Adaptive cyber security decision support to prevent cyber attacks

27 June 2017

Credit: CC0 Public Domain

Recognising the complexity of cyber attacks and the multi-stakeholder nature of tackling cyber security are the key components of a new data-driven cyber security system being developed by experts led by the University of Nottingham. The aim is to support organisations of all sizes in maintaining adequate levels of cyber security through a semi-automatic, regularly updated, organisation-tailored security assessment of their digital infrastructures.

The £1 million project, funded by the Engineering and Physical Sciences Research Council (EPSRC) and the National Cyber Security Centre (formerly CESG), will establish the foundations for a digital 'Online Cyber Security System' decision support service (OCYSS) which is designed to rapidly bring together information on system vulnerabilities and alert organisations which may be affected.

The interdisciplinary project brings together academics in different areas of cyber security, information integration and decision making from the University of Nottingham, UK and Carnegie Mellon University, USA. They will be working closely with the UK's National Cyber Security Centre.

Dr Christian Wagner, from the School of Computer Science at the University of Nottingham, who is currently also a visiting professor at Michigan Technological University, USA, is the lead academic. He said: "While the UK has access to some of the world's leading experts in cyber security, the scale and variety of systems in UK organisations, both public and private, make it extremely challenging to flag potential system threats in a timely fashion. This international collaborative project targets a novel approach to semi-automatically identify system vulnerabilities, thus greatly increasing the efficiency and capacity to respond to emerging threats." Also involved as co-investigators are Prof. Garibaldi, who has previously worked with the team at CESG on modelling expert decision making, and Prof. McAuley, who is Director of the Horizon Digital Economy Hub and has specific expertise in security and privacy research.

The UK cyber security sector already has world-leading capabilities and is worth over £6 billion, employing 40,000 people. Cyber attacks are increasing in severity and sophistication and companies are struggling to recruit the expertise needed to defend their organisations.

Cyber security underpinned with scientific expertise

The system will be designed to directly address the acute shortage of availability and access to highly qualified cyber security experts by small-to-large scale organisations - from government to industry.

Dr Wagner notes: "The lack of sufficient access to highly trained and experienced cyber security experts is a key challenge for the UK. It prevents a

range of users from establishing and maintaining continuously adequate levels of protection of their assets in a rapidly changing security landscape. We view this challenge as a multi-stakeholder problem because a number of human stakeholders, from users and IT managers, with varying levels of expertise, to cyber security and software providers, need to effectively communicate and work together in order to deliver systems with an appropriate level of cyber security assurance."

This new, semi-automatic, data-driven approach is underpinned by novel research on integrating information from a number of different sources while managing discord and potential dependencies of individual components within systems. The aim is to enable systems which are capable of maximizing the utility of the available cyber security insights and to rapidly deliver user-tailored, up-to-date threat analysis and decision support to help organisations mitigate potential cyber attacks before they happen.

Dr Travis Breaux, from the School of Computer Science at Carnegie Mellon University in Pittsburgh, is supporting the project and is especially concerned about the challenge of system composability. Dr Breaux notes: "Increasingly, computer systems are built from hundreds, if not thousands, of hardware and software components that interact with one another. To improve security, system analysts must pay special attention to how these components interact, and they must place these interactions in the context of specific threats. The number of configurations and possible cyber threats is simply insurmountable for human analysts to effectively comprehend and evaluate on their own, which necessitates a semi-automated approach that can stay ahead of emerging technology. Our goal is to empower these analysts to comprehend a larger attack surface without being overwhelmed by increasingly complex systems."

A system tailored to real-world cyber security challenges

Expertise to assess the level of security of a particular IT system is not commonly available in one location. In addition, knowledge on vulnerabilities in systems develops rapidly, making it essential for organisations to maintain up-to-date awareness of their systems' potential exposure. The proposed approach is designed to capture and integrate security assessments, including associated uncertainty, from a number of sources, including government services such as the NCSC and third party security providers. The key challenge here is to develop ways to gather and model this often complex information effectively, while also dealing systematically with discord in the security assessments provided by individual sources.

By building up a continuously evolving database of system vulnerabilities, the OCYSS framework is designed to provide organisations with an up-to-date threat assessment, incl. associated uncertainty, tailored to their specific systems, thus supporting them in their decision making on threat mitigation.

A key aspect here is that the OCYSS approach is designed to avoid delays in threat detection and potential mitigation by providing a direct pathway for newly emerging vulnerabilities arising from individual system components or their interactions.

Dr Wagner said: "Going beyond the scope of theoretical research and developing advances in data science and human computer interaction, the project will also deliver a functioning prototype of the OCYSS framework, enabling us to conduct an exceptional level of evaluation tailored to real-world cyber security challenges, working closely with our partners at the UK's National Cyber Security Centre. The idea is to deliver both internationally published novel science and re-usable open source software, thus facilitating the reproduction of results, as well as substantially boosting the potential of commercial up-take of the project outcomes."

The University of Nottingham is currently recruiting additional cyber security experts at post-doctoral level.

Provided by University of Nottingham