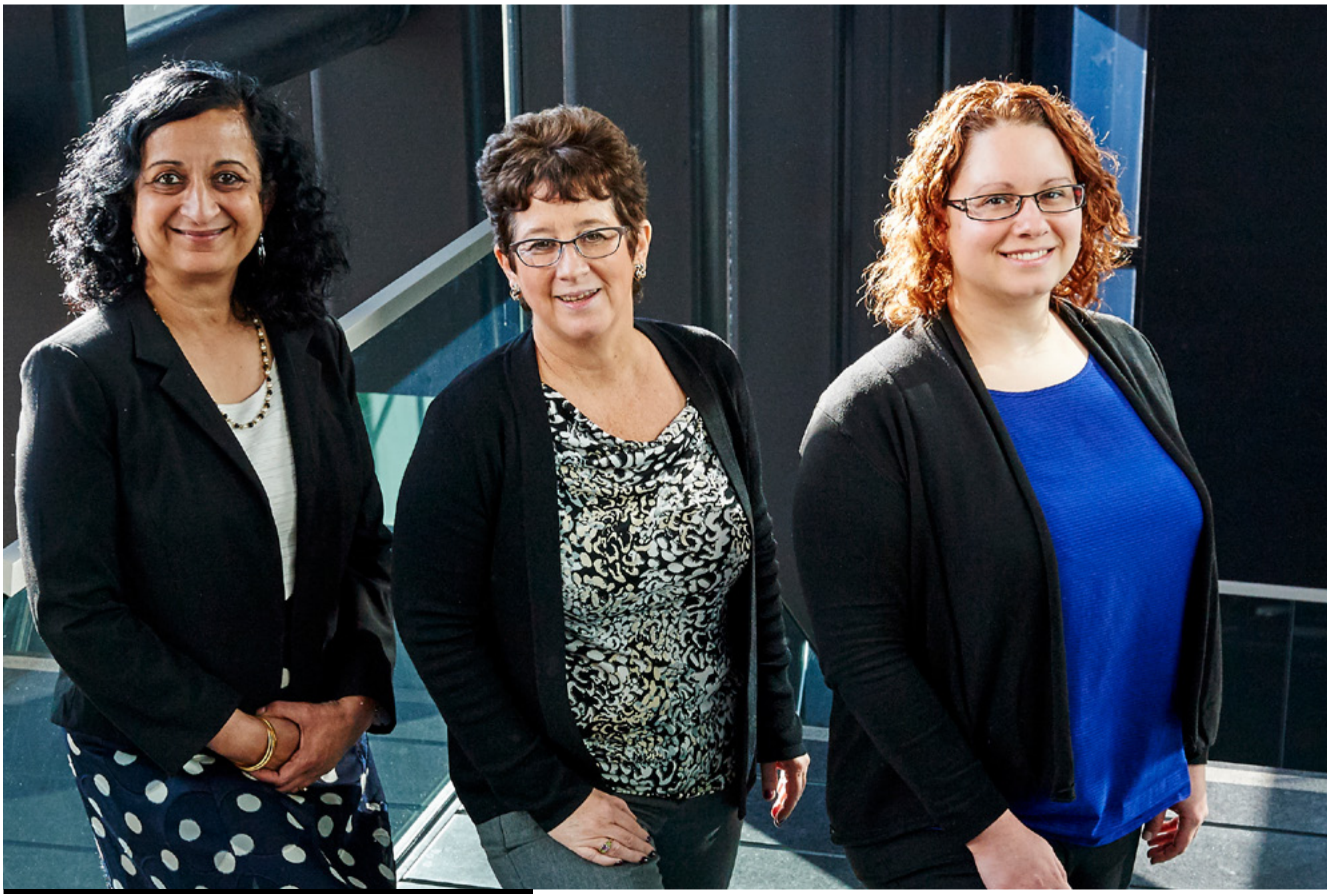
‘The bad guys can experiment on the whole world wide web, while the good guys are playing with LEGO. We need testbeds in a realistic environment to simulate what happens when some critical infrastructure is attacked, and what we can do to prevent or stop such an attack.’ This statement of NCSRA Symposium 2015 session leader Sandro Etalle pretty well summarizes the vision of American researchers Anuradha Annaswamy, Terry Benzel and Benessa Defend. Door Sonja Knols

Advancing science by connections



From left to right: Anuradha Annaswamy, Terry Benzel and Benessa Defend.

Cybersecurity and privacy were the main themes of the second National Cyber Security Research Agenda Symposium, held last November 2nd in The Hague. The symposium attracted about 500 visitors, who saw presentations and held discussions about issues like Cyber Security Education, Research Challenges in the Privacy Domain, the EU Phishing Initiative and the Protection of Critical Infrastructures. In the latter research domain an important role is played by the American DeterLab, a large scale open facility which consists of some 500 nodes which scientists, industries and governmental organisations can use to model and emulate cyberattacks on networks and physical infrastructures.

>>

‘What we actually do at the DeterLab, is research on research,’ states Terry Benzel, Deputy Director of the Computer Networks Division at the University of Southern California and in charge of DeterLab. ‘Collaboration is key for the success of the lab. We have connected several different testbeds from all over the world through secure connections, and we are still looking for new collaboration partners in academia and industry.’
‘The testbed is an ideal environment for our research into the resilience of self-governing and self-healing systems, such as smart energy grids,’ says Anuradha Annaswamy, Director of the Active-adaptive Control Laboratory at MIT. One of the strengths lies in the fact that the lab can be considered a collection of different testbeds in different countries, she emphasizes. ‘Different infrastructures in different countries behave in different ways, due to organisational differences, variations in legislation and so on. Therefore it is essential that as researchers, we get access to different testbeds, representing different situations.’

DeterLab

The DeterLab is an advanced testbed facility, where researchers from all over the world can conduct cybersecurity experiments on a system that resembles the real world in complexity and scale. The testbed is free to use and accessible through an online application process. It’s operator DETER (cyber DEfense Technology Experimental Research Laboratory) enables experimenters to share data, lab set-up, software, procedures and results in order to advance cybersecurity research as a whole.
More information: *http://deter-project.org/about_deterlab*

Cooperating with Japan

Benessa Defend, Senior Research Consultant at the European Network for Cyber Security (ENCS), agrees that international cooperation is essential in the cybersecurity field. ‘As ENCS, a non-profit organisation that aims to secure European critical infrastructures, we recently signed a letter of intent with the National Institute of Advanced Industrial Science and Technology in Japan. We are going to cooperate with them on research into smart metering and smart grids. Japan has ample experience with the security and safety of critical infrastructures, especially in the energy sector.’ Annaswamy adds: ‘In fact I will be travelling to Japan in due course. The disaster with the tsunami and the Fukushima nuclear power plant has been a major driver for Japan’s interest in this field of research into so-called cyber-physical systems. But besides that tragic event, Japan also wants to push the solar energy portfolio. That raises questions on how to integrate solar power into the existing electricity grid.’

One of the main challenges in the cybersecurity of cyber-physical systems lies in the heterogeneous multi-agent character, Annaswamy explains. ‘Take for example the smart grid: We see a tremendous growth of sustainable power sources such as solar power and wind power. This energy must be fed into the grid in a controlled way. At the same time, we see advances in the cyber world, enabling us to understand and collect information about generation and use of energy. Eventually, we want to use as much green energy as possible, and achieve zero net energy consumption. That means we have to use electricity efficiently, infrastructure wide.’ Peaks in energy generation by sustainable sources have to be matched with demands of customers. One of the ways to do this, is by installing agents in households, which negotiate with the energy supplier on timing and pricing of the energy. These agents can for example be smart meters, recording consumption of electric energy and communicating that information back to the utility for monitoring and billing. But these meters introduce risks.

‘Think of privacy issues,’ says Defend. ‘Recently, together with industry we constructed and implemented a privacy protocol for smart meters. Our goal as ENCS is to make lasting changes, by including the protocol in international standards. Our aim is that as soon as anyone buys a new meter, our protocol will be part of it.’ To test the protocol, Defend did not have any ready-made testbed available, she explains. So she created one herself. ‘We bought one hundred of these smart meters and tested our privacy protocol on them.’ Benzel immediately interrupts: ‘I see a great collaboration here: can’t you enter these meters into our testbed facility?’

Terry Benzel: ‘Researchers can use the testbed to look into the future with different scenarios’

Connecting cyber world to real world

Cyber-physical systems are becoming more important as a research topic at the DeterLab, she says. 'Back in 2003, when the testbed started, sponsored by the American Department of Homeland Security, it was mainly used for malware analysis. Over time, the research evolved to simulating botnets and denial of service attacks. In recent years, cyber-physical systems are becoming more and more of interest. In cyber-physical systems, physical systems such as power plants get connected through internet services.' Annaswamy adds: 'As soon as you intermingle cyber and physical worlds, you create new cyber failure nodes. All of a sudden people have an entrance to a power plant for example, from a distance. Think of the Stuxnet attack that occurred recently. That started in the cyber world, with a USB-stick, but it ended up affecting the rotation speed of a pump in a uranium production facility, which is very much the real world.'

Anuradha Annaswamy: 'More windows will be opened, and more people will get some form of access to infrastructure. These are all possible holes in the defence'

Benzel: 'To get an idea of the potential dangers we are facing, I always use the example of the municipal water systems. What if someone can break into the computer, mislead the sensors in such a way that the computer always reports that the water is clean, and then poison the water reservoir. In that case it will take ages before anyone finds out something is wrong, and many people may have died before the problem is even found.' Since many of these critical infrastructures are not only important locally or nationally, these kinds of security hazards ask for international cooperation.

Annaswamy: 'For researchers, the main challenge lies in controlling multiple agents. We are moving towards the often mentioned internet of things. That means more windows will be opened, and more people will get some form of access to infrastructure. These are all possible holes in the defence.' But people do not only get windows to look into data, they are also interfering with the performance of the infrastructure itself. In the case of smart grids, there will be negotiations between consumers and electricity suppliers for example. 'We are introducing more points of decision-making which are critical to the behaviour of the infrastructure as a whole. What does this mean to the customer, and what investments does the owner of the infrastructure have to make to secure its performance? These are very complicated relations, which are very hard to simulate on a single computer.'

>>

AFNOC Mission
Execute AFNETOPS/CC authority to command and control the operation and defense of the AF Network
AFNetOps C2 Relationship
SIPRNET

The US cyber command, which centralises the army command of cyber space operations.

Benzel: ‘It is exactly these type of questions the DeterLab can help with. The testbed can be used for any question about complexity and scaling issues. Researchers can use it to look into the future with different scenario’s. You can do an experiment 3000 times to see how the outcome varies when you vary different parameters. The DeterLab is open for anyone from anywhere. We have some 8000 users from over 40 countries. But as mentioned before, also organisations can make their own testbeds and connect them to DETER. We are now looking into the possibilities to cooperate with The Netherlands. You have a good reputation on cybersecurity research, and you have unique problems such as with the flooding since the country is below water level. Perhaps The Netherlands decide to develop a testbed of their own, based on this unique expertise.’

This would fit into the vision DETER has laid out for the future, says Benzel. ‘We recently issued a report on Cyber Experimentation of The Future. In the next ten years, we hope to see large collections of testbeds being developed. That way we can seek for communalities, for universal problems, and for similarities in solutions. ‘I want to make a comment on that matter,’ says Annaswamy. ‘With this search for universality, you need to be careful. Genericity should indeed be captured, but I don’t believe in one cure for all. For example, in urban mobility transport, laws are different than in energy management. The implications of a hack also vary greatly. The result of a traffic congestion is of a different order than the problems arising from a general power failure. You have to stay truthful to underlying physical laws of different cyber-physical systems. And I strongly believe we need to develop different layers of defence tailored to individual needs.’ Benzel agrees. ‘We indeed will have to create domain specific approaches.’ Defend closes the conversation by stating: ‘In the cases of cyberattacks to critical infrastructure there is no silver bullet. Research, industry and government will have to work together, and share information on an international level.’ I/O

Benessa Defend: ‘In the cases of cyberattacks to critical infrastructure there is no silver bullet’

Samenvatting

Tijdens het tweede National Cyber Security Research Agenda Symposium op 2 november jongstleden, werd onder andere gesproken over het belang van internationale samenwerking en grootschalige testbeds om cruciale infrastructuur zoals energiecentrales en watervoorzieningen te beschermen tegen aanvallen van hackers. In dit artikel vertellen Anuradha Annaswamy, Benessa Defend en Terry Benzel over hun ervaringen met internationale samenwerking, en de mogelijkheden die het Amerikaanse testbed DeterLab biedt om op grote schaal cyberaanvallen te simuleren en nieuw ontwikkelde verdedigingsmechanismen te testen.