Dina Hadžiosmanović's research

After studying Computer Science at the University of Sarajevo (Bosnia and Herzegovina) Dina Hadžiosmanović started working on her PhD thesis at the Distributed and Embedded Security group. Her research concerns the security of critical infrastructures, such as gas and water supply, and in particular intrusion detection.

What is the topic of your thesis?
"I am researching two complementary approaches to detect anomalous activities in computer systems that control critical infrastructures. The first approach is log analysis, on which I have worked during the first two years of my research. Log analysis is all about detecting abnormal behaviour. I am focusing on analysing anomalous user behaviour. It could be the case that a user makes mistakes and thereby unintentionally harms the system. But it could also be that an attacker has gained user access rights and is performing actions which look legitimate but may disrupt the process. I have developed a methodology and a tool to detect this in the log. The feedback I have received about this tool is very positive. I am working in a nationally funded project in which I collaborate with five industrial partners and two security companies. They have provided me with logs from real environments and they acknowledge the significance of the analysis results. One project partner, SecurityMatters, a spin-off company from our research group, is turning part of this research into an actual product for the industry."

What do you hope to achieve?
"In the second part of my project I am using network analysis as a way to detect possible attacks. At the moment, state-of-the-art intrusion detection tools can detect cyber attacks based on known viruses only. In critical infrastructures this is simply not enough. The idea is to detect previously unknown threats by monitoring network traffic and analysing the content of data packets (size, byte sequences, structure, etc.). By developing models of normal behaviour, machine learning algorithms can learn to distinguish normal behaviour from abnormal

What is the societal relevance of your research?
"The impact of a potential attack on critical infrastructures can be enormous. For example, a coordinated cyber attack can stop the power supply in a wide metropolitan area within minutes. Therefor those infrastructures should be protected in the best possible way. Since current approaches can only partially address the problem, a research area exploring advanced intrusion detection approaches for such sensitive environments is highly important."

Why did you choose this subject?
"After graduation I was not sure which topic I was going to pursue. So I made a shortlist of three topics computer networks, security, and machine learning. This project is a perfect combination of the three. I wanted to come to the Netherlands for my PhD because I have family living here. I enjoy working at the CTIT because being part of an Institute helps when collaborating with other researchers. Mostly I am working together with researchers from Design and Analysis of Communication Systems, Information Systems and the Database group. After I finish my thesis, I hope to stay in academia or else to be able to deploy my ideas and knowledge in the industry."

CTIT

Since 1994, the Centre for Telematics and Information Technology of the University of Twente (CTIT) has drawn from its broad integrated research spectrum to do cutting edge technical research, in tune with the societal and economical challenges of today and tomorrow. CTIT is a strong team player within the innovation chain at both the European and local level, through alliances, public-private partnerships and spin-off companies. Whether it's pushing the limits of cognitive radio and sensor networks, enablin

Contact
University of Twente