
A note on the UK cyber-security research landscape
Partnership for Conflict, Crime and Security Research

A note on the UK cyber-security research landscape

On behalf of the RCUK Partnership for Conflict, Crime and Security Research

Overview

There is a wealth of cyber-security research being undertaken in the UK.

To maximise the impact of such research, and thereby improve the UK's cyber capability, it is necessary to increase the level of interaction between researchers/academia and the range of stakeholders from government, civil service, policy-makers, think-tanks, and UK PLC.

Cyber-security is a broad field that encompasses a wide-range of concerns. At present, engagement is hindered, as there is little available for navigating the vast research landscape.

This note provides a high-level overview of UK publicly funded cyber-security research. It represents a first step in encouraging greater stakeholder-researcher engagement, by highlighting particular areas of investigation, and introducing services for discovering relevant research projects.

The cyber-security research landscape

Table 1 presents categories describing the broad themes of cyber-security research.

Category	Description
Verification and Engineering	Software and system verification, validation, formal analysis, and software engineering processes.
Cryptography	Theoretical and applied aspects of cryptography/encryption. This category includes quantum computing.
Networking	The mechanism for communication, including protocols, lower-level networking, radio technologies, etc.
Distributed Systems	Networked systems: cloud, mobile, peer-to-peer and pervasive computing, including the management of ad-hoc and sensor networks.
Access Controls	Mechanisms for regulating access to data and resources. Covers authorisation, authentication, biometrics and identity management.
Intrusion	Malware, exploits, intrusion detection and protection.
Data Analytics	Algorithms, machine learning, privacy, trust, and personal/aggregated data issues ('big-data').
Control Systems and Hardware	Systems that regulate the behaviour of other systems, often in an industrial context. Includes low-level, hardware-centric security approaches.
Human Factors	Usability, behaviours, incentives, and more general economic, social and legal concerns.
Policy Aspects	Issues that directly affect policy, government or business. Includes best-practices (e.g. BYoD), ownership (e.g. copyright, DRM), regulation and compliance.
Sectors and Applications	Targets the concerns of particular sectors or applications. Includes general areas such as healthcare and cities, to specific issues, e.g. e-voting, and detecting extremist activity.

Table 1: Categories of cyber-security research

The publicly funded cyber-security research projects were classified into these categories, to indicate the type and scale of research being conducted.[1] Figure 1 presents this breakdown.[2]

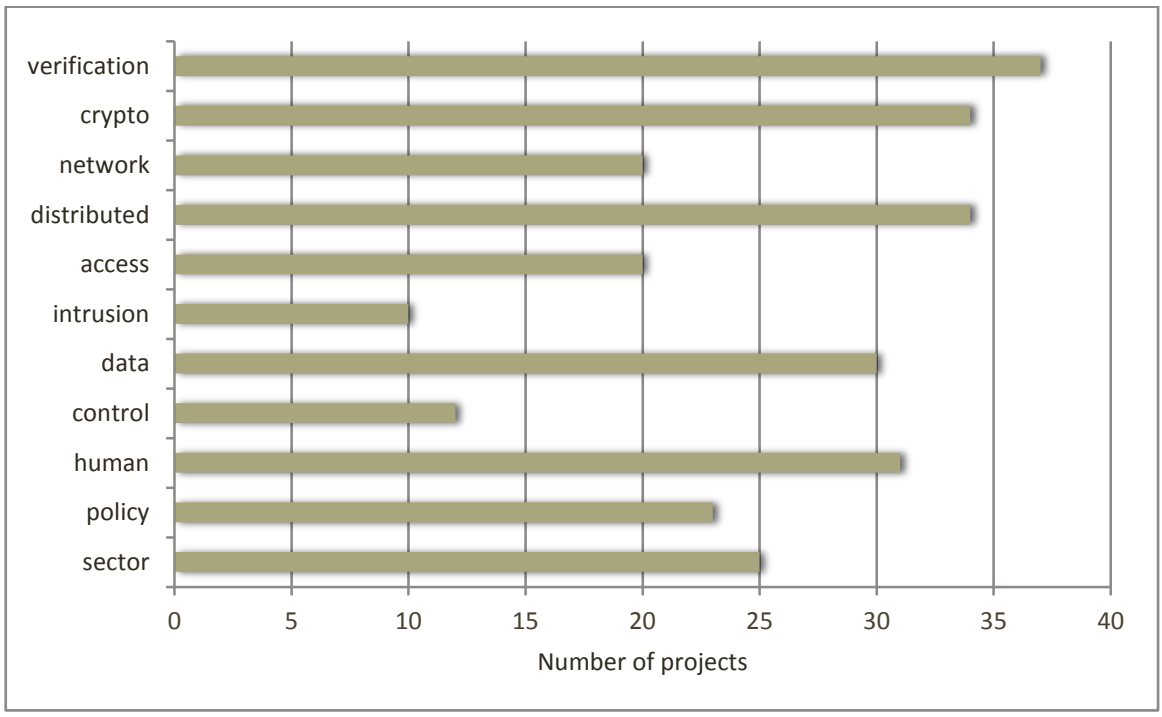

Figure 1: RCUK cyber-security research projects by classification (212 projects, 276 data points)

The Figure indicates a healthy spread of research across the range of cyber-security topics.

As one would expect, the more traditional security concerns, such as cryptography, access control and verification are all well represented.

Encouragingly, there is also much research relevant to concerns emerging from the ever-increasing digital society. These include issues such as 'big-data', privacy, analytics, cloud and the 'internet of things', public policy, legal aspects, economics, and human behaviour.

There are notably fewer projects in the areas of intrusion and control systems/hardware. However, this does not necessarily imply a general deficiency in capability. In these areas much work targets the protection and control of particular products, infrastructure and/or commercial implementations. This often better aligns with commercial undertakings, rather than general, publicly funded research.

[1] The categories represent common areas of focus in cyber-security. These were derived independently from the research data, in order to better indicate the spread of research.

[2] Data was provided by RCUK, representing the projects funded from 2004 to Mar 2014. The vast majority of projects were EPSRC funded. Only the projects addressing a particular cyber-security topic were classified; more general grants, such as those for an institute or centre, were omitted. There were 212 projects classified. Projects with several grant codes, e.g. cross-institutional collaborations, were considered in aggregate as a single project, classified only once. *The classification is only indicative*, based on the project's title, and in some cases, its abstract. Projects were placed into the most relevant category, according to the perceived main area of contribution. There were 64 projects that were placed into two categories, giving 276 data points in total.

The means of engagement

The landscape illustrates the breadth of UK cyber-security research. The analysis indicates that there will often be research relevant to stakeholder interests, wherever such concerns lie across the cyber-security spectrum. As such, there appears much potential for stakeholder-researcher engagement.

The first step in the engagement process involves discovering the research projects that are relevant to particular concerns.

The Academic Centres of Excellence in Cyber Security Research scheme is a cross-government sponsored initiative that recognises institutions conducting world-class research in the field. An explicit goal is to "make it easier for potential users of research to identify the best cyber research […] that the UK has to offer".[3] Currently 11 universities are recognised, with more to follow. An overview of their areas of specialty, along with contact details, can be found in the report: Developing our capability in cyber security.[4]

RCUK provides information on all publicly funded research projects (across all academic disciplines) through their web portal: Gateway to Research.[5] The portal offers search functionality over the funded research proposals, providing information on titles, abstracts, and the people and organisations involved. As this data can be quite dense, this resource is particularly useful for those seeking detail on particular projects.

CLUE[6] is a non-commercial offering by Crossword Cybersecurity that aims to improve the visibility of cyber-security research projects. Based on funding data, CLUE simplifies project discovery by categorising projects by application area, offering brief project summaries, and for more detail, linking to project websites and the associated research proposals. CLUE is live (though in beta), currently with data on over 300 projects from UK and EU-based institutions. For access, please contact Tom Clark[7] mentioning this note.

The External Champion to the Partnership for Conflict, Crime and Security Research will be working with Crossword Cybersecurity in the future to help shape the development of CLUE. Any comments or feedback towards this, or regarding the note in general, are most welcome.

Authorship

Dr Jatinder Singh
Senior Research Associate, Computer Laboratory, University of Cambridge
Jatinder.Singh@cl.cam.ac.uk

Commissioned by Dr Tristram Riley-Smith
External Champion, RCUK Partnership for Conflict, Crime and Security Research (PaCCS)
http://www.paccsresearch.org.uk

December 2014

[3] http://www.epsrc.ac.uk/research/centres/acecybersecurity
[4] https://www.gov.uk/government/publications/cyber-security-research-capability-academic-centres-of-excellence
[5] http://gtr.rcuk.ac.uk
[6] https://clue.crosswordcybersecurity.com
[7] tom.clark@crosswordcybersecurity.com