US-NL cooperation in cyber security research

dcypher

NWO

Preface

NWO, the Dutch research council, has an objective to communicate about results of the research they fund. Platform dcypher has an agenda setting role in cyber security research and higher education. As such it brings parties together nationally and internationally. Both organisations decided to publish this booklet about international collaboration in cyber security research. To make this collaboration work at two sides of the atlantic taylor made funding instruments were required. This makes this collaboration unique and special. But there is more.

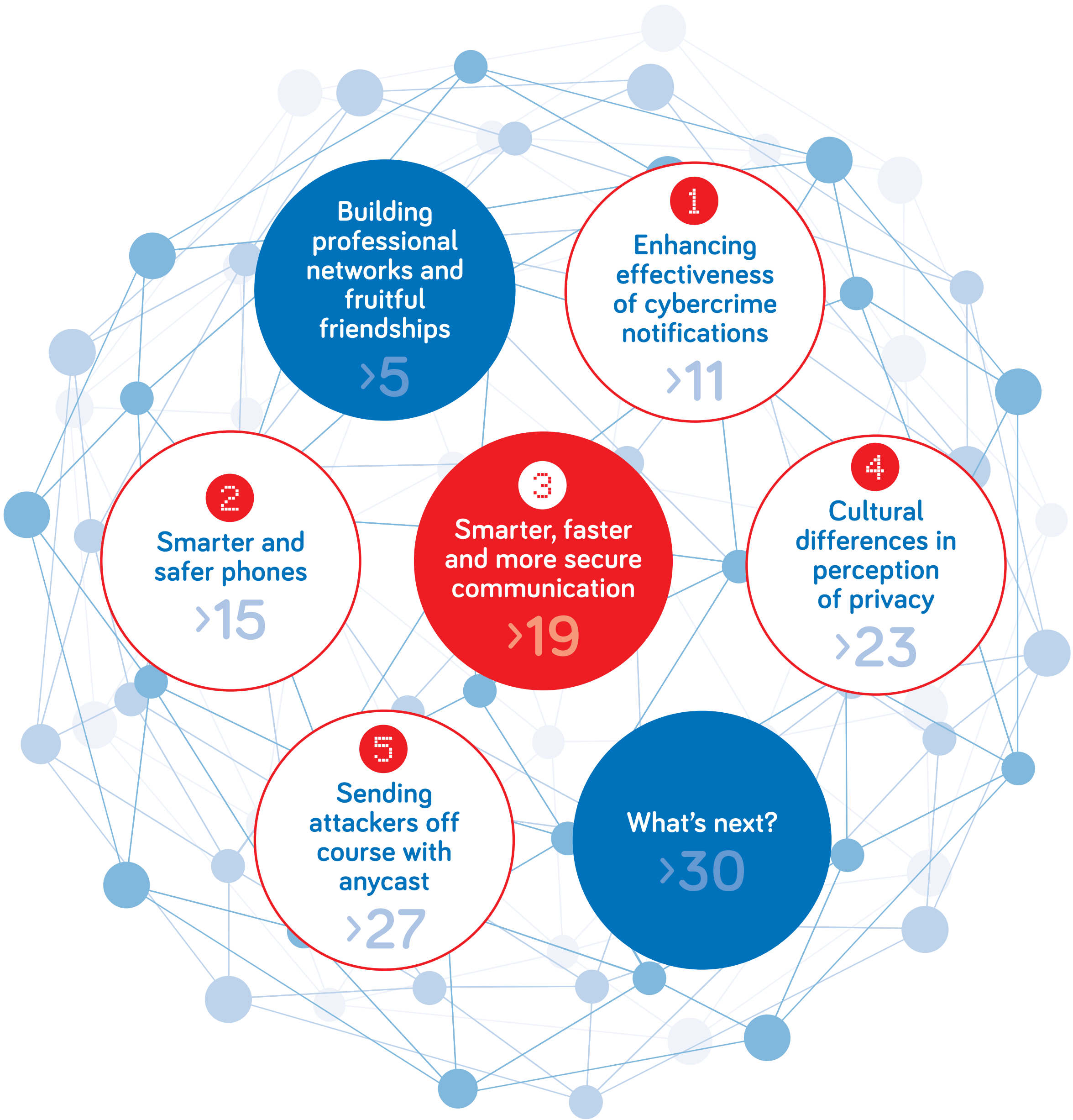
Developing and maintaining a high level of cyber security is a global challenge. In doing R&D as well as in using the results of R&D international collaboration is a must. Countries which are self-sufficient in cyber security do not exist. Investigation and persecution of cybercriminals for instance demands for an international approach. Deployment of IT equipment of a foreign brand requires cross-border trust.

In the last eight years, organisations in the US (DHS and NSF) and the Netherlands (NWO & NCSC) developed multiple joint funding programs on the topics of cyber security and privacy that involved researchers from both countries. The key motivation for these joint programs was a strong belief that the fields of cyber security and privacy would benefit from having the research communities from both countries explore these problems together.

To date thirteen US-NL project proposals were granted by DHS, NSF, NCSC and NWO together. Currently projects are at different stages. Some are finished, others still running. In this booklet five out of these thirteen jointly funded projects are briefly explained and put in perspective by their executors. Pictures associate faces with the research. The effect of these collaborations transcends the teams immediately involved: student exchanges were not limited to those working on the joint projects, not only the US and the Netherlands benefitted from methods developed, also other countries deployed the research. In other words, a high multiplication factor was reached. Progress is reported in showcase meetings, Principal Investigator meetings and workshops periodically organized and held in both countries. These served different purposes: sharing knowledge, reporting status, exchanging ideas, and above all building trans-atlantic teams and friendships!

Jan Piet Barthel
Cyber security program manager NWO
Director dcypher

Content



Building professional networks and fruitful friendships

It was February 2012, when the foundation was laid for a fruitful cooperation between the Netherlands and the United States on cyber security research. To date, this cooperation has resulted in three joint calls, in which 13 projects were funded. Dutch organizers Jan Piet Barthel (Netherlands Organization for Scientific Research), Raymond Doijen (National Cyber Security Center) and their American counterparts Douglas Maughan (Department of Homeland Security) and Susanne Wetzel (National Science Foundation), discuss the merits of this bilateral collaboration.

'On February 22nd 2012, at the Dutch embassy in Washington, the Dutch minister for Security and Justice Ivo Opstelten and the American Secretary of Homeland Security Janet Napolitano signed a Letter of Intent describing the intention to cooperate to create a safe and resilient cyber world. That was the starting point for the joint calls between NWO, NCSC and DHS,' recollects Jan Piet Barthel.

'We looked across the spectrum and noticed that we had no international agreement with the Dutch yet,' says Douglas Maughan. 'The Netherlands is an important player in the cyber security domain. When you look at Europe, you basically have the United Kingdom, Germany and the Netherlands who stand out. The official visit of the Dutch minister for Security and Justice was an excellent occasion to decide to cooperate between government agencies when it came to cyber security. Research was part of that agreement.'

Later that same year, the first pilot call for joint research in cyber security was organized. At the embassy meeting, five research topics had been identified which would be of interest for both countries. Researchers were asked to submit an Expression of Interest. Three of those were selected and asked to prepare full proposals, which were then granted in fall 2013. The projects started in 2014.

'The global challenges of cyber security, the appreciation of the research community on both sides for the joint initiative and the results of this pilot convinced us to continue and strengthen our valuable partnership with DHS,' motivates Barthel about the decision to organize a second call in 2017. This call resulted in 13 joint proposals, of which 5 were granted.

Second partnership

In the meantime, a second bilateral transatlantic partnership had been formed. Susanne Wetzel: 'At NSF, we had a Secure and Trustworthy Cyberspace (SaTC) program. This program involves 7 directorates, including not only computer science but also education, engineering and physics and mathematics, and is one of the longest running programs of NSF. Since for NWO, NSF would be the more natural partner to set up collaborations with, it was evident that we should cooperate. We settled on privacy in a cyber environment as a suitable topic for such a joint program. Because of the cultural differences between the US and the Netherlands when it comes to how people perceive privacy, we thought that this topic would lead to added value when studied in an international context. We organized a joint workshop in 2016 in Washington DC, where scientists from the US and the Netherlands could meet and could explore common interests.'

As is the case in the NWO/NCSC/DHS program, all projects within the resulting Privacy Research in a Cyber Environment (PRICE) program include a Netherlands-based principle investigator, who works closely together with a US-based principle investigator. In the PRICE call, NWO invested 1.25 million euros to fund the Netherlands-based researchers, while the NSF matched this by allocating 1.25 million dollars to fund the US-based researchers. The interest was high, since fourty four admissible project proposals were received. Five projects were granted, which started in 2017.

> 'Cyber is a global sport. It doesn't stop at borders'

Setting up procedures

In all three joint programs, the basic principle is the same: no money transfers the border. So DHS and NSF pay for the American part of the research, whereas NCSC and NWO pay for the Dutch part. Maughan: 'For us, this was the first time that we organized actual joint calls. That meant we had to change our process. Finally, we ended up with two different granting procedures, in which each country uses its own review process to rank the proposals. Eventually we grant the proposals that end highest in both competitions.'

Wetzel: 'For us, setting up the procedures was not that hard. We have several international joint projects, for example with Israel and Brazil, so we already had something in place with regard to the legal documents and involvement of several departments.'

Since NSF and DHS are different types of organizations, with different aims, also the aims of both collaborations differ slightly. Maughan: 'With this program, our first priority is to raise the technical value of both performers and create useful new technology. Secondly, we want to educate students and realize technical exchange between different universities. So in our review process, an important question project leaders have to answer is how they are planning the transition of knowledge to the market.' Wetzel: 'For us, this program is not only about improving research by incorporating different perspectives and combining expertise, but also about creating new opportunities for students to travel and explore cultural exchanges, which is extremely important to understand the other side.'

Added value

All four organizers agree that the international cooperation has a clear added value over national initiatives. Doijen: ‘As a small country, the Netherlands has small budgets for research. These types of collaborations have a multiplier effect: you get twice the research capacity for the same price. And we get access to knowledge we don’t have ourselves.’ Barthel: ‘But also within the country itself, these programs have led to a multiplier effect. The privacy topic introduced in the NWO/NSF program gave the natural sciences domain the opportunity to work together with the social sciences domain, leading to additional financial means for the research program.’ Wetzel: ‘A cooperation is a success when one and one adds up to more than two. In that sense, I like the joint project of the University of Maryland, the University of Wisconsin and the Erasmus University Rotterdam. They look at the introduction of Google Home in both countries, and compare between the different perspectives before and after implementation. This is vital information if you want to translate different cultural perspectives on technology into policy and regulations.’

Global sport, global cooperation

The bilateral collaboration in the three calls hopefully will turn out to be a starting point for more, they all say. Maughan: ‘We have funded some projects that have a clear impact on cyber security worldwide. And we were able to establish a model that can be built upon for other topics than cyber, and also for other countries that want to cooperate with us.’ Barthel: ‘By investing a little in connecting people, you create a flywheel that goes on. Though it may not always have been easy, with all kinds of legal issues that had to be overcome, now we are very enthusiastic about this transatlantic partnership.’ Doijen: ‘Cyber is a global sport. It doesn’t stop at the borders. So I hope we can now take the next step, and try and see if there are possibilities for multinational programs in which more than two countries cooperate in a similar way.’

Douglas Maughan
Department of
Homeland Security

Raymond Doijen
National Cyber
Security Center

Jan Piet Barthel
Netherlands Organization
for Scientific Research

Susanne Wetzel
National Science
Foundation

Projects granted within US/NL bilateral cooperation schemes

NWO-NCSC-DHS research projects (first -pilot- call)

Dates granting letters: 2013

Project title	PI’s
Increasing the impact of voluntary action against cybercrime	Prof. dr. M.J.G. van Eeten, Delft University of Technology, NL Prof. dr. T. Moore, University of Tulsa, US
Malware on smartphones: collection, analysis, and defensive measures	Prof. dr. ir. H.J. Bos, VU University Amsterdam, NL Prof. dr. C. Kruegel, University of California Santa Barbara, US
In-depth defense of SCADA and ICSs	Prof. dr. S. Etalle, Eindhoven University of Technology, NL A. Valdes, University of Illinois at Urbana Champaign, US

page 11

page 15

NWO-NSF research projects (PRICE program)

Dates granting letters: 2016

Project title	PI’s
Faster and Stronger Onion Routing (FASOR)	Prof. dr. T. Lange, Eindhoven University of Technology, NL Dr. J.A. Solworth, University of Illinois at Chicago, US R. Dingledine, The TOR Project, US
Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems: Practices and Contexts in the Netherlands and US	Dr. J.H. Pridmore, Erasmus University, Rotterdam, NL Dr. J.M. Vitak, University of Maryland, US Dr. M.T. Zimmer, University of Wisconsin-Milwaukee, US
Transparency Bridges: Bridging Transparency Requirements in Smartphone Ecosystems	Prof. dr. N.A.N.M. van Eijk, University of Amsterdam, NL Prof. dr. J.V.J. van Hoboken, University of Amsterdam, NL Dr. D.J. Weitzner, MIT, US
Bridging The Gap Between Theory and Practice in Data Privacy	Dr. B. Skoric, Eindhoven University of Technology, NL Prof. N. Li, Purdue University, US
Using process tracing to improve household IoT users’ privacy decisions	Dr. ir. M.C. Willemsen, Eindhoven University of Technology, NL Dr. B.P. Knijnenburg, Clemson University, US Prof. dr. A. Kobsa, University of California, Irvine, US

page 19

page 23

NWO-NCSC-DHS research projects (second -official- call)

Dates granting letters: November 2018

Project title	PI’s
Planning Anycast for Anti-DDoS	Prof. dr. ir. A. Pras, University of Twente, NL Prof. dr. J. Heidemann, University of Southern California, US
Deep packet intelligence for industrial control systems	Prof. dr. S. Etalle, Eindhoven University of Technology, NL Dr. A.A. Cardenas, University of Texas at Dallas, US
MADDVIPR - Mapping DNS DDoS Vulnerabilities to Improve Protection and Prevention	Dr. A. Sperotto, University of Twente, NL Dr. K.C. Claffy, University of California San Diego, US
TROPICS Timely and RObust Patching of Industrial Control Systems	Prof. dr. ir. H.J. Bos, VU University Amsterdam, NL Prof. dr. C. Kruegel, University of California Santa Barbara, US
MitigatINg IOt-based DDoS attacks via DNS	Dr. ir. C. Hernandez Gañán, Delft University of Technology, NL Dr. D. McCoy, Tandon School of Engineering, New York University, US

page 27

NWO/NCSC/DHS call 2013:
Increasing the impact of voluntary action against cybercrime

Prof. Tyler Moore
University of Tusla

Prof. Michel van Eeten
Delft University of Technology

Enhancing effectiveness of cybercrime notifications

Most of today's actions taken to protect people against cybercrime are carried out by private actors. The bulk of incident response is based on voluntary action by parties like security companies or internet providers who notify each other about potential abuse, and ask to act against it. An American and a Dutch research group group jointly investigated the effectiveness of these voluntary actions.

'Michel and I met back in 2008 while I was still a PhD student in Cambridge and he visited our research group for a study on malware he was conducting for the OECD,' US researcher Tyler Moore recollects when asked how his cooperation with Dutch Michel van Eeten came about. Prior to this project, Moore had conducted an initial experiment in sending abuse report notifications to webmasters in order to measure their effectiveness. 'Michel wanted to partner with me to scale up this approach further by conducting more such experiments to better quantify the effectiveness of voluntary abuse reporting in combating cybercrime.' 'There are only a few groups in the world which are active in the field of "economy of cyber security",' adds Carlos Hernandez Gañán, postdoc in van Eeten's group at Delft University of Technology and daily supervisor of the Dutch PhD student in the project. ‘The father of the field actually was Tyler’s PhD supervisor, and there is only one yearly conference on this specific theme that everyone involved attends.’

Most of the efforts to combat cybercrime are carried out by private actors, not law enforcement. This is because so much of the internet infrastructure is privately held, and individual compromises don’t typically rise to the level prompting a law enforcement action. ‘So it was clear to us that the incentives for actors responsible for the affected system or service receiving an abuse report, such as a message explaining that a computer or resource is compromised and that it should be fixed, were important. We were interested in studying how effective these abuse reports were, and we tried to identify characteristics that were associated with more successful responses,’ says Moore.

Complementary data

Moore’s group had access to data about recent infections via a partnership with a private company that works on threat intelligence. And in the Netherlands, a PhD student tracked particular botnets to look for abuse that the researchers could notify affected parties about firsthand. The researchers used these data on threats and vulnerabilities to conduct five different experiments. In these experiments, they varied both the contents and the sender of the notification message. ‘We also used different channels to notify people through,’ adds Hernandez Gañán. ‘Because of our cooperation with the Dutch internet provider KPN, we had access to both email addresses and phone numbers of individual clients. We either sent them an email, or notified them over the phone.’

Varying contents and senders

In their experiments, the researchers played around with the content, Hernandez Gañán says. ‘We went from generic “He, we see that something is wrong with your system or service and you have to do something about it”, to providing very specific information about the exact vulnerability or infection and how to fix it. In the latter case, people tend to act sooner, especially when you send them a step by step guide to fix the problem.’ The research team also created a tool that people could use to test if their system had vulnerabilities or not. But since often individual users lack the knowledge to fix any vulnerability they might find, this tool was mostly used by server operators.

The influence of the reputation of sender of the notification was studied by sending messages either from a personal Gmail account, from a company, or from a well-known university. Surprisingly, the reputation of the sender doesn’t matter for how many receivers tend to act upon a warning about a security breach, say both researchers. ‘We confirmed that providing detailed messages concerning the nature of compromise in abuse reports is the single most important factor influencing whether or not they are acted upon. The notification should be actionable – preferably containing a step by step plan –, precise and

‘People tend to act sooner, especially when you send them a step by step guide to fix the problem.’

Dr. Nicolas Christin
Carnegie Mellon University, Pittsburg

‘Adjust the channels you use and the contents of the notification to the target audience.’

explicit: this is wrong, it is happening in your network or computer at that location, and you can fix it by doing this and that.’

Spin-off

This finding does not lead to a ‘one-size-fits-all’ notification though, since responsibility and social norms differ in different cultures. ‘You will have to adjust the channels you use and the contents of the notification to the target audience,’ emphasizes Hernandez Gañán. ‘In fact, as a spin-off of this project, a Japanese team is going to do the same type of research with a Japanese equivalent of KPN, and also in Taiwan some replication studies are planned. This research might have initially been funded by the US and the Netherlands, but also other countries benefit. And in our country, government departments like the department of Justice and Security, and that of Economic Affairs and Climate Policy, are very interested in our work.’

The project also led to a spin-off project which is fully funded by the US Department of Homeland Security. Moore: ‘In this project called “Towards Outcome-Based Cyber security Risk Management” we are working with Nicolas Christin at Carnegie Mellon University as well to empirically examine the causal relationship between investment in security controls and whether those investments improve security and ultimately reduce the likelihood of experiencing significant breaches.’

‘This joint US/NL instrument allowed us to put Delft on the global map,’ concludes Hernandez Gañán. ‘Tyler introduced us to some prestigious American universities and companies as a trusted party. We have gained more visibility worldwide. Anytime we have a vacancy, we receive top level MSc student applications from all over the world.’

‘We gained more visibility worldwide.’

Prof. Tyler Moore
University of Tulsa

Prof. Michel van Eeten
Delft University of Technology

Dr. Carlos Hernandez Gañán
Delft University of Technology

NWO/NCSC/DHS call 2013:
Malware on smartphones: collection, analysis, and defensive measures

Prof. Christopher Kruegel
University of California,
Santa Barbara

Prof. Herbert Bos
VU University, Amsterdam

Smarter and safer phones

Smartphones essentially are very potent pocketsize computers. And that makes them interesting for hackers, who not only want to break into a phone to steal personal data, but also to use its computing power, for example to mine cryptocurrency. Martina Lindorfer and Victor van der Veen delved into the world of mobile malware and developed new methods to detect and defend against malicious activity on mobile platforms.

'The Dutch group of Herbert Bos, where Victor worked as a PhD researcher, has ample expertise in overall systems security. The group of Christopher Kruegel in the United States, where I was a postdoctoral researcher, is known for its expertise on malware analysis. So it made sense to cooperate on potential attacks on mobile phones,' says Martina Lindorfer, who is now an Assistant Professor at TU Wien in Austria.

Essentially, the project consisted of two parts, Lindorfer and Van der Veen explain. 'First, we looked at malware on mobile phones. There are many malware analysis tools available today, but when we started this project back in 2014, malware analysis for mobile phones was not that well-developed yet.' The researchers built an analysis environment for Android apps called ANDRUBIS and made that platform publicly available for integration into other tools and services.

'We also used this toolkit to get an idea about how malware in a mobile phone environment typically works,' says Lindorfer. Users could submit apps and get a report on what these apps were doing. The tool analyzes requested versus used permissions; monitors what activities the app initiates on files, the network, and the phone itself; and detects if any private information is leaked while using the app.

Eventually, over 1,5 million apps were analyzed with ANDRUBIS. 'In the mobile environment the most important malware behavior turned out to be phishing, ransomware attacks, denial of service attacks and cryptomining, just as is the case on desktop computers,' says Lindorfer. 'But for mobile phones, this list is completed with advertisement fraud, spyware that steals private information like contacts, premium SMS fraud, and apps interfering with the two-factor authentication that is used for example by banking apps.'

Sweeping cryptominers

The researchers decided to focus their attention on the relatively new phenomenon of cryptojacking: a user's browser is used to mine cryptocurrency. The problem with this cryptomining is that it is stealthy: a user visits a website, and the webserver fetches a mining payload in the background. The only thing the user notices is that his battery life shortens, his phone gets slower, or even crashes completely. 'Cryptojacking fortunately turned out to be not that widespread,' says Lindorfer. 'We studied over a million websites, and found only 1,735 performed cryptomining without their visitors' consent. However, the current defenses are relatively easy to evade, so we came up with a better way of detecting and battling this kind of malware. The resulting application called MINESWEEPER could be integrated into browsers and operating systems.'

'We came up with a better way of detecting and battling this kind of malware.'

'Cryptojacking fortunately turned out to be not that widespread.'

The second part of the project was aimed at bug-free exploitation. One of the problems of current computing devices is that they are pushing the limits of physics in terms of hardware. Moore's law, which drives the semiconductor industry, states that the number of transistors in an integrated circuit doubles about every two years. 'Squeezing ever more DRAM (dynamic random access memory) cells on a square millimeter leads to interference errors that can be exploited by hackers,' says Van der Veen. As a result of electric charges leaking out of individual memory cells, it is possible to flip a bit by repetitively addressing the adjacent cell. 'It is known that this

Dr. Martina Lindorfer
University of California,
Santa Barbara

so called Rowhammer principle can be exploited to hack into desktops, browsers, and the cloud. We wondered if this would be a problem for mobile phones as well.'

Exploiting hardware vulnerabilities

The researchers used the Rowhammer principle to develop Drammer: the first Rowhammer-based Android root exploit that does not rely on a software vulnerability and requires no user permissions. They used Drammer to analyze several popular smartphones and found that many of them were indeed susceptible to their Drammer attack.
'The vulnerability we found in Android phones has been partly fixed back in 2016,' says Van der Veen with pride. 'Furthermore, our work gained quite some attention from the international press, and earned us a number of prestigious prizes, including a Pwnie at Blackhat.' In the meantime, the research team has developed a prototype defense mechanism called GuardION that stops attacks which make use of the Rowhammer principle.

Both Lindorfer and Van der Veen appreciated the cooperation. The project has been very useful to expand their personal networks. 'A Dutch student visited us for six months to work on the cryptominer project,' says Lindorfer. 'And I also spent three months in Santa Barbara to work on Drammer,' adds Van der Veen. 'Furthermore, we Skyped on a regular basis. We will keep collaborating, also now Martina has transferred to Vienna.'
Both young researchers praise the amount of freedom the funding agencies gave them to change course during the project: 'We started with dynamic analysis of malware, but we were able to jump in on recent developments during the project. Flexibility is essential in this field. Everything moves so fast, it is impossible to plan ahead your research for several years. Sometimes even the amount of time it takes to get a paper published is too long to stay relevant.'

> 'Flexibility is essential in this field. Everything moves so fats, it is impossible to plan ahead.'

Prof. Christopher Kruegel
University of California,
Santa Barbara

Prof. Herbert Bos
VU University, Amsterdam

Dr. Victor van der Veen
VU University, Amsterdam

NWO-NSF call 2016:
Faster And Stronger Onion Routing

Dr. Jon Solworth
University of Illinois at Chicago

Prof. Tanja Lange
Eindhoven University of Technology

Smarter, faster, and more secure communication

How can we enable privacy-friendly communication through a network that is less complex and better resistant to attacks than the current Tor network? That is the main challenge Tanja Lange and Jon Solworth address in their joint work. In the FASOR project, they combine a clean-slate low-latency encrypted network protocol that reduces complexity and increases security and privacy, with state-of-the-art post-quantum cryptography that enables the network to even resist attacks by future quantum computers.

The Internet was not originally designed with privacy in mind,’ Tanja Lange explains the motivation behind this project. In a traditional network, the header of an Internet packet contains the final destination address for routing. This enables adversaries to connect the source – you sitting behind your computer – with the destination – the address of the website you are visiting. Tor, an acronym for The Onion Router, was developed as a privacy-friendly alternative. Tor encrypts the data together with the next node destination IP address in multiple layers. The packet is sent through a virtual circuit comprising successive, randomly-selected Tor relays. Each relay decrypts one layer of encryption to only reveal the next node destination. The final relay decrypts the innermost layer of encryption and, by doing so, is the only one to know the final destination.

Within this project, Solworth and Lange are developing a new onion-routing protocol, called

FASOR (Faster and Stronger Onion Routing). This protocol will support low-latency connections that protect both content and metadata, even against retroactive attacks by future quantum computers.

Currently, Tor has a large user community, composed of, for example, journalists, the police, activists, companies, whistleblowers, and ordinary people who want protect their web browsing against surveillance. The network has some disadvantages though. Tor was introduced some fifteen years ago. Since then, multiple attacks have been developed that enable adversaries to deduce the source to destination path. A network observer on the path from exit-router-to-server can see individual service connections and can correlate those with observations on the path from client-to-entry. Furthermore, the Tor network is set up like a telescope which requires multiple bilateral handshakes. That makes it slow.

Simpler, more secure and faster

FASOR is set-up in a simpler fashion. 'We had the advantage that we could start from scratch with our design,' Solworth says. 'That way you can really optimize a system, without having to deal with legacy from previous versions of the software.' Essentially, FASOR is composed of a limited number of building blocks. The FASOR system starts with the unmodified client application. The information from this app is sent to a client proxy, which splits up the message into fixed sized packets. The router then forwards these packets cells to a neighbor. Different packets are distributed across many different paths, to make it impossible for adversaries to track down which packets originate from the same source and are heading for the same destination. At the end point, a server proxy reassembles the different packets into the client message. All of the authentication and encryption takes place within the server, increasing security and reducing complexity of the network itself.

'We had the advantage that we could start from scratch with our design'

'You won't find this specific combination of expertise anywhere else in the world'

Unique combination of expertise

Both Lange and Solworth highly value the cooperation. 'You won't find this specific combination of expertise anywhere else in the world,' Lange says proudly. 'Solworth's group is known worldwide for their expertise in building a truly secure operating system and networking protocols. Even companies like Google are adopting some of the features his group developed in their own networks.' 'We are working on Ethos, a clean-slate, intrinsically secure operating system', Solworth explains. 'This operating systems makes it far easier to create robust applications on top of it that can withstand attacks. Lange's group specializes in cryptography. They have ample experience in developing useable cryptography for small systems, which have to be fast and shouldn't use up too much computing power. Furthermore, they are extremely good in efficient post-quantum cryptography, with their solutions being widely deployed in both commercial and open-source applications.

Emmanouil Doulgerakis
Eindhoven University
of Technology

The post-quantum cryptography was especially important to us, as quantum computers are under active development and when they are realized they will be able to break common cryptography (including that used in Tor).' Lange: 'In this project, we bring these strengths together to build an inherently secure, anonymous communication service.'

The transatlantic collaboration is simplified by personal interactions: Daniel J. Bernstein is a long-term colleague of Jon Solworth and received a Vici grant in Eindhoven. All three knew Roger Dingledine and during a long evening at a conference discussed some existing limitations in Tor. The discussion was so lively that it turned towards new designs and the blueprint for FASOR. The recent funding opportunity provided by NWO and NSF kicked the collaboration into a higher gear, Solworth says. 'It is very nice that both sides decided to fund the same project. We'll certainly continue with this long-term collaboration. The only question is how intense it can be, which depends on the funding.'

Implementation in the real world

Perhaps the nicest thing about this specific project is that Tor is actively involved, both academics conclude. Together, the three groups want to radically improve the state of privacy-respecting networks. FASOR will be ready within a year. As soon as it is finished, we will implement it into clients and routers, to act as a new option alongside Tor. And then, slowly but surely, we hope that increasing groups of people will adopt our approach, and that FASOR will become the next generation network that enables truly privacy-friendly, secure and fast communication.

> 'We 'll certainly continue with this long-term collaboration'

Gabriele Milauro
University of Illinois
at Chicago
🇺🇸

Dr. Jon Solworth
University of Illinois
at Chicago
🇺🇸

Prof. Tanja Lange
Eindhoven University
of Technology
🇳🇱

Dr. Daniel Bernstein
Eindhoven University
of Technology
🇳🇱

NWO/NSF call 2016:
Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems:
Practices and Contexts in the Netherlands and US

Dr. Jessica Vitak
University of Maryland

Dr. Jason Pridmore
Erasmus University Rotterdam

Cultural differences in perception of privacy

What privacy and security risks do consumers perceive when adopting and using voice-activated services on mobile devices and in their homes? And how are these perceptions influenced by culture? Jessica Vitak, Jason Pridmore and Michael Zimmer aim to answer these questions with their comparative study carried out simultaneously in the United States and the Netherlands.

In 2018, data privacy was a global subject of interest in several ways. Cases like the Facebook/Cambridge Analytica data exploit made it painfully clear how easy it is to misuse personal data. On the other hand, 2018 also saw Europe's first significant update of data protection laws in over twenty years, when the General Data Protection Regulation came into effect.

'This is indeed a very interesting time to study how people perceive privacy and security in relation to new technologies,' states Jason Pridmore from the Erasmus University Rotterdam. 'There is great value in seeing different responses to a certain technology, given the increasing amount of data streaming out of our cars, houses, wearables and so on. In our research, we find that people have a growing aversion against data collecting technologies, because they "don't want to be under constant surveillance." The funny thing is that these same people don't hesitate for a second to use apps like Google maps, which enables companies like Google to know exactly where they are all the time...'

Looking for differences

This project is set up as a comparative study between the US and the Netherlands. ‘It is very nice that this joint NSF/NWO funding scheme enables us to conduct the exact same studies in both countries. This makes it possible to compare results and get a clear view on cultural differences,’ says Michael Zimmer from the University of Wisconsin-Milwaukee. ‘Since there are so many similarities between the US and the Netherlands in terms of tech savviness and the appreciation of the latest gadgets, you tend to miss out on significant differences,’ adds Pridmore. One of the most prominent differences between the two countries is that in the Netherlands, users are very much aware of the platform behind the device, he says. ‘Dutch people tend to be skeptical about the company behind a technology. They wonder: “What do they want from me, how will they try to make more money over my back?” In the US, people usually are more accustomed to these large companies and don’t question their motivations as much.’

The research focuses on voice-activated intelligent personal assistants, such as Siri, Google Assistant, Google Home, and Amazon Echo. These devices are increasingly popular in the US. Even back in 2016, about a third of the smartphone users used applications like Siri or Google Assistant at least once a month. Juniper Research predicts 55 percent of US households will have at least one voice-activated device by 2022. In America, voice-activated technology is integrated into phones, homes, cars, and more, and is for example used in university dorms and hotel chains. ‘The nice thing is that while in the US, voice activated systems can be found in many homes already, the first Google Homes have just arrived in the Netherlands. So we are still trying to figure out what to do with such systems,’ adds Pridmore. ‘It is great to be able to re-see this process of getting used to the technology happening in a very different culture.’

Conference connection

‘My group is interested in apps where privacy and security are not top of mind, for example in fitness health apps,’ Vitak says. ‘When I saw the call for this specific program, I put out a tweet and asked if anybody knew Dutch researchers working in a similar area. The group that responded turned out to be a group Michael knew, because he met them during a surveillance seminar as a graduate student.’ Pridmore: ‘I had indeed met Michael before, but had never got acquainted with Jessica. One of my former colleagues had worked with her though, and recommended me to get in touch. So, due to this joint call, what started out as a conference connection blossomed into a very nice and productive cooperation.’

Both groups nicely complement each other, Pridmore says. ‘Jessica tends to go for quantitative analysis based on extensive surveys. My research usually is of a more qualitative nature.’ For this project, the teams combined their approaches in a joint design of their study. Early 2018 they conducted a survey at three universities in both countries and asked both users and non-users about their privacy and security concerns. US **users** turned out to be mostly concerned about the security issues of linking smart systems to other devices like lighting or home security. They were especially afraid that hackers would be able to threaten their physical security,

‘It is great to be able to re-see this process of getting used to the technology happening in a very different culture’

Anouk Mols
Erasmus University
Rotterdam

> ‘Technologies that are borderless should be researched across borders as well’

by hacking their Alexa or Google Home devices. Fear for security breaches also was the main reason for US **non-users** to decide against buying a voice-activated smart system. In the Netherlands, people are also afraid of hackers, but even more so, they have concerns about what using a Google Home system means in terms of information. They express the feeling that a Google Home would be ‘constantly eavesdropping’ on them, not only allowing hackers to get an idea of when you are at home and when you are not, but also enabling Google to gather and sell more personal information than they are willing to share.

The researchers are now planning the next phase, in which they are going to conduct a full scale survey in both countries, Pridmore explains. ‘We will present participants in both countries with scenarios. Imagine this or that technology, what do you think about it? Currently, we are working on the narrative, and looking for situations that apply both in the US and the Dutch context.’

Extend to other countries

All three researchers are very happy with the opportunity the NSF/NWO grant gives them. ‘Technologies that are borderless should be researched across borders as well. That is the only way to pinpoint how cultural differences influence things like security and privacy,’ says Pridmore. ‘It would therefore be wise to extend this funding scheme to other countries as well,’ adds Vitak. These kinds of joint calls are not only beneficiary for the research itself, but also for educational purposes, she emphasizes. ‘It is good for students to see how academic research works in different countries, and how different perspectives can influence not only the outcomes, but also the setup of a research project.’

Dr. Michael Zimmer
University of
Wisconsin-Milwaukee

Dr. Jessica Vitak
University of
Maryland

Dr. Jason Pridmore
Erasmus University
Rotterdam

Yutting Liao
University of
Maryland

/Administration
/Human Resources
/Legal
/Accounting
/Finance
/Marketing
/Publicity

NWO-DHS call 2018:
Planning for Anycast as Anti-DDoS

Prof. John Heidemann
University of Southern California

Prof. Aiko Pras
University of Twente & Research

Sending attackers off course with anycast

The Internet-of-Things opens up a whole new range of possibilities for attackers to shut down services with Distributed Denial of Service (DDoS) attacks. In their joint project, Aiko Pras and John Heidemann want to develop and improve tools that use anycast as a defense. With the anycast method, one service can be provided at multiple, distributed sites, which increases its resilience to attacks.

‘The DDoS problem has been around for about twenty years and remains very hard to solve,’ says John Heidemann from the University of Southern California. ‘Current-day companies can only do business if they accept traffic from their customers. But by doing so, they make themselves vulnerable to these types of attacks as well, since it can be hard to distinguish between legitimate and illegitimate traffic.’ And with the increasing number of Internet-of-Things devices around, DDoS attacks will only become more prominent, adds his Dutch colleague Aiko Pras from the University of Twente. ‘For most of these IoT devices, security is not the first priority. Not one buyer of a coffee machine with a WiFi connection asks how its security updates will be managed. For a DDoS attack, you need a large number of systems that overwhelm a target with a flood of simultaneous Internet traffic. IoT devices often are easy to hack, abundantly available, and therefore perfectly suited for such a job.’

The joint research project of Heidemann and Pras that recently was granted within the NWO-DHS cooperation scheme focusses on so-called anycast systems as a defense mechanism. In an anycast network, multiple servers at multiple locations represent the same IP address. Routers in the network select a desired nearby destination on the basis of path length. If the IP address is targeted by a DDoS attack, in an anycast network this effectively means that only the servers closest to the attacker will be overwhelmed, and that the service will remain accessible to other users through other servers.

Follow the traffic

In their previous work, the groups have jointly developed and tested a tool called Verfploeter, that maps anycast catchments and provides calibrated predictions of anycast changes. The tool determines which part of the network is directed towards specific anycast sites. As strange as it may sound, the actual routing of internet traffic on these types of networks currently is a black box, Pras explains. 'There are many different parties involved in these routing processes, which all apply their own set of rules.' By observing the internet traffic, the researchers map the actual anycast routing, and get an idea of the most vulnerable nodes in the network. The ultimate aim is to determine where you should put the servers in an anycast network in order to increase its resilience, and to develop ways to optimize the network capacity during an attack. 'Our first few measurements with the tool showed some pretty strange effects,' Pras says. 'For example, we observed that some Domain Name Server requests done from The Netherlands on the .nl domain are led through servers in Iran.'

Useful contacts

On the US side, the Verfploeter tool has been used to evaluate the new anycast deployment for B-Root, the Domain Name Server that is operated by the University of Southern California, where Heidemann works. This contact with one of the world's most important domain name servers - Pras: 'Anytime you type in some internet address ending at .com, the DNS root determines where you end up' – makes the cooperation very valuable for the Dutch partners in the project.

And in their turn, the Dutch contacts are of great value to the American researchers, says Heidemann. 'Aiko has tight bonds with the Dutch SIDN labs, which is responsible for the .nl domain. Since the Netherlands and SIDN are so much smaller than their US counterparts, it is much easier to influence the direction they are taking with their technology. Organizations like SIDN or B-root can benefit from our tools to defend their networks against catastrophic results of DDoS attacks. In fact, both organizations currently already deploy an early version of our tools.'

Sharing knowledge with society

Heidemann is passionate about sharing his knowledge with society and industry. 'We are working on a technology that enables companies and governments to meet the attack risk at a reasonable cost. Of course there are a few companies around that already specialize in this. Google for example has ample expertise in this field. But I don't think it is wise to put all of our eggs into the basket of a few multinationals. Many people use anycast today, but how they use it is not well described nor well known. I want to democratize the knowledge of how to optimize anycast networks for defense against DDoS attacks. That is why we also present our work regularly at operator forums and open meetings.'

Pras feels a slightly different moral obligation to make all of the research results publicly available. 'I value this cooperation with the US highly. But I sincerely hope that in the future, there will also be opportunities for similar joint international

> 'Cyber security is crucial for countries' infrastructure. The Netherlands should broaden its horizon.'

projects with European countries. Cyber security is crucial for a countries' infrastructure. The Netherlands should broaden its horizon, and not only turn to the UK and the US when it comes to such a vital topic.'

Catalyst for collaboration

This first formal joint project is the icing on the cake of Pras' and Heidemanns existing collaboration. Pras: 'Around 2015, Ricardo de Oliveira Schmidt, who was one of my postdoctoral researchers at the time, spent a couple of months at John's research group. I knew about John and his work from conferences and papers and so on, but had not cooperated with him before that visit. But ever since, we have done multiple things together.'

And with success: the joint research has led to quite some impactful publications, Heidemann adds. 'The nice thing is that in most of these papers, both teams are well-represented in the list of authors. There is an actual collaboration: ideas and results go back and forth. Aiko's group has expertise in network management, mine works on network measurement and protocol design. That way we complement each other.' This new joint project can act as a catalyst for the collaboration, they hope. 'I am very impressed that both the DHS and NWO recognized the need for this rare type of international funding. I hope this joint project will tighten the bonds between our groups, and that it will lead to useful solutions that can actually help mitigate DDoS attacks,' Heidemann concludes.

'Very impressed that both DHS and NWO recognized the need for this rare type of international funding.'

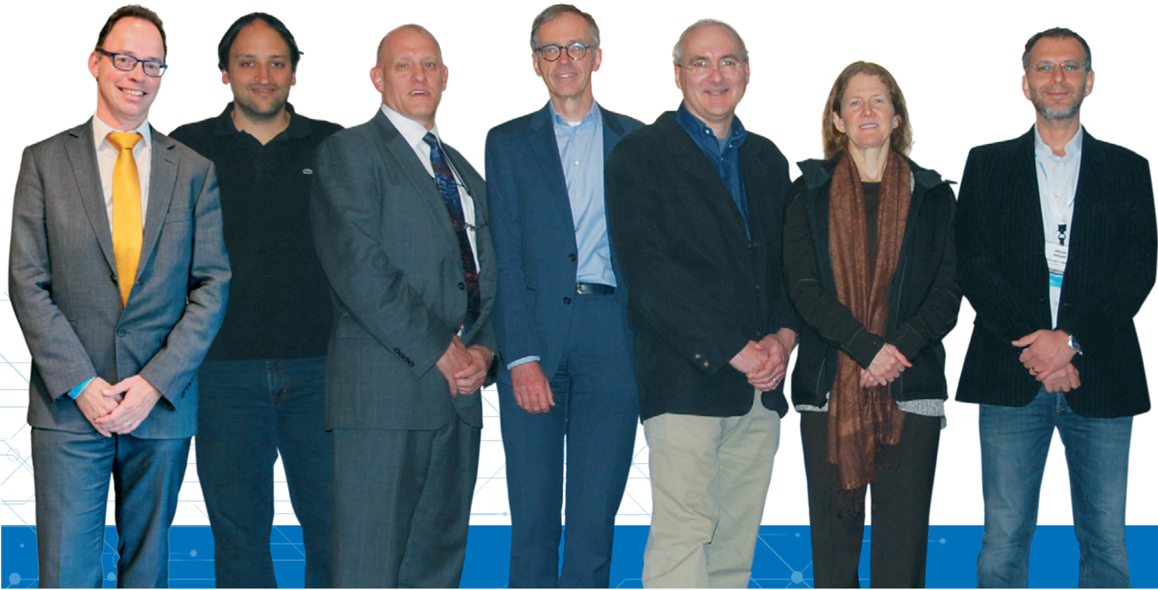
Prof. John Heidemann
University of Southern California

Prof. Aiko Pras
University of Twente & Research

What’s next?

Most joint projects are still running. The last interview in this booklet is about a project that was recently kicked off. All projects are monitored and will be given the opportunity to present their progress at forthcoming showcase meetings, like the dcypher Symposium. The recently held DDoS workshop around the three DDoS projects, granted in 2018, was a nice example of international knowledge exchange in the research on the detection of and defense against DDoS attacks. In the years ahead more exchange opportunities like this will be created. We also seek feedback on the three different programs with the purpose of considering improvements in future calls and solicitations.

In the Netherlands the dcypher Advisory Council (representing the public-private cyber security sectors) is developing an advice for an international cyber security research strategy, in connection with cyber security policy dialogues and cyber diplomacy. On one hand a continuation of the research collaboration with the US is considered important, on the other hand an extension of the Dutch focus on Europe is felt to be essential as well. Discussions between NSF and NWO are about the determination of themes of common interest to both countries, while exploring possibilities of organizing a future call.



Raymond Doijen 🇳🇱

Cristiano Giuffrida 🇳🇱

Douglas Maughan 🇺🇸

Jan Piet Barthel 🇳🇱

John Heidemann 🇺🇸

Kimberly Claffy 🇺🇸

Alberto Dainotti 🇺🇸

During the 2019 NSF Secure and Trustworthy Cyberspace Meeting, in a meeting between NSF and NWO program managers and US Principal Investigators in the PRICE program, there was strong support for future programs that leverages the research expertise and strengths in both countries. So we have a challenge ahead of us: how to build, based on the experience gained so far, an even stronger international research collaboration, involving more countries, and expanding the multiplier.

Joao
Ceron
🇳🇱

Christopher
Kruegel
🇺🇸

Alvaro
Cardenas
🇺🇸

Colophon

Text
Sonja Knols, Ingenieuse
Jan Piet Barthel, NWO | dcypher

Images
Sjoerd van der Hucht Photography
GettyImages

Design
Haagsblauw

Print
Zalsman

Production
Juul Brouwers, NWO | dcypher

NWO

NWO is committed to a strong science system in the Netherlands, in the belief that scientific research contributes to our prosperity and wellbeing. As a national research organisation with an active contribution to various parts of the national science and innovation policies, NWO plays different roles: financing, programming, bringing together, supporting and influencing.

dcypher

dcypher is the Dutch public-private agenda-setting platform for cyber-security research and higher education, which was established in 2016 by the ministries of Economic Affairs & Climate Policy, Justice & Security, Education Culture & Science and the Dutch Organisation for Scientific Research. As off 2018 dcypher is also supported by the Ministry of Defence.

The greatest possible care was taken in the composition of this booklet. Acquisition of items from this booklet is permitted provided with full source information.

October 2019

dcypher

NWO