Contrails: finding, understanding and countering crime in the cloud

Call type: Invitation for proposals

Closing date: 16 September 2014

Related themes: Digital economy, Global uncertainties, ICT

Summary

As part of their contribution to the Partnership for Conflict, Crime and Security Research (RCUK GU programme), and working with the Metropolitan Police Service (MPS) and the National Crime Agency (NCA), EPSRC and ESRC are jointly requesting proposals for a research Centre which will over the next five years inform understanding of, and responses to, criminal activities and behaviour in the cloud.

Only one Centre will be funded. Its focus will be on research which will ultimately benefit the users of cloud services and those who might be affected by their misuse.

The Centre will address four inter-related challenges of equal importance, each of which will drive and engage with the others. Its programme of work must be strongly multi- and interdisciplinary. It will advance the state of knowledge in a range of fields with relevance to crime in the cloud, including but not limited to criminology, cyber security, law, ethics, forensics and distributed systems.

Background

Widespread adoption of cloud computing creates enormous opportunities for those with malicious intent. As well as making life easier or more lucrative for criminals by enabling, amplifying or simplifying tried-and-tested activities, cloud services have potential to allow the development of brand new crimes which are unique to the cloud environment.

The huge range of cloud service (IaaS, PaaS, SaaS...) and deployment (public, private, hybrid...) models imparts great complexity to issues of security in the cloud. This is further multiplied by the existence of two key threat receptors – the cloud service provider and the cloud service user – and of overlap between the two. Rapid change as a result of mergers and acquisitions between companies using or providing services in the cloud, the resulting vaguely defined and/or poorly understood business perimeters and the certainty of future significant technological change add to this complexity. Coping with and unravelling this increasingly intricate and interconnected picture will be
extraordinarily challenging, but progress will be essential if we want to make the most of the cloud.

Purely technological aspects of cloud security have received much attention over the last few years. Research has often focused on the question of how providers might offer a better (more private or secure, more reliable, better specified and more transparent) cloud service for their customers. Other work has been carried out within a framework which seeks to isolate the user from threats, or to create provider-agnostic cloud services, such that the location, nature and activities of other users of the cloud can have no effect on individuals’ experiences within it.

Despite some real progress on these fronts there will always be security issues in the cloud. And so, inevitably, there will always be opportunities for criminality in the cloud. As well as protecting users and providers by developing more secure cloud systems, we will need to be able to detect and pursue criminals, to secure convictions and perhaps even to deter criminals or make the cloud a less attractive place for them to operate.

Criminal behaviour in the cloud could, in principle, be identifiable in real time or retrospectively if only we knew what to look for and how to do it. Alternatively, criminals may create and leave exploitable traces of their presence in the cloud as they carry out activities which may well, by virtue of their criminal nature, in some way differ from the pattern of a normal user of cloud services. Between them these represent a ‘contrail’ of evidence.

Advances in finding, understanding and countering cloud crime will require new academic thought within and between several disciplines. Progress will be made more difficult by a range of features of the cloud which are simply not encountered either in the physical world or in other cyber contexts: the transient and volatile nature of cloud data; its logical rather than geographical placement; the sheer volume of data (this is definitely a ‘big data’ issue); the variety and complexity of business activity in the cloud; the potential absence of any audit trail, accountability or reliable attribution; and the increasingly routine use of high-grade cryptography, among other issues.

**Centre specification**

This call requests proposals for a single Centre which will over the next four to five years inform our understanding of, and responses to, criminal opportunities and behaviour in the cloud. The focus will be on benefit to either the users of cloud services or those who might be affected by their misuse, rather than the providers of those services, although clearly there is potential for spillover value to providers as a result of better understanding of the threats they and their customers might face in future.

The Centre will address four inter-related challenges of equal importance, each of which should drive and engage with the others. This suggests a metaphor for the Centre, pictured below, as a reconfigurable set of gears, the arrangement of which will vary during its life.
A crucial fifth gear of engagement with key stakeholders and users will underlie and help to drive the Centre’s work. Formal involvement of the MPS and NCA with the successful project is built in to this vision. The exact model for their work with the Centre will be decided once the successful host has been identified. To ensure fairness neither MPS nor NCA should be approached to be project partners on grants. The involvement of other project partners or collaborators is however strongly encouraged.

**Research challenges**

Our key requirement is that proposals must set out new ideas for research which will contribute to the creation of a better understanding of crime in the cloud. Proposals should be based broadly but not rigidly on the four challenges, addressing their general concepts without necessarily following their structure. All four challenges will need to be pursued simultaneously with comparable levels of effort and in an integrated fashion. As always, the onus remains on applicants to identify key issues, exciting hypotheses or directions, and to formulate appropriate plans for research into them.

- Challenge 1 – Understanding. What criminality might be found in a cloud environment?

The form of crime which might be encountered in the cloud is not well known or understood. A better understanding of the nature, motivation, precedents, skill base, culture, limitations and future directions of criminality in the cloud is essential if we are to identify when it is happening. Cloud crimes will inevitably be a mixture of old and new, in which the cloud-nature of the platform has varying degrees of impact on their successful execution – from ‘better in the cloud’ to ‘only thanks to the cloud’. The motivations of criminals and their career pathways will reflect
the move to cloud. The trans-national aspects of cyber crime will be of particular interest, and will impart further complexity to this challenge. The Centre will need to consider the full range of criminality. While this includes the use of cloud services to organise or promote terrorist activities this should not be the sole or even major focus.

- **Challenge 2 – Identifying. What indicators of criminality might exist?**

Even with effective countermeasures in place it is inevitable that cloud crime will occur. We can be just as certain that despite the best efforts of criminals, and although the cloud is a fundamentally ephemeral and fast moving environment, there will be indicators that it is happening. The scale of operation of even a small cloud service means that it is impossible to know and understand everything that exists or occurs within it – indeed it is undesirable to even try to do so. Knowledge of the likely avenues that criminals might pursue we may help to narrow down the search space, making crime detection practical. And if new indicators appear, they may point to the emergence of new crimes which could not otherwise be predicted.

- **Challenge 3 – Detecting. How might we detect criminality, in real-time or retrospectively, while maintaining privacy?**

Having broadly established that something undesirable is going on, what it might be and the signals it might create, we will also need to know how to look for it. The presence of undesirables in the cloud is a given and there will always be ‘intrusion’ so research in this challenge will need to go beyond current approaches to intrusion detection. There is a need for more targeted and intelligent analysis which is automated and scalable in a first pass but then directed and forensic in its approach. All of this must be compatible with the expectation of privacy among the cloud’s users. The increased use of cryptography will change the cloud – how can we detect crime if most bulk data are to all intents and purposes private forever? Knowledge of what forms of detection are or are not possible will be invaluable in determining what types of activities might be attractive to criminals.

- **Challenge 4 – Demonstrating. How can we demonstrate the past or ongoing existence of criminality in the cloud to an actionable or even legal standard?**

There is a significant leap to be made from mere suspicion of crime to the point at which action to counter it might be justified, or at which it might be said that there is formal evidence of a criminal act. It is relatively straightforward to create a basic warning system, much harder to put in place a response which will withstand scrutiny and even legal challenge. Better understanding of the requirements of evidence will inform approaches to detection. The very question of legality and jurisdiction as a result of the trans-national nature of some cloud crime will feed through into work on the criminological aspects of cloud behaviour – is this behaviour even illegal? If so where, who should deal with it and how? Advances in this challenge also have potential to the creation of new ways to gather and secure evidence of crimes committed outside the cloud but for which the cloud is the repository.
**Funding available**

Up to £2.0M of funding from EPSRC and ESRC jointly (80% of the fEC value, meaning that applicants should outline a research programme costing up to £2.5M in total) is available for the Centre, for a grant of between four and five years’ duration.

Only one Centre will be funded and we expect that the Centre’s work will be carried out within a single research institution. We consider this model to be the most appropriate as a result of:

- the need to closely integrate the various strands of its work to ensure mutual support and learning
- the need to facilitate simple and efficient engagement with users
- the requirement that projects should be able to adjust resourcing flexibly and at short notice

That said, we will still consider proposals which are spread across two (but no more than two) sites. Two-site proposals must take extra steps to explain how they will meet the three expectations above and provide strong evidence of their willingness and ability to do so, not just assertions that this will be the case. Multi-institutional projects should be submitted as a single proposal on behalf of both partners. We will not accept joint proposals or any which involve more than two UK institutions.

Sufficient funds for effective outreach and engagement with users must be included in the proposal, as must costs of coordinating the Centre’s activities and disseminating its results. These should include resources to support work with MPS and NCA as well as any formal project partners included on the application. Given that neither MPS nor NCA will be named on any application at this stage we can tolerate some degree of latitude and speculation in the resourcing for this.

The Centre’s programme of work must have a strong inter- and multidisciplinary ethos and offer opportunities to genuinely advance knowledge in a range of fields including but not limited to criminology, cyber security, law, ethics, forensics and distributed systems. There should be true equality among the various strands with no cases of one discipline solely providing a ‘service function’ to any other. Opportunities for interdisciplinary working should be maximised and acted on. We expect to see this reflected in the range of Co-Investigators listed in the application, and in the way that resources are allocated between them.

**Equipment**

Where possible, researchers are asked to make use of existing facilities and equipment, including those hosted at other universities. If equipment is needed as part of the research proposal, applicants must follow EPSRC’s rules for requesting equipment over £10,000 in value. Individual items of equipment up to the current OJEU (Official Journal of the European Union) procurement threshold can be included on research proposals submitted through this call, but research organisations will be expected to make a contribution to the cost. Requests for single items of equipment above the current OJEU threshold will not be accepted.
For more information on equipment funding, please see: http://www.epsrc.ac.uk/research/facilities/equipment/.

**Eligibility**

For information on the eligibility of organisations and individuals to receive EPSRC funding, see the EPSRC Funding Guide: http://www.epsrc.ac.uk/funding/howtoapply/fundingguide/

As this call is a targeted funding opportunity provided by EPSRC, higher education institutions, and some research council institutes and independent research organisations are eligible to apply. A list of organisations eligible to apply to EPSRC is provided at: http://www.rcuk.ac.uk/funding/eligibilityforrcs/

**How to apply**

**Submitting application**

You should prepare and submit your proposal using the Research Councils’ Joint electronic Submission (Je-S) System (https://je-s.rcuk.ac.uk/).

When adding a new proposal, you should select:

- Council ‘EPSRC’
- Document type ‘Standard Proposal’
- Scheme ‘Standard’
- On the Project Details page you should select the ‘Contrails’ call.

Note that clicking ‘submit document’ on your proposal form in Je-S initially submits the proposal to your host organisation’s administration, not to EPSRC. Please allow sufficient time for your organisation’s submission process between submitting your proposal to them and the call closing date. EPSRC must receive your application by 16:00 on 16 September 2014.

Guidance on the types of support that may be sought and advice on the completion of the research proposal forms are given on the EPSRC website (http://www.epsrc.ac.uk/funding/howtoapply/) which should be consulted when preparing all proposals.

**Guidance on writing application**

Applications should comply with the normal requirements for EPSRC Standard proposals except that the ‘Case for Support’ may be up to 11, rather than eight, pages long in total.

The extra pages should be used in part to explain and justify the balance of disciplines and individuals involved in the project, the potential for interdisciplinary working associated with them and how it will be realised. In particular it will be important to make good use of the extra space to explain:

- the contribution that each discipline or the interdisciplinary approach will make to the overall aims of the Centre, and
• the potential for the Centre’s work to contribute to the advancement of the disciplines which have a stake in it

If the attachments are uploaded as Word documents, please be aware that once the application has been submitted to the Council/Funder, all the attachments will be converted and held as an Adobe Acrobat file (PDF). Also please note, that whilst we support a wide range, we do not support all MS Word font types. Therefore if an unsupported font type is used a different font type may be substituted which may result in changes to the layout of the document. For this reason we recommend that the documents are converted to PDF files before uploading.

For advice on writing proposals see:

http://www.epsrc.ac.uk/funding/howtoapply/preparing/

User Engagement Strategy
Successful applicants will be required to develop and actively pursue a strategy for engaging with potential users of the research funded in the project (resources for this activity should be requested as part of the Pathways to Impact and must be justified in the application). This strategy should be reviewed and updated regularly as part of the formal management of the grant and in light of planned future input from MPS and NCA.

The strategy should cover:

• how and when potential users have been / will be identified;

• what form the engagement will take;

• what steps will be taken to ensure that outputs of the research are made available to potential users;

• suitable metrics for determining the success of the strategy in delivering value to users.

Some of the work of the Centre may be of immediate use to cloud providers, allowing them to enhance their customers’ security without compromising other requirements or obligations they have to them. Some of it may be less generally useful as it might only be legitimately deployed within the framework of law enforcement. A successful user engagement strategy will clearly identify who might benefit from the research and how.

Assessment

Assessment process
Proposals which comply with the basic requirements set out in this call document will be sent for anonymous review by experts. The Principal Investigator will be given the opportunity to respond to their comments before a meeting of a specially convened assessment panel who will be asked to identify the successful application.
Assessment criteria

At the first review stage proposals will be assessed using the standard EPSRC form. This can be found at: http://www.epsrc.ac.uk/funding/assessmentprocess/assessmentcriteria/. It includes the following assessment criteria:

a. Quality
b. Importance
c. Impact
d. Applicant
e. Resources and Management

For each application, the assessment panel will be asked to apply the following additional criterion:

f. Relevance of the proposal to the challenges and scope of the call

Guidance for reviewers

Information about the EPSRC peer review process and guidance for reviewers can be found at: http://www.epsrc.ac.uk/funding/assessmentprocess/review/advice/

Additional grant conditions

Key dates

<table>
<thead>
<tr>
<th>Activity</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2014</td>
<td>Call issued</td>
</tr>
<tr>
<td>16 September 2014</td>
<td>Call closes</td>
</tr>
<tr>
<td>February 2015</td>
<td>Panel meeting</td>
</tr>
<tr>
<td>March 2015</td>
<td>Result announced</td>
</tr>
</tbody>
</table>

Contacts

Any queries regarding the submission of proposals through Je-S should be directed to the UK Je-S helpdesk:

JeSHelp@rcuk.ac.uk, tel. 01793 444164

If you have any questions about this Call please contact:

Dr Alex Hulkes
EPSRC
Polaris House
North Star Avenue
Swindon SN2 1ET

Tel: 01793 444116
alex.hulkes@epsrc.ac.uk
### Change log

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
<th>Version</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alex Hulkes</td>
<td>26/6/2014</td>
<td>1</td>
<td>N/A</td>
</tr>
</tbody>
</table>