Predicting future threats on the Internet: Inria, International University of Rabat and Carnegie Mellon University are collaborating on the NATO-funded ThreatPredict project

The goal of ThreatPredict is to improve prediction of cyber security threats using a novel approach that combines artificial intelligence, big data and heterogeneous input data. The results it produces will make it possible to best prepare for future attacks and limit their impact. It is funded by the North Atlantic Treaty Organisation (NATO) under the Science for Peace and Security (SPS) program.

“It is often difficult for a company to know whether it has been attacked, or is even currently under attack. As a result, we must dissect the malicious acts after the fact, once the harm has been done. Giving warning about a probable attack that is imminent or in progress will considerably reduce the damage caused. This may seem obvious, but it is extremely complex to implement because the forces involved are very well trained, agile and very often change modus operandi,” explains Jérôme François, Inria researcher with Resist, a joint Inria-Loria research team.

The project’s main novelty lies in its combining technical data with societal and publicity data, and trends from social networks.

Attackers have numerous motivations. During the recent election campaigns in France and the United States, there were attacks which highlighted the societal dimension of certain threats. “Major sporting or political events are often targeted. The impact of attacks can also have strong repercussions on a company’s business activity: monitoring political, societal or even economic indicators has real relevance and significant added value for cyber security,” points out Ghita Mezzour, Assistant Professor at the International University of Rabat (UIR) in Morocco.

The major difficulty in the field is the number of sources to integrate, for each one is different. The challenge is to develop predictive models by combining technical data, such as those collected by security probes, for example, with non-technical data, particularly from social media.

Scientists, institutions and private partners give themselves three years for the challenge.

The three-year ThreatPredict project will bring together three major institutions in cybersecurity research until December 2020: Inria, through its RESIST team and the High Security Laboratory, both based in Nancy, France; the TICLab laboratory at the International University of Rabat in Morocco; and the Center for Computational Analysis of Social and Organizational Systems (CASOS) at Carnegie Mellon University in the United States.

The project is also supported by two public partners: the US Army Research Lab (Unites-States), the General Directorate of Information System Security (Morocco), and one private partner: Thales (France). They play the role of end users by providing their views on the project’s results and direction.

For more details: http://threatpredict.inria.fr/
About Inria: Inria, the French national research institute for the digital sciences, promotes scientific excellence and technology transfer to maximise its impact. It employs 2,400 people. Its 200 agile project teams, generally with academic partners, involve more than 3,000 scientists in meeting the challenges of computer science and mathematics, often at the interface of other disciplines. Inria works with many companies and has assisted in the creation of over 160 startups. It strives to meet the challenges of the digital transformation of science, society and the economy.

www.inria.fr

About the Inria Nancy – Grand Est research centre: Settled in Lorraine since 1986 to contribute to the economic revival of the region, the center has grown steadily from 7 project-teams and 50 people to 21 project-teams and 450 people today; the project-teams are located in three sites: the main building in Villers-lès-Nancy, the IECL and Strasbourg.

Inria Nancy – Grand Est research centre conducts most of its scientific activities in partnership with the French National Centre for Scientific Research (CNRS), the University of Lorraine and the University of Strasbourg. We also maintain close ties with research institutes and universities from the wider region, notably in Saarbrücken and Luxembourg.

Read more about our four main research themes on: https://www.inria.fr/en/centre/nancy/overview/inria-nancy-grand-est-centre

About LORIA, the Lorraine Research Laboratory in Computer Science and its Applications: joint research unit of Inria, CNRS and Université de Lorraine. Since its creation in 1997, its mission has been basic and applied computer science research. The scientific work is carried out in 28 teams, 15 of which are shared with Inria. The RESIST team is one of them.

www.loria.fr

About TICLab (ICT Research Laboratory): TICLab is a research laboratory in the fields of information and communication technologies, which has a particular focus on data science (big data), artificial intelligence, and the internet of things, and their applications in various domains such as smart cities, urban mobility, energy efficiency, cyber-security, health, logistics and social issues. Since its creation in 2010, TICLab has secured 15 research grants from national and international funding agencies, published over 200 papers in journals and conferences, and filed 30 patents. TICLab is a coordinator of the CNRS-associated international laboratory LIA DATANET, in the field of big data, which brings together many Moroccan research entities and LORIA and CRAN laboratories of Lorraine University.

www.uir.ac.ma

SCIENTIFIC CONTACTS

Inria - Jérôme FRANCOIS, Inria researcher, joint Inria-Loria RESIST team
jerome.francois@inria.fr

UIR - Ghita MEZZOUR, Assistant Professor
ghita.mezzour@uir.ac.ma
  - Mounir Ghogho, Director of TICLab
mounir.ghogho@uir.ac.ma

PRESS CONTACTS

Inria - Laurence Goussu - +33 (0)6 81 44 17 33
Laurence.goussu@inria.fr

UIR - Loan Duong - +212 (0) 5 30 10 30 40
loan.duong@uir.ac.ma

CASOS - Daniel Tkacik - +1 412 268 1187
dtkacik@andrew.cmu.edu