornell University, USA

CONFERENCES AND WORKSHOPS IN 2014

›› **UK Cyber Security Research Conference 2014 at BIS**
Organisers: Philippa Gardner, Angela Sasse
Highlights conference aimed at leading figures in government, industry, academia

›› **FMATS3: Scientific Meeting at Microsoft Research Cambridge**
Organisers: Philippa Gardner, Andrew Gordon, Mike Gordon, Andy J, Graham Steel
Workshop on Formal Methods and Tools for Security aimed at leading experts

›› **INVEST: Introduction to Verification and Testing workshop at Imperial College London**
Organisers: Philippa Gardner, Cristian Cadar, Alastair Donaldson
Workshop aimed at young researchers to attract them to verification and testing

›› **Sponsored Programming Languages Mentoring Workshop (PLMW) at Principles of Programming Languages (POPL) 2014, San Diego, USA**
Workshop aimed at young researchers to introduce them to programming languages and verification

›› **Organised Concurrency Verification workshop at POPL 2014**
Organisers: Philippa Gardner, Derek Dreyer, Aaron Turon

SPONSORS

GCHQ

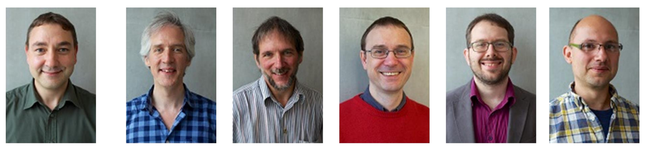
Department for Business Innovation & Skills

EPSRC Pioneering research and skills

APP GUARDEN: RESILIENT APPLICATION STORES

›› University of Edinburgh

Aims to improve resilience of application stores by producing methods to automatically analyse and sign apps for safety properties.



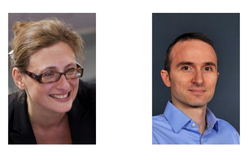
David Aspinall, Andrew Gordon, Don Sannella, Ian Stark, Charles Sutton, Björn Franke

Industrial partners: Google New York, RIM, McAfee, Kotican, Metaforic
Academic partners: LMU Munich, UCM Madrid, Birmingham University, Glasgow Caledonian

CERTIFIED VERIFICATION OF CLIENT-SIDE WEB PROGRAMS

›› Imperial College London

Aims to provide a mechanised specification of the JavaScript standard on which to develop theories and tools for proving correctness, safety and security properties of JavaScript programs.



Philippa Gardner, Sergio Maffeis

Industrial partners: Mozilla Foundation, Google California
Academic partners: INRIA Rennes, KU Leuven

COMPOSITIONAL SECURITY ANALYSIS FOR BINARIES

›› Queen Mary University of London ›› University of Kent ›› University College London

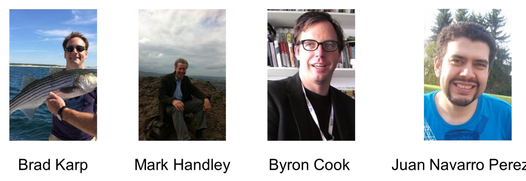
Aims to develop a framework and tools for scalable security analysis for binaries.

Pasquale Malacaria, Andy King, Byron Cook, Michael Tautschnig

PROGRAM VERIFICATION TECHNIQUES FOR UNDERSTANDING SECURITY PROPERTIES OF SOFTWARE

›› University College London

Aims to develop automatic program verification methods (drawing on static and dynamic techniques) that help security engineers to understand software that they have not written themselves.



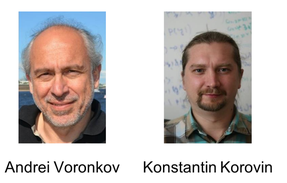
Brad Karp, Mark Handley, Byron Cook, Juan Navarro Perez

Industrial partners: Google USA, Microsoft (Trustworthy Computing Group, UK), Microsoft Research UK

REVES: REASONING IN VERIFICATION AND SECURITY

›› The University of Manchester

Aims to enhance first-order theorem provers to use them in program analysis (Vampire) and to develop methods for verifying access policies in web services using such provers.



Andrei Voronkov, Konstantin Korovin

Industrial partner: Intel
Academic partners: TU Vienna, Chalmers University of Technology

SEMAMATCH: SEMANTIC MALWARE MATCHING

›› University of Kent ›› University College London

Aims to derive robust semantic signatures for malware classification based on a static and dynamic analysis.

Andy King, David Clark, Earl Barr

Industrial partner: McAfee Labs

CONTACT US

www.verificationinstitute.org