Automated analysis of cyber-attacks using attack-defence graphs

Author: Frank Fransen
Date: 5 July 2017

Basic information

Division: Technical Sciences – Cyber Security & Robustness
Location: Groningen
Level of Experience: Master's graduation project
Education: University, technical degree (computer science)
Duration of project: 6 - 9 months

WHAT WILL YOU BE DOING?

The cyber threat landscape is continuously evolving. The complexity and speed at which cyber-attacks occur is increasing. These developments require automation to aid human analysis and execute defensive actions at machine-speed.

Within the master project you will work on development of technology and tools for automatically analysing the vulnerability of (a model) of an ICT infrastructure against (new) cyber threats, and determine the best approach to respond to these threats. You will work on modelling cyber threats and defences in so called attack-defence graphs, modelling of an ICT infrastructure, and applying the attack-defence graphs on the ICT infrastructure model to determine if and how attacks can propagate through the ICT infrastructure. As a next step, you will work on how to map detected security events onto an attack graph, and how to determine the best defences against a new threat or ongoing attacks.

WHAT DO WE REQUIRE OF YOU?

You are working on a Master's degree on Information Science and you would like to work on ICT security. You are familiar with information security, experience with programming, modelling and IP network technology. You are analytical and you are capable of working autonomously. In addition, you have good communication skills and you are creative and innovative. However, most important is your motivation to work in the cyber security field.

WHAT CAN YOU EXPECT OF YOUR WORK SITUATION?

TNO is an independent research organisation whose expertise and research make an important contribution to the competitiveness of companies and organisations, to the economy and to the quality of society as a whole. Innovation with purpose is what TNO stands for. We develop knowledge not for its own sake but for practical application. To create new products that make life more pleasant and valuable and help companies innovate. To find creative answers to the questions posed by society. We work for a variety of customers: governments, the SME sector, large companies, service providers and non-governmental organisations. Working together on new knowledge, better products and clear recommendations for policy and processes. In everything we do, impact is the

key. Our product and process innovations and recommendations are only worth something if our customers can use them to boost their competitiveness.

This department Cyber Security & Robustness (CSR) employs approximately 48 professionals who work on issues related to the security of IT networks, systems and smartphones to help our clients and associates take charge of their ICT security, detect fraud, review their architecture or develop a security design for new systems. The division is located at two locations: Groningen and The Hague.

WHAT CAN TNO OFFER YOU?
You want to work on the precursor of your career; a work placement gives you an opportunity to take a good look at your prospective future employer. TNO goes a step further. It's not just looking that interests us; you and your knowledge are essential to our innovation. That's why we attach a great deal of value to your personal and professional development. You will, of course, be properly supervised during your work placement and be given the scope for you to get the best out of yourself. Naturally, we provide suitable work placement compensation.

APPLICATION PROCESS
For this vacancy it may be required that the AIVD issues a security clearance after conducting a security screening. Please visit for more information the AIVD website.

Contact persons: Frank Fransen
Phone number: +31 (0)88-86 67729