Dr. Do and the detectives
… and the Internet-wide search for code errors

Since 2017, Dr. Quoc Huy Do has been working on making life difficult for hackers at the University of Stuttgart's Institute of Information Security (SEC). Together with his colleagues at the SEC the Vietnamese native has been searching for security loopholes in basic Internet standards and protocols.

By comparison with the corridors throughout the SEC, with their many seating areas and mirrored kitchenettes, Dr. Quoc Huy Do's office appears almost Spartan. There are no papers on his desk, just a laptop, flat screen and a cup of tea. A photo of his family is his only concession to his private life. It appears as if the 36-year-old wants to protect his work from all distractions so that he does not make the same mistakes that many programmers fall victim to: they program security loopholes into Internet code, and nothing motivates a hacker more than a security loophole. “We work very hard here”, is Do's smiling summary of the office environment.
In terms of the data-hunter and collector powerplay, Dr. Do is one of the good guys. With his research group colleagues at the SEC the Vietnamese native has been searching for security loopholes in basic Internet standards and protocols. Asked if he is a kind of detective searching for clues to possible points of attack with persistence and intelligence, Do nods and agrees one could say that.

Not a traditional crime scene

Of course – and this is where the complexity of the subject already starts – the Internet is not like a crime scene that detectives search thoroughly for fingerprints, murder weapons and traces of DNA. Whilst the Internet appears to be something physical when presented on screens of every kind, it is, in reality, intangible; nor is it invulnerable. On the contrary, the Internet is a kind of developing organism, continuously expanding in every dimension. The fact that loopholes, points of attack for hackers, arise in the course of this is the result of natural human fallibility. “Nothing in the world is perfect, and no code either”, says Dr. Do. That’s why the institute team, which works under the directorship of institute leader, Professor Ralf Küsters, has set its sights on the development of a tool designed to reveal vulnerabilities in code to web developers before they put it online, a kind of non-bribable auditor that identifies code errors on a logical-mathematical basis.
The outlines of the tool have already been sketched out on paper – and this was a highly-complex project. By the end of the year, Do hopes, a structural framework of the auditing tool should also have been programmed.

Rooted in computer science

Computer science has been a constant aspect of Quoc Huy Do’s career right from the start of his university studies. And, with each subsequent step, the Vietnamese national probed deeper into the material, till now when he has practically reached the foundations of the Internet here in Stuttgart.
Born in Hanoi, the capital of Vietnam, Do attended the People's Security Academy, where he first studied the basics before going on to conduct his initial research into program verification at the National University in Hanoi – “the best university in Vietnam”. Of course, there was no hint at that time of the route that would finally lead him to Stuttgart.
For his doctorate, Do conducted research at the TU Darmstadt in a research group headed up by Professor Reiner Hähnle. “There, I work on dataflow security”, Do explains. Whilst that sounds similar to non-experts, the researcher assures us that it was “something entirely different: we programmed a tool for Java developers, which checks whether a piece of software contains hidden dataflows”.

However, Quoc Huy Do had already become obsessed with the topic of security whilst there: “After getting my doctorate, I wanted to carry on working in this direction”. And, an opportunity to do just that seemed to open up at the University of Stuttgart: Professor Küsters had been working on a comprehensive security analysis of the OAuth-2.0 protocol in Trier and had just transferred to the University of Stuttgart at that time.

Do was fascinated by the research being carried out in a newly inaugurated research group and applied for a post there, and, although he also received other offers at the same time, opted for Stuttgart. “The atmosphere and close collaboration are great and Stuttgart is also a beautiful city”, says the research fellow, who took up his post at the SEC in September 2017.

Do first lived with his family in the University guest house, but the City of Stuttgart's Welcome Center soon introduced him to potential landlords, assisted him with various official questions (“a nightmare”) and even organized a Christmas party for the new arrivals. “My kids thought it was great” he says. In the meantime, not only has the family found accommodation, it has also grown: “My son was born in Stuttgart”, Do says, adding that his two daughters are attending primary school here.

Photo: University of Stuttgart / Max Kovalenko

Fan of research freedom

“I hadn’t originally planned to become a researcher”, says the security expert. Today, the 36-year-old feels very comfortable in the world of academic research. “I like to learn and to tackle new challenges. Research is a great opportunity to do precisely that”. Even though he has never worked for a company, he says, he places great store in research freedom. “We focus on specific topics, whereas, in industry, you always have to keep the final product in mind”.

OAuth 2.0 (Open Authorization), a popular Internet authorization and authentication protocol, is at the center of the project that Quoc Huy Do and his colleagues are working on. It is designed to ensure the secure authorization of web-services and applications without giving third-party providers access to confidential data. In practice, one uses one's private data to dial-in to a specific service provider after which one can also use the services of third-party providers without having to log in again every time. There have already been several hacker attacks on OAuth 2.0 in the past, which have usually been responded to by rapid program code fixes. The tool on which the SEC is working is intended to help identify potential gateways for criminals at an early stage by using the pattern of known points of weakness in OAuth.

Do's contract of employment at the Institute ends in September 2019. He is not yet sure whether or not he will continue to work in Stuttgart after that. He is, on the other hand, certain that he will continue to work in the field of cyber security.

Jens Eber